TREND MICRO™

7.0

TREND MICRO™ Control Manager

Guide du widget et de la gestion des stratégies

Gestion centralisée de la sécurité pour l'entreprise

Trend Micro Incorporated se réserve le droit de modifier ce document et le produit décrit ici sans notification préalable. Avant d'installer et d'utiliser le produit, veuillez consulter les fichiers Lisez-moi, les notes de mise à jour et/ou la dernière version de la documentation utilisateur applicable que vous trouverez sur le site Web de Trend Micro à l'adresse suivante :

http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx

Trend Micro, le logo t-ball de Trend Micro, OfficeScan et Control Manager sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produits ou de sociétés peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 2017 Trend Micro Incorporated. Tous droits réservés.

Document n° : CMEM78096/171121

Date de publication : Février 2018

Protégé par le brevet américain n°: 5,623,600 ; 5,889,943 ; 5,951,698 ; 6,119,165

Cette documentation présente les fonctionnalités principales du produit et/ou fournit les instructions d'installation pour un environnement de production. Lisez attentivement cette documentation avant d'installer ou d'utiliser le produit.

Pour plus d'informations concernant l'utilisation des fonctionnalités spécifiques de produit, consultez notre Trend Micro Centre d'aide en ligne et/ou notre Trend Micro base de connaissances.

Trend Micro cherche constamment à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Évaluez cette documentation sur le site Web suivant :

http://www.trendmicro.com/download/documentation/rating.asp

Table des matières

Préface

Préface xv
Documentation xvi
Public concerné xvii
Conventions typographiques du document xvii
Terminologie xviii

Partie I: Présentation

Chapitre 1: Le Tableau de bord

À propos du Tableau de bord 1-2
Onglets et widgets 1-2
Le Centre des opérations 1-6
Onglet Résumé 1-16
Onglet Investigation sur les incidents de DLP 1-30
Onglet Prévention contre la perte de données 1-34
Onglet Conformité 1-37
Onglet Détection des menaces 1-45
Configuration des paramètres de Smart Protection Network 1-52

Chapitre 2: Gestion des stratégies

Gestion des stratégies 2-2
Prévention contre la perte de données 2-27
État de la stratégie 2-47

Partie II: Widgets des produits Deep Discovery

Chapitre 3: Widgets des tableaux de bord de Deep Discovery Analyzer et de Deep Discovery Email Inspector

Widgets Deep Discovery Analyzer 3-2

Widgets Deep Discovery Email Inspector 3-3

Chapitre 4: Intégration de Deep Discovery Inspector

Récapitulatif de l'intégration de Deep Discovery Inspector 4-2

Paramètres de stratégie de Deep Discovery Inspector 4-10

Partie III: Widgets Endpoint Encryption

Chapitre 5: Tableau de bord d'Endpoint Encryption

Utilisateurs d'Endpoint Encryption 5-3

Périphériques Endpoint Encryption 5-10

État de Full Disk Encryption 5-16

Connexion de périphérique infructueuse à Control Manager 5-19

Connexion d'utilisateur infructueuse à Control Manager 5-21

Verrouillage des dispositifs Control Manager 5-23

Rapport sur les violations de la sécurité de Control Manager 5-25

Chapitre 6: Stratégies Endpoint Encryption

Vue d'ensemble de l'authentification 6-2

Stratégies dans Control Manager 6-6

Création d'une stratégie 6-10

Configuration des règles des utilisateurs de Control Manager 6-13

Configuration des règles de Full Disk Encryption 6-16

Configuration des règles de File Encryption 6-19

Configuration des règles de stratégie communes 6-22

Migration de groupes vers Control Manager 6-26

Partie IV: Widgets des produits InterScan

Chapitre 7: Paramètres de stratégie d'InterScan Messaging Security Virtual Appliance

Règles IMSVA 7-2

Ajout de règles IMSVA 7-2

Modification de règles IMSVA existantes 7-7

Suppression de règles IMSVA 7-8

Chapitre 8: Paramètres de stratégie d'InterScan Web Security Suite

Liste des règles de prévention contre la perte de données 8-2

Chapitre 9: Paramètres de stratégie d'InterScan Web Security Virtual Appliance

Liste des règles de prévention contre la perte de données 9-2

Partie V: Widgets Trend Micro Mobile Security

Chapitre 10: Widgets Mobile Security

État de santé du dispositif Android 10-4

Widget Récapitulatif de l'état de chiffrement des dispositifs Android . 10-4

Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs Android 10-5

Widget Récapitulatif de l'état de débridage des dispositifs Android 10-5

Widget État de sécurité du dispositif Android 10-5

Widget Récapitulatif de la recherche des programmes malveillants sous Android 10-6

Widget Récapitulatif de l'analyse des applications modifiées sous Android 10-6

Widget Récapitulatif de l'analyse de divulgation des données de confidentialité sous Android 10-7
Widget Récapitulatif de l'analyse de la vulnérabilité sous Android 10-7
Widget État de la mise à jour des composants 10-8
Widget Actualités de la cybersécurité pour dispositifs mobiles 10-9
Widget Récapitulatif de l'état de chiffrement des dispositifs iOS 10-9
Widget État de santé du dispositif iOS 10-9
Widget État de sécurité du dispositif iOS 10-10
Widget Récapitulatif de l'état de débridage des dispositifs iOS 10-10
Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs iOS 10-11
Widget Récapitulatif des recherches de programmes malveillants iOS 10-11
Widget Récapitulatif de l'état de contrôle des applications des dispositifs mobiles 10-11
Widget Récapitulatif de l'état de chiffrement des dispositifs mobiles 10-12
Widget État de santé du dispositif mobile 10-12
Widget Récapitulatif de l'état de débridage des dispositifs mobiles ... 10-13
Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs mobiles 10-13
Widget Récapitulatif du scan de ransomware sur les dispositifs mobiles 10-14
Widget État de sécurité du dispositif mobile 10-14
Widget Récapitulatif des distributeurs des dispositifs mobiles 10-15
Widget Récapitulatif de l'état de mise à jour des stratégies 10-15
Widget Récapitulatif de l'état de santé des composants du serveur ... 10-15
Widget Récapitulatif des entreprises de téléphonie 10-16
Widget Les 10 principales applications installées 10-16
Widget Cinq principaux logiciels de rançon Android détectés 10-16
Widget Cinq principaux sites Web bloqués 10-17

Cinq principaux logiciels de rançon iOS détectés 10-17

Widget Cinq principaux programmes malveillants détectés 10-17

Widget Récapitulatif de l'état de chiffrement des appareils Windows Phone 10-17

Widget État de santé du dispositif Windows Phone 10-18

Widget Récapitulatif de la version du système d'exploitation du dispositif Windows Phone 10-18

Chapitre 11: Stratégies de sécurité dans Trend Micro Mobile Security

Protection des dispositifs avec des stratégies 11-2

Partie VI: Gestion des stratégies de l'agent OfficeScan

Chapitre 12: Paramètres du programme de l'agent OfficeScan

Paramètres des services complémentaires 12-2

Privilèges et autres paramètres 12-4

Agents de mise à jour 12-20

Chapitre 13: Paramètres des stratégies de surveillance des comportements

Surveillance des comportements 13-2

Configuration des règles et des exceptions de surveillance des comportements 13-15

Chapitre 14: Paramètres de stratégie de protection contre les programmes malveillants

Types de méthodes de scan 14-2

Scan manuel 14-5
Scan en temps réel 14-13
Scan immédiat 14-22
Scan programmé 14-29
Actions de scan 14-38
Support d'exclusion de scan 14-49

Chapitre 15: Paramètres de stratégie de Web Reputation

Web Reputation 15-2
Configuration de Stratégie de Web Reputation 15-2

Chapitre 16: Protection contre les menaces inconnues

Apprentissage automatique prédictif 16-2
Configuration des paramètres de soumission d'échantillons 16-6
Configuration des paramètres de connexion suspecte 16-6

Chapitre 17: Paramètres de stratégie de contrôle des dispositifs

Contrôle des dispositifs 17-2
Configuration des paramètres de contrôle des dispositifs 17-2

Chapitre 18: Liste des exclusions de scan

Liste des spywares/graywares approuvés 18-2
Liste des programmes approuvés 18-3

Partie VII: Widgets de Prévention contre la perte de données OfficeScan

Chapitre 19: Paramètres de la stratégie de prévention contre la perte de données OfficeScan

Prévention contre la perte de données (DLP) 19-2

Configuration d'une stratégie de prévention contre la perte de données 19-3

Chapitre 20: Widgets Data Discovery

Widget Principales détections de stratégies de fichiers sensibles 20-2

Widget Principaux endpoints sur lesquels se trouvent des fichiers sensibles 20-4

Widget Principales correspondances de modèles Data Discovery 20-6

Widget Principaux fichiers sensibles 20-7

Chapitre 21: Paramètres de stratégie d'OfficeScan Data Discovery

Création de stratégies de découverte des données 21-2

Partie VIII: Widgets Endpoint Application Control

Chapitre 22: Widgets du tableau de bord d'Endpoint Application Control

Widget Indicateurs de performance clés de Endpoint Application Control 22-2

Gestion des règles de Endpoint Application Control 22-7

Widget Récapitulatif des utilisateurs et des endpoints de Endpoint Application Control 22-8

Principales applications lancées 22-13

Widget Événements d'application, de règle et de stratégie de Endpoint Application Control 22-14

Principales stratégies Endpoint Application Control déclenchées 22-23

Principaux utilisateurs déclenchant des règles de blocage Endpoint Application Control 22-23

Chapitre 23: Widget Paramètres de stratégie de Endpoint Application Control

Règles de stratégie 23-2

Journalisation de stratégie 23-3

Déploiement de stratégies 23-5

Connexion au serveur PolicyServer 23-6

Expérience utilisateur – Stratégies 23-7

Partie IX: Widgets ScanMail for Microsoft Exchange

Chapitre 24: Configuration de la prévention contre la perte de données

Configuration d'une stratégie de prévention contre la perte de données 24-2

Partie X: Widgets Trend Micro Security (for Mac)

Chapitre 25: Widgets Trend Micro Security (for Mac)

Widget Indicateurs de performance de Security (for Mac) 25-2

Chapitre 26: Paramètres de stratégie de Trend Micro Security (for Mac)

Types de méthode de scan 26-2

Types de scan 26-8
Paramètres de cache des scans 26-31
Exclusions de scan 26-32
Autoprotection de l'agent 26-36
Mises à jour des agents 26-37
Réputation de sites Web 26-41

Partie XI: Widgets Endpoint Sensor

Chapitre 27: Widgets Trend Micro Endpoint Sensor

Résumé de surveillance intelligente par hôte 27-2
Investigation Endpoint Sensor 27-2

Chapitre 28: Intégration de Capteur de Endpoint Trend Micro

Intégration de Control Manager dans cette version 28-2
Enregistrement auprès de Control Manager 28-2
Ajout des widgets Endpoint Sensor 28-3
Utilisation de Control Manager pour vérifier l'état 28-5
Utilisation du widget Investigation Endpoint Sensor 28-6
Utilisation des mises à jour automatiques 28-7
Stratégie Trend Micro Endpoint Sensor 28-8

Partie XII: Widgets Deep Security Manager

Chapitre 29: Widgets Deep Security Manager

Widget Deep Security – Historique des événements de la protection anti-programmes malveillants 29-3

Widget Deep Security – État de la protection anti-programmes malveillants (programme malveillant) 29-4

Widget Deep Security – Activité du type d'applications (détection) 29-5

Widget Deep Security – Activité du type d'applications (prévention) . 29-6

Widget Résumé des composants Deep Security 29-7

Widget Résumé des fonctions Deep Security 29-9

Widget Deep Security – Activité du pare-feu (détection) 29-10

Widget Deep Security – Activité du pare-feu (prévention) 29-11

Widget Deep Security – Historique des événements du pare-feu 29-12

Widget Deep Security – Activité de surveillance de l'intégrité 29-13

Widget Deep Security – Historique des événements de surveillance de l'intégrité 29-13

Widget Deep Security – Historique des événements de prévention contre les intrusions 29-14

Widget Deep Security – Activité de l'IPS (détection) 29-15

Widget Deep Security – Activité de l'IPS (prévention) 29-16

Widget Deep Security – Activité d'inspection des journaux 29-17

Widget Deep Security – Historique des événements d'inspection des journaux 29-18

Widget Deep Security - Historique des événements du scan de reconnaissance 29-18

Widget Résumé d'état Deep Security 29-19

Widget Deep Security – Historique des événements de la réputation de sites Web 29-21

Widget Deep Security – Activité d'URL de la réputation de sites Web 29-22

Partie XIII: Widgets Control Manager

Chapitre 30: Widgets du tableau de bord de Control Manager

Widget de vérification de la protection des points finaux 30-2
Widget Principales menaces critiques par durée de résidence 30-3
Widget Hôtes sur lesquels ont été effectuées des tentatives de rappel C&C 30-5
Widget Principales menaces de fichiers de Control Manager 30-6
Widget Hôtes compromis uniques au fil du temps 30-7
État de la stratégie 30-8
Lancement rapide 30-9

Partie XIV: Widgets Smart Protection Server

Chapitre 31: Widgets Smart Protection Server

Utilisateurs actifs pour File Reputation 31-2
Utilisateurs actifs pour la réputation de sites Web 31-2
Rapport sur le trafic HTTP pour File Reputation 31-3
Rapport sur le trafic HTTP pour la réputation de sites Web 31-3
État en temps réel 31-4
10 premiers ordinateurs infectés pour File Reputation 31-5
10 premiers ordinateurs bloqués pour la réputation de sites Web 31-6

Partie XV: Widgets Virtual Mobile Infrastructure

Chapitre 32: Widgets Virtual Mobile Infrastructure

Widget 5 principales applications lancées d'après Trend Micro Virtual Mobile Infrastructure 32-2
Widget 5 principales applications Web lancées d'après Trend Micro Virtual Mobile Infrastructure 32-2

Widget 5 principaux utilisateurs en ligne d'après Trend Micro Virtual Mobile Infrastructure 32-3

Widget État de l'utilisation des processeurs des serveurs Trend Micro Virtual Mobile Infrastructure 32-3

Widget État de l'utilisation des disques des serveurs Trend Micro Virtual Mobile Infrastructure 32-4

État de l'utilisation de la mémoire des serveurs Trend Micro Virtual Mobile Infrastructure 32-4

Widget État des utilisateurs de Trend Micro Virtual Mobile Infrastructure 32-5

Partie XVI: Widgets Vulnerability Protection Manager

Chapitre 33: Widgets Vulnerability Protection

Widget Vulnerability Protection – Activité du type d'applications (détection) 33-2

Widget Vulnerability Protection – Activité du type d'applications (prévention) 33-3

Widget Résumé des fonctions Vulnerability Protection 33-4

Widget Vulnerability Protection – Historique des événements du pare-feu 33-5

Widget Vulnerability Protection – Historique des événements de prévention contre les intrusions 33-6

Widget Vulnerability Protection – Activité de l'IPS (détection) 33-6

Widget Vulnerability Protection – Activité de l'IPS (prévention) 33-7

Widget Vulnerability Protection – Indicateur de performance clé 33-8

Widget Vulnerability Protection – Historique des événements du scan de reconnaissance 33-9

Widget Vulnerability Protection – Récapitulatif de l'état 33-10

Widget Vulnerability Protection – Endpoints vulnérables 33-11

Partie XVII: Widgets Safe Mobile Workforce

Chapitre 34: Widgets Safe Mobile Workforce

Widget État de l'utilisation de l'unité centrale des serveurs Safe Mobile Workforce 34-2

Widget État de l'utilisation de la mémoire des serveurs Safe Mobile Workforce 34-2

Widget État de l'utilisation du disque des serveurs Safe Mobile Workforce 34-2

Widget État des utilisateurs Safe Mobile Workforce 34-3

Widget 5 principales applications lancées Safe Mobile Workforce 34-4

Widget 5 principales applications Web lancées Trend Micro Safe Mobile Workforce 34-4

Widget 5 principaux utilisateurs en ligne Safe Mobile Workforce 34-4

Index

Index IN-1

Préface

Préface

Bienvenue dans le *Guide de gestion des stratégies et des widgets* de Trend Micro™ Control Manager™ Ce document explique comment configurer les widgets du **tableau de bord** et les widgets de **gestion des stratégies** dans Control Manager.

Sujets abordés dans cette section :

- *Documentation à la page xvi*
- *Public concerné à la page xvii*
- *Conventions typographiques du document à la page xvii*
- *Terminologie à la page xviii*

Documentation

La documentation sur Control Manager comprend les éléments suivants :

DOCUMENT	DESCRIPTION
Fichier Lisez-moi	Contient la liste des problèmes connus ; peut également contenir des informations de dernière minute sur le produit, qui ne se trouvent pas dans l'aide en ligne ou dans la documentation imprimée
Guide d'installation et de mise à niveau	Document PDF qui traite des exigences et des procédures d'installation de Control Manager **Remarque** Le Guide d'installation et de mise à niveau peut ne pas être disponible pour les versions, les Service Pack ou les patchs mineurs.
Configuration système requise	Document PDF qui traite des exigences et des procédures d'installation de Control Manager
Manuel de l'administrateur	Document PDF qui fournit des instructions détaillées sur la configuration et la gestion de Control Manager et des produits gérés, ainsi que des explications sur les concepts et fonctions de Control Manager
Aide en ligne	Fichiers HTML compilés au format WebHelp fournissant des procédures, des conseils d'utilisation et des informations spécifiques aux champs. L'aide est également accessible depuis la console de Control Manager
Tour d'horizon des défenses contre les menaces connectées	Document PDF expliquant comment utiliser Control Manager pour rassembler un grand nombre de produits et solutions Trend Micro afin de vous permettre de détecter les attaques ciblées et les menaces avancées, de les analyser et d'y répondre avant qu'elles ne provoquent des dommages durables
Guide de gestion des stratégies et des widgets	Document PDF expliquant comment configurer les paramètres de gestion des stratégies et des widgets du tableau de bord dans Control Manager

DOCUMENT	DESCRIPTION
Listes concernant la protection des données (chapitre 1 uniquement)	Document PDF répertoriant les identificateurs de données prédéfinis et les modèles de prévention contre la perte de données
Base de connaissances	Base de connaissances en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus des produits. Pour accéder à la base de connaissances, consultez le site Web suivant : http://esupport.trendmicro.com

Téléchargez la dernière version des documents PDF et du fichier Lisez-moi à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx

Public concerné

La documentation sur Control Manager est destinée aux utilisateurs suivants :

- Administrateurs de Control Manager : personnes responsables de l'installation, la configuration et la gestion de Control Manager. Ces utilisateurs doivent posséder des connaissances approfondies en matière de réseaux et de gestion des serveurs.
- Administrateurs des produits gérés : utilisateurs gérant les produits Trend Micro intégrés à Control Manager. Ces utilisateurs doivent posséder des connaissances approfondies en matière de réseaux et de gestion des serveurs.

Conventions typographiques du document

La documentation utilise les conventions suivantes.

TABLEAU 1. Conventions typographiques du document

NOMENCLATURE	DESCRIPTION
MAJUSCULE	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets et options
Italique	Références à d'autres documents
`Police monospace`	Échantillons de lignes de commande, code du programme, URL Web, noms de fichiers et sortie d'un programme
Chemin > **de navigation**	Chemin de navigation permettant d'accéder à un écran particulier Par exemple, **Fichier** > **Enregistrer** signifie que vous devez cliquer sur **Fichier**, puis sur **Enregistrer** dans l'interface.
Remarque	Remarques sur la configuration
Conseil	Recommandations ou suggestions
Important	Informations sur les paramètres de configuration et les limites du produit obligatoires ou par défaut
AVERTISSEMENT!	Actions critiques et options de configuration

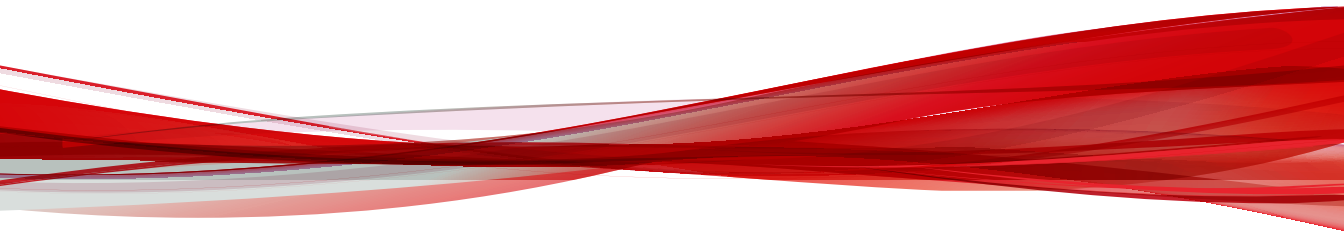
Terminologie

Le tableau suivant présente la terminologie officielle employée dans toute la documentation de Control Manager :

TERMINOLOGIE	DESCRIPTION
Administrateur (ou administrateur de Control Manager)	Personne gérant le serveur Control Manager
Agent	Programme de produits gérés installé sur un endpoint
Composants	Responsables du scan, de la détection et des actions contre les risques de sécurité.
Console Control Manager, console Web ou console d'administration	Interface utilisateur Web permettant d'accéder au produit Control Manager, de le configurer et de l'administrer **Remarque** Les consoles des produits gérés intégrés sont indiquées par le nom du produit géré. Exemple : console Web d'OfficeScan.
Endpoint géré	Endpoint sur lequel est installé l'agent de produit géré
Produit géré	Produit Trend Micro intégré à Control Manager
Serveur géré	Endpoint sur lequel est installé le produit géré
Serveur	Endpoint sur lequel est installé le serveur Control Manager
Risques de sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Web.
Service produit	Services Control Manager hébergés via Microsoft Management Console (MMC).
Double pile	Entités ayant à la fois une adresse IPv4 et une adresse IPv6.
IPv4 pur	Une entité n'ayant qu'une adresse IPv4.
IPv6 pur	Une entité n'ayant qu'une adresse IPv6.

Partie I

Présentation



Chapitre 1

Le Tableau de bord

Cette section explique comment utiliser les onglets et les widgets du tableau de bord Control Manager.

Les rubriques sont les suivantes:

- *À propos du Tableau de bord à la page 1-2*
- *Onglets et widgets à la page 1-2*
- *Le Centre des opérations à la page 1-6*
- *Onglet Résumé à la page 1-16*
- *Onglet Investigation sur les incidents de DLP à la page 1-30*
- *Onglet Prévention contre la perte de données à la page 1-34*
- *Onglet Conformité à la page 1-37*
- *Onglet Détection des menaces à la page 1-45*
- *Configuration des paramètres de Smart Protection Network à la page 1-52*

À propos du Tableau de bord

Le **Tableau de bord** s'affiche lorsque vous ouvrez la console Web de Control Manager ou que vous cliquez sur **Tableau de bord** dans le menu principal. Chaque compte utilisateur Control Manager possède un tableau de bord totalement indépendant. Toute modification apportée au tableau de bord appartenant à un compte utilisateur spécifique n'affectera pas les tableaux de bord des autres comptes utilisateurs.

Le **Tableau de bord** contient les éléments suivants :

- Onglets
- Widgets

Onglets et widgets

Les widgets sont les principaux composants du **Tableau de bord**. Ils fournissent des informations spécifiques sur divers événements liés à la sécurité.

Les informations affichées par les widgets proviennent des sources suivantes :

- base de données Control Manager
- Produits gérés enregistrés
- Trend Micro Smart Protection Network

Les onglets contiennent les widgets. Le **Tableau de bord** prend en charge jusqu'à 30 onglets.

Utilisation des onglets

Gérez les onglets en ajoutant, renommant, modifiant la disposition, supprimant et basculant automatiquement entre les affichages d'onglets.

Procédure

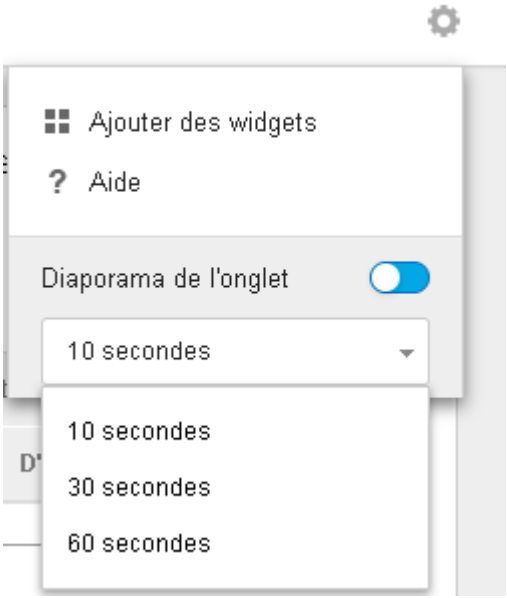
1. Accédez au **Tableau de bord**.
2. Pour ajouter un onglet :
   a. Cliquez sur l'icône Ajouter (+).

   b. Entrez un nom pour le nouvel onglet.
3. Pour renommer un onglet :
   a. Survolez le nom de l'onglet à l'aide du curseur et cliquez sur la flèche vers le bas.

   b. Cliquez sur **Renommer** et saisissez le nom du nouvel onglet.
4. Pour modifier la disposition des widgets dans un onglet :
   a. Survolez le nom de l'onglet à l'aide du curseur et cliquez sur la flèche vers le bas.
   b. Cliquez sur **Modifier la disposition**.
   c. Sélectionnez la nouvelle disposition dans l'écran qui apparaît.
   d. Cliquez sur **Enregistrer**.
5. Pour supprimer un onglet :
   a. Survolez le nom de l'onglet à l'aide du curseur et cliquez sur la flèche vers le bas.
   b. Cliquez sur **Supprimer** et confirmez.

6. Pour lire un diaporama d'onglets :

   a. Cliquez sur le bouton **Paramètres** à droite de l'affichage d'onglets.



   b. Activez le contrôle **Diaporama de l'onglet**.

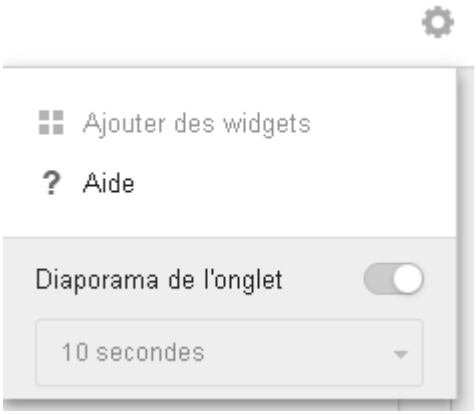
   c. Sélectionnez la durée d'affichage de chaque onglet avant de passer à l'onglet suivant.

Utilisation des widgets

Gérez les widgets en ajoutant, déplaçant, redimensionnant, renommant et supprimant des éléments. Vous pouvez également modifier les produits fournissant les données du widget.

Procédure

1. Accédez au **Tableau de bord**.
2. Cliquez sur un onglet.
3. Pour ajouter un widget :
   a. Cliquez sur le bouton **Paramètres** à droite de l'affichage d'onglets.



   b. Cliquez sur **Ajouter des widgets**.
   c. Sélectionnez les widgets à ajouter.
      - Dans la liste déroulante située en haut des widgets, sélectionnez une catégorie pour restreindre les sélections.
      - Utilisez la zone de recherche de texte située en haut de l'écran pour rechercher un widget spécifique.
   d. Cliquez sur **Ajouter**.
4. Pour déplacer un widget vers un nouvel emplacement dans le même onglet, faites glisser le widget et déposez-le à un nouvel emplacement.

5. Redimensionnez un widget dans un onglet à plusieurs colonnes en pointant le curseur sur la bordure droite du widget, puis en déplaçant le curseur vers la gauche ou la droite.

6. Pour renommer un widget :

   a. Cliquez sur l'icône Paramètres (>).

   b. Saisissez le nouveau titre.

   c. Cliquez sur **Enregistrer**.

7. Pour modifier la portée de produit du widget :

   a. Cliquez sur l'icône Paramètres (>).

   b. Cliquez sur le bouton représentant une double flèche (>>) dans le champ **Portée**.

   c. (Facultatif) Cliquez sur l'icône en forme d'entonnoir ( ) pour filtrer et rechercher des produits.

   d. Sélectionnez les produits qui fournissent des données au widget et cliquez sur **OK**.

   e. Cliquez sur **Enregistrer**.

8. Pour supprimer un widget, cliquez sur l'icône Supprimer (>).

Le Centre des opérations

Le **Centre des opérations** est un onglet/widget spécial qui fournit un résumé global de l'état de protection de votre réseau en regroupant des données relatives aux niveaux de conformité, aux détections de menaces critiques et aux détections arrêtées sur votre réseau. Vous pouvez également utiliser le graphique du **Centre des opérations** pour identifier rapidement les utilisateurs et les groupes exposés à des risques importants à partir d'une structure Active Directory intégrée.

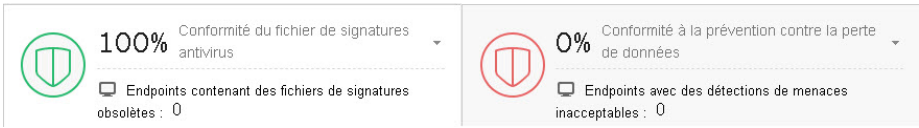
Remarque

Pour modifier les données de l'exemple de graphique et afficher les sites ou les structures hiérarchiques en fonction du réseau de votre entreprise, activez l'intégration Active Directory ou créez des sites personnalisés à partir d'adresses IP.

Cliquez sur l'icône Paramètres (>) pour modifier les informations suivantes qui s'affichent dans l'onglet.

- **Entreprise** : indiquez le nom d'affichage de l'entreprise.
- **Regroupement Active Directory** : indiquez si les nœuds du graphique représentent des **Sites** ou des **Structures hiérarchiques** issus de votre annuaire Active Directory.
- **Période** : indiquez la période des données qui s'affichent sur le graphique.

Indicateurs de conformité



Cette section de l'onglet **Centre des opérations** fournit des informations sur le niveau de conformité du fichier de signatures antivirus ou sur le niveau de conformité à la prévention contre la perte de données de votre réseau.

La couleur de l'icône d'indicateur de conformité change à mesure que le niveau de conformité de votre réseau évolue pour refléter les seuils configurés dans l'écran **Paramètres Active Directory et de conformité**.

L'affichage par défaut présente des informations sur l'indicateur **Conformité du fichier de signatures antivirus**.

Remarque

Si vous modifiez l'indicateur de conformité, les informations sur le niveau de conformité qui s'affichent dans le graphique Opérations de sécurité seront également modifiées.

Pour modifier les informations de conformité qui s'affichent, cliquez sur le nom de l'indicateur de conformité sélectionné en regard de l'icône représentant une flèche vers le bas ( ), puis sélectionnez l'un des indicateurs suivants dans la liste déroulante.

INDICATEUR	DESCRIPTION
Conformité du fichier de signatures antivirus	Affiche les informations suivantes : • Le pourcentage d'agents OfficeScan et Worry-Free Business Security Services qui utilisent des versions acceptables du fichier de signatures de virus et du fichier de signatures d'agent Smart Scan • Le nombre total d'endpoints dont les fichiers de signatures antivirus sont obsolètes sur votre réseau Cliquez sur le nombre en regard de **Endpoints avec des fichiers de signatures obsolètes** pour afficher des informations détaillées sur les endpoints impactés dans le Répertoire des utilisateurs/endpoints.
Conformité à la prévention contre la perte de données	Affiche les informations suivantes : • Le pourcentage d'agents OfficeScan sur lesquels la prévention contre la perte de données est activée et dont le nombre de détections de menaces est acceptable • Le nombre total d'endpoints pour lesquels des menaces liées à Data Discovery ont été détectées Cliquez sur le nombre en regard de **Endpoints avec des détections de menaces inacceptables** pour afficher des informations détaillées sur les endpoints impactés dans le Répertoire des utilisateurs/endpoints.

Menaces critiques

Cette section de l'onglet **Centre des opérations** affiche le nombre total de détections de menaces critiques sur votre réseau, le nombre total d'utilisateurs affectés et le nombre d'utilisateurs importants affectés (repérés par l'étoile).

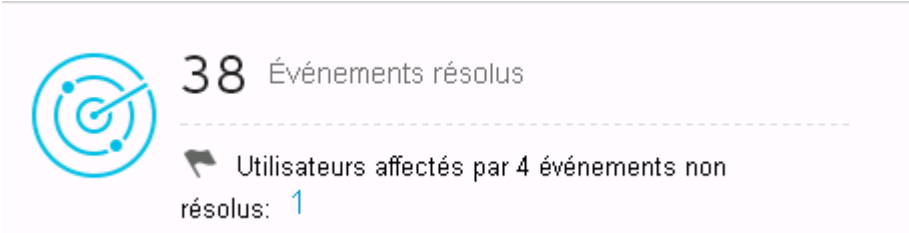
Cliquez sur le nombre d'utilisateurs affectés pour afficher des détails supplémentaires dans l'écran **Répertoire des utilisateurs/endpoints**.

Les détections de menaces critiques incluent les types de menace suivants.

TYPE DE MENACE	DESCRIPTION
Rappel C&C	Tente de communiquer avec un serveur C&C (Command-and-control) pour envoyer des informations, recevoir des instructions et télécharger d'autres programmes malveillants
Menace persistante avancée (APT) connue	Intrusions d'attaquants qui poursuivent et compromettent de manière agressive des cibles choisies, qui sont souvent menées dans le cadre de campagnes (série de tentatives ayant réussi et échoué au fil du temps visant à pénétrer de plus en plus profondément un réseau cible) et qui ne correspondent pas à des incidents isolés
Mouvement latéral	Recherche des répertoires, des courriers électroniques, des serveurs d'administration et autres actifs afin de mapper la structure interne d'un réseau, d'obtenir les informations d'authentification pour accéder à ces systèmes et de permettre à l'attaquant de se déplacer d'un système à un autre
Logiciel de rançon	Programme malveillant qui empêche ou limite l'accès d'un utilisateur à son système à moins qu'une rançon soit payée

TYPE DE MENACE	DESCRIPTION
Attaque d'ingénierie sociale	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité détectée dans les documents, tels qu'un fichier PDF
Menaces inconnues	Objets suspects (adresses IP, domaines, valeurs de hachage SHA-1 de fichier, messages électroniques) avec un niveau de risque « élevé », tels qu'ils sont détectés par Deep Discovery Inspector, les produits de sécurité d'endpoints ou autres produits avec Virtual Analyzer
Attaque de faille	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité généralement détectée dans les programmes et les systèmes d'exploitation

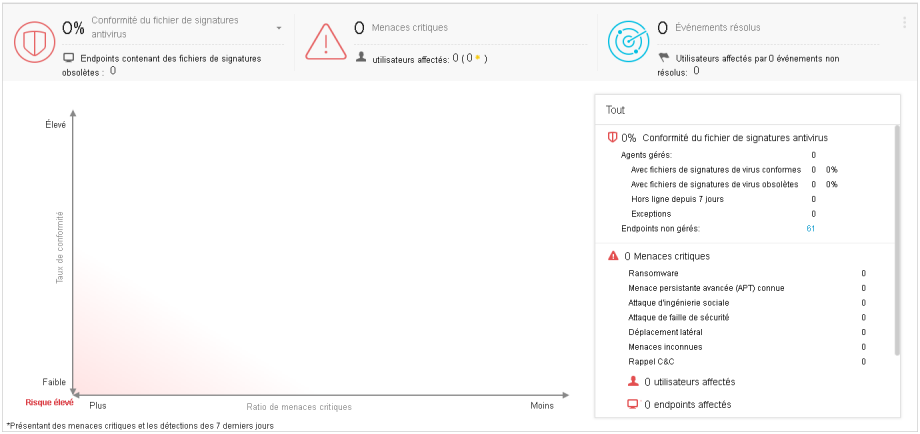
Événements résolus



Cette section de l'onglet **Centre des opérations** affiche le nombre total d'événements résolus et non résolus sur votre réseau.

Cliquez sur le nombre dans le champ **Utilisateurs affectés par __ événements non résolus** pour afficher des informations détaillées sur les utilisateurs affectés par des événements non résolus sur votre réseau.

Graphique du Centre des opérations



Le graphique de l'onglet **Centre des opérations** présente la relation entre le ratio de menaces critiques et le niveau de conformité de votre réseau. L'axe des X indique le ratio des menaces critiques par rapport au nombre total d'endpoints au sein d'un site ou d'une structure hiérarchique. L'axe des Y indique les niveaux de conformité des sites ou des structures hiérarchiques pour l'indicateur de conformité sélectionné. Vous pouvez utiliser ces données pour identifier rapidement les utilisateurs et les groupes exposés à des risques importants à partir d'une structure Active Directory intégrée.

Remarque

Pour modifier les données de l'exemple de graphique et afficher les sites ou les structures hiérarchiques en fonction du réseau de votre entreprise, activez l'intégration Active Directory ou créez des sites personnalisés à partir d'adresses IP.

Survolez un nœud à l'aide de la souris pour afficher les informations sur la conformité et les menaces critiques pour des sites ou des structures hiérarchiques spécifiques. La queue d'un nœud indique la source du changement d'état de sécurité sur la période spécifiée.

- Cliquez sur l'icône Paramètres (>) pour modifier le **Regroupement Active Directory** (**Sites**, **Structures hiérarchiques**) représenté par le nœud.

- Vous pouvez également personnaliser les sites et les structures hiérarchiques dans l'écran **Paramètres Active Directory et de conformité**.

L'affichage par défaut présente les informations sur l'indicateur de conformité sélectionné pour tous les nœuds de votre réseau ces 7 derniers jours.

- Sélectionnez un autre indicateur de conformité pour modifier les informations de conformité qui s'affichent.
- Cliquez sur l'icône Paramètres (>) pour modifier la **Période** des données qui s'affichent.
- Cliquez sur un nœud pour afficher des informations détaillées sur celui-ci dans le panneau récapitulatif situé à droite.

Panneau de détails du Centre des opérations

Le panneau de détails de l'onglet **Centre des opérations** contient des informations détaillées sur les niveaux de conformité, les détections de menaces critiques et le nombre total d'événements résolus/non résolus sur votre réseau.

L'affichage par défaut présente les informations sur l'indicateur de conformité sélectionné pour tous les nœuds de votre réseau ces 7 derniers jours.

- Sélectionnez un autre indicateur de conformité pour modifier les informations de conformité qui s'affichent.
- Cliquez sur un nœud du graphique pour afficher uniquement des informations sur celui-ci.
- Cliquez sur l'icône Paramètres (>) pour modifier la **Période** des données qui s'affichent.

TABLEAU 1-1. Informations de conformité

INDICATEUR	DESCRIPTION

Conformité du fichier de signatures antivirus	Affiche le pourcentage d'agents OfficeScan et Worry-Free Business Security Services qui utilisent des versions acceptables du fichier de signatures de virus et du fichier de signatures d'agent Smart Scan
	
	Vous y trouverez également les détails suivants :
	
	• **Agents gérés** : nombre d'endpoints sur lesquels des agents OfficeScan et Worry-Free Business Security Services sont installés
	  • **Avec fichiers de signatures de virus conformes** : nombre d'agents gérés qui utilisent des versions acceptables de fichiers de signatures de virus et de fichiers de signatures d'agent Smart Scan
	  • **Avec fichiers de signatures de virus obsolètes** : nombre d'agents gérés qui n'utilisent pas de versions acceptables de fichiers de signatures de virus et de fichiers de signatures d'agent Smart Scan
	  • **Hors ligne depuis 7 jours** : nombre d'agents gérés qui n'ont pas communiqué avec le serveur du produit géré depuis 7 jours ou plus
	  • **Exceptions** : nombre d'utilisateurs ou d'endpoints exclus des calculs de conformité
	• **Endpoints non gérés** : nombre d'endpoints sur lesquels des agents OfficeScan ou Worry-Free Business Security Services sont installés
	
	Développez les catégories et cliquez sur un nombre pour afficher des détails supplémentaires sur les endpoints affectés.

INDICATEUR	DESCRIPTION

Conformité à la prévention contre la perte de données	Affiche le pourcentage d'agents OfficeScan sur lesquels la prévention contre la perte de données est activée et dont le nombre de détections de menaces est acceptable
	
	Vous y trouverez également les détails suivants :
	
	• **Agents gérés** : nombre d'endpoints sur lesquels des agents OfficeScan sur lesquels la prévention contre la perte de données est activée sont installés
	  • **Avec détections de menaces acceptables** : nombre d'agents gérés dont le nombre de détections de menaces est acceptable
	  • **Avec détections de menaces inacceptables** : nombre d'agents gérés dont le nombre acceptable de détections de menaces a été dépassé
	  • **Hors ligne depuis 7 jours** : nombre d'agents gérés qui n'ont pas communiqué avec le serveur du produit géré depuis 7 jours ou plus
	  • **Exceptions** : nombre d'utilisateurs ou d'endpoints exclus des calculs de conformité
	• **Endpoints non gérés** : nombre d'endpoints sur lesquels aucun agent OfficeScan sur lequel la prévention contre la perte de données est activée n'est installé
	
	Développez les catégories et cliquez sur un nombre pour afficher des détails supplémentaires sur les endpoints affectés.

TABLEAU 1-2. Menaces critiques

SECTION	DESCRIPTION
Menaces critiques	Affiche le nombre total de menaces critiques détectées sur votre réseau Répertorie tous les types de menace critique qui affectent votre réseau Pour les types de menace avec détections : • Développez le type de menace pour afficher la liste des détections. • Cliquez sur une détection pour afficher des détails supplémentaires dans l'écran **Informations sur la menace**.
Utilisateurs affectés	Affiche le nombre total d'utilisateurs affectés par les menaces critiques • Développez la section pour afficher les utilisateurs affectés. • Cliquez sur un utilisateur affecté pour afficher des détails supplémentaires dans l'écran d'information **Utilisateur**.
Endpoints affectés	Affiche le nombre total d'endpoints affectés par les menaces critiques • Développez la section pour afficher les endpoints affectés. • Cliquez sur un endpoint affecté pour afficher des détails supplémentaires dans l'écran d'information **Endpoint**.

TABLEAU 1-3. Nombre total d'événements

DONNÉES	DESCRIPTION
Nombre total d'événements	Affiche le nombre total d'événements détectés
Événements résolus	Affiche le nombre d'événements résolus sur votre réseau
Événements non résolus	Affiche le nombre d'événements non résolus sur votre réseau nécessitant une action

DONNÉES	DESCRIPTION
Utilisateurs affectés	Affiche le nombre d'utilisateurs affectés par les événements non résolus sur votre réseau Cliquez sur le nombre pour afficher des détails sur les utilisateurs affectés.

Onglet Résumé

L'onglet **Résumé** contient un ensemble prédéfini de widgets qui offre un aperçu de l'état de la sécurité de votre réseau.

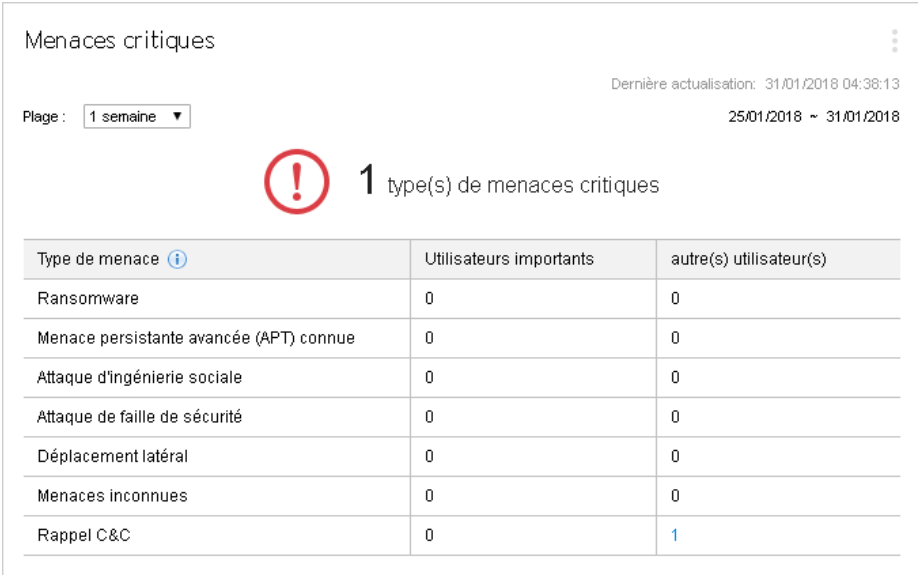
Remarque

Vous pouvez ajouter, supprimer ou modifier les widgets qui s'affichent dans l'onglet **Résumé**.

Widgets disponibles :

- Menaces critiques
- Utilisateurs avec des menaces
- Endpoints présentant des menaces
- Principales menaces de Control Manager
- État de la connexion du produit
- État des composants du produit

Widget Menaces critiques



Il affiche le nombre total de types de menace critique détectées sur votre réseau ainsi que le nombre d'**utilisateurs importants** et d'**autres utilisateurs** affectés par chaque type de menace.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

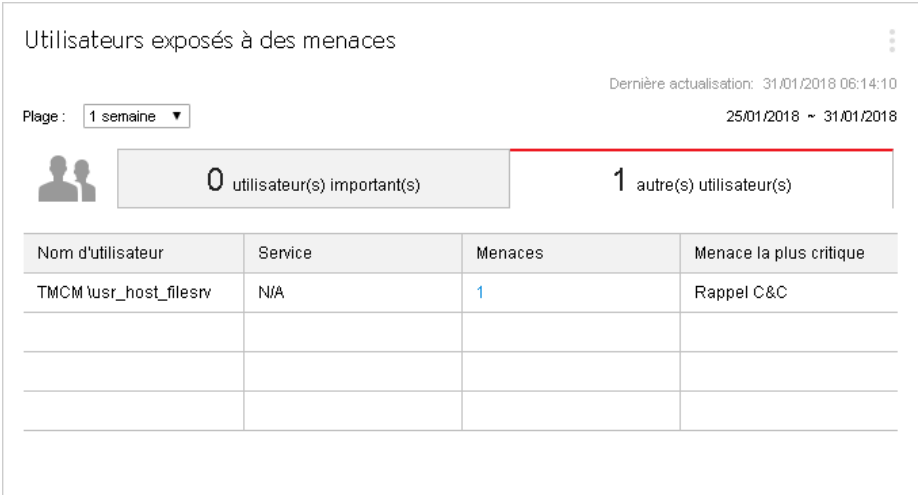
Le tableau répertorie les types de menace critique par ordre de gravité.

- Cliquez sur un nombre dans les colonnes **Utilisateurs importants** ou **Autres utilisateurs**, puis cliquez sur l'utilisateur que vous voulez afficher.

La colonne **Type de menace** contient les types de menace suivants.

Type de menace	Description
Rappel C&C	Tente de communiquer avec un serveur C&C (Command-and-control) pour envoyer des informations, recevoir des instructions et télécharger d'autres programmes malveillants
Menace persistante avancée (APT) connue	Intrusions d'attaquants qui poursuivent et compromettent de manière agressive des cibles choisies, qui sont souvent menées dans le cadre de campagnes (série de tentatives ayant réussi et échoué au fil du temps visant à pénétrer de plus en plus profondément un réseau cible) et qui ne correspondent pas à des incidents isolés
Mouvement latéral	Recherche des répertoires, des courriers électroniques, des serveurs d'administration et autres actifs afin de mapper la structure interne d'un réseau, d'obtenir les informations d'authentification pour accéder à ces systèmes et de permettre à l'attaquant de se déplacer d'un système à un autre
Logiciel de rançon	Programme malveillant qui empêche ou limite l'accès d'un utilisateur à son système à moins qu'une rançon soit payée
Attaque d'ingénierie sociale	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité détectée dans les documents, tels qu'un fichier PDF
Menaces inconnues	Objets suspects (adresses IP, domaines, valeurs de hachage SHA-1 de fichier, messages électroniques) avec un niveau de risque « élevé », tels qu'ils sont détectés par Deep Discovery Inspector, les produits de sécurité d'endpoints ou autres produits avec Virtual Analyzer
Attaque de faille	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité généralement détectée dans les programmes et les systèmes d'exploitation

Widget Utilisateurs exposés à des menaces



Ce widget affiche des informations sur les utilisateurs pour lesquels des menaces de sécurité ont été détectées.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Cliquez sur les onglets **Utilisateurs importants** ou **Autres utilisateurs** pour basculer entre les différents affichages.

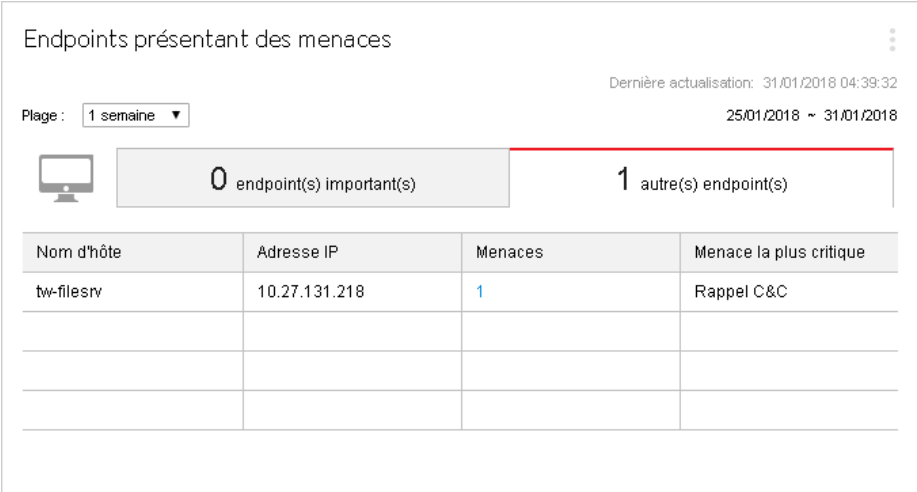
Le tableau répertorie les utilisateurs affectés dans l'ordre suivant : par gravité du type de menace critique en premier, puis par nombre de détections de menaces pour l'utilisateur.

- Cliquez sur le nombre dans la colonne **Menaces** associée à l'utilisateur que vous voulez afficher.

La colonne **Menace la plus critique** contient les types de menace suivants.

Type de menace	Description
Rappel C&C	Tente de communiquer avec un serveur C&C (Command-and-control) pour envoyer des informations, recevoir des instructions et télécharger d'autres programmes malveillants
Menace persistante avancée (APT) connue	Intrusions d'attaquants qui poursuivent et compromettent de manière agressive des cibles choisies, qui sont souvent menées dans le cadre de campagnes (série de tentatives ayant réussi et échoué au fil du temps visant à pénétrer de plus en plus profondément un réseau cible) et qui ne correspondent pas à des incidents isolés
Mouvement latéral	Recherche des répertoires, des courriers électroniques, des serveurs d'administration et autres actifs afin de mapper la structure interne d'un réseau, d'obtenir les informations d'authentification pour accéder à ces systèmes et de permettre à l'attaquant de se déplacer d'un système à un autre
Logiciel de rançon	Programme malveillant qui empêche ou limite l'accès d'un utilisateur à son système à moins qu'une rançon soit payée
Attaque d'ingénierie sociale	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité détectée dans les documents, tels qu'un fichier PDF
Menaces inconnues	Objets suspects (adresses IP, domaines, valeurs de hachage SHA-1 de fichier, messages électroniques) avec un niveau de risque « élevé », tels qu'ils sont détectés par Deep Discovery Inspector, les produits de sécurité d'endpoints ou autres produits avec Virtual Analyzer
Attaque de faille	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité généralement détectée dans les programmes et les systèmes d'exploitation

Widget Endpoints présentant des menaces



Ce widget affiche des informations sur les endpoints pour lesquels des menaces de sécurité ont été détectées.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Cliquez sur les onglets **Utilisateurs importants** ou **Autres utilisateurs** pour basculer entre les différents affichages.

Le tableau répertorie les utilisateurs affectés dans l'ordre suivant : par gravité du type de menace critique en premier, puis par nombre de détections de menaces pour l'utilisateur.

- Cliquez sur le nombre dans la colonne **Menaces** associée à l'utilisateur que vous voulez afficher.

La colonne **Menace la plus critique** contient les types de menace suivants.

Type de menace	Description
Rappel C&C	Tente de communiquer avec un serveur C&C (Command-and-control) pour envoyer des informations, recevoir des instructions et télécharger d'autres programmes malveillants
Menace persistante avancée (APT) connue	Intrusions d'attaquants qui poursuivent et compromettent de manière agressive des cibles choisies, qui sont souvent menées dans le cadre de campagnes (série de tentatives ayant réussi et échoué au fil du temps visant à pénétrer de plus en plus profondément un réseau cible) et qui ne correspondent pas à des incidents isolés
Mouvement latéral	Recherche des répertoires, des courriers électroniques, des serveurs d'administration et autres actifs afin de mapper la structure interne d'un réseau, d'obtenir les informations d'authentification pour accéder à ces systèmes et de permettre à l'attaquant de se déplacer d'un système à un autre
Logiciel de rançon	Programme malveillant qui empêche ou limite l'accès d'un utilisateur à son système à moins qu'une rançon soit payée
Attaque d'ingénierie sociale	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité détectée dans les documents, tels qu'un fichier PDF
Menaces inconnues	Objets suspects (adresses IP, domaines, valeurs de hachage SHA-1 de fichier, messages électroniques) avec un niveau de risque « élevé », tels qu'ils sont détectés par Deep Discovery Inspector, les produits de sécurité d'endpoints ou autres produits avec Virtual Analyzer
Attaque de faille	Programme malveillant ou attaques d'un pirate qui exploitent une faille de sécurité généralement détectée dans les programmes et les systèmes d'exploitation

Widget des principales menaces de Control Manager

Ce widget affiche des informations sur les fichiers et les URL malveillants détectés sur une période spécifique.

Vous pouvez choisir d'afficher les données dans un graphique à barres ou un tableau en cliquant sur les icônes d'affichage ( ).

Utilisez la liste déroulante située au-dessus du graphique/tableau pour sélectionner le type de données de menace à afficher.

- **Fichiers malveillants** : classe les fichiers malveillants détectés sur votre réseau par nombre de détections
- **URL malveillantes** : classe les URL malveillantes détectées sur votre réseau par nombre de détections

Cliquez sur une barre, un nom de menace ou un numéro de détection pour ouvrir l'écran **Requête sur le journal** qui contient des informations sur les endpoints impactés, les détails des menaces et le nombre de détections.

L'affichage par défaut présente les 10 premières menaces provenant de tous les produits gérés pour lesquels le compte utilisateur connecté dispose de droits d'accès.

- Cliquez sur l'icône Paramètres (>) pour modifier le titre du widget, la portée du produit ou le nombre de menaces qui s'affiche.

Widget d'état des composants du produit

Ce widget affiche les versions des composants et le niveau de conformité des produits gérés ou des endpoints sur votre réseau Il permet de suivre les produits gérés ou les endpoints dotés de composants obsolètes.

L'affichage par défaut présente les dernières versions des composants gérés par Control Manager ainsi que le niveau de conformité des produits gérés. Les sections **Fichier de signatures** et **Moteur** répertorient les composants du taux de non conformité le plus élevé au taux le plus bas. Vous pouvez cliquer sur la colonne **Taux** pour changer l'ordre de tri.

Cliquez sur l'un des composants de la colonne **Fichier de signatures** ou **Moteur** pour afficher un graphique circulaire qui présente le nombre de produits gérés ou d'endpoints qui utilisent chaque version du composant.

Cliquez sur les nombres de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur les produits gérés obsolètes, sur tous les produits gérés, sur les endpoints obsolètes ou sur tous les endpoints.

Cliquez sur l'icône Paramètres (>) pour configurer les options suivantes :

Remarque

L'icône Paramètres ( ) ne s'affiche pas pour les widgets de l'onglet **Résumé**.

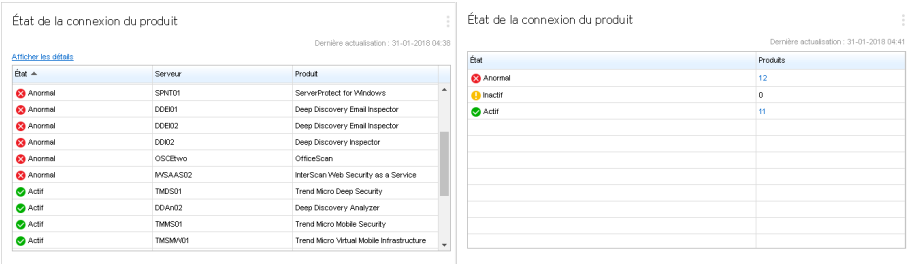
- Pour modifier la portée du produit pour le widget, cliquez sur le bouton représentant une double flèche (>>) dans le champ **Portée** et sélectionnez les produits qui fournissent des données.
- Pour modifier les composants qui s'affichent dans le widget, sélectionnez ou désélectionnez des composants dans les champs **Fichier de signatures** ou **Moteur**.
- Pour afficher les informations de conformité des produits gérés et/ou des endpoints, spécifiez la **Source**.
- Pour indiquer s'il convient d'afficher les données issues de tous les composants signalés par les produits gérés, ou uniquement des composants gérés par Control Manager, sélectionnez l'**affichage** approprié.

Données	Description
Fichier de signatures	Affiche le nom du fichier de signatures, du modèle ou de la règle anti-spam
Moteur	Affiche le nom du moteur de scan
Dernière version	Affiche les informations suivantes : • Dernière version du composant téléchargé par Control Manager • Dernière version du composant disponible en téléchargement (signalé par les produits gérés)
Obsolètes/Tous	Affiche les informations suivantes : • **Obsolètes** : nombre de produits gérés ou d'endpoints dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur les produits gérés ou les endpoints obsolètes. • **Tout** : nombre total de produits gérés ou d'endpoints utilisant le composant Cliquez sur le deuxième nombre de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur tous les produits gérés ou endpoints. **Remarque** Cette colonne s'affiche lorsque **Les deux** est sélectionné pour la **Source**.

DONNÉES	DESCRIPTION
Produit géré/Tous	• **Produit géré** : nombre de produits gérés dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Produit géré/Tout** pour afficher des informations sur les versions des composants installés sur les produits gérés obsolètes. • **Tout** : nombre total de produits gérés utilisant le composant Cliquez sur le deuxième nombre de la colonne **Produit géré/Tout** pour afficher des informations sur les versions des composants installés sur tous les produits gérés. **Remarque** Cette colonne s'affiche lorsque **Produit géré** est sélectionné pour la **Source**.
Endpoint/Tous	• **Endpoint** : nombre d'endpoints dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Endpoint/Tout** pour afficher des informations sur les versions des composants installés sur les endpoints obsolètes. • **Tout** : nombre total d'endpoints utilisant le composant Cliquez sur le deuxième nombre de la colonne **Endpoint/Tout** pour afficher des informations sur les versions des composants installés sur tous les endpoints. **Remarque** Cette colonne s'affiche lorsque l'élément **Endpoint** est sélectionné pour la **Source**.

DONNÉES	DESCRIPTION
Taux d'obsolescence	Affiche le pourcentage de produits gérés ou d'endpoints dotés de composants obsolètes **Remarque** Cette colonne s'affiche lorsque l'élément **Produit géré** ou **Endpoint** est sélectionné pour la **Source**.
Taux	Affiche le pourcentage de produits gérés ou d'endpoints dotés de composants obsolètes **Remarque** Cette colonne s'affiche lorsque **Les deux** est sélectionné pour la **Source**.

Widget État de la connexion du produit



Ce widget affiche l'état de la connexion de tous les produits gérés enregistrés auprès du serveur Control Manager.

L'affichage par défaut répertorie l'état de la connexion et le nom du serveur géré de chaque produit géré pour lequel le compte utilisateur connecté dispose de droits d'accès.

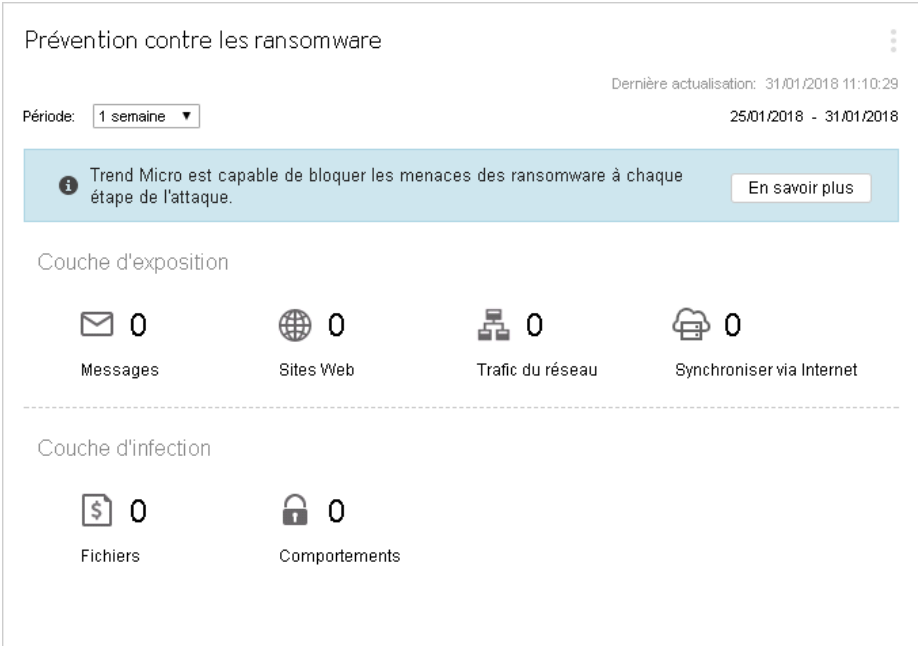
- Pour modifier la portée du produit, cliquez sur l'icône Paramètres (>) et sélectionnez une nouvelle **Portée**.

- Pour afficher un récapitulatif du nombre total de produits gérés pour chaque état de connexion, cliquez sur l'icône Paramètres (>) et basculez l'**affichage** vers **Récapitulatif**.

Cliquez sur **Afficher les détails** pour afficher des informations détaillées dans l'écran **Requête sur le journal**.

ÉTAT	DESCRIPTION
Active	Indique que le service produit est en cours d'exécution et que la communication avec le serveur Control Manager est correctement établie
Inactif	Indique que le service produit n'est pas en cours d'exécution ou ne parvient pas à établir la communication avec le serveur Control Manager
Anormal	Indique que le service produit n'a pas communiqué avec le serveur Control Manager dans l'intervalle du délai d'attente défini par l'utilisateur pour la communication avec l'agent

Widget Prévention contre les ransomwares



Ce widget offre un aperçu de toutes les tentatives d'attaques de ransomware sur une période donnée.

L'affichage par défaut récapitule toutes les détections de ransomware et classe toutes les tentatives par canal d'infection.

- Cliquez sur le nombre de détections de ransomware pour afficher des détails supplémentaires.

CANAL	DESCRIPTION
Messages	Ransomware détecté dans des messages électroniques ou des pièces jointes
Sites Web	Ransomware détecté par les services de Web Reputation

CANAL	DESCRIPTION
Trafic réseau	Ransomware détecté par les connexions suspectes à OfficeScan et par Deep Discovery Inspector
Synchroniser via Internet	Ransomware détecté par Cloud App Security sur le stockage en ligne et les serveurs Office 365 (Exchange Online, SharePoint Online et OneDrive), ou par OfficeScan dans les dossiers locaux sur les agents OfficeScan synchronisés avec le stockage en ligne
Fichiers	Ransomware détecté par les services de File Reputation
Comportements	Ransomware détecté par la surveillance des comportements d'OfficeScan

Onglet Investigation sur les incidents de DLP

L'onglet **Investigation sur les incidents de DLP** contient des widgets qui affichent des informations sur les incidents de prévention contre la perte de données (DLP) en se basant sur le statut de l'incident, les niveaux de gravité et les utilisateurs gérés.

Les widgets prédéfinis sont les suivants :

- Incidents de prévention contre la perte des données par gravité et par état
- Tendances des incidents de prévention contre la perte des données par utilisateur
- Incidents de prévention contre la perte des données par utilisateur

Widget Tendances des incidents de prévention contre la perte des données par utilisateur

Ce widget vérifie le nombre de tendances d'incidents DLP en fonction des utilisateurs gérés. Les données peuvent être filtrées par niveau de gravité ou pour afficher uniquement le nombre total d'incidents déclenchés par un utilisateur spécifique sur une période donnée. Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Cliquez sur les sections du graphique pour ouvrir l'écran **Informations sur les incidents** et examiner le récapitulatif des incidents.

Cliquez sur l'icône des paramètres du widget dans le widget pour accéder aux paramètres supplémentaires.

Paramètre	Description
Titre	Attribuez un nouveau titre pertinent au widget dans le champ.
Intervalle	Précisez l'intervalle de temps au cours duquel les incidents de prévention contre la perte des données ont été déclenchés.
Étendue	Spécifiez la portée des données affichée par le widget. • Utilisateurs directement gérés • Tous les utilisateurs gérés : les données sont collectées à partir des utilisateurs directement gérés et des personnes dépendant des utilisateurs gérés directement.
Gravité	Spécifiez les niveaux de gravité pour filtrer les données.
Utilisateurs à afficher	Spécifiez le nombre d'utilisateurs gérés à afficher.

Cliquez sur **Enregistrer** pour appliquer les modifications et mettre à jour les données du widget.

Widget Incidents de prévention contre perte des données par gravité et état

Ce widget vérifie le nombre d'incidents de prévention contre la perte des données sur la base des niveaux de gravité et des états des incidents. Les données peuvent être filtrées par niveau de gravité et le nombre total de nouveaux incidents à gravité élevée peut être affiché. Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Cliquez sur les nombres d'une colonne pour ouvrir l'écran **Informations sur les incidents** et examiner le récapitulatif des incidents.

Pour rechercher un incident spécifique, saisissez un ID dans le champ **Identifiant d'incident** et cliquez sur **Rechercher**.

Conseil

Un numéro d'identification est attribué à chaque incident. Il est possible d'accéder à ces numéros en cliquant sur le lien des tables, dans les notifications d'événements **Informations détaillées des incidents mises à jour**, ou dans les résultats de requête des journaux de **Prévention contre la perte de données**.

Cliquez sur l'icône des paramètres du widget dans le widget pour accéder aux paramètres supplémentaires.

PARAMÈTRE	DESCRIPTION
Titre	Attribuez un nouveau titre pertinent au widget dans le champ.
Intervalle	Précisez l'intervalle de temps au cours duquel les incidents de prévention contre la perte des données ont été déclenchés.
Étendue	Spécifiez la portée des données affichée par le widget. • Utilisateurs directement gérés • Tous les utilisateurs gérés : les données sont collectées à partir des utilisateurs directement gérés et des personnes dépendant des utilisateurs gérés directement
Gravité	Spécifiez les niveaux de gravité pour filtrer les données.

Cliquez sur **Enregistrer** pour appliquer les modifications et mettre à jour les données du widget.

Widget Incidents de prévention contre la perte des données par utilisateur

Ce widget vérifie le nombre d'incidents de prévention contre la perte des données sur la base des niveaux de gravité et des utilisateurs gérés. Les données peuvent être filtrées par

niveau de gravité et le nombre total de nouveaux incidents à gravité élevée déclenchés par certains utilisateurs peut être affiché. Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès. Le widget affiche un maximum de 50 utilisateurs.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Cliquez sur les nombres d'une colonne pour ouvrir l'écran **Informations sur les incidents** et examiner le récapitulatif des incidents.

Pour rechercher un utilisateur spécifique, saisissez quelques caractères dans le champ **Utilisateur** et cliquez sur **Rechercher**. Par exemple, si vous tapez `ma`, tous les noms d'utilisateur contenant `ma`, tels que « Martin » et « Emma », s'affichent. Vous pouvez également saisir un domaine et un nom d'utilisateur, par exemple `domaine1\paul`.

Remarque

Les noms d'utilisateur ne doivent pas contenir les caractères suivants : " [ ] : ; | = + * ? / \ < &> ,

Les noms de domaines ne doivent pas contenir les caractères suivants : \ * + = | : ; " ? < &> ,

Cliquez sur l'icône des paramètres du widget dans le widget pour accéder aux paramètres supplémentaires.

PARAMÈTRE	DESCRIPTION
Titre	Attribuez un nouveau titre pertinent au widget dans le champ.
Intervalle	Précisez l'intervalle de temps au cours duquel les incidents de prévention contre la perte des données ont été déclenchés.
Étendue	Spécifiez la portée des données affichée par le widget. • Utilisateurs directement gérés • Tous les utilisateurs gérés : les données sont collectées à partir des utilisateurs directement gérés et des personnes dépendant des utilisateurs gérés directement.

PARAMÈTRE	DESCRIPTION
Gravité	Spécifiez les niveaux de gravité pour filtrer les données.
Utilisateurs à afficher	Spécifiez le nombre d'utilisateurs gérés à afficher.

Cliquez sur **Enregistrer** pour appliquer les modifications et mettre à jour les données du widget.

Onglet Prévention contre la perte de données

L'onglet **Prévention contre la perte de données** contient des widgets qui fournissent des informations sur les incidents de prévention contre la perte de données (DLP), les correspondances de modèles et les sources des incidents.

Les widgets prédéfinis sont les suivants :

- Incidents de prévention contre la perte de données par canal
- Correspondances de modèles de prévention contre la perte de données
- Sources principales d'incidents de prévention contre la perte de données
- Stratégie de prévention contre la perte de données violée

Widget Incidents de prévention contre la perte de données par canal

Ce widget affiche le nombre total d'incidents DLP. Les données peuvent être filtrées par type de canal dans lequel l'incident est déclenché.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Utilisez la liste déroulante **Canal** pour filtrer les données par type de canal dans lequel l'incident est déclenché.

Ce widget affiche le nombre d'incidents de prévention contre la perte de données et le pourcentage de canaux par rapport au nombre total d'incidents. Ce widget affiche ces données par :

Données	Description
P2P.	Affiche tous les incidents de prévention contre la perte de données pair-à-pair détectés par les produits gérés spécifiés par l'étendue des données.
IM	Affiche tous les incidents de prévention contre la perte de données de messagerie instantanée détectés par les produits gérés spécifiés par l'étendue des données.
Webmail	Affiche tous les incidents de prévention contre la perte de données de courrier Internet détectés par les produits gérés spécifiés par l'étendue des données.
Message électronique	Affiche tous les incidents de prévention contre la perte de données d'e-mail détectés par les produits gérés spécifiés par l'étendue des données.
Application Web	Affiche tous les incidents de prévention contre la perte de données d'applications Web détectés par les produits gérés spécifiés par l'étendue des données.
Autres	Affiche les incidents de prévention contre la perte de données restants détectés par les produits gérés spécifiés par l'étendue des données

Si vous cliquez sur les liens de la colonne **Canal** ou sur les sections des graphiques, un écran affichant des informations détaillées s'ouvre.

Données	Description
Canal	Type de canaux dans lesquels les incidents de prévention contre la perte de données sont déclenchés.
Incidents	Nombre d'incidents de prévention contre la perte de données déclenchés
Pourcentage (%)	Pourcentage d'incidents de prévention contre la perte de données par rapport au nombre total d'incidents

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⫶⫶. Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur » et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

Widget Correspondances de modèles de prévention contre la perte de données

Ce widget affiche le type des incidents DLP sur votre réseau. Les données peuvent être filtrées par modèle.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Si vous cliquez sur les liens de la colonne **Modèle** ou des sections des graphiques, un écran affichant des informations détaillées s'ouvre.

DONNÉES	DESCRIPTION
Modèle	Modèle déclenché par des incidents de prévention contre la perte de données
Incidents	Nombre d'incidents de prévention contre la perte de données
Pourcentage (%)	Pourcentage d'incidents de prévention contre la perte de données par rapport au nombre total d'incidents

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⫶⫶. Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur » et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

Widget des sources principales d'incidents de prévention contre la perte de données

Ce widget affiche le nombre total de sources principales d'incidents de prévention contre la perte de données sur votre réseau. Ces données incluent les utilisateurs, les adresses électroniques, les noms d'hôte et les adresses IP ; elles peuvent être filtrées par source d'incident.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Utilisez la liste déroulante **Afficher** pour sélectionner les données à afficher.

Widget Stratégie de prévention contre la perte de données violée

Ce widget affiche la stratégie de prévention contre la perte de données violée. Il permet de vérifier le nombre total d'incidents DLP. Par défaut, les données sont triées par le nombre d'incidents. Pour trier les données par nom de stratégie, cliquez sur le titre de la colonne **Stratégie**.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Si vous cliquez sur les liens de la colonne **Incidents**, un écran affichant des informations détaillées s'ouvre.

Données	Description
Stratégie	Nom de la stratégie dans laquelle les incidents de prévention contre la perte de données sont déclenchés
Incidents	Nombre d'incidents de prévention contre la perte de données déclenchés

Onglet Conformité

L'onglet **Conformité** contient des widgets qui affichent des informations relatives à la conformité du composant ou de la connexion pour les produits gérés ou les endpoints.

Les widgets prédéfinis sont les suivants :

- Conformité des applications de produits
- État des composants du produit

- État de la connexion du produit
- État de la connexion de l'agent

Widget Conformité des applications de produits

Ce widget affiche la version, la langue, la compilation et l'état de mise à jour du produit pour les produits gérés. Cela permet aux administrateurs de distinguer rapidement les applications des produits gérés à jour de ceux nécessitant une mise à jour.

Vous pouvez choisir d'afficher les données dans un graphique à barres ou un tableau en cliquant sur les icônes d'affichage ( ).

Cliquez sur les nombres dans les colonnes **À jour** et **Obsolète** pour ouvrir un écran affichant des informations détaillées. Control Manager effectue une requête sur le journal pour fournir les informations détaillées.

DONNÉES	DESCRIPTION
Produit	Produit géré enregistré auprès de Control Manager
Version	Version du produit géré
Langue	Version de langue du produit géré
Compilation	Numéro de compilation du produit géré
À jour	Nombre de produits considérés comme étant à jour Modifiez le widget de sorte à spécifier la version minimale du produit qui devrait toujours être considérée comme « à jour ». Cliquez sur le nombre pour afficher plus de détails sur le produit.
Obsolète	Nombre de produits « obsolètes » Cliquez sur le nombre pour afficher plus de détails sur le produit.
Taux à jour (%)	Pourcentage de produits « à jour »

Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Spécifiez un graphique en barres ou un tableau pour l'affichage des données. Par défaut, les données sont affichées sous la forme d'un graphique en barres.

Cliquez sur **Modifier** pour accéder aux options suivantes :

- Cliquez sur **Portée** > **Parcourir** pour spécifier les produits fournissant les données du widget.

  L'étendue des données spécifie les produits utilisés par le widget pour afficher les données. Cela peut avoir un effet considérable sur l'utilité des informations affichées par le widget.

- Dans la liste déroulante **Plage de mise à jour**, spécifiez le nombre de versions du produit de retard par rapport à la dernière compilation qui devrait toujours être considérée comme « à jour ».

Cliquez sur **Enregistrer** pour appliquer les modifications et quitter.

Widget d'état des composants du produit

Ce widget affiche les versions des composants et le niveau de conformité des produits gérés ou des endpoints sur votre réseau Il permet de suivre les produits gérés ou les endpoints dotés de composants obsolètes.

L'affichage par défaut présente les dernières versions des composants gérés par Control Manager ainsi que le niveau de conformité des produits gérés. Les sections **Fichier de signatures** et **Moteur** répertorient les composants du taux de non conformité le plus élevé au taux le plus bas. Vous pouvez cliquer sur la colonne **Taux** pour changer l'ordre de tri.

Cliquez sur l'un des composants de la colonne **Fichier de signatures** ou **Moteur** pour afficher un graphique circulaire qui présente le nombre de produits gérés ou d'endpoints qui utilisent chaque version du composant.

Cliquez sur les nombres de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur les produits gérés obsolètes, sur tous les produits gérés, sur les endpoints obsolètes ou sur tous les endpoints.

Cliquez sur l'icône Paramètres (>) pour configurer les options suivantes :

Remarque

L'icône Paramètres ( ) ne s'affiche pas pour les widgets de l'onglet **Résumé**.

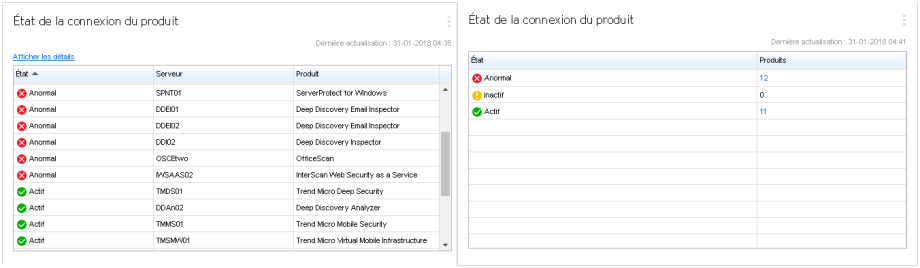
- Pour modifier la portée du produit pour le widget, cliquez sur le bouton représentant une double flèche (>>) dans le champ **Portée** et sélectionnez les produits qui fournissent des données.
- Pour modifier les composants qui s'affichent dans le widget, sélectionnez ou désélectionnez des composants dans les champs **Fichier de signatures** ou **Moteur**.
- Pour afficher les informations de conformité des produits gérés et/ou des endpoints, spécifiez la **Source**.
- Pour indiquer s'il convient d'afficher les données issues de tous les composants signalés par les produits gérés, ou uniquement des composants gérés par Control Manager, sélectionnez l'**affichage** approprié.

DONNÉES	DESCRIPTION
Fichier de signatures	Affiche le nom du fichier de signatures, du modèle ou de la règle anti-spam
Moteur	Affiche le nom du moteur de scan
Dernière version	Affiche les informations suivantes : • Dernière version du composant téléchargé par Control Manager • Dernière version du composant disponible en téléchargement (signalé par les produits gérés)

Données	Description
Obsolètes/Tous	Affiche les informations suivantes : • **Obsolètes** : nombre de produits gérés ou d'endpoints dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur les produits gérés ou les endpoints obsolètes. • **Tout** : nombre total de produits gérés ou d'endpoints utilisant le composant Cliquez sur le deuxième nombre de la colonne **Obsolètes/Tous** pour afficher des informations sur les versions des composants installés sur tous les produits gérés ou endpoints. **Remarque** Cette colonne s'affiche lorsque **Les deux** est sélectionné pour la **Source**.
Produit géré/Tous	• **Produit géré** : nombre de produits gérés dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Produit géré/Tout** pour afficher des informations sur les versions des composants installés sur les produits gérés obsolètes. • **Tout** : nombre total de produits gérés utilisant le composant Cliquez sur le deuxième nombre de la colonne **Produit géré/Tout** pour afficher des informations sur les versions des composants installés sur tous les produits gérés. **Remarque** Cette colonne s'affiche lorsque **Produit géré** est sélectionné pour la **Source**.

DONNÉES	DESCRIPTION
Endpoint/Tous	• **Endpoint** : nombre d'endpoints dotés de composants obsolètes Cliquez sur le premier nombre de la colonne **Endpoint/Tout** pour afficher des informations sur les versions des composants installés sur les endpoints obsolètes. • **Tout** : nombre total d'endpoints utilisant le composant Cliquez sur le deuxième nombre de la colonne **Endpoint/Tout** pour afficher des informations sur les versions des composants installés sur tous les endpoints. **Remarque** Cette colonne s'affiche lorsque l'élément **Endpoint** est sélectionné pour la **Source**.
Taux d'obsolescence	Affiche le pourcentage de produits gérés ou d'endpoints dotés de composants obsolètes **Remarque** Cette colonne s'affiche lorsque l'élément **Produit géré** ou **Endpoint** est sélectionné pour la **Source**.
Taux	Affiche le pourcentage de produits gérés ou d'endpoints dotés de composants obsolètes **Remarque** Cette colonne s'affiche lorsque **Les deux** est sélectionné pour la **Source**.

Widget État de la connexion du produit



Ce widget affiche l'état de la connexion de tous les produits gérés enregistrés auprès du serveur Control Manager.

L'affichage par défaut répertorie l'état de la connexion et le nom du serveur géré de chaque produit géré pour lequel le compte utilisateur connecté dispose de droits d'accès.

- Pour modifier la portée du produit, cliquez sur l'icône Paramètres (>) et sélectionnez une nouvelle **Portée**.
- Pour afficher un récapitulatif du nombre total de produits gérés pour chaque état de connexion, cliquez sur l'icône Paramètres (>) et basculez l'**affichage** vers **Récapitulatif**.

Cliquez sur **Afficher les détails** pour afficher des informations détaillées dans l'écran **Requête sur le journal**.

ÉTAT	DESCRIPTION
Active	Indique que le service produit est en cours d'exécution et que la communication avec le serveur Control Manager est correctement établie
Inactif	Indique que le service produit n'est pas en cours d'exécution ou ne parvient pas à établir la communication avec le serveur Control Manager

ÉTAT	DESCRIPTION
Anormal	Indique que le service produit n'a pas communiqué avec le serveur Control Manager dans l'intervalle du délai d'attente défini par l'utilisateur pour la communication avec l'agent

Widget État de la connexion de l'agent

Ce widget affiche l'état de la connexion des agents à leurs serveurs parents. Les agents pour les produits gérés suivants s'affichent :

- Trend Micro Endpoint Sensor
- Endpoint Encryption
- Mobile Security for Enterprise
- Trend Micro Security (pour Mac)
- OfficeScan
- Vulnerability Protection
- Worry-Free Business Security Services

Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Cliquez sur les valeurs dans les colonnes **En ligne**, **Hors ligne** ou **Total** pour afficher des informations supplémentaires. Control Manager effectue une requête ad hoc pour fournir les informations.

DONNÉES	DESCRIPTION
Serveur	Serveurs parents
En ligne	Agents connectés à leurs serveurs parents
Hors ligne	Agents déconnectés de leurs serveurs parents
Total	Nombre total d'endpoints

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⚙. Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur >> et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

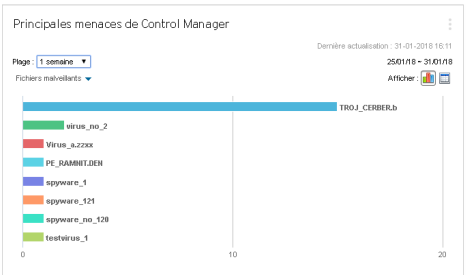
Onglet Détection des menaces

L'onglet **Détection des menaces** contient des widgets qui affichent les détections regroupées des menaces de sécurité.

Les widgets prédéfinis sont les suivants :

- Principales menaces de Control Manager
- Statistiques des menaces de Control Manager
- Résultats de la détection de menaces
- Détections de violations de stratégies
- Événements de rappel C&C

Widget des principales menaces de Control Manager



Rang	Fichier	Détections
1	TROJ_CERBER.b	15
2	virus_no_2	2
3	Virus_a.zzxx	1
4	PE_RAMNIT.DEN	1
5	spyware_1	1
6	spyware_121	1
7	spyware_no_120	1
8	testvirus_1	1

Ce widget affiche des informations sur les fichiers et les URL malveillants détectés sur une période spécifique.

Vous pouvez choisir d'afficher les données dans un graphique à barres ou un tableau en cliquant sur les icônes d'affichage ( ).

Utilisez la liste déroulante située au-dessus du graphique/tableau pour sélectionner le type de données de menace à afficher.

- **Fichiers malveillants** : classe les fichiers malveillants détectés sur votre réseau par nombre de détections
- **URL malveillantes** : classe les URL malveillantes détectées sur votre réseau par nombre de détections

Cliquez sur une barre, un nom de menace ou un numéro de détection pour ouvrir l'écran **Requête sur le journal** qui contient des informations sur les endpoints impactés, les détails des menaces et le nombre de détections.

L'affichage par défaut présente les 10 premières menaces provenant de tous les produits gérés pour lesquels le compte utilisateur connecté dispose de droits d'accès.

- Cliquez sur l'icône Paramètres (>) pour modifier le titre du widget, la portée du produit ou le nombre de menaces qui s'affiche.

Widget de statistiques des menaces de Control Manager

Ce widget affiche le nombre total de détections de menaces de sécurité sur votre réseau. Les données peuvent être filtrées par type de menace de sécurité ou en fonction de l'emplacement de la détection de la menace sur votre réseau.

- Catégorie du produit

DONNÉES	DESCRIPTION
Virus/programmes malveillants	Virus/programmes malveillants détectés par les produits gérés spécifiés par l'étendue des données
Spywares/ Graywares	Spywares/graywares détectés par les produits gérés spécifiés par l'étendue des données
Sécurité Web	Violations de sécurité Web (URL malveillantes, URL bloquées) détectées par les produits gérés spécifiés par l'étendue des données

DONNÉES	DESCRIPTION
Violation de contenu	Violations de sécurité de contenu (spams, mots-clés et expressions bloqués) détectées par les produits gérés spécifiés par l'étendue des données

- Type de menace

DONNÉES	DESCRIPTION
Serveur de fichiers	Menaces de sécurité détectées sur les serveurs de fichiers par les produits gérés spécifiés par l'étendue des données
Réseau	Menaces de sécurité détectées sur votre réseau par les produits gérés spécifiés par l'étendue des données
Inconnu	Menaces de sécurité non identifiées
Courrier	Menaces de sécurité détectées sur les serveurs de messagerie par les produits gérés spécifiés par l'étendue des données
Poste de travail	Menaces de sécurité détectées sur les postes de travail par les produits gérés spécifiés par l'étendue des données
Passerelle	Menaces de sécurité détectées au niveau de la passerelle par les produits gérés spécifiés par l'étendue des données
Serveur Control Manager	Menaces de sécurité détectées sur les serveurs Control Manager par les produits gérés spécifiés par l'étendue des données

Remarque

Le widget ne peut afficher des données que pour un type d'information à la fois.

Cliquez sur les liens de la colonne **Détections** pour ouvrir un écran affichant des informations détaillées. Control Manager effectue une requête ad hoc pour fournir les informations détaillées.

DONNÉES	DESCRIPTION
Type	Type de menace de sécurité ou produit géré dans lequel la menace est détectée
Détections	Nombre de menaces de sécurité détectées
Pourcentage (%)	Pourcentage de menaces de sécurité par rapport au nombre total de menaces détectées

Spécifiez la plage de dates relative aux données affichées par le widget :

- 24 heures
- 1 semaine
- 2 semaines
- 1 mois

Spécifiez la façon dont le widget affiche les données :

- Graphique circulaire
- Graphique en barres
- Tabulaire
- Graphique en ligne

Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⫶⫶. Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur >> et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

Widget Résultats de la détection de menaces

Ce widget affiche le nombre de détections de menaces et le ratio de menaces par rapport au nombre total de détections. Le widget ne peut afficher des données que pour un type d'information à la fois. Si vous cliquez sur les liens de la colonne **Détections**, un écran

affichant des informations détaillées s'ouvre. Control Manager effectue une requête ad hoc pour fournir les informations détaillées.

Données	Description
Résultats	Type de menace de sécurité ou produit géré dans lequel la menace est détectée **Remarque** Cette colonne ne s'affiche pas pour le type de menace **Sécurité Web**
Stratégie/règle	Le type de stratégie/règle appliqué sous le type de menace **Sécurité Web**. **Remarque** Cette colonne ne s'affiche pas pour les autres types de menace répertoriés.
Détections	Nombre de menaces de sécurité détectées
Pourcentage (%)	Pourcentage de menaces de sécurité par rapport au nombre total de menaces détectées

Ce widget affiche les détections de menaces pour les types de menace suivants :

Tableau 1-4. Types de menace

Type de menace	Description
Virus/programmes malveillants	Affiche l'action exécutée sur tous les fichiers par les produits gérés spécifiés par l'étendue des données. Par exemple : Nettoyé, Accès refusé, etc.
Spywares/ Graywares	Affiche l'action exécutée sur tous les fichiers par les produits gérés spécifiés par l'étendue des données. Par exemple : Réussite, Autre action requise, etc.
Sécurité de contenu	Affiche l'action exécutée sur tous les messages électroniques par les produits gérés spécifiés par l'étendue des données. Par exemple : Supprimé, Pièces jointes éliminées, etc.

TYPE DE MENACE	DESCRIPTION
Sécurité Web	Affiche toutes les violations de sécurité Web bloquées, via les stratégies, par les produits gérés spécifiés par l'étendue des données. Par exemple : Blocage de fichier, Nom du fichier, etc.
Virus réseau	Affiche l'action exécutée sur tous les virus réseau par les produits gérés spécifiés par l'étendue des données.

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⚙. Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur » et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

- Pour modifier le titre de votre widget **Résultats de la détection de menaces**, utilisez le champ **Titre**.
- Utilisez la liste déroulante **Type de menace** pour spécifier le type de menace.

Cliquez sur **Enregistrer** pour appliquer les modifications et quitter.

Widget de détections de violations de stratégies

Ce widget affiche les détections de violations de stratégie pour les appareils Network VirusWall Enforcer. Si vous cliquez sur les liens de la colonne **Détections**, un écran affichant des informations détaillées s'ouvre. Control Manager effectue une requête sur le journal pour fournir les informations détaillées.

DONNÉES	DESCRIPTION
Type	Répertorie les **violations de service** comme type de menace de sécurité
Mis à jour	Date de la dernière mise à jour
Détections	Nombre de violations de services détectées par les dispositifs Network VirusWall Enforcer

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⚙.

- Pour modifier le titre de votre widget **Détections de violations de stratégies**, utilisez le champ **Titre**.

- Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur >> et en sélectionnant les serveurs parents utilisés par le widget en tant que source.

Remarque

Ce widget affiche uniquement les détections de violations de stratégie pour Network VirusWall Enforcer.

Cliquez sur **Enregistrer** pour appliquer les modifications et quitter.

Widget Événements de rappel C&C

Ce widget affiche le nombre de tentatives de rappel C&C en fonction des hôtes compromis ou des adresses de rappel. Le widget ne peut afficher des données que pour un type d'information à la fois. Cliquer sur les numéros de n'importe quelle cellule du tableau permet d'ouvrir l'écran **Événements de rappel C&C** qui contient les données récapitulatives de rappel suivantes :

DONNÉES	DESCRIPTION
Hôte compromis	Adresse électronique ou hôte affectés
Adresse de rappel	L'URL, l'adresse IP ou électronique à laquelle l'hôte compromis tente un rappel
Emplacement du serveur C&C	Région et pays de l'emplacement du serveur C&C
Tentatives de rappel	Nombre de communications entre les adresses de rappel et les hôtes compromis
Dernier hôte compromis/Dernière adresse de rappel	URL, adresse IP ou électronique vers laquelle la dernière tentative de rappel a été effectuée
Adresses de rappel/ Hôtes compromis (avec numéros affichés dans les colonnes)	Nombre d'adresses de rappel ou d'hôtes compromis associés aux tentatives de rappel

DONNÉES	DESCRIPTION
Consigné par	Nom du produit géré qui a enregistré l'événement

Pour modifier les informations affichées par le widget, cliquez sur ⋮ > ⫶⫶.

- Pour modifier le titre de votre widget **Événements de rappel C&C**, utilisez le champ **Titre**.
- Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur » et en sélectionnant les serveurs parents utilisés par le widget en tant que source.
- Spécifiez les sources C&C à l'aide de la liste déroulante **Liste des sources C&C**. La liste déroulante répertorie les listes de sources C&C **Intelligence globale**, **Virtual Analyzer** et **Défini par l'utilisateur**.
- Sélectionnez le nombre d'éléments à afficher sur le widget à partir de la liste déroulante **Éléments à afficher**. La liste déroulante répertorie un maximum de 50 principaux éléments.

Cliquez sur **Enregistrer** pour appliquer les modifications et quitter.

Configuration des paramètres de Smart Protection Network

Activez Trend Micro Smart Feedback pour partager des informations sur les menaces avec Trend Micro Smart Protection Network. Votre réseau est ainsi mieux protégé dans la mesure où Trend Micro est capable d'identifier et de traiter rapidement les nouvelles menaces.

Remarque

La réputation des e-mails, File Reputation et la Web Reputation font partie du réseau Smart Protection Network.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres Smart Protection Network**.

   L'écran **Paramètres Smart Protection Network** apparaît.

2. Sélectionnez **Activer Trend Micro Smart Feedback et Smart Protection Network (recommandé)**.

3. Spécifiez à quelle fréquence Control Manager enverra des informations entièrement anonymes sur les menaces à Smart Protection Network à partir de la liste déroulante **Intervalle de temps**.

4. (Facultatif) Spécifiez le secteur d'activité auquel votre société appartient à partir de la liste déroulante **Votre secteur d'activité**.

5. Cliquez sur **Enregistrer**.

Chapitre 2

Gestion des stratégies

Cette section contient des informations sur la manière d'exécuter la gestion des stratégies sur les produits gérés et les endpoints.

Les rubriques sont les suivantes:

- *Gestion des stratégies à la page 2-2*
- *Prévention contre la perte de données à la page 2-27*
- *État de la stratégie à la page 2-47*

Gestion des stratégies

La gestion des stratégies permet aux administrateurs d'appliquer les paramètres d'un produit dans les produits gérés et les endpoints à partir d'une seule console d'administration. Les administrateurs créent une stratégie en sélectionnant les cibles et en configurant une liste des paramètres du produit.

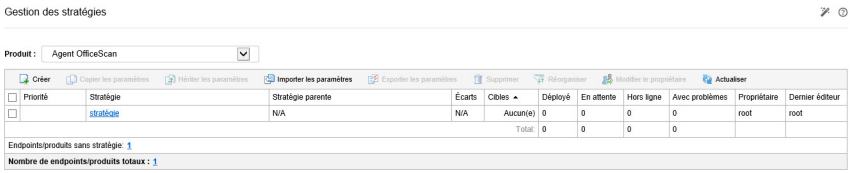
Pour effectuer une gestion des stratégies sur un nouveau produit géré ou un endpoint, déplacez le produit géré depuis le dossier **Nouvelle entité** vers un autre dossier dans la structure du répertoire Produits.

Création d'une nouvelle stratégie

Procédure

1. Allez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.



2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur **Créer**.

   L'écran **Créer une stratégie** apparaît.

4. Saisissez un nom de stratégie.

5. Spécifiez les cibles.

   Control Manager propose plusieurs méthodes de sélection de cibles, qui affectent le fonctionnement d'une stratégie.

Remarque

Pour définir un produit géré ou un endpoint comme cible, assurez-vous que la version du produit géré ou de l'endpoint prend en charge la gestion des stratégies dans Control Manager. L'écran **Paramètres de modèle de stratégie** (**Stratégies** > **Ressources de stratégies** > **Paramètres de modèle de stratégie**) contient des informations sur les versions de produits prises en charge.

La liste des stratégies classe les cibles de stratégie dans l'ordre suivant :

- **Spécifier les cibles** : Utilisez cette option pour sélectionner des points finaux ou des produits gérés spécifiques.

  Pour obtenir des informations détaillées, consultez la section *Spécifications des cibles de stratégie à la page 2-9*.

- **Filtrer par critères** : Utilisez cette option pour allouer automatiquement des points finaux en fonction des critères de filtre.

  Pour obtenir des informations détaillées, consultez la section *Filtrer par critères à la page 2-5*.

- **Aucune (Brouillon uniquement)** : Utilisez cette option pour sauvegarder la stratégie en tant qu'ébauche sans choisir de cible.

Pour plus d'informations sur la liste des stratégies, consultez la section *Description de la liste des stratégies à la page 2-21*.

6. Cliquez sur une fonctionnalité de produit géré pour la développer et configurer ses paramètres. Répétez cette étape pour configurer toutes les fonctionnalités.

   - Chaque fonctionnalité est dotée d'un lien vers une rubrique d'aide qui aborde la fonctionnalité et la façon de l'utiliser.

   - Pour certains paramètres de produit, Control Manager doit obtenir des options de paramétrage spécifiques à partir des produits gérés. Si les administrateurs sélectionnent des cibles multiples pour une stratégie, Control Manager peut uniquement obtenir les options de paramétrage à partir de la première cible sélectionnée. Pour garantir un déploiement des stratégies réussi, assurez-vous que les paramètres du produit sont synchronisés dans les cibles.

- Si vous créez une stratégie pour l'**agent OfficeScan** qui devra se comporter en parente d'une future stratégie enfant, configurez les paramètres qui peuvent être hérités, personnalisés ou étendus sur la stratégie enfant.
  - Pour obtenir la liste des paramètres de l'agent OfficeScan qui peuvent être hérités, personnalisés ou étendus, consultez la rubrique *Utilisation des paramètres de stratégie parente à la page 2-10*.
  - Pour plus d'informations sur la création d'une stratégie enfant, consultez la rubrique *Héritage des paramètres de stratégie à la page 2-15*.
- Si vous avez mis à niveau Control Manager 6.0 à 6.0 Service Pack 2 avec des **paramètres gérés localement** vers la version 6.0 Service Pack 3, consultez les instructions dans la rubrique *Utilisation des autorisations et des paramètres de stratégie hérités à la page 2-13*.

7. Cliquez sur **Déployer** ou **Enregistrer**.

   Si vous avez cliqué sur **Déployer**, Control Manager commence le déploiement. La stratégie apparaît dans la liste figurant à l'écran **Gestion des stratégies**. Quelques minutes sont nécessaires pour que Control Manager déploie la stratégie sur les cibles.

   Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies. Si l'état du déploiement est toujours en attente après une période prolongée, les cibles peuvent rencontrer des problèmes. Vérifiez la présence d'une connexion entre Control Manager et les cibles. Vérifiez également si les cibles fonctionnent correctement.

   Lorsque Control Manager déploie une stratégie sur les cibles, les paramètres définis dans la stratégie écrasent les paramètres existants dans les cibles. Control Manager applique les paramètres de stratégie aux cibles toutes les 24 heures. Bien que les administrateurs locaux puissent modifier les paramètres à partir de la console du produit géré, les modifications sont écrasées à chaque fois que Control Manager applique les paramètres de la stratégie.

   - Control Manager applique les paramètres de stratégie aux cibles toutes les 24 heures. Comme l'application de la stratégie n'a lieu que toutes les 24 heures, les paramètres du produit dans les cibles peuvent ne pas correspondre aux paramètres de la stratégie si les administrateurs locaux font des modifications via la console du produit géré entre deux périodes d'application.

- Les paramètres de la stratégie déployés vers les serveurs IMSVA ont la priorité sur les paramètres existants dans les serveurs cibles au lieu de les écraser. Les serveurs IMSVA sauvegardent ces paramètres de stratégie en haut de la liste.
- Si un agent OfficeScan auquel une stratégie Control Manager est affectée a été déplacé vers un autre domaine OfficeScan, les paramètres de l'agent seront temporairement remplacés par ceux définis par ce domaine OfficeScan. Quand Control Manager appliquera à nouveau la stratégie, les paramètres de l'agent respecteront les paramètres de la stratégie.

Filtrer par critères

Utilisez cette option pour allouer automatiquement des points finaux en fonction des critères de filtre.

Cette option :

- n'est disponible que sur les produits gérés suivants :
  - OfficeScan
  - Mobile Security for Enterprise
  - Trend Micro Security (pour Mac)
- Utilise un filtre pour affecter automatiquement des cibles actuelles et futures à la stratégie
- Utile pour le déploiement de paramètres standard sur un groupe de cibles

Les administrateurs peuvent modifier la priorité des stratégies filtrées dans la liste des stratégies. Quand un administrateur réorganise la liste des stratégies, Control Manager affecte à nouveau les cibles aux différentes stratégies filtrées en fonction des critères de la cible et des rôles utilisateurs du créateur de chaque stratégie.

Control Manager peut seulement affecter des endpoints sans stratégies dans une nouvelle stratégie filtrée. Pour réallouer un endpoint déjà affecté à une stratégie filtrée, montez une autre stratégie filtrée avec les critères correspondants dans la liste de priorité.

Pour plus d'informations sur la manière dont Control Manager affecte les cibles aux stratégies filtrées, consultez la rubrique *Affectation de endpoints aux stratégies filtrées à la page 2-7*.

Procédure

1. Dans l'écran **Créer une stratégie**, accédez à la section **Cibles**, sélectionnez **Filtrer par critères**, puis cliquez sur **Définir un filtre**.

   L'écran **Filtrer par critères** apparaît.

2. Sélectionnez les options suivantes et définissez le critère.

CRITÈRES	DESCRIPTION
Faire correspondre des mots-clés dans	Définissez des mots-clés en fonction du nom de l'hôte ou du nom d'affichage de Control Manager. **Remarque** Control Manager effectue une correspondance partielle pour les recherches à un seul mot-clé. Vous pouvez rechercher plusieurs mots-clés séparés par des virgules, mais Control Manager fournit uniquement des correspondances de chaîne complètes pour chaque mot-clé fourni.
Adresses IP	Définissez une plage d'adresses IP et cliquez sur **Ajouter**. **Remarque** • La gestion des stratégies ne prend en charge que les adresses IPv4. • Lorsqu'un nouveau produit géré ou endpoint est enregistré auprès de Control Manager, il faut environ une heure au produit géré ou au endpoint pour apparaître dans une recherche par adresse IP.
Systèmes d'exploitation	Sélectionnez un ou plusieurs systèmes d'exploitation dans la liste déroulante.

CRITÈRES	DESCRIPTION
Répertoires	Sélectionnez l'un des répertoires suivants et définissez les critères. • **Répertoire Produits** : sélectionnez des dossiers depuis la structure du Répertoire Produits • **Active Directory** : sélectionnez des unités organisationnelles depuis une structure Active Directory intégrée • **Hiérarchie de domaines OfficeScan** : saisissez au moins un mot-clé de hiérarchie de domaines OfficeScan

3. Cliquez sur **Enregistrer**.

   L'écran **Créer une stratégie** est actualisé.

Affectation de endpoints aux stratégies filtrées

Lorsqu'un nouvel endpoint s'enregistre auprès de Control Manager, il parcourt les stratégies filtrées de la liste par ordre décroissant. Control Manager affecte le nouvel endpoint à une stratégie filtrée lorsque les conditions suivantes sont toutes deux remplies :

- Le nouveau endpoint correspond aux critères de la cible dans la stratégie
- Le créateur de la stratégie a l'autorisation de gérer le nouveau endpoint

La même action s'applique à un endpoint déjà affecté à une stratégie, mais le créateur de la stratégie supprime la stratégie plus tard.

Remarque

Pour les endpoints qui viennent d'être enregistrés auprès de Control Manager et pour ceux qui viennent d'être libérés de stratégies supprimées, une période de grâce de trois minutes est appliquée durant laquelle aucune allocation d'endpoint n'a lieu. Ces endpoints ne disposent temporairement pas de stratégie pendant cette période.

Si un endpoint ne correspond pas aux critères de la cible pour aucune des stratégies filtrées, le endpoint ne s'associe à aucune stratégie. Control Manager alloue ces endpoints à nouveau lorsque les actions suivantes se produisent :

- Créer une stratégie filtrée
- Modifier une stratégie filtrée
- Réorganiser les stratégies filtrées
- Programmer l'allocation journalière de endpoints

  Control Manager utilise une programmation d'allocation journalière de endpoints pour garantir l'affectation des endpoints aux bonnes stratégies. Cette action se produit tous les jours à 15 h 15. Si les propriétés du endpoint changent, comme le système d'exploitation ou l'adresse IP, ces endpoints demandent à la programmation journalière de les réallouer aux bonnes stratégies.

Remarque

Si les endpoints sont hors ligne au moment de la programmation d'allocation des endpoints, l'état de la stratégie de ces endpoints restera en attente jusqu'à ce qu'ils soient connectés.

Lorsque les actions ci-dessus se produisent, Control Manager alloue les endpoints en fonction des conditions suivantes :

TABLEAU 2-1. Allocation de endpoints aux stratégies filtrées

	Nouveaux endpoints ou endpoints de stratégies supprimées	Endpoints sans stratégie	Endpoints avec stratégie
Créer une stratégie		●	
Modifier une stratégie	●	●	●
Réorganiser les stratégies filtrées	●	●	●

Programmer l'allocation journalière de endpoints	●	●	●

Spécifications des cibles de stratégie

Utilisez cette option pour sélectionner des points finaux ou des produits gérés spécifiques.

Cette option :

- Utilise la fonction rechercher ou parcourir pour localiser des cibles spécifiques et les affecter manuellement à la stratégie
- Utile quand les administrateurs planifient un déploiement de paramètres spécifiques uniquement sur certaines cibles
- Reste statique au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées.

Procédure

1. Dans l'écran **Créer une stratégie**, accédez à la section **Cibles**, sélectionnez **Spécifier la ou les cibles**, puis cliquez sur **Sélectionner**.

   L'écran **Spécifier les cibles** apparaît.

2. Utilisez **Rechercher** ou **Parcourir** pour localiser les cibles.

   - **Rechercher** : utilisez les critères de recherche suivants pour trouver les endpoints ou les produits gérés. Les résultats de la recherche affichent les endpoints ou les produits gérés qui correspondent à tous les critères sélectionnés.

     - **Faire correspondre des mots-clés dans** : Définissez des mots-clés en fonction du nom de l'hôte ou du nom d'affichage de Control Manager.
     - **Adresses IP** : définissez une plage d'adresses IP et cliquez sur **Ajouter**.

Remarque

- La gestion des stratégies ne prend en charge que les adresses IPv4.
- Lorsqu'un nouveau produit géré ou endpoint est enregistré auprès de Control Manager, il faut environ une heure au produit géré ou au endpoint pour apparaître dans une recherche par adresse IP.

- **Systèmes d'exploitation** : sélectionnez un ou plusieurs systèmes d'exploitation dans la liste déroulante.

- **Parcourir** : parcourez le répertoire Produits ou Active Directory pour localiser les endpoints ou les produits gérés et les affecter à la stratégie.

3. Sélectionnez les endpoints ou les produits gérés, puis cliquez sur **Ajouter les cibles sélectionnées**.
4. Attendez que les numéros changent dans **Afficher la liste des actions** et **Afficher les résultats**.
5. Cliquez sur **OK**.

   L'écran **Créer une stratégie** est actualisé.

Utilisation des paramètres de stratégie parente

Un administrateur de Control Manager qui crée une stratégie parente pour l'**agent OfficeScan** peut configurer certains paramètres de la stratégie qui doivent être hérités, personnalisés ou étendus.

Remarque

Ces options ne sont pas disponibles sur d'autres produits gérés.

- **Héritent du parent**
  - Un administrateur de la stratégie enfant ne peut pas du tout modifier le paramètre. Un administrateur OfficeScan peut modifier manuellement le paramètre à partir de la console du serveur OfficeScan. Toutefois, le

paramètre sera remplacé lorsque Control Manager déploiera des stratégies sur le serveur OfficeScan.

Par exemple, un administrateur Control Manager peut créer une stratégie parente qui impose l'exclusion des fichiers PDF d'un scan manuel.

- Les modifications apportées au paramètre de la stratégie parente sont toujours appliquées à la stratégie enfant.
- Si l'autorisation sur la stratégie parente passe de « Héritent du parent » à « Sont personnalisables » ou « S'étendent à partir du parent », l'administrateur de la stratégie enfant peut personnaliser ou étendre le paramètre actuel. Les modifications apportées au paramètre de la stratégie parente ne sont plus appliquées.

- **Sont personnalisables**
  - Une stratégie enfant peut dévier du paramètre configuré dans la stratégie parente.

    Par exemple, si le paramètre Scan programmé dans la stratégie parente s'exécute en mode hebdomadaire, mais qu'il est personnalisable, l'administrateur de la stratégie enfant peut modifier sa programmation en mode journalier.
  - Les modifications apportées au paramètre de la stratégie parente ne sont jamais appliquées à la stratégie enfant.
  - Si l'autorisation sur la stratégie parente passe de « Sont personnalisables » à « Héritent du parent », le paramètre actuel de la stratégie parente remplace celui de la stratégie enfant. Les modifications apportées au paramètre de la stratégie parente sont toujours appliquées.
- **S'étendent à partir du parent**
  - Un administrateur de la stratégie enfant peut effectuer des ajouts aux éléments configurés dans la stratégie parente.

    Par exemple, si la stratégie parente exclut 20 noms de fichiers d'un scan manuel, l'administrateur peut ajouter 10 fichiers plus sûrs et fiables à la stratégie enfant.

- Les éléments ajoutés ou supprimés de la stratégie parente sont également ajoutés ou supprimés de la stratégie enfant. Un élément supprimé peut être ajouté à l'enfant.
- Si l'autorisation sur la stratégie parente passe de « S'étendent à partir du parent » à « Héritent du parent », les éléments de la stratégie enfant qui n'ont aucune correspondance dans le parent sont supprimés. Les modifications apportées aux éléments de la stratégie parente sont toujours appliquées.

Le tableau suivant répertorie les paramètres de stratégie parente qui peuvent être hérités, personnalisés ou étendus.

PARAMÈTRES ET CHEMIN D'ACCÈS	OPTIONS DISPONIBLES		
	HÉRITENT DU PARENT	SONT PERSONNALISABLES	S'ÉTENDENT À PARTIR DU PARENT
Programmation du scan **Paramètres de scan programmé** > Onglet **Cibles** > Section **Programmation**	●	●	
Extensions des fichiers à scanner **Paramètres Scan manuel / Scan en temps réel / Scan immédiat / Scan programmé** > Onglet **Cibles** > Section **Fichiers à scanner** > Option **Fichiers portant les extensions suivantes**	●		●

Paramètres et chemin d'accès	Options disponibles		
	Héritent du parent	Sont personnalisables	S'étendent à partir du parent
Listes des exclusions de scan (répertoires, fichiers et extensions de fichiers à exclure des scans) **Paramètres Scan manuel / Scan en temps réel / Scan immédiat / Scan programmé** > Onglet **Exclusions de scan**	●		● Lorsque vous sélectionnez **S'étendent à partir du parent** dans une liste des exclusions de scan, la liste déroule une section **Restrictions de la stratégie enfant** dans laquelle les créateurs de la stratégie parente peuvent spécifier les éléments que les stratégies enfant ne peuvent pas exclure des scans.

Utilisation des autorisations et des paramètres de stratégie hérités

Dans Control Manager 6.0 à 6.0 Service Pack 2, les administrateurs de Control Manager disposent des options suivantes lors de la configuration des autorisations des paramètres du produit géré :

- **Gestion centralisée** : les cibles affectées suivront les paramètres définis dans la stratégie.
- **Gestion locale** : Control Manager ne déploie pas les paramètres de la fonction sélectionnée sur les cibles. Les administrateurs du produit géré peuvent définir les paramètres par le biais de la console du produit. Lorsque les administrateurs déploient une stratégie avec tous les paramètres des fonctionnalités définis sur Gestion locale, l'état de la stratégie des cibles est en attente.

À compter de la version 6.0 Service Pack 3, toutes les fonctions sont considérées comme gérées de manière centralisée (le changement des autorisations n'est plus possible), excepté dans le cas des fonctions configurées pour être gérées localement dans les

versions 6.0 à 6.0 Service Pack 2. Les administrateurs peuvent conserver telles quelles ces fonctionnalités gérées localement. Ils peuvent également définir l'autorisation sur « Gestion centralisée » (en faisant glisser le bouton orange vers la gauche), ce qui devient définitif et ne peut donc pas être annulé ultérieurement.

Copie des paramètres de stratégie

Les administrateurs peuvent copier les paramètres à partir d'une stratégie existante, créer une nouvelle stratégie avec les mêmes paramètres et déployer les paramètres dans différents endpoints ou produits gérés.

Remarque

Il n'est pas possible de copier les paramètres d'une stratégie enfant de l'**agent OfficeScan**. Pour déterminer si une stratégie de l'agent OfficeScan est un enfant ou un parent, vérifiez la colonne **Stratégie parente**. Une valeur sur laquelle vous pouvez cliquer s'affiche si la stratégie est un enfant et sinon, N/A s'affiche.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste Produit.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Sélectionnez une stratégie dans la liste.

4. Cliquez sur **Copier les paramètres**.

   L'écran **Copier et créer une stratégie** apparaît.

5. Dans le champ **Nom de la stratégie**, saisissez un nom pour la stratégie.

6. Affectez des **Cibles** à la stratégie.

7. (Facultatif) Modifiez les paramètres selon vos besoins.

8. Cliquez sur **Déployer**.

Remarque

- Après avoir cliqué sur **Déployer**, veuillez attendre deux minutes pour que Control Manager puisse déployer la stratégie dans les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.
- Control Manager applique les paramètres de stratégie aux cibles toutes les 24 heures.

Héritage des paramètres de stratégie

Créez une nouvelle stratégie enfant en héritant les paramètres d'une stratégie parente existante. Une stratégie enfant ne peut pas être copiée et ses paramètres ne peuvent pas être hérités.

Cette tâche nécessite une stratégie parente pour l'agent OfficeScan. Une stratégie parente pour l'agent OfficeScan a la valeur **N/A** affichée sous la colonne **Stratégie parente**.

Procédure

1. Allez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez **Agent OfficeScan** dans la liste des produits.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Sélectionnez une stratégie parente qui ne dispose pas de paramètres gérés localement.

4. Cliquez sur **Hériter les paramètres**.

   L'écran **Hériter et créer une stratégie** apparaît.

5. Dans le champ **Nom de la stratégie**, saisissez un nom pour la stratégie.

6. Affectez des **Cibles** à la stratégie.

7. (Facultatif) Vérifiez les paramètres qui peuvent être personnalisés ou étendus, puis apportez des modifications, si nécessaire. Pour obtenir la liste des paramètres à vérifier, consultez la rubrique *Utilisation des paramètres de stratégie parente à la page 2-10*.

   Remarque

   Un paramètre ne peut être ni personnalisé ni étendu si l'option sélectionnée sur la stratégie parente est **Héritent du parent**.

   Par exemple :

   - Si le paramètre Scan programmé est personnalisable, vous pouvez modifier la programmation d'Hebdomadaire en Quotidienne.
   - Si la liste des exclusions de scan en temps réel peut être étendue, vous pouvez saisir des noms de fichiers supplémentaires que vous considérez sans danger et fiables. Une fois la stratégie enfant créée, les noms de fichiers seront ajoutés à la liste des exclusions de scan.

8. Cliquez sur **Déployer**.

   Remarque

   - Après avoir cliqué sur **Déployer**, veuillez attendre deux minutes pour que Control Manager puisse déployer la stratégie dans les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.
   - Control Manager applique les paramètres de stratégie aux cibles toutes les 24 heures.

Modification d'une stratégie

Les administrateurs peuvent modifier les cibles et les paramètres des stratégies selon les besoins. Le propriétaire du compte racine peut modifier toutes les stratégies de la liste, tandis que d'autres propriétaires de compte peuvent modifier uniquement les stratégies

qu'ils ont créées. Après la modification d'une stratégie, Control Manager déploie celle-ci sur les cibles.

Pour une stratégie parente de l'agent d'OfficeScan, si vous avez modifié les cibles et les paramètres des fonctionnalités spécifiques, les modifications s'appliqueront à toutes les stratégies enfant et seront déployées sur les cibles respectives. Certains paramètres sur une stratégie parente prennent en charge des **autorisations** qui contrôlent les modifications autorisées sur les stratégies enfant. Les modifications apportées à ces autorisations de stratégie parent sont également appliquées aux stratégies enfant et déployées sur les cibles. Pour obtenir la liste des paramètres qui prennent en charge les autorisations, consultez la rubrique *Utilisation des paramètres de stratégie parente à la page 2-10*.

Par exemple :

- Si vous avez modifié les autorisations de programmation de « Héritent du parent » à « Sont personnalisables », les administrateurs peuvent commencer à personnaliser la programmation existante de leurs stratégies enfant.
- Si vous avez modifié l'autorisation relative aux extensions de fichier de scan manuel « S'étendent à partir du parent » en « Héritent du parent », toutes les extensions de fichiers que les administrateurs ont ajoutées aux stratégies enfant seront supprimées. En outre, les administrateurs ne seront plus en mesure d'ajouter des extensions de fichiers.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur le nom d'une stratégie dans la colonne **Stratégie**.

   L'écran **Modifier une stratégie** apparaît.

4. Modifiez la stratégie.

Remarque

La modification des critères de filtrage dans une stratégie filtrée peut affecter l'allocation de la cible. Control Manager peut réaffecter des cibles à d'autres stratégies filtrées ou ajouter des cibles supplémentaires à la stratégie en cours.

5. Cliquez sur **Déployer**.

   Quelques minutes sont nécessaires pour que Control Manager déploie la stratégie sur les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies. Si l'état du déploiement est toujours en attente après une période prolongée, les cibles peuvent rencontrer des problèmes. Vérifiez la présence d'une connexion entre Control Manager et les cibles. Vérifiez également si les cibles fonctionnent correctement.

   Control Manager applique les paramètres de stratégie aux cibles toutes les 24 heures.

Importation et exportation des stratégies

Exportez les stratégies en vue de les sauvegarder ou de les importer sur un autre serveur Control Manager de même version.

Remarque

- Control Manager permet d'exporter les paramètres de stratégie, mais pas les cibles de stratégie.
- Une stratégie parente conserve son état de parent après l'exportation ou l'importation.
- Une stratégie enfant devient parent après l'exportation. Par conséquent, elle devient parent après l'importation.
- Control Manager ne peut pas importer une stratégie si son nom est identique à celui d'une stratégie enfant existante. Si la stratégie existante n'est pas un enfant, Control Manager la remplace après l'importation.

Procédure

1. Allez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Pour effectuer l'exportation, sélectionnez une ou plusieurs stratégies, cliquez sur **Exporter les paramètres**, puis enregistrez le fichier de stratégie généré.

   - Si vous avez exporté une seule stratégie, le fichier généré présente l'extension `.cmpolicy`.
   - Si vous avez exporté plusieurs stratégies, le fichier généré est un fichier compressé (`.zip`) contenant des fichiers `.cmpolicy` individuels.

4. Pour effectuer l'importation, cliquez sur **Importer les paramètres**, puis localisez et chargez le fichier de stratégie.

   - Vous pouvez importer un fichier `*.zip` entier ou importer des fichiers `*.cmpolicy` individuels, en procédant un par un.
   - Si la stratégie existe déjà dans la liste des stratégies, une invite de confirmation s'affiche en vous demandant si vous souhaitez écraser la stratégie existante.

     Cliquez sur **OK** pour continuer.

   L'écran s'actualise et affiche la stratégie importée en haut de la liste.

   Pour plus d'informations sur la réorganisation de la liste des stratégies, consultez la section *Réorganisation de la liste des stratégies à la page 2-25*.

Suppression d'une stratégie

Les administrateurs peuvent supprimer une stratégie de la liste. Control Manager réalloue alors les cibles associées à la stratégie supprimée si les cibles correspondent aux critères de filtre d'une autre stratégie. Celles qui ne correspondent pas deviennent des

endpoints sans stratégie et gardent alors les paramètres définis par la stratégie supprimée sauf si un administrateur de produit géré modifie ces paramètres.

Control Manager permet uniquement la suppression des stratégies par leurs créateurs. Cependant, le compte racine peut supprimer toutes les polices de la liste.

Il n'est pas possible de supprimer une stratégie parente de l'agent OfficeScan avec les paramètres *hérités* d'une stratégie enfant existante.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Sélectionnez la stratégie à supprimer.

4. Cliquez sur **Supprimer**.

   Un écran de confirmation apparaît.

5. Cliquez sur **OK**.

Modification du propriétaire de la stratégie

Le propriétaire par défaut d'une stratégie est le compte utilisateur qui a créé la stratégie. Vous pouvez utiliser l'écran **Gestion des stratégies** pour redéfinir le propriétaire d'une stratégie sur n'importe quel compte utilisateur Control Manager. Vous pouvez également redéfinir le propriétaire d'une stratégie sur un groupe Active Directory afin de désigner tous les utilisateurs Active Directory faisant partie du groupe en tant que propriétaires de la stratégie.

Important

Si vous redéfinissez le propriétaire d'une stratégie sur un compte utilisateur qui ne dispose pas des droits d'accès aux cibles spécifiées, le nouveau propriétaire pourra modifier les paramètres de stratégie mais ne pourra pas afficher les données de stratégie.

Procédure

1. Allez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez une ou plusieurs stratégies pour lesquelles modifier le propriétaire.

3. Cliquez sur **Modifier le propriétaire**.

   L'écran **Modifier le propriétaire de la stratégie** s'affiche.

4. Sélectionnez un compte utilisateur dans la liste déroulante.

5. Cliquez sur **Enregistrer** pour modifier le propriétaire.

   Control Manager envoie une notification par e-mail à tous les comptes utilisateurs affectés au rôle « Administrateur ».

Description de la liste des stratégies

La liste des stratégies affiche les informations et l'état des stratégies créées par tous les utilisateurs. Lorsqu'un nouvel endpoint s'enregistre auprès de Control Manager, il parcourt les stratégies filtrées de la liste par ordre décroissant. Control Manager affecte le nouvel endpoint à une stratégie filtrée lorsque les conditions suivantes sont toutes deux remplies :

- Le nouveau endpoint correspond aux critères de la cible dans la stratégie
- Le créateur de la stratégie a l'autorisation de gérer le nouveau endpoint

Le tableau suivant décrit les colonnes de liste de stratégies qui s'affichent à l'écran **Gestion des stratégies**. Cliquez sur une colonne pour trier les données.

TABLEAU 2-2. Liste des stratégies

COLONNE	DESCRIPTION
Priorité	Affiche la priorité des stratégies. • Control Manager liste les stratégies en partant de la priorité la plus élevée à la priorité la plus basse. • Quand des administrateurs créent une stratégie filtrée, Control Manager enregistre la nouvelle stratégie en lui donnant la priorité la plus basse. • Une stratégie spécifiée a la priorité sur les stratégies filtrées et reste en début de liste. Les administrateurs ne peuvent pas réorganiser les stratégies spécifiées. • Control Manager place les ébauches de stratégies en fin de liste.
Stratégie	Indique le nom de la stratégie.
Stratégie parente	Cette colonne s'affiche uniquement si le produit sélectionné est **Agent OfficeScan**. Si une stratégie est une stratégie enfant (autrement dit, elle a hérité ses paramètres d'une stratégie parente), cette colonne affiche le nom de la stratégie parente. Dans le cas contraire, N/A s'affiche.
Écarts	Cette colonne s'affiche uniquement si le produit sélectionné est **Agent OfficeScan**. Si une stratégie est une stratégie enfant, cette colonne affiche le nombre de paramètres qui ont été modifiés sur la stratégie et qui, par conséquent, sont incohérents avec les paramètres de la stratégie parente. Si les paramètres sont cohérents entre la stratégie et son parent, 0 (zéro) s'affiche. Si une stratégie n'est pas une stratégie enfant, N/A s'affiche.

COLONNE	DESCRIPTION
Cibles	Indique comment les administrateurs sélectionnent les cibles de la stratégie. • **Spécifié** : utilise la fonction parcourir ou rechercher pour sélectionner les cibles spécifiques de la stratégie. Les stratégies spécifiées restent statiques au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées. • **Filtrés** : utilise un filtre pour affecter automatiquement des endpoints actuels et futurs à la stratégie. Les administrateurs peuvent réorganiser la priorité des stratégies filtrées. Survolez un élément à l'aide du curseur pour afficher facilement les critères de filtre et effectuer des modifications, si nécessaire. • **Aucune** : le créateur de la stratégie a sauvegardé la stratégie en tant qu'ébauche sans choisir de cible.
Déployé	Affiche le nombre de cibles qui ont appliqué les paramètres de la stratégie ou qui possèdent des services produit non activés. Cliquez sur le nombre pour afficher l'état de la stratégie.
En attente	Affiche le nombre de cibles qui ne respectent pas les paramètres de la stratégie **Remarque** Si le correctif 2575 n'est pas installé, la colonne **En attente** inclut le nombre de cibles qui possèdent des agents hors ligne. Cliquez sur le nombre pour afficher l'état de la stratégie.

COLONNE	DESCRIPTION
Hors ligne	Affiche le nombre de cibles qui possèdent des agents hors ligne **Important** Cette fonction nécessite l'installation du correctif 2575. Sinon, la colonne **En attente** inclut le nombre de cibles qui possèdent des agents hors ligne et la colonne **Hors-ligne** ne s'affiche pas. Cliquez sur le nombre pour afficher l'état de la stratégie.
Avec problèmes	Affiche le nombre de cibles qui n'ont pas appliqué les paramètres de la stratégie pour les raisons suivantes : déploiement de la stratégie non pris en charge, stratégie non configurée, erreurs système, erreurs de communication de l'endpoint avec le serveur du produit, endpoints non pris en charge, paramètres modifiés en local, services des produits désactivés ou déploiement partiel. Cliquez sur le nombre pour afficher l'état de la stratégie.
Propriétaire	Affiche l'utilisateur auquel la stratégie est actuellement affectée. **Remarque** Le propriétaire par défaut est l'utilisateur qui a créé la stratégie. • Si vous redéfinissez le propriétaire d'une stratégie sur un compte utilisateur qui ne dispose pas des droits d'accès aux cibles spécifiées, le nouveau propriétaire pourra modifier les paramètres de stratégie mais ne pourra pas afficher les données de stratégie. • Vous pouvez également attribuer plusieurs propriétaires en affectant la stratégie à un groupe Active Directory. Pour plus d'informations, consultez la section *Modification du propriétaire de la stratégie à la page 2-20*.
Dernier éditeur	Affiche le dernier utilisateur ayant modifié la stratégie.

Remarque

Les nombres qui apparaissent dans les colonnes **Déployé** et **En attente** ne représentent que les endpoints ou les produits gérés qu'un administrateur a le droit de gérer.

Réorganisation de la liste des stratégies

Les administrateurs peuvent utiliser le bouton **Réorganiser** pour modifier l'ordre des stratégies filtrées. La réorganisation de la liste des stratégies peut affecter l'allocation de la cible. Control Manager peut réaffecter des cibles à des stratégies filtrées différentes.

Remarque

- Les stratégies spécifiées restent statiques et ont toujours la priorité sur les stratégies filtrées.
- Cette fonction n'est disponible que pour la gestion des paramètres OfficeScan.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

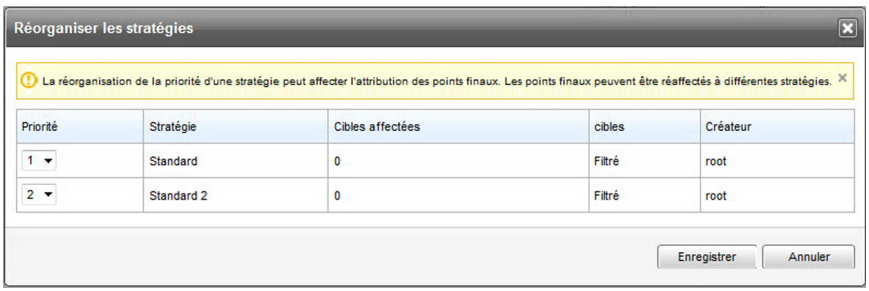
   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur **Réorganiser**.

   L'écran **Réorganiser les stratégies** apparaît.



4. Réorganisez l'ordre de la colonne **Priorité**.
5. Cliquez sur **Enregistrer**.

Remarque

Après avoir cliqué sur **Enregistrer**, veuillez attendre deux minutes pour que Control Manager puisse réaffecter les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.

Mise à jour des modèles de stratégie

L'écran **Paramètres de modèle de stratégie** liste les composants suivants disponibles pour l'activation ou la mise à niveau par les administrateurs :

- Structure de gestion des stratégies : La structure globale de la stratégie
- Assistance produit : Les modèles définis pour les produits gérés et les endpoints

Remarque

Pour vérifier les versions du produit qui prennent en charge la gestion des stratégies, déplacez le curseur de la souris sur l'icône d'information dans la colonne **Version du modèle**.

Procédure

1. Téléchargez la dernière version du composant **Pool de widgets de Control Manager et modèles de stratégie (Control Manager 6.0 et version ultérieure)**.

   Une notification en bleu apparaîtra en haut des écrans **Tableau de bord** et **Gestion des stratégies**.

2. Cliquez sur **Mettre à jour maintenant** dans la boîte de dialogue de notification sur chacun de ces écrans.
3. Cliquez sur **OK** quand la mise à jour est terminée.

   La fenêtre s'actualise et l'écran de connexion s'affiche.

4. Connectez-vous à la console Web.

5. Accédez à **Stratégies** > **Ressources de stratégies** > **Paramètres de modèle de stratégie**.

   L'écran **Paramètres de modèle de stratégie** apparaît.

6. Cliquez sur **Mise à jour <numéro de version>** dans la ligne de la structure de la stratégie.

7. Pour ajouter un nouveau modèle de stratégie, cliquez sur **Activer** dans la colonne **Action**.

   Les administrateurs peuvent alors sélectionner les nouveaux modèles définis dans la liste **Produits** de l'écran **Gestion des stratégies**.

8. Pour mettre à jour un modèle existant, cliquez sur **Mise à jour <numéro de version>** dans la colonne **Action**.

   Remarque

   Pour obtenir plus d'informations sur la mise à jour, cliquez sur **Détails** dans la colonne **Action**.

   Une fois la mise à jour terminée, les administrateurs peuvent vérifier les fonctionnalités mises à jour en modifiant les stratégies existantes. Dans la section **Paramètres**, un message en rouge apparaît à côté du titre de la nouvelle fonctionnalité.

Prévention contre la perte de données

La prévention contre la perte de données (DLP) protège les données sensibles et confidentielles d'une entreprise – appelées actifs numériques – contre les fuites de données délibérées ou accidentelles. DLP vous permet :

- d'identifier l'actif numérique à protéger ;

- de créer des stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes ;
- de renforcer la conformité à des normes de confidentialité établies.

DLP évalue les données par rapport à un ensemble de règles définies dans les stratégies. Les stratégies déterminent les données devant être protégées des transmissions non autorisées et l'action que DLP doit effectuer lorsqu'il détecte une transmission.

Types d'identificateur de données

Les actifs numériques sont des fichiers et des données qu'une entreprise doit protéger contre les transmissions non autorisées. Les administrateurs peuvent définir les actifs numériques à l'aide des identificateurs de données suivants :

- **Expressions :** données structurées.

  Pour obtenir des informations détaillées, consultez la section *Expressions à la page 2-28*.

- **Attributs de fichier :** propriétés d'un fichier, telles le type ou la taille.

  Pour obtenir des informations détaillées, consultez la section *Attributs de fichier à la page 2-34*.

- **Listes de mots-clés :** liste de mots ou d'expressions spécifiques.

  Pour obtenir des informations détaillées, consultez la section *Mots-clés à la page 2-36*.

Remarque

Les administrateurs ne peuvent pas supprimer un identificateur de données utilisé par un modèle DLP. Supprimez le modèle pour pouvoir supprimer l'identificateur de données.

Expressions

Une expression est constituée de données ayant une certaine structure. Par exemple, une carte de crédit possède généralement un numéro à 16 chiffres, présenté sous le format

« nnnn-nnnn-nnnn-nnnn », pouvant être localisé lors d'une détection basée sur les expressions.

Les administrateurs peuvent utiliser des expressions prédéfinies et personnalisées.

Pour obtenir des informations détaillées, voir *Expressions prédéfinies à la page 2-29* et *Expressions personnalisées à la page 2-30*.

Expressions prédéfinies

La prévention contre la perte de données est fournie avec un ensemble d'expressions prédéfinies. Ces expressions ne peuvent pas être modifiées ou supprimées.

La prévention contre la perte de données vérifie ces expressions au moyen du processus de vérification de la correspondance des fichiers de signatures et d'équations mathématiques. Lorsque la prévention contre la perte de données fait correspondre des données potentiellement sensibles avec une expression, les données peuvent également être soumises à des vérifications supplémentaires.

Pour obtenir la liste complète des expressions prédéfinies, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Affichage des paramètres des expressions prédéfinies

Remarque

Les expressions prédéfinies ne peuvent pas être modifiées ou supprimées.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur le nom de l'expression.
4. Consultez les paramètres sur l'écran qui s'affiche.

Expressions personnalisées

Si aucune des expressions prédéfinies ne correspond à vos besoins, vous pouvez créer des expressions personnalisées.

Les expressions constituent un outil puissant de correspondance de chaînes. Vous devez maîtriser la syntaxe pour créer des expressions. Les expressions mal formulées peuvent avoir un impact conséquent sur les performances.

Lorsque vous créez des expressions :

- Reportez-vous aux expressions prédéfinies pour savoir comment définir une expression valide. Par exemple, si vous créez une expression qui comprend une date, vous pouvez vous référer aux expressions précédées de « Date ».
- Remarque : la prévention contre la perte de données respecte les formats d'expression définis dans la bibliothèque Perl Compatible Regular Expressions (PCRE). Pour plus d'informations sur PCRE, visitez le site Web suivant :

  http://www.pcre.org/
- Commencez par des expressions simples. Modifiez les expressions si celles-ci déclenchent de fausses alertes, ou ajustez-les pour améliorer les détections.

Les administrateurs peuvent faire leur choix parmi plusieurs critères lors de la création d'expressions. Une expression doit correspondre aux critères que vous avez choisis pour que la prévention contre la perte de données puisse la soumettre à une stratégie DLP. Pour plus de détails sur les différentes actions, reportez-vous à *Critères applicables aux expressions personnalisées à la page 2-30*.

Critères applicables aux expressions personnalisées

TABLEAU 2-3. Options de critères pour des expressions personnalisées

CRITÈRES	RÈGLE	EXEMPLE
Aucune	Aucun	Tous - Noms du Bureau du recensement des États-Unis • Expression : [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

Critères	Règle	Exemple
Caractères spécifiques	Une expression doit intégrer les caractères que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	États-Unis - Numéro de routage ABA • Expression : [^\d]([0123678]\d{8})[^\d] • Caractères : 0123456789 • Nombre minimal de caractères : 9 • Nombre maximal de caractères : 9
Suffixe	Le suffixe correspond au dernier segment d'une expression. Un suffixe doit compter un certain nombre de caractères et inclure ceux que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	Tous - Adresse de domicile • Expression : \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] • Caractères de suffixe : 0123456789- • Nombre de caractères : 5 • Nombre minimal de caractères dans l'expression : 25 • Nombre maximal de caractères dans l'expression : 80

CRITÈRES	RÈGLE	EXEMPLE
Un seul caractère de séparation	Une expression doit comporter deux segments séparés par un caractère. Le caractère doit avoir une longueur d'un octet. De plus, le nombre de caractères situés à gauche du séparateur doit être compris dans les limites minimale et maximale définies. Le nombre de caractères situés à droite ne doit pas dépasser la limite maximale.	Tous - Adresse électronique • Expression : [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Séparateur : @ • Nombre minimal de caractères à gauche : 3 • Nombre maximal de caractères à gauche : 15 • Nombre maximal de caractères à droite : 30

Création d'une expression personnalisée

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Entrez un nom pour l'expression. Le nom ne doit pas dépasser 100 octets et ne peut pas contenir les caractères suivants :

   • > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets.
6. Saisissez les données affichées.

   Par exemple, si vous créez une expression pour des numéros ID, saisissez un exemple de numéro ID. Ces données sont utilisées à des fins de référence uniquement et ne figureront pas sur le produit.

7. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère (voir *Critères applicables aux expressions personnalisées à la page 2-30*) :

   - Aucun
   - Caractères spécifiques
   - Suffixe
   - Un seul caractère de séparation

8. Testez l'expression avec des données réelles.

   Par exemple, si l'expression s'applique à un ID national, entrez un numéro ID valide dans la zone de texte **Données de test**, cliquez sur **Tester**, puis vérifiez le résultat.

9. Cliquez sur **Enregistrer** si vous êtes satisfait du résultat.

Remarque

Enregistrez les paramètres uniquement si le test a réussi. Une expression qui ne détecte aucune donnée consomme les ressources du système inutilement et peut avoir une influence négative sur les performances.

Importation d'expressions personnalisées

Si le formatage du fichier `.dat` contenant les expressions est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les expressions à partir du serveur actif ou à partir de tout autre serveur.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les expressions.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une expression à importer existe déjà, elle sera ignorée.

Attributs de fichier

Les attributs de fichier sont des propriétés spécifiques à un fichier. Vous pouvez utiliser deux attributs de fichier lorsque vous définissez des identificateurs de données, à savoir le type de fichier et la taille de fichier. Par exemple, une entreprise de développement de logiciels souhaitera peut-être partager le programme d'installation de son logiciel uniquement avec les membres du service de Recherche & Développement, lesquels sont chargés de développer et tester le logiciel. Dans ce cas, l'administrateur du Control Manager peut créer une stratégie qui bloque la transmission des fichiers exécutables de 10 à 40 Mo vers l'ensemble des services, à l'exception de celui de Recherche & Développement.

Les attributs de fichier ne permettent pas, en tant que tels, d'identifier les fichiers sensibles. Dans l'exemple ci-dessus, les programmes d'installation tiers partagés par d'autres services seront probablement bloqués. Trend Micro recommande donc de combiner des attributs de fichier à d'autres identificateurs de données DLP pour une détection plus ciblée des fichiers sensibles.

Pour obtenir la liste complète des types de fichiers pris en charge, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Création d'une liste d'attributs de fichier

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **attribut de fichier**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

4. Saisissez un nom pour la liste d'attributs de fichier. Le nom ne doit pas dépasser 100 octets et ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

5. Saisissez une description ne dépassant pas 256 octets.

6. Sélectionnez vos véritables types de fichiers favoris.

7. Si un type de fichier que vous souhaitez inclure n'est pas répertorié, sélectionnez **Extensions de fichier** et entrez l'extension du type de fichier. La prévention contre la perte de données vérifie les fichiers contenant l'extension spécifiée mais pas le véritable type de fichier. Directives à suivre lorsque vous saisissez des extensions de fichiers :

   - Chaque extension doit commencer par un astérisque (*), suivi d'un point (.) et ensuite de l'extension. L'astérisque est un caractère générique qui représente un nom réel de fichier. Par exemple, `*.pol` correspond à `12345.pol` et `test.pol`.

   - Vous pouvez inclure des caractères génériques dans les extensions. Utilisez un point d'interrogation (?) pour représenter un seul caractère et un astérisque (*) pour deux caractères ou plus. Voir les exemples suivants :

     - `*.*m` correspond aux fichiers suivants : `ABC.dem`, `ABC.prm` et `ABC.sdcm`

     - `*.m*r` correspond aux fichiers suivants : `ABC.mgdr`, `ABC.mtp2r` et `ABC.mdmr`

     - `*.fm?` correspond aux fichiers suivants : `ABC.fme`, `ABC.fml` et `ABC.fmp`

   - Faites attention si vous utilisez un astérisque à la fin d'une extension car il peut correspondre à des parties de noms de fichiers et à une extension sans rapport. Par exemple : `*.do*` correspond à `abc.doctor_john.jpg` et `abc.donor12.pdf`.

   - Utilisez les points-virgules (;) pour séparer les extensions de fichier. Il n'est pas nécessaire d'ajouter un espace après un point-virgule.

8. Entrez les tailles de fichier minimale et maximale en octets. Les valeurs doivent être des entiers non nuls.

9. Cliquez sur **Enregistrer**.

Importation d'une liste d'attributs de fichier

Utilisez cette option si vous disposez d'un fichier `.dat` correctement mis en forme qui contient les listes des attributs de fichier. Pour générer le fichier, vous pouvez exporter les listes d'attributs de fichier à partir du serveur actif ou à partir de tout autre serveur.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **attribut de fichier**.
3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les listes des attributs de fichier.
4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste d'attributs de fichier à importer existe déjà, elle sera ignorée.

Mots-clés

Les mots-clés sont des expressions ou des mots spéciaux. Vous pouvez ajouter des mots-clés de la même famille à une liste de mots-clés afin d'identifier un certain nombre de données spécifiques. Par exemple, «pronostic», «groupe sanguin», «vaccination» et «médecin» sont des mots-clés pouvant apparaître dans un certificat médical. Si vous souhaitez éviter la transmission de fichiers contenant des certificats médicaux, vous pouvez utiliser ces mots-clés dans une stratégie DLP, puis configurer la prévention contre la perte de données pour qu'elle bloque les fichiers contenant ces mots-clés.

Les mots habituellement utilisés peuvent être associés afin de former des mots-clés significatifs. Par exemple, «end», «read», «if» et «at» peuvent être associés pour former des mots-clés présents dans du code source, tels que «END-IF», «END-READ» et «AT END».

Vous pouvez utiliser des listes de mots-clés prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Listes de mots-clés prédéfinies à la page 2-37* et *Listes de mots-clés personnalisées à la page 2-38*.

Listes de mots-clés prédéfinies

La prévention contre la perte de données est fournie avec un ensemble de listes de mots-clés prédéfinies. Ces listes de mots-clés ne peuvent pas être modifiées ou supprimées. Chaque liste dispose de ses propres conditions intégrées qui déterminent si le modèle doit déclencher une violation de stratégie.

Pour plus d'informations sur les listes de mots-clés prédéfinies dans la prévention contre la perte de données, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Fonctionnement des listes de mots-clés

Condition de nombre de mots-clés

Chaque liste de mots-clés contient une condition qui requiert qu'un certain nombre de mots-clés existe dans un document avant que la liste ne déclenche une violation.

La condition du nombre de mots-clés contient les valeurs suivantes :

- **Tous** : tous les mots-clés de la liste doivent exister dans le document.
- **N'importe lequel** : un des mots-clés de la liste doit exister dans le document.
- **Nombre spécifique** : le document doit comporter au moins le nombre spécifié de mots-clés. S'il y a plus de mots-clés dans le document que le nombre spécifié, la prévention contre la perte de données déclenche une violation.

Condition de distance

Certaines des listes contiennent une condition de « distance » pour savoir si une violation est présente. « Distance » se réfère au nombre de caractères existant entre le premier caractère d'un mot clé et le premier caractère d'un autre mot-clé. L'entrée suivante peut servir d'exemple :

F**irst Name:_John_ L**ast Name:_Smith_

La liste des **Formulaires - Prénom, nom** comporte une condition de « distance » de cinquante (50) et les champs de formulaire couramment utilisés de « Prénom » et « Nom ». Dans l'exemple ci-dessus, la prévention contre la perte de données déclenche une violation car le nombre de caractères entre le « F » de « First Name » et le « L » de « Last Name » est égal à dix-huit (18).

Voici un exemple d'entrée qui ne déclenche pas de violation :

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

Dans cet exemple, le nombre de caractères entre le « f » de « first name » et le « l » de « last name » est soixante et un (61). Cela dépasse le seuil de distance et ne déclenche pas de violation.

Listes de mots-clés personnalisées

Si aucune des listes de mots-clés prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Lors de la configuration d'une liste de mots-clés, plusieurs critères sont à votre disposition. Une liste de mots-clés doit correspondre aux critères que vous avez choisis avant que la prévention contre la perte de données ne puisse la soumettre à une stratégie. Pour chaque liste de mots-clés, choisissez l'un des critères suivants :

- **N'importe quel mot-clé**
- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

Pour plus d'informations concernant les règles de critères, voir *Critères des listes personnalisées de mots-clés à la page 2-39*.

Critères des listes personnalisées de mots-clés

TABLEAU 2-4. Critères pour une liste de mots-clés

CRITÈRES	RÈGLE
N'importe quel mot-clé	Un fichier doit contenir au moins un mot-clé de la liste.
Tous les mots-clés	Le fichier doit contenir tous les mots-clés de la liste.
Tous les mots-clés de <x> caractères maximum	Le fichier doit contenir tous les mots-clés de la liste. En outre, chaque paire de mots-clés ne doit pas différer de plus de <x> caractères l'une par rapport à l'autre. Par exemple, vos trois mots-clés sont DISK, WEB et USB, et le nombre de caractères spécifiés est 20. Si la fonctionnalité de prévention contre la perte de données détecte les mots-clés dans l'ordre DISK, WEB et USB, le nombre de caractères compris du « D » de DISK au « W » de Web et du « W » au « U » de USB doit être de 20 caractères au maximum. Les données suivantes correspondent aux critères : DISK####WEB############USB Les données suivantes ne correspondent pas aux critères : DISK******************WEB****USB (23 caractères entre « D » et « W ») Lorsque vous déterminez le nombre de caractères, gardez à l'esprit qu'un petit nombre, comme 10, permet généralement un scan plus rapide, mais couvre uniquement une zone relativement restreinte. La plage de détection des données sensibles risque donc d'être limitée, en particulier pour les fichiers volumineux. Plus le nombre est grand, plus la zone couverte est importante et plus la durée du scan est longue.

CRITÈRES	RÈGLE
Le score combiné des mots-clés dépasse le seuil	Un fichier doit contenir un ou plusieurs mots-clés de la liste. Si un seul mot-clé est détecté, son score doit être supérieur au seuil défini. Si plusieurs mots-clés sont détectés, leur score combiné doit être supérieur au seuil défini. Attribuez à chaque mot-clé un score de 1 à 10. Un terme ou une phrase à haute confidentialité, comme « augmentation des salaires » pour le département des ressources humaines, doit avoir un score relativement élevé. Les termes ou les phrases qui, en elles-mêmes, n'ont pas de poids significatif peuvent avoir des scores plus faibles. Pensez aux scores que vous avez attribués aux mots-clés lorsque vous configurez le seuil. Par exemple, si vous avez cinq mots-clés, dont trois avec une priorité élevée, le seuil peut être égal ou inférieur au score combiné des trois mots-clés à priorité élevée. Cela signifie que la détection de ces trois mots-clés est suffisante pour classer le fichier comme étant sensible.

Création d'une liste de mots-clés

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Entrez un nom pour la liste de mots-clés. Le nom ne doit pas dépasser 100 octets et ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets.
6. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère :

- **N'importe quel mot-clé**
- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

7. Pour ajouter manuellement des mots-clés à la liste :

a. Saisissez un mot-clé d'une longueur de 3 à 40 octets et indiquez s'il respecte la casse.

b. Cliquez sur **Ajouter**.

8. Pour ajouter des mots-clés à l'aide de l'option d'« importation » :

Remarque

Si le formatage du fichier `.csv` contenant les mots-clés est approprié, utilisez cette option. Pour générer le fichier, vous pouvez exporter les mots-clés à partir du serveur actif ou à partir de tout autre serveur.

---

a. Cliquez sur **Importer** et identifiez le fichier `.csv` contenant les mots-clés.

b. Cliquez sur **Ouvrir**.

Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un mot-clé à importer existe déjà dans la liste, il sera ignoré.

9. Pour supprimer des mots-clés, sélectionnez-les puis cliquez sur **Supprimer**.

10. Pour exporter des mots-clés :

Remarque

Utilisez la fonctionnalité « exporter » pour sauvegarder les mots-clés ou les importer sur un autre serveur. Tous les mots-clés de la liste seront exportés. Il n'est pas possible d'exporter un mot-clé individuel.

---

a. Cliquez sur **Exporter**.

b. Enregistrez le fichier `.csv` obtenu à l'emplacement de votre choix.

11. Cliquez sur **Enregistrer**.

Importation d'une liste de mots-clés

Utilisez cette option si vous disposez d'un fichier `.dat` correctement mis en forme qui contient les listes des mots-clés. Pour générer le fichier, vous pouvez exporter les listes de mots-clés à partir du serveur actif ou à partir de tout autre serveur.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Identifiants de données de prévention contre la perte de données**.
2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Importer** et identifiez le fichier `.dat` contenant les listes des mots-clés.
4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste de mots-clés à importer existe déjà, elle sera ignorée.

Modèles de prévention contre la perte de données

Un modèle DLP réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une stratégie de prévention contre la perte des données.

Par exemple, un fichier doit être un fichier Microsoft Word (attribut de fichier) ET doit contenir certains termes légaux (mots-clés) ET doit contenir des numéros d'identification (expressions) afin de devenir une stratégie de « Contrats de travail ». Cette stratégie autorise le personnel des Ressources humaines à imprimer le fichier afin que cette copie soit signée par un employé. La transmission par le biais de tous les autres canaux possibles, tels que le courrier électronique, est bloquée.

Vous pouvez créer vos propres modèles si vous avez configuré des identificateurs de données. Vous pouvez également utiliser des modèles prédéfinis. Pour obtenir des informations détaillées, voir *Modèles DLP personnalisés à la page 2-43* et *Modèles DLP prédéfinis à la page 2-43*.

Remarque

Il n'est pas possible de supprimer un modèle utilisé dans une stratégie de prévention contre la perte des données. Supprimez le modèle de la stratégie pour pouvoir la supprimer.

Modèles DLP prédéfinis

La prévention contre la perte de données est fournie avec un ensemble de modèles prédéfinis que vous pouvez utiliser afin de répondre à diverses normes de contrôle. Ces modèles ne peuvent pas être modifiés ou supprimés.

- **GLBA** : loi Gramm-Leach-Billey Act
- **HIPAA** : loi Health Insurance Portability and Accountability Act
- **PCI-DSS** : standard de sécurité de données pour les industries de carte de paiement
- **SB-1386** : loi n°1386 du Sénat américain
- **US PII** : données d'identification personnelles des États-Unis

Pour obtenir une liste détaillée de tous les modèles prédéfinis, avec des exemples de données sous protection, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Modèles DLP personnalisés

Créez vos propres modèles si vous avez configuré les identificateurs de données. Un modèle réunit des identificateurs de données et des opérateurs logiques (Et, Ou, Sauf) pour former des déclarations de condition.

Pour plus d'informations et d'exemples sur le fonctionnement des déclarations de condition et des opérateurs logiques, voir *Conditions et opérateurs logiques à la page 2-44*.

Conditions et opérateurs logiques

La prévention contre la perte de données évalue les déclarations de condition de gauche à droite. Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus.

Reportez-vous aux exemples dans le tableau ci-dessous.

TABLEAU 2-5. Exemples de conditions

CONDITION	INTERPRÉTATION ET EXEMPLE
[Identificateur de données 1] **et** [Identificateur de données 2] **sauf** [Identificateur de données 3]	Un fichier doit satisfaire [Identificateur de données 1] et [Identificateur de données 2], mais pas [Identificateur de données 3]. Par exemple : Un fichier doit être [au format Adobe PDF] et doit contenir [une adresse e-mail], mais ne doit pas contenir [tous les mots-clés de la liste].
[Identificateur de données 1] **ou** [Identificateur de données 2]	Un fichier doit safisfaire [Identificateur de données 1] ou [Identificateur de données 2]. Par exemple : Un fichier doit être [un document Adobe PDF] ou [un document Microsoft Word].
Sauf [Identificateur de données 1]	Un fichier ne doit pas satisfaire [Identificateur de données 1]. Par exemple : Un fichier ne doit pas être [un fichier multimédia].

Comme illustré dans le dernier exemple du tableau, le premier identificateur de données de la déclaration de condition peut être associé à l'opérateur « sauf » si un fichier ne

satisfait pas tous les identificateurs de données dans la décalaration. Cependant, dans la plupart des cas, le premier identificateur de données ne comporte pas d'opérateur.

Création d'un modèle

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Modèles de prévention contre la perte de données**.
2. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
3. Entrez un nom pour le modèle. Le nom ne doit pas dépasser 100 octets et ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
4. Saisissez une description ne dépassant pas 256 octets.
5. Sélectionnez des identificateurs de données puis cliquez sur l'icône « Ajouter ».

   Lorsque vous sélectionnez des définitions :

   - Sélectionnez plusieurs entrées en appuyant et en maintenant la touche CTRL, puis en sélectionnant les identificateurs de données.
   - Si vous recherchez une définition spécifique, utilisez la fonction de recherche. Vous pouvez saisir le nom complet ou partiel de l'identitificateur de données.
   - Chaque modèle peut contenir au maximum 30 identificateurs de données.
6. Pour créer une nouvelle expression, cliquez sur **expressions** puis sur **Ajouter une nouvelle expression**. Dans l'écran qui s'affiche, configurez les paramètres de l'expression.
7. Pour créer une nouvelle liste d'attributs, cliquez sur **attributs de fichier** puis sur **Ajouter un nouvel attribut de fichier**. Dans l'écran qui s'affiche, configurez les paramètres de la liste d'attributs de fichier.

8. Pour créer une nouvelle liste de mots-clés, cliquez sur **Mots-clés** puis sur **Ajouter un nouveau mot-clé**. Dans l'écran qui s'affiche, configurez les paramètres de la liste de mots-clés.

9. Si vous avez sélectionné une expression, saisissez le nombre d'occurrences, c'est-à-dire le nombre de fois qu'une expression doit se produire avant que la prévention contre la perte de données ne la soumette à une stratégie.

10. Choisissez un opérateur logique pour chaque définition.

Remarque

Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus. Pour des exemples d'utilisation correcte, voir *Conditions et opérateurs logiques à la page 2-44*.

11. Pour supprimer un identificateur de données de la liste d'identificateurs sélectionnés, cliquez sur l'icône « corbeille ».

12. Sous **Aperçu**, vérifiez la condition et effectuez des changements s'il ne s'agit pas de la condition souhaitée.

13. Cliquez sur **Enregistrer**.

Importation de modèles

Utilisez cette option si vous disposez d'un fichier `.dat`correctement formaté comprenant les modèles. Pour générer le fichier, vous pouvez exporter les modèles à partir du serveur actif ou à partir de tout autre serveur.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Modèles de prévention contre la perte de données**.

2. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les modèles.

3. Cliquez sur **Ouvrir**.

Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un modèle à importer existe déjà, il sera ignoré.

État de la stratégie

L'état des stratégies permet aux administrateurs de vérifier si Control Manager a déployé une stratégie avec succès sur ses cibles.

Pour vérifier l'état de déploiement de la stratégie, utilisez une des méthodes suivantes :

- Dans l'écran **Gestion des stratégies**, cliquez sur un nombre dans la liste des stratégies. L'écran **Requête sur le journal** apparaît.
- Dans le tableau de bord, cliquez sur un nombre dans le **widget d'état des stratégies**. L'écran **Requête sur le journal** apparaît.
- Exécutez une requête sur le journal.

Le tableau suivant fournit des descriptions et des suggestions sur chaque état de stratégie :

TABLEAU 2-6. État de la stratégie

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
En attente	Control Manager exécute la stratégie.	Attendez quelques minutes, puis vérifiez à nouveau l'état.
Sans stratégie	Control Manager n'a pas affecté de stratégie à ce endpoint ou à ce produit géré.	Affectez une stratégie au endpoint ou au produit géré.
Déployé	Control Manager a déployé la stratégie avec succès.	N/A

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
Le endpoint n'arrive pas à se connecter au serveur	• Le endpoint n'a pas reçu les paramètres de la stratégie. • Le serveur est actuellement occupé.	• Vérifiez l'état de la connexion du endpoint • Connectez le endpoint au réseau de l'entreprise • Attendez que l'état de la stratégie se mette à jour
Paramètres produit inapplicables	Le produit géré ne peut pas traiter certains des paramètres de la stratégie.	• Vérifiez les paramètres de la stratégie • Mettez à jour dans la dernière version du modèle de stratégie • Vérifiez les paramètres du produit géré • Vérifiez l'adresse IP du produit géré sur l'écran **Serveurs gérés** Si l'adresse IP est incorrecte, annulez l'enregistrement puis enregistrez à nouveau le produit géré auprès de Control Manager. • Consultez le *Manuel de l'administrateur* du produit géré.
Endpoint non pris en charge	Le endpoint ne prend pas en charge certaines fonctionnalités spécifiées dans les paramètres de la stratégie.	Mettez à niveau l'agent dans une version prise en charge.

État de la stratégie	Description	Suggestions
Paramètres modifiés localement	Certains paramètres du endpoint ou du produit géré ne correspondent pas aux paramètres spécifiés dans la stratégie, car l'administrateur du produit géré a fait des modifications via la console du produit géré.	Vérifiez les paramètres dans la console du produit géré.
Services des produits inactivés	Le produit géré n'a pas activé certains des services spécifiés dans les paramètres de la stratégie.	Activez les services en question dans le produit géré.
Services des produits désactivés	Le produit géré a désactivé certains des services spécifiés dans les paramètres de la stratégie.	Activez les services en question dans le produit géré.
Partiellement déployé	Control Manager a appliqué une partie des paramètres de la stratégie.	Attendez quelques minutes, puis vérifiez à nouveau l'état.
Géré par [nom du serveur Control Manager]	Une autre instance de Control Manager gère actuellement le produit géré.	Supprimez le produit géré de la liste du serveur géré et ajoutez à nouveau le produit géré à la liste.
Nom d'utilisateur ou mot de passe non valide.	Le nom d'utilisateur ou le mot de passe d'authentification est incorrect.	Vérifiez le nom d'utilisateur et le mot de passe.
Serveur de produit ou informations d'authentification non valide	Le nom du serveur ou les informations d'authentification sont incorrectes.	Vérifiez le nom du serveur et les informations d'authentification.

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
Connexion automatique au produit impossible	Control Manager ne peut pas utiliser la fonction de connexion unique pour accéder au produit géré.	• Cliquez sur la fonction d'authentification unique dans le répertoire Produits • Vérifiez l'état de la connexion de l'agent MCP • Passez le type de connexion au serveur de **Automatique** à **Manuel** dans la liste **Serveurs gérés**.
Erreur de configuration du serveur Web	Une erreur de service Web est survenue.	Vérifiez la configuration IIS.
Erreur de communication du produit	Impossible d'accéder à la console du produit.	• Vérifiez si vous pouvez accéder à la console Web du produit géré. • Vérifiez les paramètres du produit géré.
Connexion au produit impossible	Control Manager ne parvient pas à établir une connexion avec le produit géré.	• Vérifiez l'état de la connexion du produit géré. • Vérifiez la connexion réseau
Version du produit non prise en charge	La version du produit géré n'est pas prise en charge.	Mettez à niveau le produit géré dans une version prise en charge.
Erreur de configuration du réseau	Une erreur de connexion réseau est survenue.	Vérifiez la connexion réseau.
Erreur système. ID d'erreur : [numéro ID de l'erreur].	Une erreur système est survenue.	Contactez votre représentant d'assistance Trend Micro.

Partie II

Widgets des produits Deep Discovery

Chapitre 3

Widgets des tableaux de bord de Deep Discovery Analyzer et de Deep Discovery Email Inspector

Cette section contient des rubriques d'aide concernant les widgets des tableaux de bord de Deep Discovery Analyzer et de Deep Discovery Email Inspector qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widgets Deep Discovery Analyzer à la page 3-2*
- *Widgets Deep Discovery Email Inspector à la page 3-3*

Widgets Deep Discovery Analyzer

Cette section contient des rubriques d'aide concernant tous les widgets Deep Discovery Analyzer qui sont pris en charge dans Control Manager.

Widget Résumé Virtual Analyzer

Ce widget affiche le nombre total d'échantillons envoyés à Virtual Analyzer et le nombre de ces échantillons présentant un risque. Le widget peut afficher les données provenant d'une ou plusieurs appliances Deep Discovery Analyzer. Le widget présente les données dans un tableau et un graphique circulaire associé.

ÉTIQUETTE	DESCRIPTION
Envois	Nombre total d'envois à Virtual Analyzer.
Risques identifiés	Nombre total d'envois comportant des risques identifiés.
Risque élevé	Nombre total d'envois à risque élevé.
Risque moyen	Nombre total d'envois à risque moyen.
Risque faible	Nombre total d'envois à risque faible.
% de soumissions présentant des risques	Pourcentage des envois présentant des risques.
Distribution d'événements malveillants	Graphique circulaire représentant le pourcentage de risques identifiés à risque élevé, moyen et faible.

Changez l'intervalle de temps en sélectionnant une option dans la liste déroulante **Plage** dans la partie supérieure gauche du widget.

Spécifiez si les données affichées proviennent de toutes les appliances Deep Discovery Analyzer enregistrées ou d'une appliance spécifique en sélectionnant l'option dans la liste déroulante **Afficher** dans la partie supérieure gauche du widget.

Après avoir sélectionné une appliance, affichez des informations plus détaillées en cliquant sur le nombre total de soumissions, le nombre de soumissions à risque élevé/moyen /faible ou une section du graphique circulaire.

Widgets Deep Discovery Email Inspector

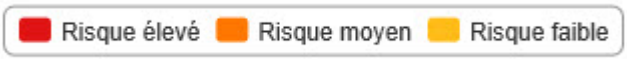
Cette section contient des rubriques d'aide concernant tous les widgets Deep Discovery Email Inspector qui sont pris en charge dans Control Manager.

Widget E-mails contenant des menaces avancées

Le widget **E-mails contenant des menaces avancées** affiche tous les messages électroniques présentant des caractéristiques malveillantes ou suspectes qui ont été détectés par Deep Discovery Email Inspector. Les caractéristiques suspectes incluent les comportements anormaux, les données fausses ou trompeuses, les fichiers de signatures au comportement suspect et malveillant ainsi que les chaînes de caractères indiquant une atteinte du système, mais qui nécessitent une investigation plus poussée.

Le graphique est basé sur la période sélectionnée. L'axe Y représente le nombre de messages électroniques. L'axe X représente la période. Placez la souris sur un point du graphique pour afficher le nombre de messages à risque élevé et la période.

Cliquez sur un élément dans la légende du widget pour afficher ou masquer les données associées à cette mesure.



Cliquez sur **Afficher les messages détectés** pour afficher toutes les détections.

Widget Principaux destinataires de messages électroniques contenant des menaces avancées

Le widget **Principaux destinataires de messages électroniques contenant des menaces avancées** affiche les destinataires qui ont reçu le plus grand volume de messages suspects sur Deep Discovery Email Inspector.

Le tableau présente les détections en fonction de la période sélectionnée. Cliquez sur un nombre sous **Détections** ou **Messages à risque élevé** pour plus d'informations sur les détections. La section **Détections** comprend tous les messages électroniques détectés, y compris les messages à risque élevé.

Chapitre 4

Intégration de Deep Discovery Inspector

Cette section décrit comment Deep Discovery Inspector s'intègre à Control Manager.

Les rubriques sont les suivantes:

- *Récapitulatif de l'intégration de Deep Discovery Inspector à la page 4-2*
- *Paramètres de stratégie de Deep Discovery Inspector à la page 4-10*

Récapitulatif de l'intégration de Deep Discovery Inspector

Cette rubrique présente le degré d'intégration entre Control Manager 7.0 et les versions prises en charge de Deep Discovery Inspector.

FONCTION/FONCTIONNALITÉ – INTÉGRATION	5,0
Enregistrement	Depuis la console d'administration de Deep Discovery Inspector (par le biais de l'agent MCP)
Authentification unique	Prise en charge
Gestion de la licence	Aucune
Suivi des commandes	Prise en charge
Composants déployés depuis Control Manager	Tous les composants
Stratégies gérées et déployées depuis Control Manager	• *Liste des refus/Liste des autorisations à la page 4-10* • *Ajout de groupes de réseaux surveillés à la page 4-12* • *Ajout de services enregistrés à la page 4-13* • *Configuration des paramètres de Virtual Analyzer à la page 4-15*
Informations affichées dans le répertoire des utilisateurs/endpoints	Aucune

FONCTION/FONCTIONNALITÉ – INTÉGRATION	5,0
Requête ad hoc	Sélectionnez les affichages de données suivants lors de l'exécution d'une requête ad hoc pour voir les informations sur le produit et les journaux : • Informations sur l'état du produit • Informations Deep Discovery
Widgets du tableau de bord spécifiques au produit	• *Widget État du système Deep Discovery Inspector à la page 4-7* • *Widget Hôtes affectés Deep Discovery Inspector à la page 4-4*
Widgets du tableau de bord partagés avec d'autres produits gérés	Aucune
Modèles de rapport statiques	Rapports Trend Micro Deep Discovery Inspector
Modèles de rapport personnalisés (prédéfinis)	• Résumé de gravité d''hôte TM-Deep Discovery Inspector • Résumé des détections de menaces suspectes TM-Deep Discovery Inspector

FONCTION/FONCTIONNALITÉ – INTÉGRATION	5,0
Notifications d'événements	Activité de menace avancée • Alerte de rappel C&C • Alerte d'épidémie de rappel C&C • Détections de Virtual Analyzer à risque élevé • Détections d'hôte à risque élevé • Détections de comportements connus d'attaque ciblée • Détections d'exploitation potentielle de document • Détections de rootkit ou d'outil de piratage • Détections de la liste des refus SHA-1 • Détections de propagation de ver ou de virus infectant les fichiers • Détections d'incidents corrélés
Gestion des incidents de prévention contre la perte de données (DLP)	Non applicable
Gestion des objets suspects et des fichiers IOC	• Envoie les objets suspects à Control Manager • Synchronise les objets suspects avec Control Manager

Widget Hôtes affectés Deep Discovery Inspector

Ce widget affiche des informations sur les détections de Deep Discovery Inspector trouvées sur des hôtes affectés.

Par défaut, l'affichage présente uniquement les 10 principaux hôtes à gravité élevée selon le **Nombre de détections**.

Pour indiquer au widget s'il doit afficher les hôtes selon le nombre de détections ou l'heure de la détection, cliquez sur l'icône Paramètres (>) et sélectionnez l'une des options suivantes :

- **Nombre de détections** : sélectionnez le nombre d'hôtes (10, 25 ou 50 principaux hôtes) dans la liste déroulante.
- **Heure de la détection** : sélectionnez le nombre d'hôtes (10, 25, 50 ou 100 hôtes les plus récents) dans la liste déroulante.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

- Si vous affichez les hôtes selon le **Nombre de détections**, vous pouvez afficher les données pour le jour même, une semaine, deux semaines ou un mois.
- Si vous affichez les hôtes selon l'**Heure de la détection**, vous pouvez uniquement afficher les données pour le jour même ou pour une semaine.

Vous pouvez également utiliser la liste déroulante **Gravité** pour indiquer le niveau de gravité en cas d'affichage des hôtes selon l'**Heure de la détection**.

COLONNE	DESCRIPTION
Adresse IP	Affiche l'adresse IP de l'hôte affecté
Nom d'hôte	Affiche le nom de l'hôte affecté
Groupe réseau	Affiche le nom du groupe des réseaux surveillés qui permettent à Deep Discovery Inspector de déterminer si les attaques proviennent de l'intérieur ou de l'extérieur du réseau

COLONNE	DESCRIPTION
Détections	Affiche le nombre d'événements détectés sur les hôtes affectés • Cliquez sur un nombre dans la colonne **Détections** pour afficher des informations supplémentaires dans l'écran **Détections**. • Cliquez sur le lien **Affichage** dans la colonne **Détails** pour vous connecter à Deep Discovery Inspector à l'aide de la fonction d'authentification unique et afficher l'écran **Détails de la requête de journal des détections**. Si le journal est purgé, la console affiche un message vous informant de cette action.
Détection la plus récente	Affiche la date et l'heure de la dernière détection d'un risque potentiel/connu par Deep Discovery Inspector.

Détections d'hôtes affectés Deep Discovery Inspector

Si vous cliquez sur une valeur dans la colonne **Détections** du widget Hôtes affectés Deep Discovery Inspector, un tableau contenant des informations sur l'hôte s'affiche :

TABLEAU 4-1. Informations sur l'hôte

NOM DE LA COLONNE	INFORMATIONS
Date	Date et heure auxquelles Deep Discovery Inspector a généré le journal de détection
Gravité	Descriptions du niveau de gravité : • Élevé : réputé malveillant ou impliqué dans des connexions à gravité élevée • Moyen : adresse IP/domaine/URL inconnu du service de réputation • Faible : service de réputation indiquant une atteinte précédente ou une implication dans du spam • Informationnel : objet très probablement inoffensif.

NOM DE LA COLONNE	INFORMATIONS
Détection	Description de la règle ou nom de programme malveillant
Type de menace	À choisir parmi les options suivantes : • Signatures de fichier • Comportement malveillant • Comportement suspect • Exploitation • Graywares • Web Reputation • Applications perturbatrices
Adresse IP source	Adresse IP de la source dont provient un objet suspect
Adresse IP de la destination	Adresse IP de la destination souhaitée d'un objet suspect
Protocole	Protocole utilisé pour transporter un objet suspect de la source à la destination
Nom du fichier	Nom de fichier extrait de l'échantillon
Enregistré par	Nom d'hôte de l'instance Deep Discovery Inspector qui a analysé l'échantillon
Détails	Cliquez sur **Afficher** pour lancer une autre fenêtre proposant une analyse détaillée de l'objet suspect dans Deep Discovery Inspector.

Widget État du système Deep Discovery Inspector

Utilisez ce widget pour afficher l'utilisation des ressources ainsi que le nombre d'échantillons en file d'attente qui attendent le traitement de Virtual Analyzer pour les dispositifs Deep Discovery Inspector sélectionnés.

Le widget affiche par défaut les données de tous les produits/serveurs gérés auxquels les privilèges de compte de son utilisateur donnent accès.

Cliquez sur l'icône Paramètres (>) pour configurer les options suivantes :

- **Titre** : spécifiez un nouveau titre pertinent pour le widget .
- **Portée : tous les produits** : cliquez sur le bouton **>>** pour spécifier les produits dont les données seront affichées.

Le widget affiche les données de ressources système suivantes pour vérifier que toutes les ressources de Deep Discovery Inspector sont conformes aux spécifications.

COLONNE	DESCRIPTION
Nom du serveur	Nom du serveur pour chaque appliance Deep Discovery Inspector • **Afficher l'état détaillé** : cliquez sur cette option pour afficher les détails de l'état du produit. Vous pouvez également afficher ces données par le biais de la requête ad hoc « État du produit ». Ce tableau contient le pourcentage d'utilisation du processeur, le pourcentage d'utilisation et l'utilisation réelle de la mémoire et du disque, ainsi que le nombre d'échantillons en file d'attente qui attendent le traitement de Virtual Analyzer. Pour faciliter le dépannage, reportez-vous aux champs Hôte du produit, Adresse IP du produit, État de la connexion et Version du produit. Deep Discovery Inspector envoie une mise à jour de l'état du système à Control Manager toutes les 5 minutes. Lorsque s'affiche, Control Manager ne reçoit pas les derniers journaux d'état du système Deep Discovery Inspector. Confirmez que Deep Discovery Inspector est actif et connecté. • **Console de connexion** : cliquez sur cette option pour accéder à la console d'administration de Deep Discovery Inspector. Aucune information d'identification de connexion n'est requise.

COLONNE	DESCRIPTION
Utilisation de l'UC	Pourcentage du processeur utilisé par le serveur • s'affiche lorsque l'utilisation moyenne du processeur par le serveur dépasse 80 %. **Remarque** L'utilisation du processeur, de la mémoire et du disque, ainsi que le nombre limite d'échantillons en file d'attente ne sont pas configurables. Si les alertes persistent, pensez à mettre à niveau vos dispositifs Deep Discovery Inspector/Virtual Analyzer.
Utilisation de la mémoire	Pourcentage de mémoire disponible sur le serveur • s'affiche lorsque l'utilisation de la mémoire dépasse 80 %. **Remarque** L'utilisation du processeur, de la mémoire et du disque, ainsi que le nombre limite d'échantillons en file d'attente ne sont pas configurables. Si les alertes persistent, pensez à mettre à niveau vos dispositifs Deep Discovery Inspector/Virtual Analyzer.
Utilisation du disque	Pourcentage d'espace disque disponible sur le serveur • s'affiche lorsque l'utilisation du disque dépasse 80 %. **Remarque** L'utilisation du processeur, de la mémoire et du disque, ainsi que le nombre limite d'échantillons en file d'attente ne sont pas configurables. Si les alertes persistent, pensez à mettre à niveau vos dispositifs Deep Discovery Inspector/Virtual Analyzer.

COLONNE	DESCRIPTION
Échantillons en file d'attente	Nombre d'échantillons en attente de traitement par Virtual Analyzer • s'affiche lorsque le nombre d'échantillons dans la file d'attente de Virtual Analyzer dépasse 40. **Remarque** L'utilisation du processeur, de la mémoire et du disque, ainsi que le nombre limite d'échantillons en file d'attente ne sont pas configurables. Si les alertes persistent, pensez à mettre à niveau vos dispositifs Deep Discovery Inspector/Virtual Analyzer.

Paramètres de stratégie de Deep Discovery Inspector

Cette section explique comment configurer les paramètres de stratégie de Deep Discovery Inspector sur l'écran **Créer une stratégie**.

Liste des refus/Liste des autorisations

L'écran Liste des refus/Liste des autorisations est divisé en plusieurs onglets : Liste des refus, Liste des autorisations et Importer/Exporter.

TABLEAU 4-2. Onglets Liste des refus et Liste des autorisations

ONGLET	DESCRIPTION
Liste des refus	Deep Discovery Inspector soit surveille uniquement, soit surveille et réinitialise la connexion aux entrées de la liste des refus.

ONGLET	DESCRIPTION
Liste des autorisations	Deep Discovery Inspector permet la connexion aux entrées de la liste des autorisations. **Conseil** Utilisez la liste des autorisations pour réduire le nombre de détections de faux positifs dans la liste des refus.
Importer/Exporter	Importez ou exportez les entrées de la liste des refus ou de celle des autorisations

Création d'une liste des refus personnalisée

Procédure

1. Sélectionnez l'onglet **Liste des refus**.
2. Pour ajouter une entité à la liste des refus, choisissez **Ajouter**.

   La fenêtre **Ajouter un élément à la liste des refus** s'affiche.
3. Dans la fenêtre **Ajouter un élément à la liste des refus**, révisez les informations, ajoutez des commentaires si besoin, puis cliquez sur **Enregistrer**.

Création d'une liste des autorisations personnalisée

Procédure

1. Cliquez sur l'onglet **Liste des autorisations**.
2. Pour ajouter une entité à la liste des autorisations, choisissez **Ajouter**.

   La fenêtre **Ajouter un élément à la liste des autorisations** s'affiche.

3. Dans la fenêtre **Ajouter un élément à la liste des autorisations**, révisez les informations, ajoutez des commentaires si besoin, puis cliquez sur **Enregistrer**.

Importation/Exportation des listes des refus ou des autorisations personnalisées

Procédure

1. Sélectionnez l'onglet **Importer/Exporter**.
2. Pour exporter la liste des refus ou des autorisations actuelle, sélectionnez une liste, puis cliquez sur **Exporter**.
3. Pour remplacer la liste des refus ou des autorisations actuelle par une autre, sélectionnez une liste, accédez à l'emplacement de stockage de la nouvelle liste, puis cliquez sur **Importer**.

   La liste sélectionnée est remplacée.

Ajout de groupes de réseaux surveillés

Établissez des groupes de réseaux surveillés en utilisant des adresses IP afin de permettre à Deep Discovery Inspector de déterminer si les attaques proviennent de l'intérieur ou de l'extérieur du réseau.

Procédure

1. Cliquez sur **Ajouter**.
2. Spécifiez un nom de groupe.

Conseil

Définissez des groupes spécifiques avec des noms descriptifs permettant d'identifier facilement le réseau auquel appartient l'adresse IP, tels que « Réseau finance », « Réseau informatique » ou « Administration ».

3. Spécifiez une plage d'adresses IP dans la zone de texte (jusqu'à 1 000 plages d'adresses IP).

   Deep Discovery Inspector est fourni avec un réseau surveillé portant le nom **Par défaut**, qui contient les blocs d'adresses IP suivants réservés aux réseaux privés par l'organisme IANA (Internet Assigned Numbers Authority) :

   - 10.0.0.0-10.255.255.255
   - 172.16.0.0-172.31.255.255
   - 192.168.0.0-192.168.255.255

   Remarque

   - Si vous n'avez pas supprimé le réseau **Par défaut**, vous n'avez pas besoin de spécifier ces blocs d'adresses IP lorsque vous ajoutez un nouveau réseau surveillé.
   - Utilisez un tiret pour spécifier une plage d'adresses IP.

     Exemple : 192.168.1.0-192.168.1.255.
   - Utilisez une barre oblique pour spécifier le masque de sous-réseau des adresses IP.

     Exemple : 192.168.1.0/255.255.255.0 ou 192.168.1.0/24.
   - Il est possible d'ajouter jusqu'à trois couches de sous-groupes.

4. Sélectionnez la zone réseau du groupe de réseaux :
   - **Sécurisé** indique qu'il s'agit d'un réseau sûr.
   - **Non sécurisé** indique qu'il existe des doutes quant à la sécurité du réseau.
5. Cliquez sur **Ajouter**.
6. Cliquez sur **Terminer**.

Ajout de services enregistrés

Ajoutez des serveurs différents pour les services spécifiques que votre entreprise utilise en interne ou juge dignes de confiance pour établir le profil réseau. L'identification des

services approuvés sur le réseau permet la détection des applications et des services non autorisés.

Ajoutez uniquement des services approuvés (jusqu'à 1 000 services) afin d'assurer l'exactitude de votre profil réseau.

Procédure

1. Sélectionnez un service dans la liste déroulante.

TABLEAU 4-3. Types de services

SERVICE	DESCRIPTION
DNS	Serveur réseau utilisé en tant que serveur DNS.
FTP	Serveur réseau utilisé en tant que serveur FTP.
Proxy HTTP	Serveur réseau utilisé en tant que serveur proxy HTTP.
SMTP	Serveur réseau utilisé en tant que serveur SMTP.
Relais ouvert SMTP	Serveur réseau utilisé en tant que serveur SMTP de relais ouvert.
Serveur de mise à jour logicielle	Serveur réseau responsable de Windows Server Update Services (WSUS) ou serveur réalisant le déploiement à distance.
Serveur d'audit de sécurité	Serveur réseau utilisé pour détecter à la fois les failles de sécurité et les configurations non sécurisées.
Active Directory	Serveur réseau utilisé en tant que serveur Active Directory.
Contrôleur de domaine	Serveur réseau utilisé en tant que serveur contrôleur de domaine.

SERVICE	DESCRIPTION
Serveur de base de données	Serveur réseau utilisé en tant que serveur de base de données.
Serveurs d'authentification – Kerberos	Serveur réseau utilisé pour permettre l'authentification Kerberos.
Serveur de fichiers	Serveur réseau utilisé pour fournir un emplacement d'accès aux fichiers partagés.
Serveur Web	Serveur réseau utilisé en tant que serveur Web.
Serveur d'administration du contenu	Serveur réseau utilisé pour la gestion du contenu.
Serveur Radius	Serveur réseau utilisé en tant que serveur d'authentification RADIUS.

Les noms des services enregistrés s'affichent dans la section **Services enregistrés définis**.

2. Spécifiez un nom de serveur.
3. Spécifiez une adresse IP.
4. Cliquez sur **Ajouter**.

Configuration des paramètres de Virtual Analyzer

Utilisez cette option pour activer ou désactiver l'analyse des fichiers de menaces.

Procédure

1. Assurez-vous que le port de gestion peut accéder à Internet. Il se peut que Virtual Analyzer ait besoin d'interroger les données via ce port.
2. Dans la fenêtre **Configuration de Virtual Analyzer**, cochez la case **Envoyer des fichiers à l'analyseur virtuel**.

3. Sélectionnez un module d'analyse.

   - Pour **Analyseur interne**, sélectionnez un type de réseau.

TABLEAU 4-4. Types de réseaux d'analyseur

OPTION DE MODULE	DESCRIPTION
Réseau de gestion	Sélectionnez ce type de réseau pour diriger le trafic de Virtual Analyzer via un port de gestion.
Réseau personnalisé/réseau spécifié	Sélectionnez ce type de réseau pour configurer un port spécifique pour le trafic de Virtual Analyzer. Assurez-vous que le port est en mesure de se connecter directement à un réseau externe.
Aucun réseau/réseau isolé	Sélectionnez ce type de réseau pour isoler le trafic de Virtual Analyzer au sein de Virtual Analyzer et lorsque l'environnement ne dispose d'aucune connexion à un réseau externe.

TABLEAU 4-5. Options de réseau personnalisé/réseau spécifié

OPTION	ACTION
Port Virtual Analyzer	Sélectionnez un port Virtual Analyzer. **Remarque** Attribuez un port Virtual Analyzer différent du port de données Deep Discovery Inspector.
Configurer IPv4	**Automatiquement (avec DHCP)** est sélectionné. Ce paramètre ne peut pas être modifié.

- Pour **Analyseur externe**, indiquez une adresse IP et une clé API Virtual Analyzer.

Conseil

L'analyseur externe (Deep Discovery Advisor ou Deep Discovery Analyzer) offre davantage de fonctions d'analyse que l'analyseur interne (Virtual Analyzer).

4. (Facultatif) Pour l'analyseur interne Virtual Analyzer, activez et configurez un proxy dédié.

Remarque

Pour configurer les paramètres proxy, le type de réseau sélectionné doit être le réseau de gestion ou le réseau personnalisé.

a. Dans **Paramètres proxy**, sélectionnez **Utiliser des paramètres de proxy dédiés**.

b. Dans **Adresse du serveur**, saisissez l'adresse IP, le nom d'hôte ou le nom de domaine complet du serveur proxy.

c. Indiquez le numéro du port.

d. (Facultatif) Saisissez les informations d'authentification du serveur proxy.

5. (Facultatif) Pour l'analyseur interne Virtual Analyzer, sélectionnez **Envoyer les menaces Mac OS possibles aux bacs à sable en ligne de Trend Micro pour analyse**.

6. Configurez les options d'**envoi du fichier** :

a. Indiquez la taille maximale du fichier. La modification de ce paramètre peut affecter les performances de Deep Discovery Inspector.

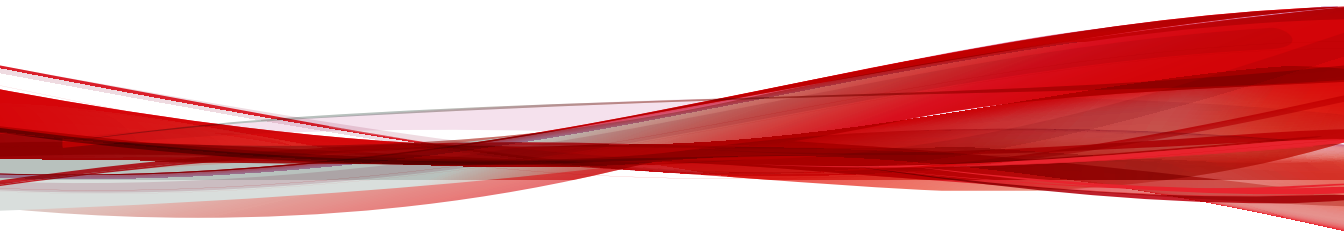
b. Activez le service Certified Safe Software Service (CSSS).

Remarque

Le service Certified Safe Software Service (CSSS) est la base de données en ligne des fichiers légitimes de Trend Micro. Deep Discovery Inspector interroge les centres de données de Trend Micro pour vérifier les fichiers envoyés en les comparant à la base de données.

Partie III

Widgets Endpoint Encryption



Chapitre 5

Tableau de bord d'Endpoint Encryption

Le tableau de bord de Control Manager fournit des informations d'ensemble du réseau Control Manager.

Chaque compte d'utilisateur affiche son propre tableau de bord. Lorsqu'un utilisateur se connecte pour la première à Control Manager, les onglets par défaut et les widgets qu'ils contiennent s'affichent dans le tableau de bord.

Chaque compte utilisateur peut personnaliser le tableau de bord, les onglets et les widgets en fonction de ses besoins spécifiques. La personnalisation du tableau de bord, des onglets ou des widgets pour un compte utilisateur n'a aucun impact sur le tableau de bord, les onglets ou les widgets d'un autre compte utilisateur. Chaque compte utilisateur dispose d'un tableau de bord, d'onglets et de widgets totalement indépendants de tout autre compte utilisateur.

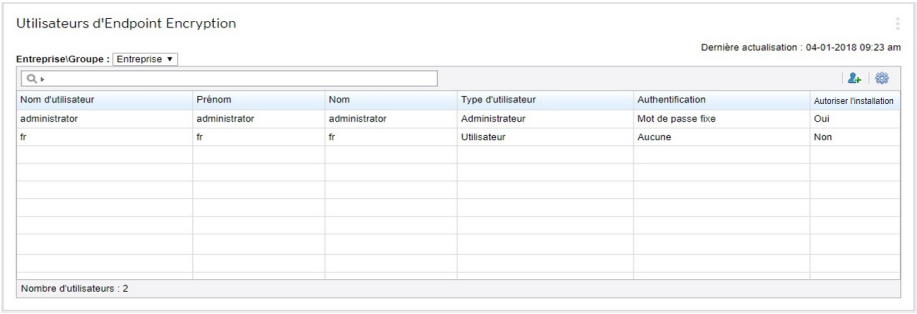
Les rubriques sont les suivantes:

- *Utilisateurs d'Endpoint Encryption à la page 5-3*
- *Périphériques Endpoint Encryption à la page 5-10*
- *État de Full Disk Encryption à la page 5-16*
- *Connexion de périphérique infructueuse à Control Manager à la page 5-19*

- *Connexion d'utilisateur infructueuse à Control Manager à la page 5-21*
- *Verrouillage des dispositifs Control Manager à la page 5-23*
- *Rapport sur les violations de la sécurité de Control Manager à la page 5-25*

Utilisateurs d'Endpoint Encryption

Le widget **Utilisateurs d'Endpoint Encryption** offre une fonction de gestion des utilisateurs directement depuis le tableau de bord de Control Manager. Utilisez le widget **Utilisateurs d'Endpoint Encryption** pour ajouter ou supprimer des comptes utilisateurs Control Manager, réinitialiser les mots de passe, modifier les autorisations, configurer la priorité des groupes de stratégies, importer des éléments à partir d'Active Directory et rechercher des comptes utilisateurs spécifiques.



Élément	Description
Afficher	Sélectionnez les utilisateurs à afficher : tous les utilisateurs de l'entreprise ou ceux d'une stratégie spécifique.
Rechercher ( )	Cliquez sur l'icône pour filtrer les utilisateurs de Control Manager qui s'affichent dans le tableau. Utilisez le champ de recherche pour spécifier les paramètres à partir desquels effectuer la recherche.
Paramètres ( ) Cliquez avec le bouton droit de la souris sur un utilisateur.	Cliquez sur l'icône pour afficher les attributs de l'utilisateur ou pour effectuer des actions sur n'importe quel utilisateur sélectionné.

Élément	Description
Ajouter des utilisateurs ( )	Cliquez sur l'icône pour ajouter des utilisateurs un par un, importer des utilisateurs à partir d'un fichier CSV ou importer des utilisateurs à partir des utilisateurs LDAP d'Active Directory.
Nombre d'utilisateurs	Affichez le nombre total d'utilisateurs dans l'ensemble de l'entreprise, la stratégie sélectionnée ou la recherche spécifiée.

Options des paramètres d'utilisateurs

Le tableau suivant présente les options disponibles sous l'icône Paramètres.

Tableau 5-1. Options des paramètres d'utilisateurs

Option	Description
Modifier le mot de passe	Spécifiez un nouveau mot de passe pour les utilisateurs à l'aide de l'authentification par mot de passe fixe. Le widget ne prend pas en charge la modification des mots de passe pour l'authentification de domaine.
Supprimer un utilisateur	Supprime l'utilisateur sélectionné.
Modifier l'utilisateur	Met à jour les propriétés de l'utilisateur sélectionné. Les propriétés suivantes peuvent être modifiées : • Nom d'utilisateur • Prénom • Nom • ID de l'employé • Adresse électronique • Geler • Type d'utilisateur • Une stratégie • Méthode d'authentification

Option	Description
Répertorier les stratégies	Affiche les stratégies dont l'utilisateur sélectionné est membre. Si la colonne **Autoriser l'installation** de l'utilisateur sélectionné indique **Oui**, l'option permettant d'autoriser ou d'interdire l'installation de stratégies sélectionnés et de sélectionner les stratégies prioritaires est activée.

Options Ajouter un nouvel utilisateur

Le tableau suivant présente les options disponibles lorsque vous ajoutez un nouvel utilisateur Control Manager.

Tableau 5-2. Options Ajouter un nouvel utilisateur

Option	Description
Nom d'utilisateur	Spécifiez le nom d'utilisateur du compte employé par l'utilisateur pour s'authentifier.
Prénom	Spécifiez le prénom de l'utilisateur.
Nom	Spécifiez le nom de l'utilisateur.
ID de l'employé	Spécifiez l'ID d'employé de l'utilisateur (facultatif).
Adresse électronique	Spécifiez l'adresse e-mail de l'utilisateur (facultatif).
Geler	Sélectionnez **Oui** pour verrouiller temporairement le compte. Un compte verrouillé ne peut pas se connecter à des dispositifs Control Manager.
Type d'utilisateur	Sélectionnez **Utilisateur**, **Authentificateur** ou **Administrateur**.

OPTION	DESCRIPTION
Un groupe	Sélectionnez **Oui** pour n'autoriser l'utilisateur à appartenir qu'à une seule stratégie à la fois. L'utilisateur ne pourra pas être ajouté à d'autres groupes de stratégies. Si vous définissez cette option sur **Oui** et que vous définissez le **Type d'utilisateur** sur **Authentificateur** ou **Administrateur**, l'utilisateur sera un authentificateur de groupe ou un administrateur de groupe respectivement.
Méthode d'authentification	Sélectionnez la méthode d'authentification disponible pour l'utilisateur.

Adhésion à la stratégie

Le tableau suivant explique comment aborder l'adhésion à une stratégie pour un utilisateur de Control Manager.

Remarque

Encryption Management for Apple FileVault et Encryption Management for Microsoft BitLocker ne nécessitent pas d'authentification et ne sont pas affectés par les stratégies d'authentification. Les stratégies relatives aux clients, à la connexion, au mot de passe et à l'authentification, ou le fait d'autoriser l'utilisateur à désinstaller le logiciel de l'agent Control Manager, affectent uniquement les agents Full Disk Encryption et Chiffrement de fichier.

EN-TÊTE	EXEMPLE	DESCRIPTION
Priorité	1, 2. 3	Affiche l'ordre dans lequel Control Manager applique les stratégies. Lorsqu'une stratégie affectant un utilisateur est déclenchée, Control Manager prend les mesures nécessaires afin qu'aucune autre stratégie n'affecte l'utilisateur pour cet événement.
Nom de la stratégie	GP1	Affiche le nom de toutes les stratégies affectées actuellement à l'utilisateur.

EN-TÊTE	EXEMPLE	DESCRIPTION
Description	Stratégie temporaire pour les employés.	Affiche la description de la stratégie.
Autoriser l'installation	Oui/Non	Indique si l'utilisateur peut ou non installer de nouveaux dispositifs Control Manager.

Importation des utilisateurs à partir d'un fichier CSV

Remarque

La fonction d'importation d'utilisateurs à partir d'un fichier CSV est uniquement disponible pour les utilisateurs qui emploient l'authentification par mot de passe fixe.

Formatez chaque ligne du fichier CSV de la façon suivante :

```
<ID utilisateur (requis)>, <prénom>, <nom>, <ID de l'employé>,
<adresse électronique>
```

Pour les champs ne comportant aucune donnée, utilisez une virgule comme espace réservé. L'exemple suivant montre une entrée CSV :

```
example_id, name,,, name@example.com
```

Procédure

1. Dans le widget **Utilisateurs d'Endpoint Encryption**, cliquez sur **Ajouter un utilisateur**, puis sélectionnez **Importer des utilisateurs à partir d'un fichier**.

   L'écran **Importer des utilisateurs à partir d'un fichier** s'affiche.

2. Cliquez sur **Choisir un fichier** pour sélectionner le fichier CSV.

   La fenêtre **Ouvrir le fichier CSV** s'ouvre.

3. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

4. Cliquez sur **Ajouter**.

Les utilisateurs contenus dans le fichier CSV sont importés.

Importation des utilisateurs Active Directory

PolicyServer conserve un répertoire d'utilisateurs séparé de la base de données Active Directory. Cela confère à PolicyServer une sécurité absolue concernant l'accès à tous les dispositifs, droits d'utilisateurs et méthodes d'authentification Control Manager.

Utilisez le widget **Utilisateurs d'Endpoint Encryption** de Control Manager pour importer des utilisateurs Active Directory.

Procédure

1. Connectez-vous à Control Manager.
2. Accédez au widget **Utilisateurs d'Endpoint Encryption**.
3. Cliquez sur l'icône .
4. Sélectionnez **Importer des utilisateurs Active Directory**.

   L'écran **Importer des utilisateurs Active Directory** s'affiche.

5. Spécifiez vos informations d'authentification pour le serveur LDAP Active Directory.

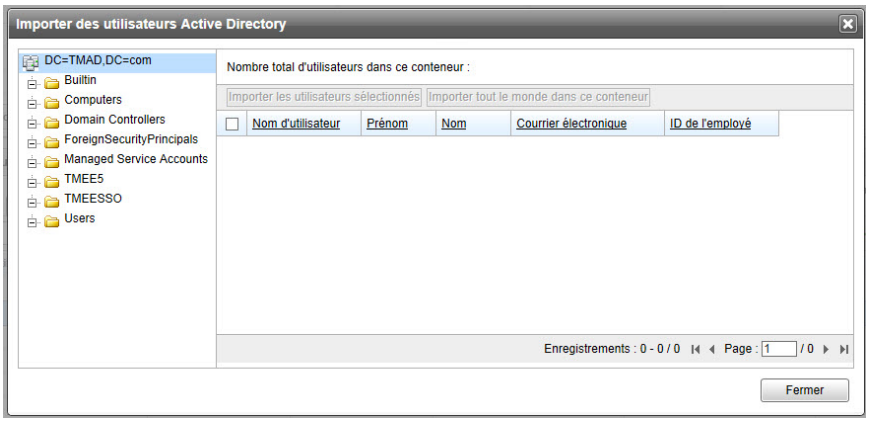
Remarque

Pour **Port**, la valeur « 0 » spécifie le port par défaut. La valeur de port par défaut est 389.

6. Cliquez sur **Suivant**.

7. Attendez que le domaine Active Directory spécifié s'ajoute.

   L'arborescence Active Directory du domaine spécifié s'affiche dans le volet de gauche.



8. Utilisez l'arborescence de navigation du volet de gauche pour sélectionner le conteneur depuis lequel vous souhaitez ajouter des utilisateurs.

   Les utilisateurs disponibles s'ajoutent dans le volet de droite.

9. Effectuez l'une des actions suivantes :

   - Sélectionnez des utilisateurs individuels, puis cliquez sur **Importer les utilisateurs sélectionnés**.
   - Cliquez sur **Importer tout le monde dans ce conteneur**.

10. Cliquez sur **OK** pour ajouter les utilisateurs à l'emplacement spécifié.

    Une fenêtre de confirmation apparaît.

11. Cliquez sur **OK** pour confirmer.

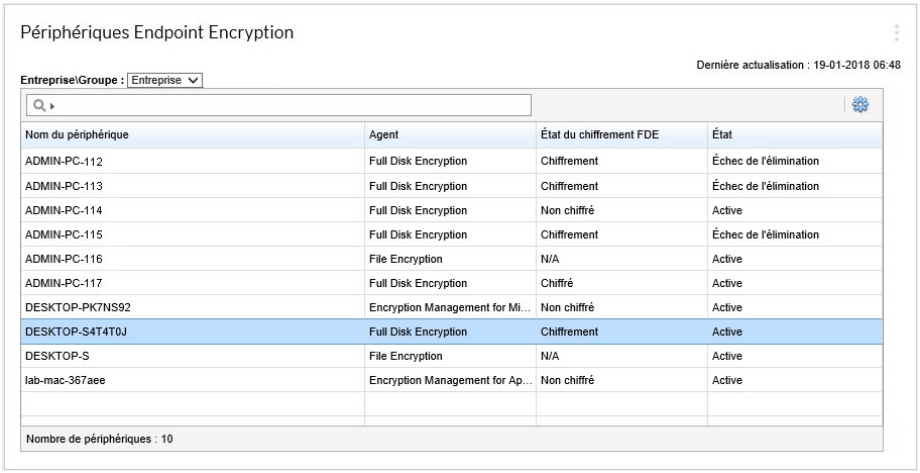
    Un message relatif à l'état d'importation s'affiche.

12. Cliquez sur **Fermer** pour terminer ou répétez la procédure pour sélectionner plus d'utilisateurs à importer.

Périphériques Endpoint Encryption

Les dispositifs Endpoint Encryption sont des agents Endpoint Encryption ayant été enregistrés auprès de PolicyServer. L'installation d'un agent Endpoint Encryption entraîne automatiquement l'enregistrement de l'endpoint auprès de PolicyServer en tant que nouveau dispositif Endpoint Encryption. Étant donné que plusieurs agents Endpoint Encryption peuvent protéger un endpoint spécifique, un seul endpoint peut correspondre à plusieurs dispositifs Endpoint Encryption dans PolicyServer.

Le widget **Périphériques Endpoint Encryption** offre une fonction de gestion des dispositifs Endpoint Encryption directement depuis le tableau de bord de Control Manager. Utilisez le widget **Périphériques Endpoint Encryption** pour surveiller l'activité, rechercher des dispositifs Endpoint Encryption ou sécuriser les données d'endpoint en établissant des commandes de verrouillage ou d'élimination lorsqu'un endpoint est perdu ou volé.



OPTIONS	DESCRIPTION
Afficher	Sélectionnez les périphériques à afficher : tous les périphériques de l'entreprise ou ceux d'une stratégie spécifique.
Rechercher ( )	Cliquez sur l'icône pour sélectionner l'agent Control Manager et filtrer les dispositifs affichés dans le tableau. Utilisez le champ de recherche pour spécifier les paramètres à partir desquels effectuer la recherche. Il est possible d'effectuer la recherche dans tous les attributs répertoriés dans les attributs des périphériques.
Paramètres ( ) Cliquez avec le bouton droit de la souris sur un périphérique.	Sélectionnez un périphérique et cliquez sur l'icône ou cliquez avec le bouton droit de la souris sur un périphérique pour en afficher les attributs ou pour y effectuer des actions.
Nombre de périphériques	Affichez le nombre total de périphériques dans l'ensemble de l'entreprise, la stratégie sélectionnée ou la recherche spécifiée.

Actions des périphériques

Sélectionnez un périphérique et cliquez sur l'icône ou cliquez avec le bouton droit de la souris sur un périphérique pour effectuer les actions suivantes :

ACTION	DESCRIPTION
Supprimer le périphérique	En supprimant un dispositif Control Manager de l'entreprise, vous supprimez également le dispositif de tous les groupes de stratégies. Le dispositif Control Manager supprimé continue de fonctionner tant que les stratégies de mot de passe et de connectivité sont valables sur le dispositif. L'agent ne sera pas en mesure de synchroniser sa stratégie avec le serveur PolicyServer. **AVERTISSEMENT!** Avant de supprimer un périphérique Full Disk Encryption, déchiffrez votre disque et désinstallez l'agent Full Disk Encryption. Si vous supprimez un périphérique Full Disk Encryption sans supprimer l'agent, il est possible que le pré-amorçage de Full Disk Encryption ne puisse pas s'authentifier auprès du serveur PolicyServer et que les données deviennent inaccessibles.
Jeton logiciel	La génération d'un « jeton logiciel » crée une chaîne unique que vous pouvez utiliser pour déverrouiller les dispositifs Control Manager et aider les utilisateurs de Control Manager à réinitialiser les mots de passe oubliés à distance. Le jeton logiciel est uniquement disponible dans la version complète de Full Disk Encryption. Il n'est pas disponible dans Encryption Management for Apple FileVault ni dans Encryption Management for Microsoft BitLocker.
Clé de restauration	La génération d'une « clé de restauration » permet à l'utilisateur de déchiffrer un disque dur lorsque l'utilisateur a oublié le mot de passe ou la clé d'origine. La clé de récupération n'est disponible qu'avec les agents Encryption Management for Apple FileVault et Encryption Management for Microsoft BitLocker, car ils n'utilisent pas les autres méthodes de récupération disponibles dans Full Disk Encryption.
Attributs du périphérique	Obtenez une copie instantanée du périphérique sélectionné.

Action	Description
Éliminer le périphérique	Le lancement d'une commande « kill » supprime toutes les données du dispositif Control Manager. Les données supprimées sont différentes en fonction de l'étendue des données gérées par l'agent Control Manager associé. Par exemple, le lancement d'une commande « kill » vers un périphérique Full Disk Encryption supprime toutes les données du point final, alors que le lancement d'une commande « kill » vers un périphérique File Encryption supprime tous les fichiers et dossiers du stockage local ou amovible protégé par l'agent File Encryption. La commande « kill » est émise lorsque l'agent Control Manager communique avec PolicyServer. **AVERTISSEMENT!** L'élimination d'un dispositif ne peut pas être annulée. Sauvegardez toutes les données avant de lancer une commande kill.
Verrouiller le périphérique	Le lancement d'une commande « lock » sur le dispositif Control Manager bloque l'accès de l'utilisateur de Control Manager tant que ce dernier n'a pas effectué une authentification correcte dans l'aide à distance. Le verrouillage d'un périphérique entraîne le redémarrage du point final et le force dans un état qui nécessite de faire appel à l'aide à distance. La commande lock est émise lorsque l'agent Control Manager communique avec PolicyServer.
Réinitialisation logicielle	Le lancement d'une commande « soft reset » redémarre le point final. La commande est émise la prochaine fois que l'agent communique avec PolicyServer.

Attributs du périphérique

Le tableau suivant décrit les attributs du dispositif Control Manager.

Nom de l'attribut	Exemple	Description
Nom NetBIOS AD	Entreprise	Nom attribué au NetBIOS AD.

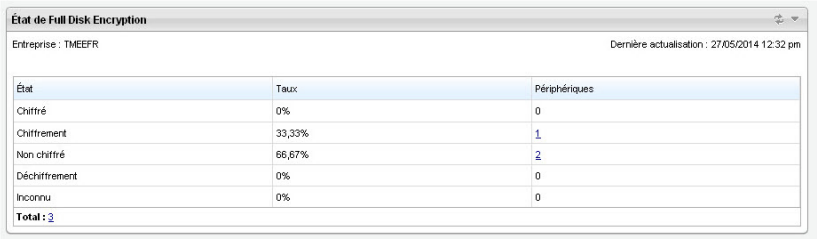
Nom de l'attribut	Exemple	Description
GUID d'objet AD	6629bdeb-99a8-456b-b7c5-dbbc50ad13d0	GUID attribué à l'objet AD.
Nombre de batteries	2	Nombre de batteries installées.
Version .NET	2.0.50727.3620	Version et numéro de compilation de l'infrastructure .NET installée
Numéro de compilation Common Framework	5.0.0.84	L'agent Control Manager utilise une structure commune pour le chiffrement. Le numéro de compilation est utilisé pour indiquer si l'agent est à jour.
Modèle de disque	IDE virtuel VMware	Modèle du disque dur.
Nom du disque	`\\.\PHYSICALDRIVE0`	Nom du disque dur.
Numéro de série du disque		Numéro de série du disque dur.
Partitions de disque	1	Nombre de partitions sur le disque contenant le programme d'installation de l'agent.
Taille du disque	10733990400	Capacité totale du disque dur (en octets).
Nom de domaine	GROUPE DE TRAVAIL	Domaine dont le point final est membre.
ID du point final :	85b1e3e2a3c25d882540ef6e4818c3e4	ID unique de l'endpoint utilisé pour l'intégration de Control Manager.
Version de File Encryption	6.0.0.1039	Version de File Encryption installée sur l'endpoint.
Nom d'hôte	TREND-4136D2DB3	Nom d'hôte du point final.
Adresse IP	`10.1.152.219`	Adresse IP du point final.

Nom de l'attribut	Exemple	Description
Langue	Anglais (États-Unis)	Langue utilisée par l'endpoint.
Local	fr-FR	Paramètres régionaux utilisés par l'endpoint.
Adresse MAC	00-50-56-01-xx-xx	Adresse MAC de l'endpoint.
Nom de l'ordinateur	TREND-4136D2DB3	Nom d'ordinateur utilisé par le point final.
Fabricant	VMware, Inc.	Fabricant du disque dur.
Modèle	Plate-forme virtuelle VMware	Modèle du disque dur.
Système d'exploitation	Microsoft Windows NT 5.1.2600 Service Pack 3	Système d'exploitation installé sur le même disque dur que l'agent.
Nom du système d'exploitation	Microsoft Windows XP Professional	Nom commun du système d'exploitation installé sur le même disque dur que l'agent.
Service Pack du système d'exploitation	Service Pack 3	Numéro du Service Pack du système d'exploitation installé sur le même disque dur que l'agent.
Version du système d'exploitation	5.1.2600.196608	Numéro de version du système d'exploitation installé sur le même disque dur que l'agent.
Schéma de partitionnement	MBR classique	Schéma de partitionnement du disque dur.
Processeur	x86 Family 6 Model 30 Stepping 5, Genuine Intel	Fabricant et modèle du processeur du point final.
Nombre de processeurs	2	Nombre de processeurs dans le point final.

Nom de l'attribut	Exemple	Description
Révision du processeur	1e05	Numéro de révision du processeur.
Fuseau horaire	Taipei	Fuseau horaire dans lequel réside le point final.
Mémoire physique totale	2 047 Mo	RAM totale installée sur le point final ou allouée à celui-ci.
Type	PC à base X86	Type de processeur du point final.
Nom d'utilisateur Windows	TREND-4136D2DB3\admin	Nom d'utilisateur du compte Windows qui s'est connecté en dernier sur le point final.
Utilisateur de l'<agent>	john_smith	Nom d'utilisateur de la dernière connexion.
Version de l'<agent>	5.0.0.260	Version et numéro de compilation pour l'installation de l'agent.

État de Full Disk Encryption

Le widget **État de Full Disk Encryption** affiche l'état de chiffrement actuel de tout dispositif Control Manager dans l'entreprise.



COLONNE	DESCRIPTION
État	État du dispositif Control Manager. Les états comprennent : • **Chiffré** : le dispositif Control Manager est entièrement chiffré. • **Chiffrement** : le dispositif Control Manager procède actuellement au chiffrement du disque dur. L'état passe à « Entièrement chiffré » lorsque le chiffrement se termine et que le point final redémarre. • **Non chiffré** : le dispositif Control Manager n'est pas du tout chiffré. • **Déchiffrement** : le dispositif Control Manager procède actuellement au déchiffrement du disque dur. L'état passe à Non chiffré lorsque le déchiffrement se termine et que le point final redémarre. • **Inconnu** : le dispositif Control Manager est synchronisé, mais PolicyServer ne parvient pas à déterminer l'état de chiffrement.
Taux	Pourcentage de chiffrement du dispositif Control Manager.
Périphériques	Nombre de dispositifs Control Manager présentant actuellement cet état. Cliquez sur le nombre indiqué pour afficher le rapport sur les dispositifs Control Manager.

Remarque

Au bas du widget, cliquez sur le nombre à côté de **Total** pour afficher le rapport sur l'état de Control Manager.

Rapport État de Full Disk Encryption

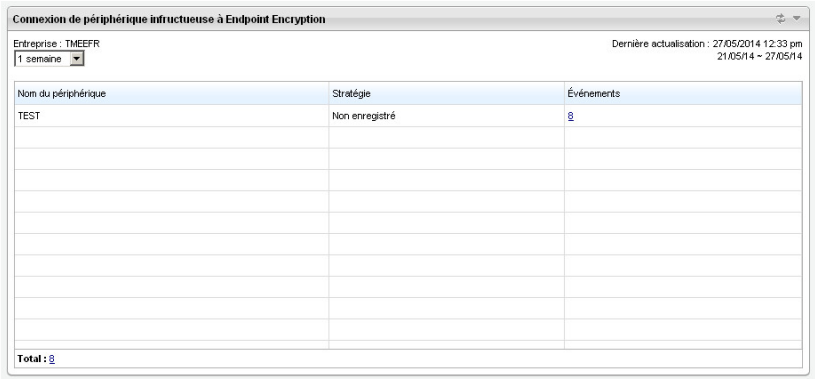
Le tableau suivant décrit le rapport **État de Full Disk Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

TABLEAU 5-3. Exemple de rapport État de Full Disk Encryption

EN-TÊTE	EXEMPLE	DESCRIPTION
Stratégie	GP1	Titre de la stratégie contrôlant le dispositif Control Manager.
Nom du dispositif	TREND-4136D2DB3	Nom de l'ordinateur utilisé par le dispositif Control Manager.
ID du dispositif	1fabfbff-0001-06e5-000c-29 7085710000	ID unique établi après que l'agent Control Manager a été installé sur l'endpoint et qu'un nouveau dispositif Control Manager a été enregistré auprès de PolicyServer.
Agent	Full Disk Encryption	Agent Control Manager actuellement installé.
État	Non chiffré	État actuel du dispositif Control Manager.
Date de la dernière synchronisation	10/07/2013 11:05 am	Date et heure auxquelles le dispositif Control Manager a pour la dernière fois mis à jour les stratégies depuis PolicyServer.
Dernière application de la stratégie	10/07/2013 11:05 am	Date et heure auxquelles Control Manager a pour la dernière fois appliqué des modifications de stratégies sur PolicyServer.

Connexion de périphérique infructueuse à Control Manager

Le widget **Connexion de périphérique infructueuse à Endpoint Encryption** affiche tous les dispositifs Control Manager dont les utilisateurs (utilisateurs Control Manager ou autres) ont effectué des tentatives de connexion infructueuses. Les événements de tentatives de connexion de périphérique infructueuses peuvent représenter une faille de sécurité ou l'utilisateur Control Manager peut avoir oublié les informations d'identification de connexion.



Colonne	Description
Nom du périphérique	Nom de l'ordinateur du périphérique Control Manager.
Stratégie	Stratégie gérant le périphérique Control Manager.
Événements	Nombre de tentatives de connexion. Cliquez sur le nombre pour afficher le rapport **Connexion de périphérique infructueuse à Endpoint Encryption**.

Rapport Connexion de périphérique infructueuse

Le tableau suivant explique le rapport **Connexion de périphérique infructueuse à Endpoint Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

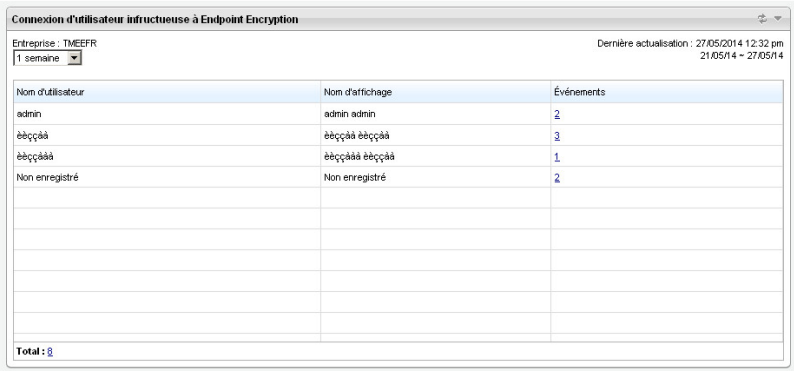
TABLEAU 5-4. Exemple de connexion de périphérique infructueuse à Control Manager

EN-TÊTE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Stratégie	GP1	Titre de la stratégie contrôlant le dispositif Control Manager.
Nom du dispositif	TREND-4136D2DB3	Nom de l'ordinateur utilisé par le dispositif Control Manager.
ID du dispositif	1fabfbff-0001-06e5-000c-297085710000	ID unique établi après que l'agent Control Manager a été installé sur l'endpoint et qu'un nouveau dispositif Control Manager a été enregistré auprès de PolicyServer.
Adresse IP	`10.1.152.219`	Adresse IP du dispositif Control Manager.
Agent	Full Disk Encryption	Agent Control Manager actuellement installé.
Nom d'utilisateur	user325	Nom d'utilisateur ayant tenté de se connecter au dispositif Control Manager.
Nom d'affichage	Mary Jones	Prénom et nom du compte utilisateur Control Manager. Si le nom d'utilisateur indiqué n'est pas un nom d'utilisateur de Control Manager valide, la colonne indique « Non enregistré ».

EN-TÊTE	EXEMPLE	DESCRIPTION
Événement	Échec de la connexion à l'aide du mot de passe fixe	Événement enregistré et méthode d'authentification.

Connexion d'utilisateur infructueuse à Control Manager

Le widget **Connexion d'utilisateur infructueuse à Endpoint Encryption** affiche toutes les tentatives de connexion d'utilisateur (utilisateur de Control Manager ou autre) à un dispositif Control Manager.



COLONNE	DESCRIPTION
Nom d'utilisateur	Nom d'utilisateur ayant tenté de se connecter au dispositif Control Manager.
Nom d'affichage	Nom d'affichage du compte utilisateur qui a tenté de se connecter au dispositif Control Manager.

COLONNE	DESCRIPTION
Événements	Nombre de tentatives d'authentification. Cliquez sur le nombre indiqué afin d'afficher le rapport de connexion d'utilisateur infructueuse à Control Manager.

Rapport Connexion d'utilisateur infructueuse

Le tableau suivant le rapport **Connexion d'utilisateur infructueuse à Endpoint Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

TABLEAU 5-5. Exemple de rapport de connexion d'utilisateur infructueuse à Control Manager

EN-TÊTE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Stratégie	GP1	Titre de la stratégie contrôlant le dispositif Control Manager.
Nom du dispositif	TREND-4136D2DB3	Nom de l'ordinateur utilisé par le dispositif Control Manager.
ID du dispositif	1fabfbff-0001-06e5-000c-297085710000	ID unique établi après que l'agent Control Manager a été installé sur l'endpoint et qu'un nouveau dispositif Control Manager a été enregistré auprès de PolicyServer.
Adresse IP	`10.1.152.219`	Adresse IP du dispositif Control Manager.
Agent	Full Disk Encryption	Agent Control Manager actuellement installé.
Nom d'utilisateur	user325	Nom d'utilisateur ayant tenté de se connecter au dispositif Control Manager.

EN-TÊTE	EXEMPLE	DESCRIPTION
Nom d'affichage	Mary Jones	Prénom et nom du compte utilisateur Control Manager. Si le nom d'utilisateur indiqué n'est pas un nom d'utilisateur de Control Manager valide, la colonne indique « Non enregistré ».
Événement	Échec de la connexion à l'aide du mot de passe fixe	Événement enregistré et méthode d'authentification.

Verrouillage des dispositifs Control Manager

Le widget **Verrouillage de périphériques d'Endpoint Encryption** indique les dispositifs Control Manager qui sont verrouillés en raison de restrictions de stratégie.

EN-TÊTE	DESCRIPTION
Nom du périphérique	Nom de l'ordinateur utilisé par le dispositif Control Manager.

EN-TÊTE	DESCRIPTION
Stratégie	Titre de la stratégie contrôlant le dispositif Control Manager.
Verrouillage	Horodateur lorsque PolicyServer a émis la commande de verrouillage du périphérique. En réalité, le dispositif Control Manager ne se verrouille qu'une fois que l'agent Control Manager a synchronisé les stratégies avec PolicyServer.
Détails	Cliquez sur l'icône des détails pour afficher le rapport de verrouillage des dispositifs Control Manager.

Au bas du widget, cliquez sur le nombre en regard de **Total** pour afficher le rapport.

Rapport de verrouillage de périphérique

Le tableau suivant explique le rapport **Verrouillage de périphériques d'Endpoint Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

TABLEAU 5-6. Exemple de rapport de verrouillage des dispositifs Control Manager

EN-TÊTE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Stratégie	GP1	Titre de la stratégie contrôlant le dispositif Control Manager.
Nom du dispositif	TREND-4136D2DB3	Nom de l'ordinateur utilisé par le dispositif Control Manager.

En-tête	Exemple	Description
ID du dispositif	1fabfbff-0001-06e5-000c-29 7085710000	ID unique établi après que l'agent Control Manager a été installé sur l'endpoint et qu'un nouveau dispositif Control Manager a été enregistré auprès de PolicyServer.
Adresse IP	`10.1.152.219`	Adresse IP du dispositif Control Manager.
Agent	Full Disk Encryption	Agent Control Manager actuellement installé.
Nom d'utilisateur	user325	Nom d'utilisateur ayant tenté de se connecter au dispositif Control Manager.
Nom d'affichage	Mary Jones	Prénom et nom du compte utilisateur Control Manager. Si le nom d'utilisateur indiqué n'est pas un nom d'utilisateur de Control Manager valide, la colonne indique « Non enregistré ».
Événement	Dispositif verrouillé en raison d'une violation de tentative de connexion incorrecte.	Événement enregistré et méthode d'authentification.

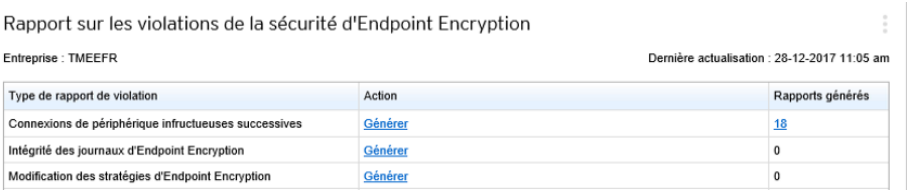
Rapport sur les violations de la sécurité de Control Manager

Le widget **Rapport sur les violations de la sécurité d'Endpoint Encryption** affiche les violations de sécurité évaluées par les rapports suivants :

- **Connexions de périphérique successives infructueuses à Endpoint Encryption**

- **Modification des stratégies d'Endpoint Encryption**
- **Intégrité des journaux d'Endpoint Encryption**

La génération d'un rapport réunit toutes les violations de sécurité consignées actuellement par PolicyServer. Une fois ce rapport généré, cliquez sur le numéro de la colonne **Rapports** pour afficher les rapports générés pour cette violation.


Rapport sur les violations de la sécurité d'Endpoint Encryption

Entreprise : TMEEFR

Dernière actualisation : 28-12-2017 11:05 am

Type de rapport de violation	Action	Rapports générés
Connexions de périphérique infructueuses successives	Générer	18
Intégrité des journaux d'Endpoint Encryption	Générer	0
Modification des stratégies d'Endpoint Encryption	Générer	0

EN-TÊTE	DESCRIPTION
Type de rapport de violation	Types de rapport disponibles pour diverses violations.
Action	Cliquez sur **Générer** pour créer un nouveau rapport.
Rapports	Nombre total de rapports générés pour cette violation. Cliquez sur le nombre pour afficher les rapports disponibles.

Remarque

Pour définir le nombre de tentatives de connexion infructueuses avant qu'elles ne soient considérées comme une violation de la sécurité, cliquez sur ▼ pour ouvrir la fenêtre **Paramètres du widget**, saisissez une valeur dans la zone de texte **Connexions infructueuses successives**, puis cliquez sur **Enregistrer**.

Rapport de connexions de périphérique infructueuses successives

Le tableau suivant explique le rapport **Connexions de périphérique successives infructueuses à Endpoint Encryption**. Utilisez-le pour identifier le moment où la

tentative de connexion a eu lieu, le dispositif Control Manager concerné et le nombre de tentatives effectuées par l'utilisateur pour se connecter au dispositif Control Manager.

TABLEAU 5-7. Exemple de rapport de connexions de dispositif infructueuses successives dans Control Manager

ENTRÉE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Nom du dispositif	TREND-4136D2DB3	Nom de l'ordinateur utilisé par le dispositif Control Manager.
Tentatives	5	Nombre de fois où l'utilisateur a tenté de se connecter au dispositif Control Manager.

Rapport Modification des stratégies

Le tableau suivant explique le rapport **Modification des stratégies d'Endpoint Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

TABLEAU 5-8. Exemple de rapport Modification des stratégies Control Manager

EN-TÊTE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Événement	Échec de vérification de l'intégrité de la valeur de la stratégie	Événement enregistré et méthode d'authentification.

Rapport Intégrité des journaux

Le tableau suivant explique le rapport **Intégrité des journaux d'Endpoint Encryption**. Utilisez-le pour comprendre comment lire les détails du rapport.

TABLEAU 5-9. Exemple de rapport Intégrité des journaux de Control Manager

EN-TÊTE	EXEMPLE	DESCRIPTION
Horodateur de l'événement	02/07/2012 13h56	Moment où l'événement s'est produit.
Événement	Enregistrement du journal d'audit manquant	Événement enregistré et méthode d'authentification.

Chapitre 6

Stratégies Endpoint Encryption

Ce chapitre explique comment utiliser les stratégies et fournit des informations détaillées sur chacune des valeurs des paramètres de stratégie.

Les rubriques sont les suivantes:

- *Vue d'ensemble de l'authentification à la page 6-2*
- *Stratégies dans Control Manager à la page 6-6*
- *Création d'une stratégie à la page 6-10*
- *Configuration des règles des utilisateurs de Control Manager à la page 6-13*
- *Configuration des règles de Full Disk Encryption à la page 6-16*
- *Configuration des règles de File Encryption à la page 6-19*
- *Configuration des règles de stratégie communes à la page 6-22*
- *Migration de groupes vers Control Manager à la page 6-26*

Vue d'ensemble de l'authentification

La principale forme de protection offerte par Control Manager consiste à empêcher les utilisateurs non autorisés d'accéder aux dispositifs et aux endpoints chiffrés. Une configuration adaptée des dispositifs, des utilisateurs et des groupes de stratégies Control Manager prévient le risque de perte de données associé à une divulgation accidentelle des informations ou à un sabotage délibéré.

Périphériques à la page 6-2	Control Manager compte le nombre de tentatives de connexion consécutives exécutées sur un dispositif donné et le temps écoulé depuis la dernière communication avec PolicyServer sur une période spécifiée. Si un dispositif ne respecte pas les critères de la stratégie, Control Manager peut réinitialiser, verrouiller ou effacer le disque.
Utilisateurs à la page 6-3	Outre sa capacité à vérifier les tentatives d'authentification sur un dispositif, Control Manager compte également le nombre de tentatives de connexion consécutives réalisées par un compte utilisateur spécifique. Si cet utilisateur ne respecte pas les critères de la stratégie, Control Manager peut réinitialiser, verrouiller ou effacer le disque.
Groupes à la page 6-4	Les groupes agissent comme un conteneur pour les utilisateurs de la gestion des stratégies. Les administrateurs et les authentificateurs d'un groupe disposent de privilèges spéciaux sur ce groupe uniquement, mais les administrateurs et les authentificateurs non attribués ont ce rôle pour toute l'entreprise.

Périphériques

Les dispositifs Control Manager sont des agents Control Manager ayant été enregistrés auprès de PolicyServer. L'installation d'un agent Control Manager entraîne automatiquement l'enregistrement de l'endpoint auprès de PolicyServer en tant que nouveau dispositif Control Manager. Étant donné que plusieurs agents Control Manager peuvent protéger un endpoint spécifique, un seul endpoint peut correspondre à plusieurs dispositifs Control Manager dans PolicyServer.

En fonction des paramètres de stratégie, Control Manager prend l'une des mesures suivantes lorsque des utilisateurs tentent de se connecter à plusieurs reprises à ce dispositif sans y parvenir :

- Retarder la tentative d'authentification suivante
- Verrouiller le périphérique
- Effacer toutes les données du périphérique

Remarque

Pour configurer des dispositifs Control Manager, utilisez le widget **Périphériques Endpoint Encryption** Consultez la section *Périphériques Endpoint Encryption à la page 5-10*.

Utilisateurs

Les utilisateurs de Control Manager sont tous les comptes utilisateurs manuellement ajoutés à PolicyServer ou synchronisés avec Active Directory.

Control Manager propose plusieurs types de rôles de compte et de méthodes d'authentification pour l'authentification basée sur l'identité et sa gestion. Avec Control Manager ou PolicyServer MMC, vous pouvez ajouter ou importer des comptes utilisateurs, contrôler l'authentification, synchroniser la structure Active Directory et gérer l'appartenance au groupe de stratégies, selon les besoins.

Le tableau suivant décrit les rôles utilisateurs de Control Manager :

RÔLE	DESCRIPTION
Administrateur	Les administrateurs peuvent accéder aux consoles d'administration et effectuer n'importe quelle tâche de configuration au sein de leur domaine. Ce rôle dispose de droits différents en fonction du niveau auquel le rôle d'administrateur est ajouté : • Administrateur d'entreprise : ces administrateurs contrôlent toutes les stratégies, les groupes, les utilisateurs et les dispositifs de l'entreprise. • Administrateur de groupe : ces administrateurs contrôlent les utilisateurs et les dispositifs qui s'authentifient dans un groupe spécifique. Control Manager crée un groupe pour chaque stratégie. Ces administrateurs peuvent donc également être appelés « administrateurs de stratégie ».

RÔLE	DESCRIPTION
Authentificateur	Les authentificateurs fournissent une assistance à distance lorsque les utilisateurs oublient leur mot de passe Control Manager ou rencontrent des problèmes techniques. Ce rôle dispose de droits différents en fonction du niveau auquel le rôle d'authentificateur est ajouté : • Authentificateur d'entreprise : ces authentificateurs aident tous les utilisateurs de l'entreprise. • Authentificateur de groupe : ces authentificateurs peuvent aider tous les utilisateurs d'un groupe spécifique. Control Manager crée un groupe pour chaque stratégie. Ces authentificateurs peuvent donc également être appelés « authentificateurs de stratégie ».
Utilisateur	Les utilisateurs finaux de base n'ont aucun privilège spécial. Le rôle utilisateur ne peut pas se connecter aux consoles d'administration de Control Manager. À moins d'y être autorisé par PolicyServer, le rôle utilisateur ne peut pas utiliser les outils de récupération.

Remarque

Pour configurer les utilisateurs de Control Manager, utilisez le widget **Utilisateurs d'Endpoint Encryption**. Consultez la section *Utilisateurs d'Endpoint Encryption à la page 5-3*.

Groupes

Control Manager gère les stratégies par groupes d'utilisateurs. La gestion des groupes est différente dans PolicyServer MMC et dans Control Manager. Après avoir modifié des stratégies et des groupes, PolicyServer synchronise les groupes entre les deux consoles.

Important

Control Manager est toujours prioritaire sur PolicyServer MMC pour l'attribution des stratégies et des groupes. Les éventuelles modifications apportées à l'attribution des groupes dans PolicyServer MMC seront automatiquement écrasées lors de la synchronisation suivante de Control Manager avec PolicyServer.

CONSOLE	ADMINISTRATION DES GROUPES
Control Manager	Control Manager crée automatiquement un groupe à chaque fois qu'une stratégie présentant des cibles spécifiques est déployée. À l'issue du déploiement, vous pouvez modifier les groupes dans lesquels se trouve un utilisateur depuis le widget **Utilisateurs d'Endpoint Encryption** ; vous pouvez également modifier les utilisateurs de la stratégie depuis l'écran **Gestion des stratégies**.
PolicyServer MMC	Ajoutez et modifiez des groupes directement depuis le volet de gauche dans PolicyServer MMC. Pour attribuer des groupes dans PolicyServer MMC, procédez comme suit : • **Groupe supérieur** : les groupes supérieurs représentent le niveau de groupes le plus élevé au sein de l'entreprise. Chaque groupe supérieur possède un nœud unique sous l'entreprise. • **Sous-groupe** : les sous-groupes sont créés au sein des groupes supérieurs. Les sous-groupes héritent des stratégies du groupe supérieur lors de leur création, mais n'héritent pas des modifications apportées au groupe supérieur. Les sous-groupes ne peuvent pas bénéficier de davantage d'autorisations que le groupe supérieur. **Remarque** Vous devez attribuer manuellement des dispositifs et des utilisateurs à chaque sous-groupe. L'ajout d'utilisateurs de Control Manager à un sous-groupe n'entraîne pas automatiquement l'ajout des utilisateurs au groupe supérieur. Vous pouvez toutefois ajouter des utilisateurs au groupe supérieur et au sous-groupe.

Remarque

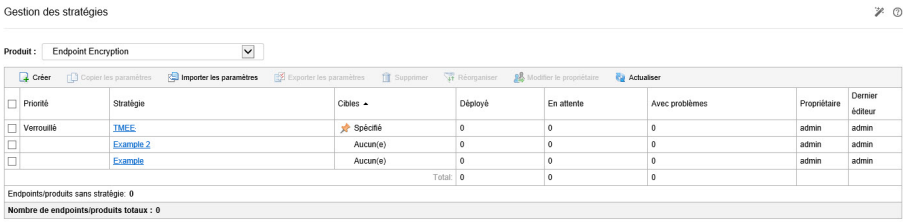
Pour configurer les utilisateurs dans un groupe de stratégies sur Control Manager, utilisez le widget **Utilisateurs d'Endpoint Encryption**.

Pour configurer des utilisateurs dans un groupe de stratégie sur PolicyServer MMC, consultez le *Manuel Endpoint Encryption PolicyServer MMC*.

Stratégies dans Control Manager

La liste des stratégies affiche les informations et l'état des stratégies créées par tous les utilisateurs. Quand un nouveau endpoint s'enregistre auprès de Control Manager, il parcourt les stratégies filtrées de la liste par ordre décroissant. Control Manager affecte le nouveau endpoint à une stratégie filtrée quand les conditions suivantes sont toutes deux satisfaites :

- Le nouveau point final correspond aux critères de la cible dans la stratégie
- Le créateur de la stratégie a l'autorisation de gérer le nouveau point final



Le tableau suivant décrit les éléments de la liste des stratégies.

Élément de menu	Description
Priorité	Cette colonne n'est pas utilisée dans Control Manager. Cette colonne affiche uniquement les éléments suivants : • Bloqué : la stratégie a été créée et est en cours d'utilisation. • Colonne vierge : la stratégie est encore à l'état de brouillon et n'est pas utilisée à l'heure actuelle.
Stratégie	Indique le nom de la stratégie.

Élément de menu	Description
Cibles	Indique comment les administrateurs sélectionnent les cibles de la stratégie. • Spécifié : utilise la fonction Parcourir ou Rechercher pour sélectionner les cibles spécifiques de la stratégie. Les stratégies spécifiées restent statiques au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées. • Filtré : cette option n'est pas utilisée dans Control Manager. • Aucun : le créateur de la stratégie a enregistré celle-ci en tant qu'ébauche sans choisir de cible.
Déployé	Affiche le nombre de cibles qui ont appliqué les paramètres de la stratégie.
En attente	Affiche le nombre de cibles qui n'ont pas appliqué les paramètres de la stratégie. Cliquez sur le nombre en attente pour vérifier l'état de la stratégie.
Créateur	Affiche l'utilisateur ayant créé la stratégie.
Endpoints/produits sans stratégie	Affiche le nombre de produits gérés ou de endpoints auxquels Control Manager n'a affecté aucune stratégie.
Nombre de points finaux/ produits totaux	Affiche le nombre de produits gérés ou de points finaux disponibles pour une gestion des stratégies.

Remarque

Les nombres dans Déployé, En attente, Endpoints/produits sans stratégie et Nombre de points finaux/produits totaux reflètent seulement les points finaux ou les produits gérés que l'administrateur est autorisé à gérer.

Options des stratégies

La gestion des stratégies permet aux administrateurs d'appliquer les paramètres d'un produit dans les produits gérés et les endpoints à partir d'une seule console

d'administration. Les administrateurs créent une stratégie en sélectionnant les cibles et en configurant une liste des paramètres du produit.

Les stratégies Control Manager contiennent les attributs suivants :

TABLEAU 6-1. Options des stratégies Control Manager

ATTRIBUT	DESCRIPTION
Nom de la stratégie	Nom de la configuration de stratégie
Cibles	Les administrateurs peuvent sélectionner des cibles auxquelles attribuer leurs stratégies. La méthode de sélection de la cible détermine le type de stratégie et le fonctionnement de cette stratégie. Les administrateurs peuvent sélectionner manuellement les cibles ou utiliser un filtre pour affecter automatiquement des cibles à leurs stratégies. La méthode de sélection de la cible détermine le type de stratégie et le fonctionnement de cette stratégie. Pour plus d'informations sur les types de stratégie, consultez la section *Types de stratégies à la page 6-9*. Pour définir un produit géré ou un endpoint comme cible, assurez-vous que la version du produit géré ou de l'endpoint prend en charge la gestion des stratégies dans Control Manager. L'écran **Paramètres de modèle de stratégie** contient des informations sur les versions de produits prises en charge.

ATTRIBUT	DESCRIPTION
Paramètres	Quand Control Manager déploie une stratégie dans les cibles, les paramètres définis dans la stratégie écrasent les paramètres existants dans les cibles. Control Manager applique les paramètres de la stratégie dans les cibles toutes les 24 heures. Bien que les administrateurs locaux puissent modifier les paramètres à partir de la console du produit géré, les modifications sont écrasées à chaque fois que Control Manager applique les paramètres de la stratégie. **Remarque** Comme l'application de la stratégie n'a lieu que toutes les 24 heures, les paramètres du produit dans les cibles peuvent ne pas correspondre aux paramètres de la stratégie si les administrateurs locaux font des modifications via la console du produit géré entre deux périodes d'application.

Remarque

Assurez-vous d'utiliser le **Répertoire Produits** pour déplacer l'instance gérée de PolicyServer du dossier Nouvelle entité vers le dossier Control Manager dans le Répertoire Produits.

Types de stratégies

Control Manager fournit trois types de stratégies pouvant être créées par les administrateurs. Chaque type de stratégie diffère dans leur méthode de sélection de la cible, ce qui affecte le fonctionnement d'une stratégie. La liste des stratégies classe les types de stratégies dans l'ordre décrit dans le tableau suivant.

TABLEAU 6-2. Types de stratégies

TYPE DE STRATÉGIE	DESCRIPTION
Spécifié	• Utilise la fonction rechercher ou parcourir pour localiser des cibles spécifiques et les affecter manuellement à la stratégie • Utile quand les administrateurs planifient un déploiement de paramètres spécifiques uniquement dans certaines cibles • Reste statique au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées.
Filtré	**Remarque** Control Manager ne prend pas en charge les stratégies filtrées.
Ébauche	Permet aux administrateurs d'enregistrer les paramètres de la stratégie en tant qu'ébauche sans choisir de cible. Control Manager enregistre les ébauches de stratégies avec la priorité la plus faible, en fin de liste.

Création d'une stratégie

La procédure suivante explique comment configurer une stratégie Control Manager qui affecte les utilisateurs et dispositifs Control Manager.

Procédure

1. Configurez vos utilisateurs et dispositifs Control Manager.

   La configuration des utilisateurs et dispositifs Control Manager utilise les widgets **Utilisateurs d'Endpoint Encryption** et **Périphériques Endpoint Encryption**.

   Si votre environnement comprend Active Directory, assurez-vous d'avoir configuré Active Directory et synchronisé tous les utilisateurs.

2. Accédez à l'écran **Créer une stratégie**.

   a. Allez à **Stratégies** > **Gestion des stratégies**.

b. Dans la liste déroulante **Produit**, choisissez **Endpoint Encryption**.

c. Cliquez sur **Créer**.

L'écran **Créer une stratégie** apparaît.

3. Spécifiez un nom de stratégie.

4. Cliquez sur l'une des options de cibles de stratégie suivantes :

   - **Aucune (Brouillon uniquement)** : créez une stratégie sans cibles (endpoints).

     Une stratégie sans cible ne peut pas être déployée. Une fois que vous avez ébauché une stratégie, vous pouvez la modifier ultérieurement pour spécifier les cibles et la déployer dans votre environnement.

   - **Filtrer par critères** : Control Manager ne prend pas en charge le filtrage par critères.

   - **Spécifier la ou les cibles** : indiquez les endpoints existants.

5. Spécifiez les paramètres de stratégie de Control Manager.

   Les paramètres de Control Manager sont répartis entre les ensembles de règles suivants :

   - **Utilisateurs**
   - **Full Disk Encryption**
   - **File Encryption**
   - **Commun**

6. Cliquez sur **Enregistrer**.

Spécifications des cibles de stratégie

Utilisez l'écran **Spécifier la ou les cibles** pour affecter des dispositifs Control Manager à la stratégie.

Remarque

L'écran **Spécifier la ou les cibles** est disponible lors de la création d'une nouvelle stratégie.

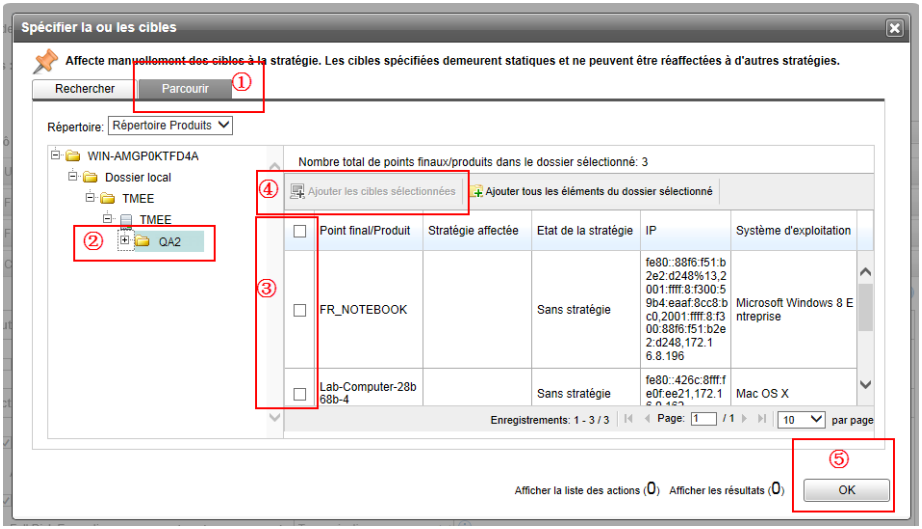


FIGURE 6-1. Spécifications des cibles de stratégie

Procédure

1. Dans l'écran **Spécifier la ou les cibles**, cliquez sur l'onglet **Parcourir**.
2. Dans le volet de gauche, développez l'arborescence pour sélectionner le dossier géré.

Exemple : **CM-PI-2K8 > Dossier local > TMEE > TMEE > QA2**

3. Sélectionnez un dispositif Control Manager approprié ou cochez la case supérieure pour sélectionner tous les dispositifs Control Manager répertoriés dans la page actuelle.

4. Cliquez sur **Ajouter les cibles sélectionnées**.

Remarque

Pour sélectionner immédiatement tous les périphériques dans le dossier géré, cliquez sur **Ajouter tous les éléments du dossier sélectionné**.

« Afficher la liste des actions » et « Afficher les résultats » se mettent à jour en fonction de la sélection.

5. Cliquez sur **OK**.

Configuration des règles des utilisateurs de Control Manager

La procédure suivante présente les options des règles de stratégie que vous pouvez configurer et qui affectent l'authentification et les comptes utilisateurs Control Manager.

Procédure

1. Créez une stratégie Control Manager.

2. Cliquez sur **Utilisateurs**.

Les paramètres des règles de stratégie **Utilisateurs** s'affichent.

FIGURE 6-2. Règles de stratégie des utilisateurs de Control Manager

3. Si des utilisateurs nécessitent une authentification de domaine, sélectionnez **Activer l'authentification de domaine** sous **Paramètres d'utilisateurs de domaine**.

   Si vous avez sélectionné **Activer l'authentification de domaine**, saisissez les informations relatives au serveur pour votre compte Active Directory (AD).

   a. Configurez le nom de domaine AD.

   b. Configurez le nom d'hôte du serveur AD.

   c. Sélectionnez le type de serveur :

      - **LDAP**
      - **Proxy LDAP**

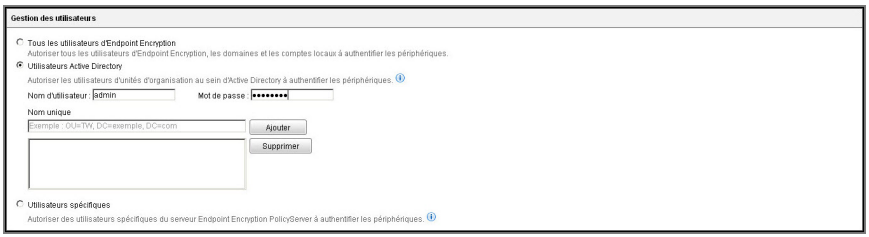
4. Dans **Gestion des utilisateurs**, configurez l'accès des utilisateurs.

OPTION	DESCRIPTION
Tous les utilisateurs d'Endpoint Encryption	Autorisez tous les utilisateurs, comptes de domaine et comptes locaux à authentifier les dispositifs Control Manager.
Utilisateurs Active Directory	Autorisez les utilisateurs issus d'unités organisationnelles au sein d'Active Directory à authentifier les dispositifs Control Manager.

OPTION	DESCRIPTION
	Remarque Sélectionnez **Activer l'authentification de domaine** pour activer l'option **Utilisateurs Active Directory**.
Sélectionner des utilisateurs spécifiques	Indiquez les utilisateurs de Control Manager pouvant s'authentifier sur les endpoints gérés parmi ceux ayant déjà été ajoutés. **Remarque** Pour sélectionner des utilisateurs avec cette option, vous devez renseigner la liste des utilisateurs. Ajoutez des unités organisationnelles à l'aide de l'option **Utilisateurs Active Directory** ou ajoutez des utilisateurs à l'aide du widget Utilisateurs de Control Manager.

5. Si vous avez sélectionné **Utilisateurs Active Directory**, ajoutez des unités organisationnelles en indiquant leur nom unique.

   Une fois l'option **Utilisateurs Active Directory** sélectionnée, les options supplémentaires suivantes s'affichent :



OPTION	DESCRIPTION
Nom d'utilisateur	Indiquez votre nom d'utilisateur Active Directory.
Mot de passe	Indiquez votre mot de passe Active Directory.
Nom unique	Indiquez chaque unité organisationnelle en saisissant sa séquence de noms uniques (RDN) séparés par des virgules.

OPTION	DESCRIPTION
	Exemple : OU=TW, DC=masociété, DC=com Après avoir saisi le nom unique de l'unité organisationnelle, cliquez sur **OK**. **Important** Control Manager prend en charge jusqu'à 12 unités organisationnelles par stratégie.

Configuration des règles de Full Disk Encryption

La procédure suivante présente les options des règles de stratégie qui affectent les dispositifs Full Disk Encryption et que vous pouvez configurer.

Remarque

Encryption Management for Apple FileVault et Encryption Management for Microsoft BitLocker ne nécessitent pas d'authentification et ne sont pas affectés par les stratégies d'authentification. Les stratégies relatives aux clients, à la connexion, au mot de passe et à l'authentification, ou le fait d'autoriser l'utilisateur à désinstaller le logiciel de l'agent Control Manager, affectent uniquement les agents Full Disk Encryption et File Encryption.

Procédure

1. Créez une stratégie Control Manager.
2. Cliquez sur **Full Disk Encryption**.

L'écran de configuration des règles de stratégie **Full Disk Encryption** s'ouvre.

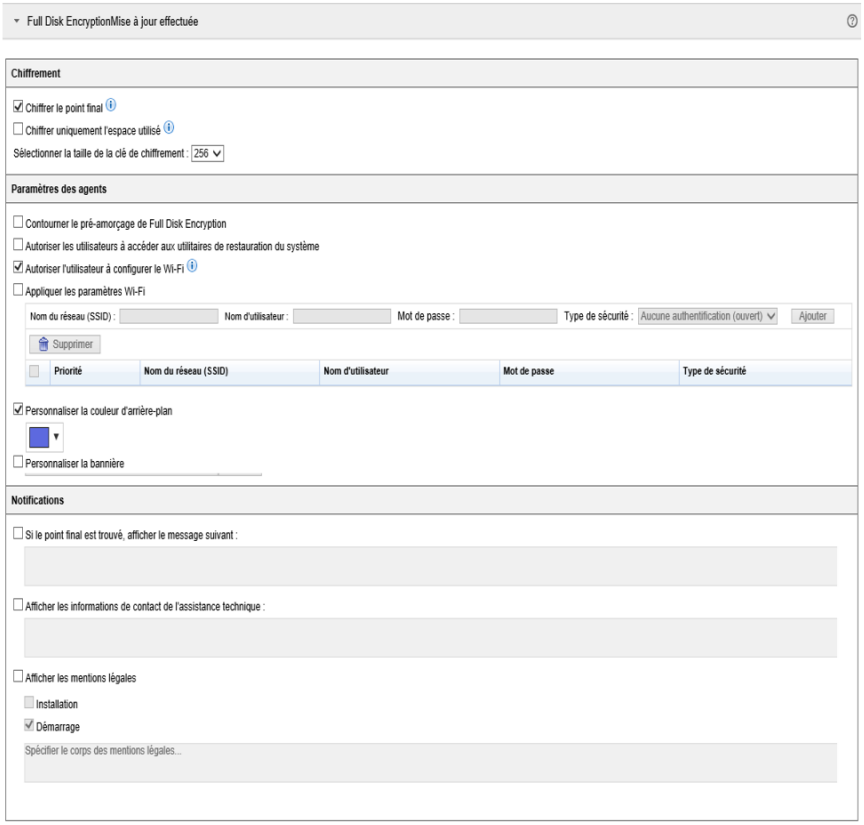


FIGURE 6-3. Règles de stratégie dans Full Disk Encryption

3. Sous **Chiffrement**, sélectionnez les options suivantes :

   - Cochez la case **Chiffrer un dispositif** pour lancer Full Disk Encryption lorsque l'agent Control Manager synchronise les stratégies avec PolicyServer.

AVERTISSEMENT!

Ne lancez pas le chiffrement sur les agents Full Disk Encryption sans avoir préparé le endpoint du disque dur.

Pour plus d'informations sur la préparation du disque dur, consultez la section *Aperçu du déploiement de Full Disk Encryption* dans le *Guide d'installation de Control Manager*.

- Cochez la case **Chiffrer uniquement l'espace utilisé** pour chiffrer uniquement l'espace utilisé.
- Entrez une valeur dans **Sélectionner la taille de la clé de chiffrement** pour indiquer une taille de clé de chiffrement de dispositif en bits.

4. Sous **Paramètres d'agent**, sélectionnez les options suivantes :

   - Cochez la case **Contourner le pré-amorçage de Full Disk Encryption** pour permettre à l'utilisateur de s'authentifier directement dans Windows, sans la protection que procure l'authentification lors du pré-amorçage.
   - Cochez la case **Les utilisateurs sont autorisés à accéder aux utilitaires de restauration du système sur le périphérique** pour permettre à l'utilisateur d'accéder à la Console de restauration.
   - Cochez la case **Autoriser l'utilisateur à configurer le Wi-Fi** pour autoriser les utilisateurs à configurer des stratégies Wi-Fi sur le dispositif pendant le pré-amorçage.
   - Cochez la case **Activer la configuration Wi-Fi** pour utiliser une configuration Wi-Fi prédéfinie pendant le pré-amorçage. Indiquez les informations suivantes :
     - Nom du réseau (SSID)
     - Nom d'utilisateur
     - Mot de passe
     - Type de sécurité
   - Cochez la case **Activer la couleur d'arrière-plan à la connexion** pour définir la couleur d'arrière-plan pendant la connexion.

- Cochez la case **Activer la bannière de connexion** pour définir une image pour la bannière de connexion.

  L'image ne doit pas dépasser 128 Ko et doit mesurer 512 x 64 pixels. Les formats acceptés sont les fichiers PNG avec transparence (recommandé), les fichiers JPG et les fichiers GIF.

5. Sous **Notifications**, configurez les options suivantes :

   - Utilisez l'option **Si trouvé, afficher le message suivant sur le périphérique** pour afficher un message lorsque la stratégie **En cas de détection** est active.
   - Utilisez l'option **Afficher les informations de contact de l'assistance technique** pour afficher un message une fois que l'utilisateur est connecté à l'agent Full Disk Encryption.
   - Cochez la case **Afficher les mentions légales** pour afficher les mentions légales au démarrage ou seulement après l'installation de l'agent Full Disk Encryption.

Configuration des règles de File Encryption

La procédure suivante explique les options configurables pour les règles de stratégie qui touchent les périphériques File Encryption.

Procédure

1. Créez une stratégie Control Manager.
2. Cliquez sur File Encryption.

Les paramètres des règles de stratégie de **File Encryption** s'affichent.

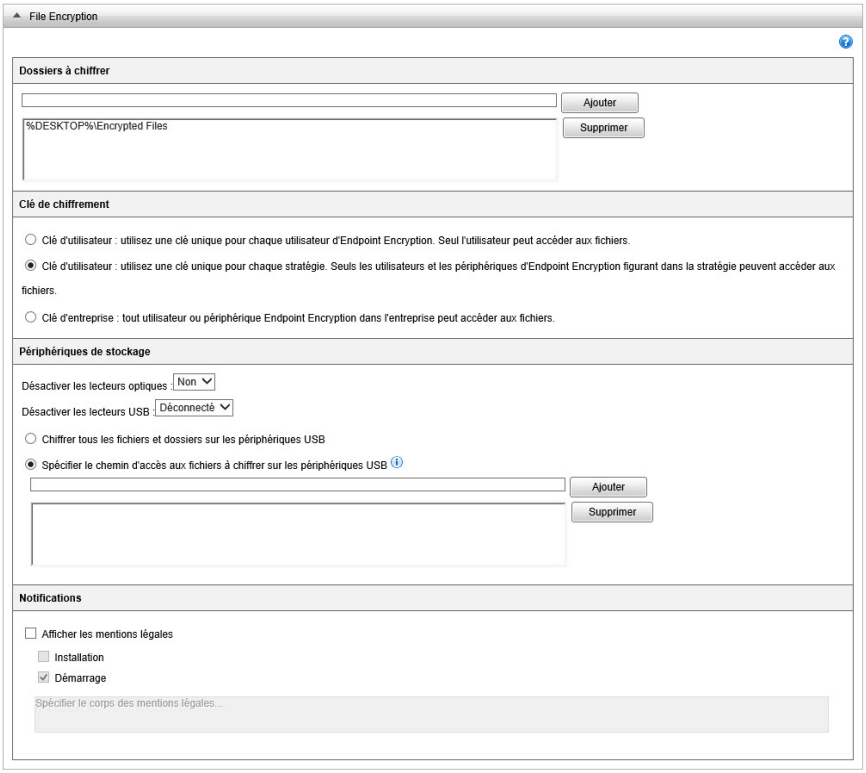


FIGURE 6-4. Règles de stratégie de File Encryption

3. Dans **Dossier à chiffrer**, spécifiez les dossiers créés et chiffrés automatiquement sur le point final lorsque l'agent File Encryption effectue la synchronisation des stratégies.

4. Dans **Clé de chiffrement**, sélectionnez le chiffrement pour le dossier chiffré File Encryption.

   - **Clé utilisateur** : utilisez une clé unique pour chaque utilisateur de Control Manager. Seul l'utilisateur de Control Manager peut déchiffrer les fichiers qu'il a lui-même chiffrés.

- **Clé de stratégie** : Utilisez une clé unique pour chaque stratégie. Seuls les utilisateurs et dispositifs Control Manager associés à la stratégie en question peuvent déchiffrer les fichiers.
- **Clé d'entreprise** : n'importe quel utilisateur ou dispositif Control Manager dans l'entreprise peut déchiffrer les fichiers.

Remarque

La sélection de **Clé de stratégie** ou **Clé d'entreprise** contrôle le partage de la clé partagée de File Encryption.

5. Dans **Périphériques de stockage**, configurez les options suivantes :
   - Sélectionnez **Désactiver les lecteurs optiques** pour contrôler si le support amovible est accessible à partir du point final.
   - Sélectionnez **Désactiver lecteurs USB** pour contrôler à quel moment les ports USB sont désactivés. Les options sont les suivantes :
     - **Toujours**
     - **Déconnecté**
     - **Jamais**
   - Sélectionnez **Chiffrer tous les fichiers et dossiers sur les périphériques USB** pour chiffrer automatiquement tous les fichiers et dossiers sur les lecteurs amovibles lorsqu'ils sont branchés sur le point final.
   - Sélectionnez **Spécifier le chemin d'accès aux fichiers à chiffrer sur les périphériques USB** pour ajouter ou supprimer des dossiers chiffrés sur les lecteurs USB. Si le dossier n'existe pas, il est créé. Si aucune lettre de lecteur n'est spécifiée, tous les lecteurs USB sont concernés.
6. Dans **Notifications**, sélectionnez **Afficher les mentions légales** pour afficher un message spécifique aux mentions légales au démarrage ou seulement après l'installation de l'agent File Encryption.

Configuration des règles de stratégie communes

Cette section présente les options des règles de stratégie qui affectent tous les dispositifs Control Manager et que vous pouvez configurer.

Procédure

1. Créez une stratégie Control Manager.
2. Cliquez sur **Commune**.

Les paramètres des règles de stratégie **Communes** s'affichent.

FIGURE 6-5. Règles de stratégie communes

3. Sous **Autoriser l'utilisateur à désinstaller**, cochez la case **Autoriser les comptes d'utilisateur (non-administrateur) à désinstaller le logiciel de l'agent** pour permettre à n'importe quel utilisateur de Control Manager de désinstaller l'agent.

Remarque

Par défaut, seuls les comptes de type Administrateur peuvent désinstaller les agents Control Manager.

4. Dans **Actions de verrouillage et de blocage de périphériques**, configurez les options suivantes :

   - Sélectionnez **Verrouiller le compte après <nombre> jours** pour indiquer le nombre de jours après lequel le dispositif Control Manager est verrouillé s'il n'est pas synchronisé avec les stratégies.

     - Utilisez **Action de verrouillage du compte** pour spécifier si le verrouillage déclenche l'action Authentification à distance ou Effacer.

   - Cochez la case **Nombre de tentatives de connexion infructueuses autorisé** pour indiquer combien de fois l'utilisateur peut tenter de s'authentifier avant que le dispositif Control Manager ne soit verrouillé.

   - Pour les périphériques Full Disk Encryption ou File Encryption, configurez séparément les éléments suivants :

     - Utilisez **Action de verrouillage du périphérique** pour spécifier si le verrouillage déclenche l'action « Authentification à distance » ou « Effacer ».

     - Utilisez l'option **Nombre de minutes de verrouillage du périphérique** pour indiquer le délai après lequel le dispositif Control Manager est verrouillé et l'authentification est rendue impossible.

5. Dans **Mot de passe**, configurez les options suivantes :

   - Sélectionnez **Les utilisateurs doivent modifier le mot de passe après <nombre> jours** pour contrôler si un utilisateur reçoit une invite pour mettre à jour son mot de passe.

   - Sélectionnez **Les utilisateurs ne peuvent pas réutiliser les <nombre> mots de passe** pour spécifier le nombre de mots de passe précédents réutilisables par l'utilisateur.

   - Sélectionnez **Nombre de caractères successifs autorisés dans un mot de passe** pour spécifier le nombre de caractères répétés qu'un utilisateur peut spécifier dans un mot de passe.

   - Sélectionnez **Longueur minimale autorisée pour les mots de passe** pour spécifier le nombre de caractères que l'utilisateur doit utiliser dans un mot de passe.

6. Dans **Conditions requises pour le mot de passe**, spécifiez les limitations de caractères relatives au mot de passe.

   - **Lettres**
   - **Caractères minuscules**
   - **Caractères majuscules**
   - **Chiffres**
   - **Symboles**

   Important

   La somme totale de lettres, chiffres et symboles ne doit pas dépasser 255 caractères.

7. Sous **Agent**, indiquez l'**intervalle de synchronisation** en minutes.

Actions de verrouillage

Certaines stratégies disposent de paramètres pour verrouiller un compte d'utilisateur ou verrouiller un périphérique en fonction de certains critères. Les actions de verrouillage de comptes ou de dispositifs affectent le dispositif Control Manager, que l'agent synchronise ou non les stratégies avec PolicyServer. Ainsi, l'agent Control Manager verrouille automatiquement le dispositif Control Manager si ce même agent ne communique pas avec PolicyServer pendant un certain temps. Utilisez les tableaux ci-dessous pour comprendre les actions disponibles pour le verrouillage de compte et de périphérique.

Le tableau suivant décrit le moment où les actions de verrouillage se produisent :

TYPE	DESCRIPTION
Verrouillage de compte	Les actions de verrouillage de comptes prennent effet lorsque l'agent Control Manager ne communique pas avec PolicyServer pendant un certain temps, défini dans la stratégie.

TYPE	DESCRIPTION
Verrouillage de périphérique Full Disk Encryption	Les actions de verrouillage d'un dispositif Full Disk Encryption prennent effet lorsque l'utilisateur de Control Manager dépasse le nombre de tentatives défini dans la stratégie pour se connecter à ce dispositif Full Disk Encryption.
Verrouillage de périphérique File Encryption	Les actions de verrouillage d'un dispositif Chiffrement de fichier prennent effet lorsque l'utilisateur de Control Manager dépasse le nombre de tentatives défini dans la stratégie pour se connecter à ce dispositif File Encryption.

Les options des actions de verrouillage sont les suivantes :

ACTION	DESCRIPTION
Effacer	PolicyServer efface toutes les données contrôlées par l'agent Control Manager associé. **AVERTISSEMENT!** L'utilisateur de Control Manager ne peut pas récupérer les données effacées.
Authentification à distance	PolicyServer verrouille le dispositif Control Manager jusqu'à ce que l'utilisateur de Control Manager ait reçu les données d'authentification de l'aide à distance, fournies par un authentificateur ou par le service d'assistance.
Temporisation	PolicyServer verrouille temporairement le dispositif Control Manager et informe l'utilisateur de Control Manager que le dispositif est verrouillé. La fonction d'authentification ou de réinitialisation du mot de passe est désactivée jusqu'à un certain délai. Ce délai est déterminé dans la stratégie. Une fois le délai expiré, l'utilisateur est autorisé à s'authentifier.

Migration de groupes vers Control Manager

Utilisez la procédure suivante pour ajouter des groupes existants de PolicyServer MMC dans Control Manager.

Procédure

1. Connectez-vous à PolicyServer MMC.
2. Rassemblez les informations suivantes :
   - Nombre total de groupes, leur nom et les sous-groupes
   - Tous les utilisateurs affectés à chaque groupe
   - La configuration de stratégie de chaque groupe
3. Connectez-vous à Control Manager.
4. Pour chaque groupe de PolicyServer MMC, configurez une nouvelle stratégie qui correspond à la configuration de stratégie de groupe correspondante.

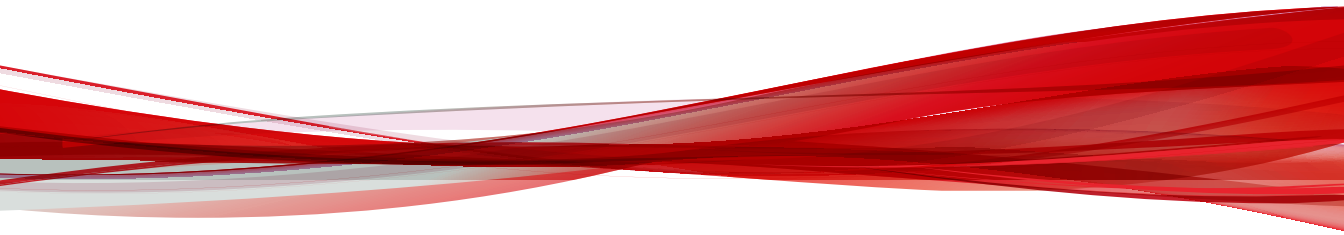
   Remarque

   Les sous-groupes ne sont pas pris en charge dans Control Manager. Pour répliquer les paramètres de la stratégie de sous-groupe, créez une stratégie séparée pour chaque sous-groupe.

5. Ajoutez des utilisateurs à chaque nouvelle stratégie correspondante.
6. Déployez chaque stratégie.

Partie IV

Widgets des produits InterScan



Chapitre 7

Paramètres de stratégie d'InterScan Messaging Security Virtual Appliance

Cette section explique comment configurer les paramètres de stratégie d'InterScan Messaging Security Virtual Appliance dans Control Manager.

Les rubriques sont les suivantes:

- *Règles IMSVA à la page 7-2*
- *Ajout de règles IMSVA à la page 7-2*
- *Modification de règles IMSVA existantes à la page 7-7*
- *Suppression de règles IMSVA à la page 7-8*

Règles IMSVA

InterScan Messaging Security Virtual Appliance (IMSVA) évalue les données contenues dans un message électronique par rapport à un ensemble de règles définies. Les règles déterminent les données devant être protégées des transmissions non autorisées et l'action qu'IMSVA doit effectuer lorsqu'il détecte une transmission.

Les règles IMSVA contiennent les composants suivants :

- Acheminement des messages : ensemble d'adresses électroniques ou de groupes d'expéditeurs et de destinataires ou bien utilisateur ou groupe LDAP auxquels la stratégie est appliquée. Vous pouvez utiliser l'astérisque (*) pour créer des expressions génériques et simplifier la configuration d'acheminement.
- Filtre : règle ou ensemble de règles qui s'appliquent à un acheminement spécifique. Dans TMCM, vous pouvez définir des règles de protection contre le vol de données au moyen de modèles.
- Action : action qu'IMSVA doit effectuer si les conditions du filtre sont remplies.

Ajout de règles IMSVA

La création d'une règle implique les étapes suivantes :

- Étape 1 : Définir le nom de la règle
- Étape 2 : Sélectionner les destinataires et les expéditeurs
- Étape 3 : Sélectionner les modèles
- Étape 4 : Sélectionner les actions

Procédure

1. Sous **Paramètres**, cliquez sur **Ajouter**.

   L'écran **Ajouter une règle** apparaît alors.

Étape 1 : Définir le nom de la règle

Procédure

1. Saisissez un nom pour la règle. La longueur du nom ne doit pas dépasser 122 octets.
2. Attribuez un numéro de classement qui représente sa position dans la hiérarchie des règles.
3. Cliquez sur **Suivant**.

   L'écran **Sélectionner les destinataires et les expéditeurs** s'affiche.

Étape 2 : Sélectionner les destinataires et les expéditeurs

Définissez les adresses e-mail ou les groupes des expéditeurs et des destinataires, ou un utilisateur ou un groupe LDAP auquel la règle s'applique. Vous pouvez aussi configurer des exceptions pour l'acheminement des messages.

Procédure

1. Cliquez sur le lien situé en regard de **À :** ou **De :**.

   L'écran **Définir les destinataires** ou **Définir les expéditeurs** s'affiche.
2. Choisissez l'une des options suivantes :
   - **Tout le monde** : sélectionnez cette option pour supprimer toute restriction sur les destinataires ou les expéditeurs.
   - **N'importe quelle adresse sélectionnée**
3. Si vous avez sélectionné **N'importe quelle adresse sélectionnée**, choisissez l'une des options suivantes dans la zone de liste :
   - **Saisir une adresse électronique** : saisissez l'adresse électronique à ajouter.

- **Rechercher des utilisateurs ou des groupes LDAP** : saisissez le nom de l'utilisateur ou du groupe LDAP et cliquez sur **Rechercher**. Les résultats s'affichent dans la liste.
- **Sélectionner des groupes d'adresses** : tous les groupes d'adresses existants s'affichent dans la liste.

Si vous sélectionnez un groupe LDAP en tant que destinataire ou expéditeur, vous pouvez utiliser des caractères génériques au début et/ou à la fin du groupe LDAP si vous avez spécifié Microsoft Active Directory ou Sun iPlanet Directory en tant que serveur LDAP. Pour plus d'informations, consultez la section Utilisation du caractère générique Astérisque.

4. Si vous ajoutez une adresse électronique, cliquez sur **Ajouter >**. Si vous ajoutez un utilisateur ou un groupe LDAP, ou un groupe d'adresses, sélectionnez-le dans la liste, puis cliquez sur **Ajouter >**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Suivant**.

   L'écran **Étape 3 : Sélectionner les modèles** s'affiche.

Configuration des exceptions

Vous pouvez configurer un chemin applicable à un large groupe d'expéditeurs ou de destinataires en dehors d'utilisateurs spécifiques auxquels la règle ne s'appliquera pas.

Procédure

1. Cliquez sur le lien situé en regard de l'intitulé **Exceptions**.

   L'écran **Définir les exceptions** s'affiche.
2. Sous **Sélectionner des adresses**, sélectionnez l'une des options suivantes pour les adresses d'origine et de destination :
   - **Saisir une adresse électronique** : saisissez l'adresse électronique à ajouter.

- **Rechercher des utilisateurs ou des groupes LDAP** : saisissez le nom de l'utilisateur ou du groupe LDAP et cliquez sur Rechercher. Les résultats s'affichent dans la liste.
- **Sélectionner des groupes d'adresses** : tous les groupes d'adresses existants s'affichent dans la liste.

3. Si vous ajoutez une adresse électronique, cliquez sur **Ajouter >**. Si vous ajoutez un élément LDAP ou un groupe d'adresses, sélectionnez-le dans la liste, puis cliquez sur **Ajouter >**.
4. Cliquez sur **Enregistrer**.

Utilisation du caractère générique Astérisque

Vous pouvez utiliser l'astérisque (*) comme caractère générique dans les adresses e-mail lors de la définition des chemins.

Les caractères génériques peuvent apparaître dans les sections du nom ou du domaine d'une adresse e-mail. Les exemples suivants sont valides :

- *@* : représentation valide de toutes les adresses e-mail.
- *@domaine.tld, nom@*.tld : représentation valide du nom complet ou du domaine (pas le domaine de niveau supérieur (TLD)).
- *@*.tld : représentation valide du nom et du domaine (pas le TLD).

Les caractères génériques ne peuvent pas apparaître dans un sous-domaine ou dans le domaine de niveau supérieur. Les caractères génériques ne peuvent pas être accompagnés d'autres lettres ; ils doivent être utilisés seuls. Les exemples suivants ne sont pas valides :

- nom@domaine.*.tld : représentation non valide d'un sous-domaine.
- nom@domaine.* : représentation non valide d'un TLD.
- nom@domaine.tld : utilisation non valide en conjonction avec un nom.

Étape 3 : Sélectionner les modèles

Les modèles empêchent vos actifs numériques de quitter le réseau de votre entreprise (par exemple, numéros de sécurité sociale et de cartes de crédit). Ils permettent aussi d'être en conformité avec la réglementation du gouvernement en ce qui concerne la confidentialité.

Procédure

1. Dans la liste Modèles disponibles, sélectionnez des modèles, puis cliquez sur **>>**.

   Appuyez sur la touche Ctrl et maintenez-la enfoncée en cliquant sur plusieurs modèles pour les sélectionner.

2. Cliquez sur **Suivant**.

   L'écran **Étape 4 : Sélectionner les actions** s'affiche.

Étape 4 : Sélectionner les actions

IMSVA exécute une ou plusieurs actions lorsqu'il détecte une tentative de transmission des actifs numériques.

Procédure

1. Choisissez l'une des actions suivantes :

   - **Mettre en quarantaine dans** : demande à IMSVA d'intercepter les messages et de les empêcher d'atteindre les destinataires.
   - **Envoyer des notifications** : demande à IMSVA d'envoyer une notification par e-mail à un ou plusieurs destinataires.

2. Si vous avez sélectionné **Envoyer des notifications**, sélectionnez le type de message de notification que vous voulez utiliser à partir de la liste déroulante.

   Les messages de notification disponibles dépendent des cibles que vous avez sélectionnées.

3. Cliquez sur **Terminer**.

Modification de règles IMSVA existantes

Procédure

1. Cliquez sur le nom de la règle à modifier.

   L'écran **Résumé** de la règle s'affiche.

2. Dans l'onglet **Règle**, cliquez sur **Modifier** pour **Si les destinataires et les expéditeurs sont**.

3. Configurez les paramètres d'acheminement.

   Pour plus d'informations, consultez la section *Étape 2 : Sélectionner les expéditeurs et les destinataires à la page 7-3*.

4. Cliquez sur **Modifier** pour **Et les conditions de scan correspondent**.

5. Configurez les paramètres du modèle.

6. Cliquez sur **Modifier** pour **L'action à lancer est alors**.

7. Configurez les paramètres de l'action.

   Remarque

   Si Trend Micro Control Manager ne parvient pas à se connecter aux cibles sélectionnées, certaines options d'action peuvent être indisponibles.

8. Cliquez sur **Enregistrer**.

Suppression de règles IMSVA

Procédure

1. Cochez la case située en regard de la règle à supprimer.
2. Cliquez sur **Supprimer**.

Chapitre 8

Paramètres de stratégie d'InterScan Web Security Suite

Cette section explique comment configurer les paramètres de stratégie d'InterScan Web Security Suite dans Control Manager.

Les rubriques sont les suivantes:

- *Liste des règles de prévention contre la perte de données à la page 8-2*

Liste des règles de prévention contre la perte de données

Lorsque vous activez l'option Prévention contre la perte de données, vous pouvez également activer ou désactiver chaque règle de prévention contre la perte de données. La coche verte indique que la règle est activée. La croix rouge indique que la règle est désactivée. Vous pouvez cliquer sur l'icône pour basculer entre l'état activé et désactivé.

Les options suivantes sont disponibles dans cet écran :

Règle : cliquez sur cette option pour modifier la règle.

Ajouter : ouvre l'écran **Ajouter une règle**, qui vous permet de configurer une nouvelle règle.

Copier : vous permet de copier une règle sélectionnée dans la liste.

Supprimer : vous permet de supprimer une règle dans la liste.

Priorité : cliquez sur la flèche pour modifier la priorité de la règle.

État : cliquez sur cette icône pour activer ou désactiver la règle.

Enregistrer : cliquez sur cette option pour enregistrer la règle.

Étape 1 : Définir le nom de la règle

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Activer** : sélectionnez cette option pour activer la règle.
- **Nom de la règle** : tapez un nom à afficher pour cette règle.
- **Suivant >** : cliquez pour continuer.

Étape 2 : Sélectionner des comptes

La section qui suit décrit brièvement les options disponibles dans cet écran.

Remarque

Certaines options ne sont pas disponibles lors de la création de projets de règle. Spécifiez un serveur afin d'activer toutes les options.

- Spécifiez les adresses IP des comptes s'appliquant à la règle.
  - Saisissez une plage IP dans les champs **De** et **À**, l'adresse IP ou le nom d'hôte d'un compte spécifique dans **Adresse IP/Nom d'hôte** ou un sous-réseau IP dans **Adresse** et **Longueur de préfixe**.
  - Cliquez sur **Ajouter** pour créer un ou plusieurs comptes dans le tableau de droite.
  - Cliquez sur **Supprimer** pour supprimer un ou plusieurs comptes dans le tableau de droite.
- **< Précédent** : cliquez pour revenir à la page précédente.
- **Suivant >** : cliquez pour continuer.

Étape 3 : Sélectionner le modèle de conformité à bloquer

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Spécifiez les modèles de conformité que vous souhaitez bloquer à l'aide de cette règle.**
  - **Modèle(s) disponible(s)** : les modèles listés peuvent être utilisés avec cette règle.
  - **Modèle(s) sélectionné(s) à bloquer** : la règle utilisée pour le blocage est appliquée aux modèles de cette liste.

    Conseil

    Sélectionnez plusieurs modèles à la fois en maintenant enfoncée la touche Maj ou Ctrl lorsque vous cliquez sur les noms des comptes.

  - **>>** : cliquez sur cette option pour ajouter des modèles disponibles à la liste des modèles sélectionnés.

- **<<** : cliquez sur cette option pour supprimer des modèles de la liste des modèles sélectionnés.

- **< Précédent** : cliquez pour revenir à la page précédente.
- **Suivant >** : cliquez pour continuer.

Étape 4 : Sélectionner les modèles de conformité à contrôler

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Spécifiez les modèles de conformité que vous souhaitez contrôler à l'aide de cette règle.**
  - **Modèle(s) disponible(s)** : les modèles listés peuvent être utilisés avec cette règle.
  - **Modèle(s) sélectionné(s) à contrôler** : la règle utilisée pour le contrôle est appliquée aux modèles de cette liste.

    Conseil

    Sélectionnez plusieurs modèles à la fois en maintenant enfoncée la touche Maj ou Ctrl lorsque vous cliquez sur les noms des comptes.

  - **>>** : cliquez sur cette option pour ajouter des modèles disponibles à la liste des modèles sélectionnés.
  - **<<** : cliquez sur cette option pour supprimer des modèles de la liste des modèles sélectionnés.
- **< Précédent** : cliquez pour revenir à la page précédente.
- **Terminer** : cliquez pour revenir à la liste des règles.

Chapitre 9

Paramètres de stratégie d'InterScan Web Security Virtual Appliance

Cette section explique comment configurer les paramètres de stratégie d'InterScan Web Security Virtual Appliance dans Control Manager.

Les rubriques sont les suivantes:

- *Liste des règles de prévention contre la perte de données à la page 9-2*

Liste des règles de prévention contre la perte de données

Lorsque vous activez l'option Prévention contre la perte de données, vous pouvez également activer ou désactiver chaque règle de prévention contre la perte de données. La coche verte indique que la règle est activée. La croix rouge indique que la règle est désactivée. Vous pouvez cliquer sur l'icône pour basculer entre l'état activé et désactivé.

Les options suivantes sont disponibles dans cet écran :

Règle : cliquez sur cette option pour modifier la règle.

Ajouter : ouvre l'écran **Ajouter une règle**, qui vous permet de configurer une nouvelle règle.

Copier : vous permet de copier une règle sélectionnée dans la liste.

Supprimer : vous permet de supprimer une règle dans la liste.

Priorité : cliquez sur la flèche pour modifier la priorité de la règle.

État : cliquez sur cette icône pour activer ou désactiver la règle.

Enregistrer : cliquez sur cette option pour enregistrer la règle.

Étape 1 : Définir le nom de la règle

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Activer** : sélectionnez cette option pour activer la règle.
- **Nom de la règle** : tapez un nom à afficher pour cette règle.
- **Suivant >** : cliquez pour continuer.

Étape 2 : Sélectionner des comptes

La section qui suit décrit brièvement les options disponibles dans cet écran.

Remarque

Certaines options ne sont pas disponibles lors de la création de projets de règle. Spécifiez un serveur afin d'activer toutes les options.

- Spécifiez les adresses IP des comptes s'appliquant à la règle.
  - Saisissez une plage IP dans les champs **De** et **À**, l'adresse IP ou le nom d'hôte d'un compte spécifique dans **Adresse IP/Nom d'hôte** ou un sous-réseau IP dans **Adresse** et **Longueur de préfixe**.
  - Cliquez sur **Ajouter** pour créer un ou plusieurs comptes dans le tableau de droite.
  - Cliquez sur **Supprimer** pour supprimer un ou plusieurs comptes dans le tableau de droite.
- **< Précédent** : cliquez pour revenir à la page précédente.
- **Suivant >** : cliquez pour continuer.

Étape 3 : Sélectionner le modèle de conformité à bloquer

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Spécifiez les modèles de conformité que vous souhaitez bloquer à l'aide de cette règle.**
  - **Modèle(s) disponible(s)** : les modèles listés peuvent être utilisés avec cette règle.
  - **Modèle(s) sélectionné(s) à bloquer** : la règle utilisée pour le blocage est appliquée aux modèles de cette liste.

Conseil

Sélectionnez plusieurs modèles à la fois en maintenant enfoncée la touche Maj ou Ctrl lorsque vous cliquez sur les noms des comptes.

  - **>>** : cliquez sur cette option pour ajouter des modèles disponibles à la liste des modèles sélectionnés.

- **<<** : cliquez sur cette option pour supprimer des modèles de la liste des modèles sélectionnés.

- **< Précédent** : cliquez pour revenir à la page précédente.
- **Suivant >** : cliquez pour continuer.

Étape 4 : Sélectionner les modèles de conformité à contrôler

La section qui suit décrit brièvement les options disponibles dans cet écran.

- **Spécifiez les modèles de conformité que vous souhaitez contrôler à l'aide de cette règle.**
  - **Modèle(s) disponible(s)** : les modèles listés peuvent être utilisés avec cette règle.
  - **Modèle(s) sélectionné(s) à contrôler** : la règle utilisée pour le contrôle est appliquée aux modèles de cette liste.

    Conseil

    Sélectionnez plusieurs modèles à la fois en maintenant enfoncée la touche Maj ou Ctrl lorsque vous cliquez sur les noms des comptes.

  - **>>** : cliquez sur cette option pour ajouter des modèles disponibles à la liste des modèles sélectionnés.
  - **<<** : cliquez sur cette option pour supprimer des modèles de la liste des modèles sélectionnés.
- **< Précédent** : cliquez pour revenir à la page précédente.
- **Terminer** : cliquez pour revenir à la liste des règles.

Partie V

Widgets Trend Micro Mobile Security

Chapitre 10

Widgets Mobile Security

Cette section contient des rubriques d'aide concernant tous les widgets Mobile Security qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *État de santé du dispositif Android à la page 10-4*
- *Widget Récapitulatif de l'état de chiffrement des dispositifs Android à la page 10-4*
- *Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs Android à la page 10-5*
- *Widget Récapitulatif de l'état de débridage des dispositifs Android à la page 10-5*
- *Widget État de sécurité du dispositif Android à la page 10-5*
- *Widget Récapitulatif de la recherche des programmes malveillants sous Android à la page 10-6*
- *Widget Récapitulatif de l'analyse des applications modifiées sous Android à la page 10-6*
- *Widget Récapitulatif de l'analyse de divulgation des données de confidentialité sous Android à la page 10-7*
- *Widget Récapitulatif de l'analyse de la vulnérabilité sous Android à la page 10-7*
- *Widget État de la mise à jour des composants à la page 10-8*
- *Widget Actualités de la cybersécurité pour dispositifs mobiles à la page 10-9*

- *Widget Récapitulatif de l'état de chiffrement des dispositifs iOS à la page 10-9*
- *Widget État de santé du dispositif iOS à la page 10-9*
- *Widget État de sécurité du dispositif iOS à la page 10-10*
- *Widget Récapitulatif de l'état de débridage des dispositifs iOS à la page 10-10*
- *Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs iOS à la page 10-11*
- *Widget Récapitulatif des recherches de programmes malveillants iOS à la page 10-11*
- *Widget Récapitulatif de l'état de contrôle des applications des dispositifs mobiles à la page 10-11*
- *Widget Récapitulatif de l'état de chiffrement des dispositifs mobiles à la page 10-12*
- *Widget État de santé du dispositif mobile à la page 10-12*
- *Widget Récapitulatif de l'état de débridage des dispositifs mobiles à la page 10-13*
- *Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs mobiles à la page 10-13*
- *Widget Récapitulatif du scan de ransomware sur les dispositifs mobiles à la page 10-14*
- *Widget État de sécurité du dispositif mobile à la page 10-14*
- *Widget Récapitulatif des distributeurs des dispositifs mobiles à la page 10-15*
- *Widget Récapitulatif de l'état de mise à jour des stratégies à la page 10-15*
- *Widget Récapitulatif de l'état de santé des composants du serveur à la page 10-15*
- *Widget Récapitulatif des entreprises de téléphonie à la page 10-16*
- *Widget Les 10 principales applications installées à la page 10-16*
- *Widget Cinq principaux logiciels de rançon Android détectés à la page 10-16*
- *Widget Cinq principaux sites Web bloqués à la page 10-17*
- *Cinq principaux logiciels de rançon iOS détectés à la page 10-17*
- *Widget Cinq principaux programmes malveillants détectés à la page 10-17*
- *Widget Récapitulatif de l'état de chiffrement des appareils Windows Phone à la page 10-17*

- *Widget État de santé du dispositif Windows Phone à la page 10-18*
- *Widget Récapitulatif de la version du système d'exploitation du dispositif Windows Phone à la page 10-18*

État de santé du dispositif Android

Ce widget affiche un récapitulatif de l'état de santé des dispositifs mobiles Android enregistrés.

Un état **Sain** indique que l'appareil mobile Android est inscrit sur le serveur d'administration Mobile Security et que tous les composants et stratégies présents sur l'appareil mobile Android sont à jour.

ÉTAT	DESCRIPTION
Sain	Nombre d'appareils mobiles Android sains
Douteux	Nombre d'appareils mobiles Android malsains

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de chiffrement des dispositifs Android

Ce widget affiche un récapitulatif de l'état de chiffrement des dispositifs mobiles Android enregistrés.

ÉTAT	DESCRIPTION
Codé	Nombre d'appareils mobiles Android chiffrés
Non chiffré	Nombre d'appareils mobiles Android non chiffrés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs Android

Ce widget affiche un récapitulatif des versions des systèmes d'exploitation installés sur les appareils mobiles Android enregistrés.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de débridage des dispositifs Android

Ce widget affiche un récapitulatif de l'état de débridage des dispositifs mobiles Android enregistrés.

ÉTAT	DESCRIPTION
Débridé	Nombre d'appareils mobiles débridés
Non débridé	Nombre d'appareils mobiles non débridés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de sécurité du dispositif Android

Ce widget affiche un récapitulatif de l'état de sécurité des dispositifs mobiles Android enregistrés.

- Non analysé
- Risqué

- Protégé
- Dangereux

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de la recherche des programmes malveillants sous Android

Ce widget affiche un récapitulatif des résultats de la recherche des programmes malveillants dans toutes les applications Android installées.

Le widget regroupe les résultats dans les catégories suivantes :

- Inconnu
- Objets potentiellement indésirables
- Normal
- Programmes malveillants

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'analyse des applications modifiées sous Android

Ce widget affiche un récapitulatif de l'analyse des applications modifiées dans toutes les applications Android installées.

Le widget regroupe les résultats dans les catégories suivantes :

- Inconnu
- Modifié

- Non modifiée

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'analyse de divulgation des données de confidentialité sous Android

Ce widget affiche un récapitulatif des résultats de l'analyse de la confidentialité dans toutes les applications Android installées.

Le widget regroupe les résultats dans les catégories suivantes :

- Inconnu
- Objets potentiellement indésirables
- Normal
- Programmes malveillants

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'analyse de la vulnérabilité sous Android

Ce widget affiche un récapitulatif des résultats de l'analyse de la vulnérabilité dans toutes les applications Android installées.

Le widget regroupe les résultats dans les catégories suivantes :

- Inconnu
- Normal

- Élevé
- Moyen

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de la mise à jour des composants

Ce widget affiche un récapitulatif de l'état de mise à jour des appareils mobiles enregistrés.

COLONNE	DESCRIPTION
Version actuelle	Numéro de version actuelle de Mobile Device Agent ou des composants sur le serveur d'administration Mobile Security
À jour	Nombre d'appareils mobiles pour lesquels les versions de Mobile Device Agent ou des composants sont à jour
Obsolète	Nombre d'appareils mobiles utilisant des composants obsolètes
Fréquence de mise à jour	Pourcentage d'appareils mobiles qui utilisent les versions des composants les plus récentes
Mis à niveau	Nombre d'appareils mobiles qui utilisent les versions de Mobile Device Agent les plus récentes
Non mis à niveau	Nombre d'appareils mobiles qui n'ont pas été mis à niveau pour utiliser les dernières versions de Mobile Device Agent
Fréquence de mise à niveau	Pourcentage d'appareils mobiles utilisant les agents Mobile Device Agent les plus récents

Widget Actualités de la cybersécurité pour dispositifs mobiles

Ce widget affiche les informations de cybersécurité liées aux appareils mobiles et publiées par Trend Micro. .

Widget Récapitulatif de l'état de chiffrement des dispositifs iOS

Ce widget affiche un récapitulatif de l'état de chiffrement des dispositifs mobiles iOS enregistrés.

ÉTAT	DESCRIPTION
Codé	Nombre d'appareils mobiles iOS chiffrés
Non chiffré	Nombre d'appareils mobiles iOS non chiffrés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de santé du dispositif iOS

Ce widget affiche un récapitulatif de l'état de santé des dispositifs mobiles iOS enregistrés.

Un état **Sain** indique que l'appareil mobile iOS est inscrit sur le serveur d'administration Mobile Security et que tous les composants et stratégies présents sur l'appareil mobile iOS sont à jour.

ÉTAT	DESCRIPTION
Sain	Nombre d'appareils mobiles iOS sains

ÉTAT	DESCRIPTION
Douteux	Nombre d'appareils mobiles iOS malsains

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de sécurité du dispositif iOS

Ce widget affiche un récapitulatif de l'état de sécurité des dispositifs mobiles iOS enregistrés.

- Non analysé
- Risqué
- Protégé
- Dangereux

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de débridage des dispositifs iOS

Ce widget affiche un récapitulatif de l'état de débridage des dispositifs mobiles iOS enregistrés.

ÉTAT	DESCRIPTION
Débridé	Nombre d'appareils mobiles débridés
Non débridé	Nombre d'appareils mobiles non débridés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs iOS

Ce widget affiche un récapitulatif des versions des systèmes d'exploitation installés sur les appareils mobiles iOS enregistrés.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif des recherches de programmes malveillants iOS

Ce widget affiche un récapitulatif des résultats de la recherche de programmes malveillants dans toutes les applications iOS installées.

Le widget regroupe les résultats dans les catégories suivantes :

- Inconnu
- Programmes malveillants
- Normal

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de contrôle des applications des dispositifs mobiles

Ce widget affiche un récapitulatif de l'état de contrôle des applications des appareils mobiles enregistrés.

ÉTAT	DESCRIPTION
Conforme	Nombre d'appareils mobiles qui respectent la stratégie de conformité et de contrôle d'application Mobile Security
Non conforme	Nombre d'appareils mobiles qui ne respectent pas la stratégie de conformité et de contrôle d'application Mobile Security

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de chiffrement des dispositifs mobiles

Ce widget affiche un récapitulatif de l'état de chiffrement des dispositifs mobiles enregistrés.

ÉTAT	DESCRIPTION
Codé	Nombre d'appareils mobiles chiffrés
Non chiffré	Nombre d'appareils mobiles non chiffrés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de santé du dispositif mobile

Ce widget affiche un récapitulatif de l'état de santé des dispositifs mobiles enregistrés.

ÉTAT	DESCRIPTION
Sain	Le dispositif est inscrit sur le serveur d'administration Mobile Security et les composants et stratégies présents sur l'appareil mobile sont à jour

État	Description
Non conforme	Le dispositif est inscrit sur le serveur d'administration Mobile Security, mais ne respecte pas les stratégies du serveur
Désynchronisé	Le dispositif est inscrit sur le serveur d'administration Mobile Security, mais les composants ou les stratégies sont obsolètes
Inactif	Le dispositif n'est pas encore inscrit sur le serveur d'administration Mobile Security

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de débridage des dispositifs mobiles

Ce widget affiche un récapitulatif de l'état de débridage des dispositifs mobiles enregistrés.

État	Description
Débridé	Nombre d'appareils mobiles débridés
Non débridé	Nombre d'appareils mobiles non débridés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif des versions des systèmes d'exploitation des dispositifs mobiles

Ce widget affiche un récapitulatif des versions des systèmes d'exploitation installés sur les appareils mobiles enregistrés.

SYSTÈME D'EXPLOITATION	DESCRIPTION
Android	Nombre d'appareils mobiles Android enregistrés
iOS	Nombre d'appareils mobiles iOS enregistrés
Windows Phone	Nombre d'appareils mobiles Windows Phone enregistrés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif du scan de ransomware sur les dispositifs mobiles

Ce widget affiche un récapitulatif des résultats de la recherche des logiciels de rançon dans toutes les applications installées.

Le widget regroupe les résultats par système d'exploitation mobile.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de sécurité du dispositif mobile

Ce widget affiche un récapitulatif de l'état de sécurité des dispositifs mobiles enregistrés.

- Non analysé
- Risqué
- Protégé
- Dangereux

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif des distributeurs des dispositifs mobiles

Ce widget affiche un récapitulatif des fournisseurs des appareils mobiles enregistrés.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de mise à jour des stratégies

Ce widget affiche un récapitulatif de l'état de mise à jour des stratégies des appareils mobiles enregistrés.

ÉTAT	DESCRIPTION
À jour	Nombre d'appareils mobiles s'exécutant avec une version ou des composants mis à jour de l'agent Mobile Device Agent
Obsolète	Nombre d'appareils mobiles s'exécutant avec des composants obsolètes

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de santé des composants du serveur

Ce widget affiche l'état de mise à jour des composants du serveur, ainsi que les numéros de version respectifs.

COLONNE	DESCRIPTION
Serveur	Nom du module

COLONNE	DESCRIPTION
Adresse	Nom de domaine ou adresse IP de l'ordinateur hébergeant le module
Version actuelle	Numéro de version des modules du serveur d'administration Mobile Security installés
Dernière mise à jour	Heure et date de la dernière mise à jour

Widget Récapitulatif des entreprises de téléphonie

Ce widget affiche un récapitulatif des entreprises de téléphonie utilisées par les appareils mobiles Android enregistrés.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Les 10 principales applications installées

Ce widget affiche la liste des dix principales applications installées sur les dispositifs mobiles enregistrés. Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Cinq principaux logiciels de rançon Android détectés

Ce widget affiche la liste des cinq principaux ransomwares Android détectés par Mobile Security, en fonction du nombre de fois où le ransomware spécifié a été détecté.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Cinq principaux sites Web bloqués

Ce widget affiche la liste des cinq principaux sites Web bloqués par Mobile Security, en fonction du nombre d'accès à chacun des sites. Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Cinq principaux logiciels de rançon iOS détectés

Ce widget affiche la liste des cinq principaux ransomware détectés par Mobile Security, en fonction du nombre de fois où le ransomware spécifié a été détecté. Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Cinq principaux programmes malveillants détectés

Ce widget affiche la liste des principaux programmes malveillants détectés par Mobile Security, en fonction du nombre de fois où le programme malveillant spécifié a été détecté. Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de l'état de chiffrement des appareils Windows Phone

Ce widget affiche un récapitulatif de l'état de chiffrement des dispositifs mobiles Windows Phone enregistrés.

ÉTAT	DESCRIPTION
Codé	Nombre d'appareils mobiles Windows Phone chiffrés
Non chiffré	Nombre d'appareils mobiles Windows Phone non chiffrés

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget État de santé du dispositif Windows Phone

Ce widget affiche un récapitulatif de l'état de santé des appareils mobiles Windows Phone enregistrés.

Un état **Sain** indique que l'appareil mobile Windows Phone est inscrit sur le serveur d'administration Mobile Security et que tous les composants et stratégies présents sur l'appareil mobile Windows Phone sont à jour.

ÉTAT	DESCRIPTION
Sain	Nombre d'appareils mobiles Windows Phone sains
Douteux	Nombre d'appareils mobiles Windows Phone malsains

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Widget Récapitulatif de la version du système d'exploitation du dispositif Windows Phone

Ce widget affiche un récapitulatif des versions du système d'exploitation installé sur les appareils mobiles Windows Phone enregistrés.

Sélectionnez **Tout** ou le nom du groupe dans la liste déroulante pour afficher les informations des appareils concernés.

Chapitre 11

Stratégies de sécurité dans Trend Micro Mobile Security

Cette section présente les stratégies de sécurité disponibles dans Mobile Security.

À l'aide du compte de super-utilisateur, vous pouvez spécifier une stratégie pour qu'elle serve de modèle aux administrateurs de groupes lors de la création d'autres stratégies de sécurité dans Mobile Security. Cependant, une fois qu'une stratégie de sécurité est définie comme modèle, vous ne pouvez plus l'attribuer à un groupe.

Protection des dispositifs avec des stratégies

Vous pouvez configurer les stratégies de sécurité pour un groupe Mobile Security sur le serveur d'administration. Ces stratégies s'appliquent à tous les appareils mobiles du groupe. Vous pouvez appliquer des stratégies de sécurité à tous les groupes Mobile Security en sélectionnant le groupe **Appareils mobiles** (groupe racine). Le tableau suivant répertorie les stratégies de sécurité disponibles dans Mobile Security.

TABLEAU 11-1. Stratégies de sécurité dans Mobile Security

GROUPE DE STRATÉGIES	STRATÉGIE	RÉFÉRENCES
Généralités	Stratégie commune	Pour le mode de déploiement de la version complète, voir *Stratégie commune en mode de déploiement de la version complète à la page 11-5*. Pour le mode de déploiement du scan de sécurité, voir *Stratégie commune en mode de déploiement du scan de sécurité à la page 11-6*.

Groupe de stratégies	Stratégie	Références
Approvisionnement	Stratégie WiFi	Consultez la section *Stratégie WiFi à la page 11-7*.
	Stratégie Exchange ActiveSync	Consultez la section *Stratégie Exchange ActiveSync à la page 11-7*.
	Stratégie des certificats	Consultez la section *Stratégie des certificats à la page 11-7*.
	Stratégie VPN	Consultez la section *Stratégie VPN à la page 11-7*.
	Stratégie du proxy HTTP global	Consultez la section *Stratégie du proxy HTTP global à la page 11-8*.
	Stratégie d'authentification unique	Consultez la section *Stratégie d'authentification unique à la page 11-8*.
	Stratégie de réseau cellulaire	Voir *Stratégie de réseau cellulaire à la page 11-9*
	Stratégie AirPlay/AirPrint	Voir *Stratégie AirPlay/AirPrint à la page 11-9*
	Stratégie de thème	Voir *Stratégie de thème à la page 11-9*.
	Stratégie de domaines gérés	Consultez la section *Stratégie de domaines gérés à la page 11-10*.

GROUPE DE STRATÉGIES	STRATÉGIE	RÉFÉRENCES
Sécurité du dispositif	Stratégie de sécurité	Pour la stratégie de sécurité en mode de déploiement de la version complète, voir *Stratégie de sécurité en mode de déploiement de la version complète à la page 11-11*. Pour la stratégie de sécurité en mode de déploiement du scan de sécurité, voir *Stratégie de sécurité en mode de déploiement du scan de sécurité à la page 11-14*.
	Stratégie de prévention anti-spam	Consultez la section *Stratégie de prévention anti-spam à la page 11-16*.
	Stratégie de filtrage des appels	Consultez la section *Stratégie de filtrage des appels à la page 11-19*.
	Stratégie de protection contre les menaces Internet	Consultez la section *Stratégie de protection contre les menaces Internet à la page 11-21*.
Périphériques	Stratégie de mot de passe	Consultez la section *Stratégie de mot de passe à la page 11-24*.
	Stratégie de verrouillage des fonctions	Consultez la section *Stratégie de verrouillage des fonctions à la page 11-24*.
	Stratégie de conformité	Consultez la section *Stratégie de conformité à la page 11-35*.

GROUPE DE STRATÉGIES	STRATÉGIE	RÉFÉRENCES
Gestion des applications	Stratégie de surveillance et de contrôle des applications	Consultez la section *Stratégie Surveillance et contrôle des applications à la page 11-36*.
	Stratégie du programme d'achats en grande quantité	Consultez la section *Stratégie du programme d'achats en grande quantité à la page 11-38*.
Samsung KNOX	Stratégie de conteneur	Voir *Stratégie de conteneur à la page 11-41*.

Stratégie commune en mode de déploiement de la version complète

La stratégie commune contient les stratégies de sécurité communes destinées aux dispositifs mobiles. Pour configurer les paramètres de la stratégie de sécurité commune, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie commune**.

- **Privilèges utilisateur** : vous pouvez activer ou désactiver la fonction qui permet aux utilisateurs de désinstaller Mobile Device Agent. Vous pouvez également décider d'autoriser ou non les utilisateurs à configurer les paramètres de l'agent de dispositif Mobile Security.

  Voici la liste des fonctions associées à la désinstallation de la protection :

  - Il est possible d'activer et de désactiver la fonction de désinstallation de la protection depuis la console d'administration.
  - Le mot de passe doit contenir entre 6 et 12 caractères, et peut inclure des chiffres, des caractères et des symboles.
  - Le mot de passe peut se définir pour chaque groupe depuis la console d'administration.

  Vous devez cocher la case **Autoriser les utilisateurs à configurer les paramètres du client Mobile Security** pour que les utilisateurs soient en mesure de modifier les paramètres de Mobile Device Agent. L'activation de cette case n'a aucune influence sur les listes de filtrage définies pour la **stratégie de prévention anti-**

spam, la **stratégie de filtrage des appels** et la **stratégie de protection contre les menaces Internet**. Pour plus d'informations, consultez *Stratégie de prévention anti-spam à la page 11-16*, *Stratégie de filtrage des appels à la page 11-19* et *Stratégie de protection contre les menaces Internet à la page 11-21*.

- **Paramètres de mise à jour** : vous pouvez configurer le serveur d'administration Mobile Security de manière à informer les agents Mobile Device Agent dès que la mise à jour d'un composant est disponible ou sélectionner l'option de vérification automatique, auquel cas les agents Mobile Device Agent vérifient régulièrement sur le serveur d'administration Mobile Security s'il existe des mises à jour de composant ou de configuration.

- **Paramètres de journaux** : lorsque des agents Mobile Device Agent détectent un risque de sécurité, comme un programme malveillant dans un système d'exploitation Android, un journal est généré sur les appareils mobiles.

Stratégie commune en mode de déploiement du scan de sécurité

La stratégie commune contient les stratégies de sécurité communes destinées aux dispositifs mobiles. Pour configurer les paramètres de la stratégie de sécurité commune, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie commune**.

- **Privilèges utilisateur** :

  - Vous pouvez décider d'autoriser ou non les utilisateurs à configurer les paramètres d'agent du dispositif Mobile Security.

    Vous devez cocher la case **Autoriser les utilisateurs à configurer les paramètres du client Mobile Security** pour que les utilisateurs soient en mesure de modifier les paramètres de Mobile Device Agent. L'activation de cette case n'a cependant aucune influence sur les listes de filtrage définies pour la **stratégie de protection contre les menaces Internet**. Pour plus d'informations, consultez la section *Stratégie de protection contre les menaces Internet à la page 11-21*.

  - Vous pouvez sélectionner l'option de vérification automatique de sorte que les agents Mobile Device Agent vérifient régulièrement sur le serveur

d'administration Mobile Security s'il existe des mises à jour de composant ou de configuration.

Stratégie WiFi

La stratégie Wi-Fi vous permet d'envoyer aux dispositifs mobiles Android et iOS les données du réseau Wi-Fi de votre organisation, y compris le nom du réseau, le type de sécurité et le mot de passe.

Pour configurer les paramètres de la stratégie Wi-Fi, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie Wi-Fi**.

Stratégie Exchange ActiveSync

La stratégie Exchange ActiveSync vous permet de créer pour votre organisation une stratégie de type Exchange ActiveSync qui sera livrée aux périphériques mobiles iOS.

Pour configurer les paramètres de la stratégie Exchange ActiveSync, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie Exchange ActiveSync**.

Stratégie des certificats

La stratégie de certificat vous permet d'importer les certificats que vous devez déployer sur les périphériques mobiles iOS.

Pour configurer les paramètres de la stratégie de certificat, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de certificat**.

Stratégie VPN

Les paramètres de stratégie VPN vous permettent de créer une stratégie VPN pour votre organisation et de l'appliquer aux appareils mobiles iOS.

Pour configurer les paramètres de la stratégie VPN, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie VPN**.

Stratégie du proxy HTTP global

La stratégie du proxy HTTP global vous permet de fournir des informations sur le proxy de votre organisation aux dispositifs mobiles. Cette stratégie s'applique uniquement aux dispositifs mobiles iOS en mode Surveillé.

Pour configurer les paramètres de la stratégie du proxy HTTP global, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie du proxy HTTP global**.

Stratégie d'authentification unique

La stratégie de fonction d'authentification unique (SSO) permet l'utilisation des mêmes informations d'authentification sur plusieurs applications, y compris Mobile Security et les applications de l'App Store. Chaque fois que vous configurez une nouvelle application pour la fonction d'authentification unique (SSO), les autorisations de l'utilisateur aux ressources de l'entreprise sont vérifiées, et l'utilisateur est connecté à cette application sans devoir entrer de nouveau son mot de passe.

La stratégie de fonction d'authentification unique inclut les informations suivantes :

- **Nom** : le nom principal Kerberos.
- **Zone** : le nom de la zone Kerberos.

  L'usage des majuscules dans le nom de la zone doit être conforme.

- **Préfixes d'URL** (facultatif) : liste des adresses URL qui doivent correspondre pour l'authentification Kerberos via HTTP à l'aide d'un compte. Si ce champ est vide, toutes les adresses URL http et https peuvent s'appliquer au compte en question. Les modèles de concordance d'URL doivent commencer par http ou par https.

  Un préfixe URL doit être ajouté à chacun des éléments de cette liste. Seules les adresses URL commençant par l'une des chaînes d'un compte peuvent accéder au ticket Kerberos. Les modèles de concordance d'URL doivent inclure le schéma. Par exemple, http://www.exemple.com/. Si un modèle de concordance ne termine pas par le symbole /, ce symbole est automatiquement ajouté à l'adresse URL.

- **Identifiants d'application** (facultatif) : liste des identifiants d'application autorisés à utiliser le compte. Si ce champ est vide, tous les identifiants d'application peuvent s'appliquer au compte en question

Parmi les **identifiants d'application**, certains doivent correspondre à des identifiants de paquets d'application, soit sous forme de correspondance exacte (par exemple, com.monentreprise.monapp), soit en indiquant à l'aide du caractère générique * un préfixe qui doit correspondre dans l'identifiant de paquet. Le caractère générique doit être précédé d'un point (.) et être placé à la fin de la chaîne (par exemple, com.monentreprise.*). Lorsqu'un caractère générique est utilisé, toute application dont l'identifiant de paquet commence par le préfixe peut accéder au compte.

Pour configurer les paramètres de la stratégie d'authentification unique pour iOS, cliquez sur **Stratégies**, puis sur le nom de la stratégie, et enfin sur **Stratégie d'authentification unique**.

Stratégie de réseau cellulaire

Les paramètres de stratégie de réseau cellulaire vous permettent de configurer pour votre organisation des paramètres de réseau cellulaire qui seront envoyés aux appareils mobiles iOS.

Pour configurer les paramètres de stratégie de réseau cellulaire, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de réseau cellulaire**.

Stratégie AirPlay/AirPrint

Les paramètres de stratégie AirPlay/AirPrint vous permettent de créer pour votre organisation des stratégies de type AirPlay et AirPrint qui seront envoyées aux appareils mobiles iOS.

Pour configurer les paramètres de stratégie AirPlay ou AirPrint, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie AirPlay/AirPrint**.

Stratégie de thème

Les paramètres de stratégie de thème vous permettent de transmettre une police et de définir un papier peint pour l'écran d'accueil et l'écran de verrouillage des appareils mobiles iOS. Cette stratégie s'applique uniquement aux appareils mobiles iOS en mode Surveillé.

Pour configurer les paramètres de la stratégie de thème, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de thème**.

Stratégie de domaines gérés

La stratégie de domaines gérés vous permet de configurer les domaines de messagerie et/ou Web que votre organisation gère.

- Domaines de messagerie non marqués : lorsqu'un utilisateur rédige un courrier électronique à l'aide du client de messagerie du système, toute adresse électronique saisie qui ne correspond pas aux domaines configurés est surlignée (marquée) en rouge. Il est recommandé aux administrateurs d'utiliser cette fonctionnalité afin d'alerter les utilisateurs qui, par inadvertance, tenteraient d'envoyer des informations sensibles à des adresses électroniques non approuvées.

- Domaines Web Safari gérés : vous pouvez configurer le système de sorte que les fichiers téléchargés à partir de domaines spécifiques à l'aide de Safari puissent uniquement être ouverts avec des applications gérées. Par exemple, un PDF téléchargé à partir du domaine internal.example.com pourra être ouvert avec Adobe Reader (application gérée), mais pas avec Dropbox (application non gérée). Cela améliore la conteneurisation de Safari et élargit l'utilisation en tant que navigateur d'entreprise.

Important

Vous devez désactiver les fonctions iOS suivantes dans la stratégie de verrouillage des fonctions. Dans le cas contraire, les paramètres de domaines Web Safari gérés n'auront aucun effet, étant donné que les fichiers téléchargés pourront être ouverts avec d'autres applications (non gérées) :

- Ouvrir des documents d'applications gérées dans d'autres applications (version 7.0 ou supérieure)
- Ouvrir des documents d'autres applications dans des applications gérées (version 7.0 ou supérieure)

Pour configurer les paramètres de la stratégie de domaines gérés, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de domaines gérés**.

Stratégie de sécurité en mode de déploiement de la version complète

Vous pouvez configurer les **Paramètres de sécurité** depuis l'écran **Stratégie de sécurité**.

Pour configurer les paramètres de la stratégie de protection de la sécurité, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de sécurité**.

Le tableau suivant décrit les paramètres disponibles pour cette stratégie.

TABLEAU 11-2. Paramètres de la stratégie de sécurité

SECTION	ÉLÉMENT	DESCRIPTION	SYSTÈMES D'EXPLOITATION D'APPAREILS MOBILES PRIS EN CHARGE
Paramètres de sécurité	**Analyser uniquement les applications installées**	Sélectionnez cette option si vous souhaitez scanner uniquement les applications installées	
	Analyser les applications installées et les fichiers	Sélectionnez cette option si vous souhaitez scanner les applications installées et les autres fichiers enregistrés sur l'appareil mobile. Si vous sélectionnez cette option, indiquez si vous souhaitez scanner uniquement les fichiers APK ou tous les fichiers.	

SECTION	ÉLÉMENT	DESCRIPTION	SYSTÈMES D'EXPLOITATION D'APPAREILS MOBILES PRIS EN CHARGE
	Analyser après mise à jour des signatures	Activez cette option si vous souhaitez exécuter le scan anti-programmes malveillants après chaque mise à jour de fichier de signatures. Mobile Security exécute automatiquement un scan après une mise à jour correcte des fichiers de signatures sur les appareils mobiles Android.	
	Activer l'analyse de Facebook	Activez cette option pour scanner les paramètres de confidentialité de Facebook.	

SECTION	ÉLÉMENT	DESCRIPTION	SYSTÈMES D'EXPLOITATION D'APPAREILS MOBILES PRIS EN CHARGE
		Remarque L'activation du **Scan de Facebook** permet aux utilisateurs de protéger leurs informations et de s'assurer qu'ils partagent uniquement des données avec des personnes en lesquelles ils ont confiance.	
Planification d'analyse	**Quotidien**	Le scan s'exécute chaque jour selon l'**Heure de début** spécifiée.	
	Hebdomadaire	Le scan s'exécute une fois par semaine selon le jour et l'**Heure de début** spécifiés.	
	Mensuel	Le scan s'exécute une fois par mois selon le jour et l'**Heure de début** spécifiés.	

Stratégie de sécurité en mode de déploiement du scan de sécurité

Vous pouvez configurer les **Paramètres de sécurité** depuis l'écran **Stratégie de sécurité**.

Pour configurer les paramètres de la stratégie de protection de la sécurité, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de sécurité**.

Le tableau suivant décrit les paramètres disponibles pour cette stratégie.

TABLEAU 11-3. Paramètres de la stratégie de sécurité

SECTION	ÉLÉMENT	DESCRIPTION	SYSTÈMES D'EXPLOITATION D'APPAREILS MOBILES PRIS EN CHARGE
Paramètres de sécurité	**Analyser uniquement les applications installées**	Sélectionnez cette option si vous souhaitez scanner uniquement les applications installées	
	Analyser les applications installées et les fichiers	Sélectionnez cette option si vous souhaitez scanner les applications installées et les autres fichiers enregistrés sur l'appareil mobile. Si vous sélectionnez cette option, indiquez si vous souhaitez scanner uniquement les fichiers APK ou tous les fichiers.	

SECTION	ÉLÉMENT	DESCRIPTION	SYSTÈMES D'EXPLOITATION D'APPAREILS MOBILES PRIS EN CHARGE
	Analyser après mise à jour des signatures	Activez cette option si vous souhaitez exécuter le scan anti-programmes malveillants après chaque mise à jour de fichier de signatures. Mobile Security exécute automatiquement un scan après une mise à jour correcte des fichiers de signatures sur les appareils mobiles Android.	
Planification d'analyse	**Quotidien**	Le scan s'exécute chaque jour selon l'**Heure de début** spécifiée.	
	Hebdomadaire	Le scan s'exécute une fois par semaine selon le jour et l'**Heure de début** spécifiés.	
	Mensuel	Le scan s'exécute une fois par mois selon le jour et l'**Heure de début** spécifiés.	

Stratégie de prévention anti-spam

La stratégie de prévention anti-spam de Mobile Security protège contre le spam de type WAP Push et les messages SMS.

Pour configurer les paramètres de la stratégie de prévention anti-spam, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de prévention anti-spam**.

Stratégies de prévention anti-spam par SMS

Cette fonction vous permet de contrôler les stratégies de prévention anti-spam SMS depuis le serveur. Voici les fonctions disponibles lors de la configuration des stratégies de prévention anti-spam SMS :

- Activation ou désactivation de la prévention anti-spam SMS pour les dispositifs mobiles.
- Mise en place de l'utilisation d'une liste bloquée ou d'une liste approuvée par le dispositif mobile ou désactivation de la protection anti-spam SMS sur le dispositif.
- Définition d'une liste approuvée depuis la console d'administration.
- Définition d'une liste bloquée depuis la console d'administration.

Consultez le tableau suivant pour obtenir des informations détaillées sur la configuration des listes bloquée ou approuvée pour le filtrage.

TABLEAU 11-4. Configuration des listes pour le filtrage relatives à la stratégie de prévention anti-spam SMS

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Désactivé	Activé	L'utilisateur peut modifier la liste approuvée/ bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les messages selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Désactivé	L'utilisateur peut uniquement modifier la liste approuvée et la liste bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les messages selon la priorité suivante : 1. Liste approuvée ou liste bloquée sur le serveur 2. Liste approuvée sur Mobile Device Agent 3. Liste bloquée sur Mobile Device Agent
Activé	Activé	L'utilisateur peut à la fois afficher et modifier la liste approuvée/bloquée définie par l'administrateur. Il peut aussi utiliser cette liste sur Mobile Device Agent. Lorsque les stratégies de sécurité se synchronisent avec Mobile Device Agent, les listes pour le filtrage ne sont pas synchronisées et toutes les autres fonctions sont mises à jour en fonction des stratégies. Mobile Security autorise ou bloque les messages selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent 3. Liste approuvée ou liste bloquée sur le serveur

Remarque

Le format de la liste approuvée et de la liste bloquée pour les SMS doit être le suivant : « [nom1:]numéro1;[nom2:]numéro2;... ».

La longueur de l'élément « nom » ne doit pas dépasser 30 caractères ; celle de l'élément « numéro de téléphone » doit comporter entre 4 et 20 caractères et peut contenir les élément suivants : chiffres entre 0 et 9, signe +, signe -, signe #, signe (, signe) et espaces. Le nombre maximal d'entrées ne doit pas dépasser 200.

Stratégie de prévention anti-spam WAP Push

Cette fonction vous permet de contrôler la prévention WAP Push depuis le serveur. Lorsqu'elle est activée, vous pouvez décider d'utiliser ou pas une liste approuvée WAP.

Remarque

Le format de la liste approuvée WAP doit être le suivant : « [nom1:]numéro1; [nom2:]numéro2;... ».

La longueur de l'élément « nom » ne doit pas dépasser 30 caractères ; celle de l'élément « numéro de téléphone » doit comporter entre 4 et 20 caractères et peut contenir les élément suivants : chiffres entre 0 et 9, signe +, signe -, signe #, signe (, signe) et espaces. Le nombre maximal d'entrées ne doit pas dépasser 200.

La liste suivante présente les fonctions disponibles lors de la configuration de stratégies de prévention WAP Push :

- Activation ou désactivation de la prévention WAP Push pour l'appareil mobile
- Configuration de l'appareil mobile pour utiliser une liste approuvée ou désactivation de la prévention WAP Push sur l'appareil mobile
- Définition d'une liste approuvée depuis la console d'administration.
- Si l'administrateur a activé le contrôle côté serveur, l'utilisateur ne sera pas en mesure de modifier le type de prévention WAP Push défini par l'administrateur
- Si l'administrateur a désactivé le contrôle côté serveur, et a autorisé les utilisateurs à configurer les paramètres de Mobile Security sur leur appareil mobile, l'utilisateur ne sera pas en mesure d'afficher ou de modifier la liste de prévention WAP Push configurée par l'administrateur. Il pourra toutefois modifier la liste personnelle de prévention WAP Push du côté de l'appareil mobile

Remarque

Lorsque la stratégie de prévention anti-spam est appliquée aux agents Mobile Device Agent, les paramètres personnels de l'utilisateur concernant les messages de spam sont effacés.

Stratégie de filtrage des appels

Cette fonction vous permet de contrôler les stratégies de filtrage des appels depuis le serveur. Pour configurer les paramètres de la stratégie de filtrage des appels, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de filtrage**.

Voici les fonctions disponibles lors de la configuration des stratégies de filtrage des appels :

- Activation ou désactivation du filtrage des appels pour les périphériques mobiles.
- Configuration du dispositif mobile de manière à utiliser une liste bloquée ou approuvée.
- Définition d'une liste approuvée depuis la console d'administration.
- Définition d'une liste bloquée depuis la console d'administration.

Consultez le tableau suivant pour obtenir des informations détaillées sur la configuration des listes bloquée ou approuvée pour le filtrage.

TABLEAU 11-5. Configuration des listes pour le filtrage relatives à la stratégie de filtrage des appels

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Désactivé	Activé	L'utilisateur peut modifier la liste approuvée/ bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les adresses URL selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Désactivé	L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les appels entrants selon la priorité suivante : 1. Liste bloquée sur le serveur 2. Liste approuvée sur Mobile Device Agent 3. Liste bloquée sur Mobile Device Agent Vous pouvez également configurer un contrôle sur le serveur pour les appels sortants émis depuis les périphériques mobiles Android.
Activé	Activé	L'utilisateur peut à la fois afficher et modifier la liste approuvée/bloquée définie par l'administrateur. Il peut aussi utiliser cette liste sur Mobile Device Agent. Lorsque les stratégies de sécurité se synchronisent avec Mobile Device Agent, les listes pour le filtrage ne sont pas synchronisées et toutes les autres fonctions sont mises à jour en fonction des stratégies. Mobile Security autorise ou bloque les appels entrants selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent 3. Liste bloquée sur le serveur Vous pouvez également configurer un contrôle sur le serveur pour les appels sortants émis depuis les périphériques mobiles Android.

Remarque

Le format des listes approuvée/bloquée pour le filtrage des appels doit être le suivant : « [nom1:]numéro1;[nom2:]numéro2;... ».

La longueur de l'élément « nom » ne doit pas dépasser 30 caractères ; celle de l'élément « numéro de téléphone » doit comporter entre 4 et 20 caractères et peut contenir les élément suivants : chiffres entre 0 et 9, signe +, signe -, signe #, signe (, signe) et espaces. Le nombre maximal d'entrées ne doit pas dépasser 200.

Stratégie de protection contre les menaces Internet

Gérez la stratégie de protection contre les menaces Web depuis le serveur d'administration Mobile Security et déployez-la sur les appareils mobiles Android et iOS. Vous pouvez aussi faire en sorte que les dispositifs mobiles Android envoient au serveur le journal issu de la protection contre les menaces Web.

Remarque

La protection contre les menaces Web de Mobile Security est uniquement prise en charge par le navigateur par défaut Android et Google Chrome.

Pour configurer les paramètres de la stratégie de protection contre les menaces Web, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de protection contre les menaces Web**.

Protection contre les menaces Web pour les dispositifs mobiles Android

La fonction Protection contre les menaces Web vous permet de contrôler depuis le serveur les stratégies de protection contre les menaces Web des dispositifs mobiles Android. Elle propose trois niveaux de sécurité prédéfinis : **Faible**, **Normal** et **Élevé**. Elle contient également des listes approuvées et bloquées pour bloquer ou autoriser certaines URL. Mobile Security bloquera toutes les URL que vous ajoutez dans la liste bloquée, et autorisera toutes les URL se trouvant dans la liste approuvée.

Remarque

Sur les dispositifs mobiles, la stratégie de protection contre les menaces Web prend en charge uniquement Google Chrome et le navigateur Web par défaut d'Android.

Consultez le tableau suivant pour obtenir des informations détaillées sur la configuration des listes bloquée ou approuvée pour le filtrage.

TABLEAU 11-6. Configuration des listes pour le filtrage relatives à la stratégie de protection contre les menaces Web

CONTRÔLE SERVEUR	CONTRÔLE UTILISATEUR	DESCRIPTION
Désactivé	Activé	L'utilisateur peut modifier la liste approuvée/bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les adresses URL selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent
Activé	Désactivé	L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur Mobile Device Agent. Mobile Security autorise ou bloque les adresses URL selon la priorité suivante : 1. Liste approuvée sur le serveur 2. Liste bloquée sur le serveur 3. Liste approuvée sur Mobile Device Agent 4. Liste bloquée sur Mobile Device Agent

CONTRÔLE SERVEUR	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Activé	L'utilisateur peut à la fois afficher et modifier la liste approuvée/bloquée définie par l'administrateur. Il peut aussi utiliser cette liste sur Mobile Device Agent. Lorsque les stratégies de sécurité se synchronisent avec Mobile Device Agent, les listes pour le filtrage ne sont pas synchronisées et toutes les autres fonctions sont mises à jour en fonction des stratégies. Mobile Security autorise ou bloque les adresses URL selon la priorité suivante : 1. Liste approuvée sur Mobile Device Agent 2. Liste bloquée sur Mobile Device Agent 3. Liste approuvée sur le serveur 4. Liste bloquée sur le serveur

Remarque

Le format de la liste approuvée et de la liste bloquée pour le filtrage des menaces Web doit être le suivant : [URL1] [URL2] [URL3] (avec un espace vide ou un retour à la ligne entre les différentes adresses URL).

Protection contre les menaces Web pour les dispositifs mobiles iOS

La protection contre les menaces Web vous permet de contrôler depuis le serveur les dispositifs mobiles iOS en mode Surveillé en spécifiant l'accès à ce qui suit :

- Sites Web spécifiques uniquement
- Contenu réservé aux adultes

Consultez le tableau suivant pour plus de détails sur les fonctions :

TABLEAU 11-7. Configuration des listes pour le filtrage relatives à la stratégie de protection contre les menaces Web

FONCTION	DESCRIPTION
Sites Web spécifiques uniquement	Cette option permet de restreindre l'accès uniquement aux sites Web que vous aurez précédemment configurés sur le serveur. Ajoutez les adresses URL que vous souhaitez autoriser dans l'onglet iOS de la stratégie de protection contre les menaces Web ; elles seront alors ajoutées au navigateur Web Safari du dispositif mobile des utilisateurs.
Contenu réservé aux adultes	Cette option permet de contrôler, depuis le serveur et à l'aide de listes de filtrage, les sites Web qui sont autorisés ou bloqués sur les appareils mobiles iOS. Ces filtres permettent de bloquer ou d'autoriser l'accès aux sites Web sans tenir compte des paramètres de filtrage par défaut définis sur les appareils mobiles iOS.

Remarque

Le format de la liste approuvée et de la liste bloquée pour le filtrage des menaces Web doit être le suivant : [URL1] [URL2] [URL3] (avec un espace vide ou un retour à la ligne entre les différentes adresses URL).

Stratégie de mot de passe

La stratégie de mot de passe empêche tout accès non autorisé aux données présentes sur des appareils mobiles.

Pour configurer les paramètres de la stratégie de mot de passe, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de mot de passe** dans le menu de gauche.

Stratégie de verrouillage des fonctions

Cette fonction vous permet de limiter (désactiver) ou d'autoriser (activer) l'usage de certaines fonctions ou de certains composants du dispositif mobile. Par exemple, vous pouvez désactiver l'appareil photo de tous les dispositifs mobiles d'un groupe spécifique.

Pour configurer les paramètres de la stratégie de verrouillage des fonctions, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de verrouillage des fonctions** dans le menu à gauche.

Consultez *Fonctions prises en charge sur le système d'exploitation des dispositifs mobiles à la page 11-25* pour obtenir la liste des fonctions et composants pris en charge.

AVERTISSEMENT!

Soyez prudent lorsque vous désactivez la fonction WLAN/WIFI et/ou Microsoft ActiveSync. Il est possible que le dispositif mobile ne puisse pas communiquer avec le serveur si les deux fonctions sont indisponibles.

Dans le cas des dispositifs mobiles Android, vous pouvez également ajouter un ou plusieurs points d'accès afin de contrôler la disponibilité des composants du dispositif dans la portée de ce ou ces points d'accès.

Fonctions prises en charge sur le système d'exploitation des dispositifs mobiles

Le tableau suivant présente la liste des fonctions prises en charge par Mobile Security sur chaque plate-forme.

TABLEAU 11-8. Liste des fonctions pour Trend Micro Mobile Security 9.7

STRATÉGIE	FONCTIONS	SETTINGS			
Approvisionnement	WiFi	Configuration standard du Wi-Fi	·	·	
		Configuration des hotspots hérités	·		
		Configuration Hotspot 2.0	·		
	Exchange ActiveSync	Configuration Exchange ActiveSync	·		
	VPN	Configuration VPN	·		

STRATÉGIE	FONCTIONS	SETTINGS			
	Proxy HTTP global	Configuration du proxy HTTP global	·		
	Authentification unique	Configuration de la fonction d'authentification unique	·		
	Certificat	Configuration du certificat	·		
	Réseau cellulaire	Configuration du réseau cellulaire	·		
	AirPlay/AirPrint	Configuration d'AirPlay/ AirPrint	·		
	Thèmes (mode Surveillé uniquement)	Configuration du papier peint	·		
		Configuration de la police	·		
	Domaines gérés	Domaines de messagerie non marqués	·		
		Domaines Web Safari gérés	·		
Sécurité du dispositif	Paramètres de sécurité	Scan en temps réel		·	
		Analyser après mise à jour des signatures		·	
		Scan manuel	·	·	
		Scan de Facebook	·	·	
Protection des données	Prévention anti-spam SMS	Contrôle depuis le serveur		·	
		Utilisation de liste bloquée		·	
		Utilisation de liste approuvée		·	
	Prévention anti-spam WAP Push	Contrôle depuis le serveur		·	
		Utilisation de liste approuvée		·	
	Filtrage des appels	Contrôle depuis le serveur		·	

STRATÉGIE	FONCTIONS	SETTINGS			
		Utilisation de liste bloquée		•	
		Utilisation de liste approuvée		•	
	Protection contre les menaces Web	Contrôle depuis le serveur		•	
		Utilisation de liste bloquée		•	
		Utilisation de liste approuvée		•	
		Autoriser des sites Web spécifiques uniquement	•		
		Autoriser le contenu réservé aux adultes	•		
Protection des données	Paramètres de mot de passe	Utiliser un mot de passe pour la connexion	•	•	•
		Utiliser un mot de passe simple	•	•	•
		Demander un mot de passe alphanumérique	•	•	•
		Longueur minimale du mot de passe	•	•	•
		Expiration du mot de passe	•	•	•
		Historique du mot de passe	•	•	•
		Verrouillage automatique	•	•	•
		Action en cas d'échec du mot de passe	•	•	•
	Verrouillage des fonctions	Appareil photo	•	•	
		FaceTime	•		
		Capture d'écran	•		
		Installation des applications	•		

STRATÉGIE	FONCTIONS	SETTINGS			
		Synchroniser en itinérance	·		
		Composition vocale	·		
		Fonction d'achat intégrée	·		
		Jeu multi-joueurs	·		
		Ajout d'amis de Game Center	·		
		Game Center (mode Surveillé uniquement)	·		
		Forcer les sauvegardes chiffrées	·		
		Musique à contenu explicite, podcast et iTunes U	·		
		Passbook lorsque le dispositif est verrouillé	·		
		Bluetooth et mode de recherche Bluetooth		·	
		WLAN/Wi-Fi		·	
		Réseau de données 3G		·	
		Mode modem		·	
		Mode développeur		·	
		Haut-parleur/téléphone à haut-parleur/microphone			
		Limiter les cartes mémoire		·	
		Siri	·		
		Siri lorsque le dispositif est verrouillé	·		

STRATÉGIE	FONCTIONS	SETTINGS			
		Activer le filtre contre les propos injurieux	·		
		Activer l'accès aux services iCloud	·		
		Sauvegarde en ligne (cloud)	·		
		Synchronisation des documents en ligne (Cloud)	·		
		Galerie de photos	·		
		Galeries de photos partagées	·		
		Données de diagnostic	·		
		Accepter des données non sécurisées du protocole TLS	·		
		Forcer iTunes à stocker les mots de passe	·		
		YouTube	·		
		Ouvrir des documents d'applications gérées dans d'autres applications	·		
		Ouvrir des documents d'autres applications dans des applications gérées	·		
		iTunes	·		
		Navigateur Web Safari	·		
		Remplissage automatique	·		
		JavaScript	·		
		Fenêtres contextuelles	·		

STRATÉGIE	FONCTIONS	SETTINGS			
		Forcer l'avertissement de fraude	·		
		Accepter les cookies	·		
		Suppression d'applications (mode Surveillé uniquement)	·		
		Librairie (mode Surveillé uniquement)	·		
		Érotique (mode Surveillé uniquement)	·		
		Installation du profil de configuration (mode Surveillé uniquement)	·		
		iMessage (mode Surveillé uniquement)	·		
		Région d'origine des évaluations	·		
		Films	·		
		Émissions de télévision	·		
		Applications	·		
		Modification de compte (mode Surveillé uniquement)	·		
		AirDrop (mode Surveillé uniquement)	·		
		Modification de l'utilisation de données cellulaires des applications (mode Surveillé uniquement)	·		
		Contenu de l'assistant (Siri) généré par les utilisateurs (mode Surveillé uniquement)	·		

STRATÉGIE	FONCTIONS	SETTINGS			
		Synchronisation de chaîne de clé Cloud	·		
		Modification de l'application Localiser mes amis (mode Surveillé uniquement)	·		
		Empreinte digitale nécessaire au déverrouillage d'un dispositif	·		
		Couplage d'hôte (mode Surveillé uniquement)	·		
		Centre de contrôle sur l'écran de verrouillage	·		
		Affichage des notifications sur l'écran de verrouillage	·		
		Affichage du jour sur l'écran de verrouillage	·		
		Mises à jour de l'infrastructure à clés publiques en mode OTA (OTAPKI)	·		
		Forcer la limitation du suivi de publicité	·		
		Forcer le mot de passe de couplage pour les demandes sortantes AirPlay	·		
		Autoriser les applications gérées à stocker des données dans iCloud	·		
		Autoriser la sauvegarde des livres d'entreprise	·		
		Autoriser la configuration de restrictions	·		

STRATÉGIE	FONCTIONS	SETTINGS			
		Autoriser l'effacement de tout le contenu et des paramètres	·		
		Autoriser le transfert	·		
		Autoriser les résultats Internet dans Spotlight	·		
		Autoriser la synchronisation des remarques et des recommandations pour les livres d'entreprise	·		
		Autoriser le partage des documents administrés à l'aide d'AirDrop	·		
		Autoriser la bibliothèque de photos iCloud	·		
		Autoriser l'installation d'applications sur le dispositif	·		
		Autoriser les raccourcis clavier	·		
		Autoriser le couplage avec Apple Watch	·		
		Autoriser la modification du code secret	·		
		Autoriser la modification du nom du dispositif	·		
		Autoriser la modification du papier peint	·		
		Autoriser le téléchargement automatique des applications	·		
		Autoriser les applications d'entreprise de confiance	·		

STRATÉGIE	FONCTIONS	SETTINGS			
	Paramètres de conformité	Débridé	·	·	
		Non chiffré	·	·	
		Vérification de la version du système d'exploitation	·	·	
Gestion des applications	Surveillance d'application & contrôle	Applications requises	·	·	
		Applications autorisées	·	·	
		Verrouillage pour application (mode Surveillé uniquement)	·		
	Programme d'achats en grande quantité	Programme d'achats en grande quantité	·		
Contrôle à distance	Enregistrer		·	·	
	Mise à jour		·	·	
	Antivol	Localisation à distance		·	
		Verrouillage à distance	·	·	
		Suppression à distance	·	·	·
		Réinitialiser le mot de passe	·	·	
	Samsung KNOX Workspace	Créer un conteneur		·	
		Supprimer le conteneur		·	
		Verrouiller le conteneur		·	
		Déverrouiller le conteneur		·	
		Réinitialiser le mot de passe du conteneur		·	
Stratégie Samsung KNOX Workspace	Configuration de compte de conteneur	Liste bloquée		·	
		Liste approuvée		·	

STRATÉGIE	FONCTIONS	SETTINGS			
	Paramètres de restriction	Autoriser les utilisateurs à utiliser l'appareil photo		·	
		Autoriser l'affichage du partage via la liste des applications		·	
	Paramètres du navigateur	Paramètre Activer le remplissage automatique		·	
		Paramètre Activer les cookies		·	
		Paramètre Activer les messages contextuels		·	
		Paramètre Activer l'avertissement forcé de fraude		·	
		Paramètre Activer JavaScript		·	
		Activer le proxy Internet		·	
Stratégie Samsung KNOX Workspace	Paramètres de mot de passe du conteneur	Activer la visibilité du mot de passe		·	
		Longueur minimale de modification de mot de passe		·	
		Longueur minimale du mot de passe		·	
		Délai d'inactivité maximal		·	
		Nombre maximal de tentatives infructueuses		·	
		Historique du mot de passe		·	
		Âge maximal du mot de passe		·	

STRATÉGIE	FONCTIONS	SETTINGS			
		Nombre minimal de caractères spéciaux requis dans un mot de passe		·	
		Complexité du mot de passe		·	
	Paramètres des applications	Installation de la liste approuvée		·	
		Installation de la liste bloquée		·	
		Applications requises		·	
		Applications désactivées		·	
Programme d'inscription de dispositif			·		

Stratégie de conformité

La stratégie de conformité vous permet de définir les critères de conformité à appliquer aux périphériques mobiles. Si un dispositif mobile ne répond pas aux critères définis, Mobile Security affiche cette information sur l'interface du serveur. En outre, s'il s'agit d'un périphérique iOS, Mobile Security envoie un e-mail au périphérique en question et, s'il s'agit d'un périphérique Android, il affiche une notification sur ce dernier. Voici les composants de la liste de contrôle de conformité :

- **Rooté/Débloqué** : vérifie si le dispositif mobile est rooté/débloqué ou non.
- **Déchiffré** : vérifie si le chiffrement est activé sur le dispositif mobile ou non.
- **Vérification de la version du système d'exploitation** : vérifie si la version du système d'exploitation correspond aux critères ou non.

Pour configurer les paramètres de la stratégie de conformité, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de conformité**.

Stratégie Surveillance et contrôle des applications

Les stratégies de surveillance et de contrôle des applications vous permettent de contrôler depuis le serveur les applications installées sur les périphériques mobiles, ainsi que d'envoyer les applications requises vers ces périphériques.

Pour configurer les paramètres de la stratégie de surveillance et de contrôle des applications, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie Surveillance et contrôle des applications**.

- **Applications requises** : cette option permet d'envoyer aux appareils mobiles toutes les applications ajoutées à la liste. Vous pouvez également lier un VPN à des applications, afin que les applications utilisent toujours ce VPN pour se connecter au réseau.

- **Applications autorisées** : cette option permet de contrôler les applications installées sur les périphériques mobiles par le biais de listes approuvée ou bloquée.

  Dans le cas des appareils mobiles iOS, Mobile Security envoie une notification à l'administrateur et à l'utilisateur s'il rencontre une application qui ne remplit pas les conditions de la stratégie.

  Dans le cas des appareils mobiles Android, Mobile Security bloque l'application qui ne remplit pas les conditions de la stratégie et autorise les autres.

  - **Activer le blocage des applications du système** (Android uniquement) :

    si cette option est sélectionnée, Mobile Security bloque toutes les applications du système sur les appareils mobiles Android.

  - **Activer la catégorie d'application** : choisissez la catégorie d'application que vous souhaitez activer ou désactiver sur les périphériques mobiles. Vous pouvez également créer des exceptions en ajoutant les applications appartenant à ces catégories à la liste bloquée ou approuvée. Par exemple, si vous avez désactivé un type de catégorie nommé Jeux, Mobile Security bloque toutes les applications appartenant à cette catégorie, sauf si l'application fait partie de la liste approuvée.

    Mobile Security autorise ou bloque les applications selon la priorité suivante :

1. **Liste approuvée** : Mobile Security autorise les applications contenues dans la liste approuvée, même si elles appartiennent à une catégorie ayant été désactivée.

2. **Liste bloquée** : Mobile Security bloque les applications contenues dans la liste bloquée, même si elles appartiennent à une catégorie ayant été activée.

3. **Autorisations des applications** : Mobile Security autorise ou bloque les applications en fonction de l'état d'autorisation que vous sélectionnez pour la catégorie à laquelle elles appartiennent.

- **Activer les autorisations des applications** (pour Android uniquement) : choisissez les services d'application que vous souhaitez activer ou désactiver sur les périphériques mobiles Android. Vous pouvez également créer des exceptions en ajoutant les applications utilisant ces services à la liste bloquée ou approuvée. Par exemple, si vous avez désactivé le type de service **Lire les données**, Mobile Security bloque toutes les applications utilisant ce service, sauf si l'application fait partie de la liste approuvée.

  Mobile Security autorise ou bloque les applications selon la priorité suivante :

  1. **Liste approuvée** : Mobile Security autorise les applications contenues dans la liste approuvée, même si elles utilisent des services ayant été désactivés.

  2. **Liste bloquée** : Mobile Security bloque les applications contenues dans la liste bloquée, même si elles utilisent des services ayant été activés.

  3. **Autorisations des applications** : Mobile Security autorise ou bloque les applications en fonction de l'état d'autorisation que vous sélectionnez pour les services qu'elles utilisent.

- **Autoriser seulement les applications suivantes** : ajoutez à la liste approuvée les applications dont vous souhaitez autoriser l'usage sur périphériques mobiles. Si cette option est activée :

  - Mobile Security affiche un message d'avertissement sur les appareils mobiles Android si une application qui n'est pas dans la liste approuvée est détectée.

- Mobile Security envoie une notification par e-mail à l'utilisateur d'appareil mobile iOS si une application qui n'est pas dans la liste approuvée est détectée.

- **Bloquer seulement les applications suivantes** : ajoutez à la liste bloquée les applications dont vous souhaitez bloquer l'usage sur périphériques mobiles. Si cette option est activée :

  - Mobile Security affiche un message d'avertissement sur les appareils mobiles Android si une application qui est dans la liste bloquée est détectée.

  - Mobile Security envoie une notification par e-mail à l'utilisateur d'appareil mobile iOS si une application qui est dans la liste bloquée est détectée.

- **Verrouiller dans l'application (pour mode Surveillé uniquement)** : limite le dispositif mobile iOS à l'application spécifiée.

Mobile Security effectue une recherche d'applications limitées et envoie des alertes par e-mail aux utilisateurs de l'une des façons suivantes :

- Automatiquement, en fonction des paramètres **Fréquence de collecte des informations** dans **Administration** > **Paramètres du serveur de communication** > **Paramètres communs (onglet)**.

- Lors de la mise à jour des paramètres **Fréquence de collecte des informations** dans **Administration** > **Paramètres du serveur de communication** > **Paramètres communs (onglet)**.

Stratégie du programme d'achats en grande quantité

Cette stratégie permet à l'administrateur d'importer dans la console Web d'administration de Mobile Security les applications iOS achetées via le Programme d'achat en volume d'Apple. Mobile Security transfère toutes les applications de la liste Programme d'achats en volume vers les dispositifs mobiles d'un groupe.

Pour configurer la stratégie Programme d'achats en volume :

1. Ajoutez des applications à l'App Store d'entreprise. Voir *Ajout d'une application à la page 11-39* pour obtenir une description de la procédure.

2. Cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie Programme d'achats en volume**.
3. Cliquez sur **Importer**, puis sélectionnez les applications à importer depuis l'App Store d'entreprise.
4. Cliquez sur **Enregistrer** pour transférer toutes les applications aux dispositifs mobiles iOS.

Ajout d'une application

Procédure

1. Dans la console Web d'administration de Mobile Security, accédez à **Applications** > **App Store d'entreprise**.

   L'écran **App Store d'entreprise** s'affiche.

2. Cliquez sur l'onglet **Android** ou **iOS**.
3. Cliquez sur **Ajouter**.

   L'écran **Ajouter une application** s'affiche.

4. Ajoutez une application à la liste à l'aide de l'une des options suivantes :

   - **Ajouter depuis l'ordinateur local** : sélectionner un fichier d'installation pour dispositifs mobiles Android ou iOS.
   - **Ajouter un webclip** : saisissez l'adresse URL de l'application pour afficher l'icône correspondante sur l'écran d'accueil de l'appareil mobile de l'utilisateur. Si l'utilisateur clique sur le lien, l'application s'ouvre dans le navigateur Web par défaut de l'appareil mobile.
   - (Android) **Ajouter depuis un magasin d'applications externe** : saisissez le lien vers l'application dans un magasin d'applications externe. L'icône de l'application s'affiche sur l'écran d'accueil de l'appareil mobile de l'utilisateur. Si l'utilisateur clique sur le lien, l'application s'ouvre dans le navigateur Web par défaut de l'appareil mobile.
   - (iOS) **Saisissez un mot-clé de recherche** : saisissez le nom de l'application du Programme d'achats en volume que vous souhaitez rechercher. Choisissez

ensuite un pays (la recherche s'effectuera dans l'App Store d'Apple de ce pays), puis sélectionnez l'application dans les résultats de la recherche. Une fois ajoutée, l'application du Programme d'achats en volume (VPP) est disponible uniquement dans l'**App Store** de la console Web d'administration de Mobile Security. Pour la transférer vers des dispositifs mobiles, vous devez l'ajouter à la **stratégie Programme d'achats en volume**. Voir *Stratégie du programme d'achats en grande quantité à la page 11-38* pour obtenir une description de la procédure.

5. Cliquez sur **Continuer**.

   L'écran **Modifier une application** s'affiche.

6. Configurez les éléments suivants :

   - **Nom de l'application** : indiquez un nom pour l'application.
   - **Icône de l'application** : si l'icône de l'application n'apparaît pas, cliquez sur « Télécharger l'icône de l'application » pour la sélectionner et la télécharger.
   - **Identifiant de l'application** : si l'identifiant de l'application n'apparaît pas, saisissez-le.
   - **Fichier de codes VPP** : pour les applications du Programme d'achats en volume (VPP), vous devez télécharger les fichiers VPP que vous a envoyés Apple.
   - **Catégorie** : sélectionnez la catégorie de l'application.

     Remarque

     Vous devez sélectionner la catégorie dans la liste déroulante. Pour ajouter une catégorie à la liste ou l'en supprimer, cliquez sur le bouton **Catégorie**.

   - **Description** : saisissez la description de l'application.
   - **Publier** : choisissez l'une des options suivantes :
     - **Ne pas publier** : pour télécharger l'application sur le serveur, mais ne pas la mettre à disposition des dispositifs mobiles.

- **Publier en tant que version de production** : pour télécharger l'application sur le serveur et la mettre à disposition au téléchargement sur les dispositifs mobiles.
- **Publier en tant que version bêta** : pour télécharger l'application sur le serveur et la mettre à disposition au téléchargement sur les dispositifs mobiles en tant que version bêta.

- **Captures d'écran** : sélectionnez des captures d'écran de l'application et téléchargez-les.

7. Cliquez sur **Continuer**.

   L'application apparaît dans la liste des applications.

Stratégie de conteneur

Cette stratégie vous permet de gérer les paramètres de sécurité du conteneur Samsung KNOX. Vous pouvez configurer la liste approuvée ou la liste bloquée pour les comptes, appliquer des restrictions et configurer le navigateur, le mot de passe et les paramètres des applications.

Remarque

Vous devez configurer la licence KNOX dans Mobile Security avant d'activer cette stratégie. Pour configurer la licence KNOX, accédez à **Administration** > **Licence du produit** sur la console Web d'administration.

- **Paramètres du compte** : spécifiez les comptes qui peuvent être ajoutés ou soumis à restriction sur les conteneurs Samsung KNOX à l'aide des listes approuvées et/ou bloquées.
- **Paramètres de restriction** : désactivez l'appareil photo ou le partage de fichiers sur les conteneurs Samsung KNOX.
- **Paramètres du navigateur** : configurez les paramètres de sécurité du navigateur Web Android natif sur les conteneurs Samsung KNOX.
- **Paramètres de mot de passe** : configurez les paramètres de sécurité du mot de passe du conteneur Samsung KNOX.

- **Paramètres des applications** : configurez les listes suivantes :
  - **Filtrer les listes d'applications** : configurez la liste approuvée ou la liste bloquée pour restreindre l'installation des applications sur le conteneur Samsung KNOX.
  - **Applications requises** : configurez la liste des applications requises pour indiquer les applications qui doivent être installées sur Samsung KNOX.
  - **Applications désactivées** : configurez la liste des applications désactivées afin de désactiver certaines applications sur l'appareil mobile. Si les applications de cette liste sont installées sur l'appareil mobile, elles ne seront pas désinstallées, mais l'utilisateur ne sera pas en mesure de les utiliser.

Pour configurer les paramètres de la stratégie de conteneur, cliquez sur **Stratégies**, sur le nom de la stratégie, puis sur **Stratégie de conteneur**.

Partie VI

Gestion des stratégies de l'agent OfficeScan

Chapitre 12

Paramètres du programme de l'agent OfficeScan

Cette section décrit comment gérer le programme de l'agent OfficeScan installé sur des Endpoints.

Les rubriques sont les suivantes :

- *Paramètres des services complémentaires à la page 12-2*
- *Privilèges et autres paramètres à la page 12-4*
- *Agents de mise à jour à la page 12-20*

Paramètres des services complémentaires

Le programme de l'Agent OfficeScan impose l'activation de services supplémentaires pour permettre le bon fonctionnement de certaines fonctions. Le tableau suivant décrit les services disponibles et les fonctions requises.

SERVICE	DESCRIPTION	FONCTIONS
Service de prévention des modifications non autorisées (`TMBMSRV.exe`)	Régule le comportement des applications et vérifie la fiabilité des programmes	• Apprentissage automatique prédictif • Surveillance des comportements • Contrôle des dispositifs • Certified Safe Software Service • Autoprotection de l'agent
Service de pare-feu (`TmPfw.exe`)	Régule les autorisations d'accès de la connexion réseau	• Pare-feu OfficeScan
Service des connexions suspectes	Fournit une protection avancée contre les rappels C&C	• Listes des adresses IP approuvées et bloquées définies par l'utilisateur • Liste d'adresses IP C&C globale (moteur d'inspection du contenu réseau) • Système de reconnaissance réseau des programmes malveillants (fichier de signatures de règle de pertinence)
Service de protection des données (`dsagent.exe`)	Fournit une surveillance avancée des données sensibles et restreint l'accès au dispositif sur des Endpoints	• Prévention contre la perte de données • Contrôle des dispositifs (pour bloquer l'accès)

SERVICE	DESCRIPTION	FONCTIONS
Service de protection avancé (`TMCCSF.exe`)	Met en œuvre des fonctions avancées de scan et de protection	• Apprentissage automatique prédictif • Prévention contre l'exploitation du navigateur • Surveillance des comportements

Configuration de services supplémentaires pour agents OfficeScan

Procédure

1. Sélectionnez cette option pour activer le service requis sur les **postes de travail Windows** ou les **plates-formes Windows Server** dans les sections suivantes :

   - **Service de prévention des modifications non autorisées**
   - **Service de pare-feu**

     Important

     L'activation ou la désactivation temporaire du service déconnecte des Endpoints du réseau. Assurez-vous de modifier les paramètres uniquement pendant les heures non critiques pour limiter les risques de coupure de connexion.

   - **Service de connexion suspecte**
   - **Service de protection des données**

     Important

     L'activation ou la désactivation temporaire du service déconnecte des Endpoints du réseau. Assurez-vous de modifier les paramètres uniquement pendant les heures non critiques pour limiter les risques de coupure de connexion.

   - **Service de protection avancé**

Important

L'activation de services supplémentaires sur les plates-formes Windows Server peut affecter les performances du serveur. Après l'activation d'un service sur une plate-forme Windows Server, Trend Micro vous recommande de surveiller le serveur pendant un certain temps pour vous assurer qu'aucun impact sur les performances ne s'est produit.

Privilèges et autres paramètres

Configurez les Agents OfficeScan pour octroyer aux utilisateurs des droits leur permettant de configurer des paramètres personnalisés, d'afficher des messages de notification et de protéger des fichiers et des services d'Agent OfficeScan critiques.

Configuration des privilèges d'agent

Procédure

1. Configurez les paramètres selon les besoins.

SECTION	SETTINGS
Mode indépendant	**Activer le mode indépendant** : permet aux utilisateurs de désactiver les fonctions suivantes sur l'Agent OfficeScan pour empêcher l'Agent OfficeScan d'altérer les performances du système : • L'Agent OfficeScan n'accepte pas de paramètres de stratégie du serveur • L'Agent OfficeScan n'initie pas de commandes de scan à partir du serveur • L'Agent OfficeScan n'envoie pas de journaux au serveur Les utilisateurs finaux peuvent manuellement lancer des scans ou des mises à jour sur des agents en mode indépendant.

SECTION	SETTINGS
Scans	• **Configurer le scan manuel** : permet aux utilisateurs de configurer les paramètres de **Scan manuel** sur la console de l'Agent OfficeScan • **Configurer le scan en temps réel** : permet aux utilisateurs de configurer les paramètres de **Scan en temps réel** sur la console de l'Agent OfficeScan • **Configurer le scan programmé** : permet aux utilisateurs de configurer les paramètres de **Scan programmé** sur la console de l'Agent OfficeScan
Scans programmés	• **Différer le scan programmé** : permet aux utilisateurs de différer un scan programmé avant son démarrage ou d'arrêter un scan en cours d'exécution pour une période spécifiée **Remarque** Les utilisateurs ne peuvent arrêter un scan en cours d'exécution qu'une seule fois. Une fois que le scan a redémarré, l'Agent OfficeScan rescanne tous les fichiers sur l'Endpoint. • **Annuler et arrêter le scan programmé** : permet aux utilisateurs d'annuler ou d'arrêter un scan programmé une seule fois **Remarque** Les utilisateurs ne peuvent pas ignorer ni arrêter un scan programmé à plusieurs reprises. Même après un redémarrage du système, le scan programmé reprend, selon les paramètres de la prochaine exécution programmée.

SECTION	SETTINGS

Pare-feu	• **Afficher les paramètres du pare-feu sur la console de l'agent OfficeScan** : permet aux utilisateurs de configurer les paramètres du **pare-feu** sur la console de l'Agent OfficeScan
	  • **Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu** : affiche les options du menu **Activer/désactiver le pare-feu** et **Activer/désactiver le mode IDS** sur l'icône de la barre d'état système de l'Agent OfficeScan
	  Remarque
	  Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection », à un scan antivirus de réseau hautes performances et à l'élimination des virus réseau. Si vous accordez aux utilisateurs le privilège d'activation ou de désactivation du pare-feu et de ses fonctions, avertissez-les de ne pas désactiver le pare-feu trop longtemps afin d'éviter d'exposer l'Endpoint aux intrusions et aux attaques de pirates.
	• **Autoriser les agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan** : configure l'Agent OfficeScan pour envoyer les journaux du pare-feu au serveur, vous permettant ainsi d'analyser le trafic réseau

Surveillance des comportements	**Afficher les paramètres de surveillance des comportements sur la console de l'agent OfficeScan** : permet aux utilisateurs de configurer les paramètres de **surveillance des comportements** sur la console de l'Agent OfficeScan
Liste des programmes approuvés	**Afficher la liste des programmes approuvés sur la console de l'agent OfficeScan** : permet aux utilisateurs de configurer la **liste des programmes approuvés** sur la console de l'Agent OfficeScan

SECTION	SETTINGS
Scan du courrier	**Afficher les paramètres du scan du courrier sur la console de l'agent OfficeScan** : permet aux utilisateurs de configurer les paramètres du **scan du courrier** sur la console de l'Agent OfficeScan Si l'option est activée, le scan en temps réel détecte et agit sur les messages électroniques POP3 récupérés à partir du serveur de messagerie contenant des menaces malveillantes.
Paramètres proxy	**Autoriser les utilisateurs à configurer des paramètres proxy** : permet aux utilisateurs d'utiliser les paramètres proxy configurés par l'utilisateur uniquement dans les instances suivantes : • Lorsque les Agents OfficeScan exécutent l'option « Mettre à jour ». • Lorsque l'utilisateur désactive les paramètres proxy automatiques ou que l'Agent OfficeScan ne parvient pas à les détecter. **AVERTISSEMENT!** Des paramètres proxy configurés par l'utilisateur incorrects peuvent entraîner des problèmes de mise à jour. Soyez prudent lorsque vous autorisez les utilisateurs à configurer leurs propres paramètres proxy.

SECTION	SETTINGS
Mises à jour des composants	• **Exécuter l'option « Mettre à jour »** : affiche l'option de menu **Mettre à jour** sur l'icône de la barre d'état système de l'Agent OfficeScan • **Activer/Désactiver les mises à jour programmées** : affiche l'option de menu **Activer/Désactiver les mises à jour programmées** sur l'icône de la barre d'état système de l'Agent OfficeScan **Remarque** Les administrateurs doivent sélectionner le paramètre **Activer les mises à jour programmées sur les agents OfficeScan** dans l'onglet **Autres paramètres** pour que cette option apparaisse dans le menu de l'Agent OfficeScan.
Décharger et déverrouiller	Le privilège de déchargement et de déverrouillage de l'Agent OfficeScan autorise les utilisateurs à arrêter momentanément l'Agent OfficeScan ou à accéder à certaines fonctionnalités avancées de la console Web, avec ou sans mot de passe. • **Aucun mot de passe n'est requis** • **Un mot de passe est requis** : saisissez le mot de passe requis et le mot de passe de confirmation **Remarque** Si vous sélectionnez **Un mot de passe est requis**, mais ne spécifiez aucun mot de passe, Control Manager applique le mot de passe par défaut suivant : • Pour OfficeScan local : le mot de passe fourni lors de l'installation du serveur • Pour OfficeScan SaaS : le nom de compte utilisé pour provisionner la console

SECTION	SETTINGS
Désinstallation	Le privilège de désinstallation de l'Agent OfficeScan permet aux utilisateurs de désinstaller le programme de l'Agent OfficeScan sur les Endpoints locaux. • **Aucun mot de passe n'est requis** • **Un mot de passe est requis** : saisissez le mot de passe requis et le mot de passe de confirmation **Remarque** Si vous sélectionnez **Un mot de passe est requis**, mais ne spécifiez aucun mot de passe, Control Manager applique le mot de passe par défaut suivant : • Pour OfficeScan local : le mot de passe fourni lors de l'installation du serveur • Pour OfficeScan SaaS : le nom de compte utilisé pour provisionner la console

Configuration d'autres paramètres de l'agent

Procédure

1. Configurez les paramètres selon les besoins.

SECTION	SETTINGS
Conversion en mode coexistence	**Convertissez définitivement des agents OfficeScan en agents OfficeScan entièrement opérationnels à l'aide du mode coexistence** : active toutes les fonctions sur les Agents OfficeScan installés en « Mode coexistence » **Important** Vous ne pouvez pas annuler cette action. Après la conversion des Agents OfficeScan de mode coexistence en Agents OfficeScan entièrement fonctionnels, le programme de l'agent tente de désinstaller tout logiciel tiers incompatible sur l'Endpoint. Après la conversion, OfficeScan active tous les services et fonctions nécessaires associés au fonctionnement normal de l'Agent OfficeScan. Si vous avez besoin d'utiliser un Agent OfficeScan en mode coexistence sur un Endpoint convergé, vous devez désinstaller le programme de l'Agent OfficeScan, puis réinstaller un Agent OfficeScan en mode coexistence.

Section	Settings

Paramètres de mise à jour	• **Les agents OfficeScan téléchargent des mises à jour depuis le Trend Micro ActiveUpdate Server** : configure les Agents OfficeScan qui ne peuvent pas se connecter à la source de mise à jour spécifiée pour tenter une mise à jour à partir du serveur Trend Micro ActiveUpdate
	• **Activer les mises à jour programmées sur les agents OfficeScan** : configure tous les Agents OfficeScan pour activer les mises à jour programmées par défaut
	• **Les agents OfficeScan mettent uniquement à jour les composants suivants** : cette option contrôle comment les mises à jour de composants s'effectuent sur les Agents OfficeScan
	  • **Tous les composants (y compris les correctifs de type hotfix et le programme de l'agent)** : les Agents OfficeScan mettent à jour tous les composants
	  • **Fichiers de signatures, moteurs, pilotes** : les Agents OfficeScan ne mettent pas à niveau le programme de l'Agent OfficeScan ou ne déploient pas de correctifs
	  • **Fichiers de signatures** : les Agents OfficeScan ne mettent pas à niveau le programme de l'Agent OfficeScan, ne déploient pas de correctifs ou ne mettent pas à jour les moteurs et les pilotes

Paramètres de Web Reputation	**Afficher une notification lorsqu'un site Web est bloqué** : affiche un message de notification sur l'Agent OfficeScan après le blocage d'une URL qui viole une stratégie de Web Reputation
Paramètres de surveillance des comportements	**Afficher une notification lorsqu'un programme est bloqué** : affiche un message de notification sur l'Agent OfficeScan après le blocage d'un programme qui enfreint une stratégie de surveillance des comportements
Paramètres d'alerte de contact C&C	**Afficher une notification lorsqu'un rappel C&C est détecté** : affiche un message de notification sur l'Agent OfficeScan après la détection d'un rappel C&C

SECTION	SETTINGS
Paramètres de restauration depuis la mise en quarantaine centrale	**Afficher une notification lorsqu'un fichier mis en quarantaine est restauré** : affiche un message de notification sur l'Agent OfficeScan après la restauration d'un fichier mis en quarantaine
Paramètres de l'apprentissage automatique prédictif	**Afficher une notification lorsqu'une menace est détectée** : affiche un message de notification sur l'Agent OfficeScan après que l'apprentissage automatique prédictif a détecté une menace inconnue
Autoprotection de l'agent OfficeScan	• **Protéger les services de l'agent OfficeScan** : empêche les utilisateurs des applications de mettre fin aux services de l'Agent OfficeScan • **Protéger les fichiers du dossier d'installation de l'agent OfficeScan** : empêche les utilisateurs ou les applications de modifier ou de supprimer des fichiers dans le dossier d'installation de l'Agent OfficeScan • **Protéger les clés de Registre de l'agent OfficeScan** : empêche les utilisateurs ou les applications de modifier, de supprimer ou d'ajouter des valeurs de registre utilisées par le programme de l'Agent OfficeScan • **Protéger les processus de l'agent OfficeScan** : empêche les utilisateurs ou les applications de mettre fin au processus de l'Agent OfficeScan Pour plus d'informations, voir *Autoprotection de l'agent OfficeScan à la page 12-14*.
Paramètres de scan programmé	**Afficher un message de notification avant le début d'un scan programmé** : affiche un message de notification sur l'Agent OfficeScan avant le démarrage d'un scan programmé configuré

SECTION	SETTINGS
Paramètres du cache pour les scans	• **Activer le cache de la signature numérique** : configure l'Agent OfficeScan pour utiliser le modèle de signature numérique de surveillance des comportements pour exclure des fichiers des scans manuels, des scans programmés et du scan immédiat • **Activer le cache du scan à la demande** : configure l'Agent OfficeScan pour maintenir un cache de scan à la demande local afin d'exclure des fichiers pendant un scan manuel, un scan programmé et un scan immédiat pour améliorer les performances de scan Pour plus d'informations, voir *Paramètres du cache pour les scans à la page 12-16*.
Paramètres de scan de la messagerie POP3	**Scanner la messagerie POP3** : permet le scan de la messagerie POP3 sur l'Agent OfficeScan Pour plus d'informations, voir *Scan du courrier POP3 à la page 12-19*.
Restriction de l'accès à l'agent OfficeScan	**Ne pas autoriser les utilisateurs à accéder à la console de l'agent OfficeScan depuis la barre d'état système ou le menu Démarrer de Windows** : interdit l'accès de l'utilisateur à la console de l'Agent OfficeScan à l'aide de la barre d'état système ou du menu Démarrer de Windows **Remarque** Ce paramètre ne désactive pas l'Agent OfficeScan. L'Agent OfficeScan s'exécute en arrière-plan et continue d'assurer une protection contre les risques de sécurité.
Notification de redémarrage	**Afficher une notification si l'Endpoint doit redémarrer pour terminer le nettoyage des fichiers infectés** : affiche un message de notification sur l'Agent OfficeScan si l'utilisateur doit redémarrer l'Endpoint pour terminer le nettoyage d'un fichier malveillant

Autoprotection de l'agent OfficeScan

L'autoprotection de l'Agent OfficeScan permet à l'Agent OfficeScan de protéger les processus et autres ressources dont il a besoin pour fonctionner correctement. Elle permet d'empêcher des programmes ou des utilisateurs de désactiver la protection contre les programmes malveillants.

Protéger les services de l'agent OfficeScan

OfficeScan bloque toutes les tentatives visant à mettre fin aux services suivants de l'Agent OfficeScan :

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- Service proxy d'OfficeScan NT (`TmProxy.exe`)
- Pare-feu d'OfficeScan NT (`TmPfw.exe`)
- Service de protection des données OfficeScan (`dsagent.exe`)
- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)

Remarque

Si cette option est activée, l'Agent OfficeScan peut empêcher l'installation de produits tiers sur les Endpoints. Si vous rencontrez ce problème, vous pouvez désactiver temporairement l'option, puis la réactiver une fois le produit tiers installé.

- Structure de la solution client commune Trend Micro (`TmCCSF.exe`)

Protéger les fichiers du dossier d'installation de l'agent OfficeScan

Pour empêcher d'autres programmes ou l'utilisateur de modifier ou de supprimer des fichiers d'Agent OfficeScan, OfficeScan verrouille les fichiers suivants dans la racine `<dossier d'installation de l'agent>` :

- Tous les fichiers signés numériquement possédant les extensions `.exe`, `.dll` et `.sys`
- Certains fichiers sans signature numérique, dont :
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`
  - `PiReg.exe`
  - `ssleay32.dll`
  - `Tmeng.dll`
  - `TMNotify.dll`
  - `zlibwapi.dll`

Protéger les clés de Registre de l'agent OfficeScan

L'Agent OfficeScan bloque toutes les tentatives de modification, suppression ou ajout de nouvelles entrées sous les clés et sous-clés de registre suivantes :

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Protéger les processus de l'agent OfficeScan

L'Agent OfficeScan bloque toutes les tentatives visant à mettre fin aux processus répertoriés dans le tableau suivant.

PROCESSUS	DESCRIPTION
TmListen.exe	Reçoit des commandes et des notifications du serveur OfficeScan et facilite la communication entre l'Agent OfficeScan et le serveur
NTRtScan.exe	Effectue des scans en temps réel, programmés et manuels sur les Agents OfficeScan
TmProxy.exe	Scanne le trafic réseau avant que celui-ci ne puisse atteindre l'application cible
TmPfw.exe	offre des fonctions de pare-feu au niveau des paquets, de recherche de virus de réseau et de détection d'intrusions.
TMBMSRV.exe	Régule l'accès aux périphériques de stockage externes et empêche la modification non autorisée des clés de registre et des processus
DSAgent.exe	Surveille la transmission de données sensibles et contrôle l'accès aux périphériques
PccNTMon.exe	Processus responsable du lancement de la console de l'Agent OfficeScan
TmCCSF.exe	effectue la prévention contre l'exploitation du navigateur et le scan de la mémoire.

L'Agent OfficeScan peut également assurer une protection contre l'ajout de processus aux stratégies de restriction logicielle de Windows. Ces stratégies empêchent les applications figurant dans la liste de s'exécuter sur le endpoint. Si vous ne souhaitez pas qu'Agent OfficeScan ajoute des processus À la liste des stratégies de restriction logicielle:

1. Activez **Protéger les processus de l'agent OfficeScan**.
2. Activez le **service de prévention des modifications non autorisées**

Paramètres du cache pour les scans

L'Agent OfficeScan peut générer des fichiers de mémoire cache du scan à la demande et des fichiers de signature numérique pour améliorer les performances du scan. Lors de l'exécution d'un scan à la demande, l'Agent OfficeScan vérifie tout d'abord le fichier de cache de signature numérique, puis le fichier de mémoire cache du scan à la demande,

pour déterminer les fichiers à exclure du scan. La durée du scan est réduite si de nombreux fichiers sont exclus du scan.

Cache de signature numérique

Le fichier de cache de signature numérique est utilisé lors des scans manuel, programmé et immédiat. Les agents ne scannent pas les fichiers dont les signatures ont été ajoutées à ce fichier de cache.

L'Agent OfficeScan génère le fichier de cache de signature numérique à l'aide du même fichier Digital Signature Pattern que celui utilisé pour la surveillance des comportements. Le Digital Signature Pattern contient une liste de fichiers que Trend Micro estime fiables et qui sont, par conséquent, exclus des scans.

Remarque

La surveillance des comportements est désactivée pour les plates-formes de serveur Windows (prise en charge des plate-formes 64 bits pour Windows XP et 2003 non disponible). Si le cache de signature numérique est activé, les Agents OfficeScan de ces plates-formes téléchargent le fichier Digital Signature Pattern en vue d'une utilisation dans le cache, mais ne téléchargent pas les autres composants de la surveillance des comportements.

Les agents génèrent le fichier de cache de signature numérique selon une programmation, configurable à partir de la console Web. Cela permet aux agents d'effectuer les opérations suivantes :

- Ajouter les signatures des nouveaux fichiers intégrés au système depuis la génération du dernier fichier de cache
- Supprimer les signatures des fichiers qui ont été modifiés ou supprimés du système

Pendant le processus de génération du cache, les agents recherchent des fichiers fiables dans les dossiers suivants, puis ajoutent les signatures de ces fichiers au fichier de cache de signature numérique :

- `%PROGRAMFILES%`
- `%WINDIR%`

La génération du cache n'affecte pas les performances de l'Endpoint, car les agents utilisent peu de ressources système pendant le processus. Les agents peuvent également reprendre une tâche de génération du cache qui a été interrompue (par exemple, lorsque l'ordinateur hôte est mis hors tension ou que l'adaptateur secteur d'un Endpoint sans fil est débranché).

Mémoire cache du scan à la demande

Le fichier de mémoire cache du scan à la demande est utilisé lors des scans manuel, programmé et immédiat. Les Agents OfficeScan ne scannent pas les fichiers dont les caches ont été ajoutés à ce fichier de mémoire cache.

À chaque exécution du scan, l'Agent OfficeScan vérifie les propriétés des fichiers fiables. Si un fichier fiable n'a pas été modifié depuis un certain temps (période à configurer), l'Agent OfficeScan ajoute son cache au fichier de mémoire cache du scan à la demande. Lors du scan suivant, le fichier n'est pas scanné si son cache n'a pas expiré.

Le cache d'un fichier fiable expire au bout d'un certain nombre de jours (période également à configurer). Lorsque le scan est exécuté pendant ou après l'expiration du cache, l'Agent OfficeScan supprime le cache expiré et scanne le fichier à la recherche de menaces. Si le fichier ne présente aucune menace et qu'aucune modification n'y a été apportée, le cache de ce fichier est de nouveau ajouté au fichier de cache de scan à la demande. Si le fichier ne présente aucune menace, mais qu'une modification y a été récemment apportée, le cache n'est pas ajouté et ce fichier sera scanné lors du prochain scan.

Un cache de fichier fiable expire pour éviter que des fichiers infectés ne soient exclus des scans, comme l'illustrent les exemples suivants :

- Il est possible qu'un fichier de signatures trop ancien ait considéré un fichier infecté non modifié comme ne présentant aucune menace. S'il n'y a pas d'expiration de cache, le fichier infecté reste dans le système jusqu'à ce qu'il soit modifié et détecté par un scan en temps réel.
- Si un fichier mis en cache a été modifié et que le scan en temps réel ne fonctionne pas depuis la modification du fichier, il est nécessaire que le cache expire pour que le fichier modifié puisse être scanné à la recherche de menaces.

Le nombre de caches ajoutés au fichier de cache de scan à la demande dépend du type de scan et de la cible visée. Par exemple, le nombre de caches peut être réduit si l'Agent

OfficeScan scanne uniquement 200 fichiers sur les 1 000 que compte un endpoint au cours d'un scan manuel.

Si l'exécution de scans à la demande est fréquente, le fichier de cache de scan à la demande réduit la durée de scan de façon significative. Au cours d'une tâche de scan pour laquelle aucun cache n'a expiré, la durée d'un scan demandant généralement 12 minutes peut être réduite à 1 minute. Pour améliorer les performances, vous pouvez réduire le nombre de jours pendant lequel un fichier n'a pas à être modifié et prolonger la période d'expiration du cache. Étant donné que les fichiers doivent rester inchangés pendant une période relativement courte, vous pouvez ajouter un nombre de caches plus important au fichier de cache. La période d'expiration des caches est également plus longue, ce qui signifie qu'un nombre de fichiers plus important est ignoré au cours de scans.

Si les scans à la demande ne sont que rarement exécutés, vous pouvez désactiver la mémoire cache du scan à la demande car les caches expireront avant l'exécution du prochain scan.

Scan du courrier POP3

Si les Agents OfficeScan disposent des privilèges du scan de courrier, l'onglet **Scan du courrier** s'affiche sur la console de l'Agent OfficeScan. L'option **Scan du courrier** affiche le scan du courrier POP3.

Le tableau suivant décrit le programme de scan du courrier POP3.

TABLEAU 12-1. Programmes de scan de messagerie

DÉTAILS	DESCRIPTION
Objet	Scanne les messages de la boîte POP3 à la recherche de virus/programmes malveillants.

DÉTAILS	DESCRIPTION
Prérequis	• Doit être activé par les administrateurs à partir de la console Web au préalable. **Remarque** Vous devez activer le privilège **Afficher les paramètres du scan du courrier sur la console de l'agent OfficeScan** pour activer le scan du courrier POP3. Pour plus d'informations, voir *Configuration des privilèges d'agent à la page 12-4*. • Action à entreprendre contre les virus/programmes malveillants. Doit être définie à l'aide de la console de l'Agent OfficeScan et non de la console Web
Types de scan pris en charge	Scan en temps réel Le scan s'effectue lors de la récupération des messages électroniques à partir du serveur de messagerie POP3.
Résultats de scan	• Informations relatives aux risques de sécurité détectés, disponibles après l'exécution du scan. • Résultats de scan non consignés dans l'écran **Journaux** de la console de l'Agent OfficeScan • Résultats de scan non envoyés au serveur.
Autres informations	Partage le service proxy d'OfficeScan NT (`TMProxy.exe`) avec la fonction d'évaluation de Web Reputation.

Agents de mise à jour

Pour distribuer la tâche de déploiement des composants, de paramètres de domaine, ou de programmes et de correctifs d'agents sur les Agents OfficeScan, attribuez à certains Agents OfficeScan le rôle d'agents de mise à jour ou de sources de mise à jour pour d'autres Agents OfficeScan. Cela permet de s'assurer que les Agents OfficeScan

reçoivent les mises à jour en temps et en heure et évite au serveur OfficeScan la gestion d'un trafic réseau trop important.

Si le réseau est segmenté par sites et si le lien réseau entre les segments présente un trafic élevé, affectez au moins un agent de mise à jour à chaque site.

Remarque

Les Agents OfficeScan configurés pour mettre à jour leurs composants depuis un agent de mise à jour reçoivent uniquement les composants et paramètres mis à jour de l'agent de mise à jour. Tous les Agents OfficeScan dépendent toujours du serveur OfficeScan.

Attribuer à des agents OfficeScan le rôle d'agents de mise à jour

Procédure

1. Sélectionnez les éléments que les agents de mise à jour peuvent partager.
   - Mises à jour des composants
   - Paramètres de domaine
   - Programmes et correctifs de type hot fix des agents OfficeScan

Chapitre 13

Paramètres des stratégies de surveillance des comportements

Cette section décrit comment configurer les stratégies de surveillance des comportements sur les Agents OfficeScan.

Les rubriques sont les suivantes :

- *Surveillance des comportements à la page 13-2*
- *Configuration des règles et des exceptions de surveillance des comportements à la page 13-15*

Surveillance des comportements

La surveillance des comportements surveille continuellement les endpoints, guettant les modifications inhabituelles du système d'exploitation ou des logiciels installés. La surveillance des comportements protège les endpoints via le **blocage du comportement des programmes malveillants** et la **surveillance des événements**. Une **liste d'exceptions** configurée par l'utilisateur et **Certified Safe Software Service** viennent compléter ces deux fonctionnalités.

Important

- La surveillance des comportements ne prend pas en charge les plates-formes 64 bits Windows XP ou Windows 2003.
- Par défaut, la surveillance des comportements est désactivée sur toutes les versions des plates-formes Windows Server.

Blocage des comportements de malwares

Le blocage du comportement des programmes malveillants fournit un niveau nécessaire de protection supplémentaire contre les menaces pour les programmes qui affichent un comportement malveillant. Il observe les événements du système sur une période de temps. Pendant que les programmes exécutent différentes combinaisons ou séquences d'actions, le blocage du comportement des programmes malveillants détecte les comportements malveillants connus et bloque les programmes associés. Elle vous permet d'assurer un haut niveau de protection contre les nouvelles menaces inconnues et émergentes.

La surveillance des comportements de programmes malveillants fournit les options de scan de niveau de menace suivantes :

- **Menaces connues** : bloque les comportements associés aux menaces de programmes malveillants connues.
- **Menaces connues et potentielles** : bloque le comportement associé aux menaces connues et prend des mesures en cas de détection d'un comportement potentiellement malveillant.

Après le blocage d'un programme dont les notifications sont activées, l'Agent OfficeScan affiche une notification sur l'Endpoint.

Protection contre les ransomwares

La protection contre les ransomwares permet d'éviter la modification et le chiffrement non autorisés des fichiers sur des agents par des menaces de « ransomwares ». Ransomware est un type de programme malveillant qui restreint l'accès à des fichiers et exige un paiement pour restaurer les fichiers affectés.

OfficeScan propose les méthodes suivantes pour protéger votre environnement contre les menaces de ransomwares.

Remarque

Pour éviter que l'Agent OfficeScan ne détecte un processus sûr comme étant malveillant, vérifiez que l'agent peut accéder à Internet afin de procéder à des vérifications supplémentaires à l'aide des serveurs Trend Micro.

OPTION	DESCRIPTION
Protéger des documents contre toute opération de chiffrement ou de modification non autorisée	Vous pouvez configurer la surveillance des comportements afin qu'elle détecte une séquence spécifique d'événements susceptibles d'indiquer une attaque de Ransomware. Si tous les critères suivants sont réunis, l'Agent OfficeScan arrête les programmes malveillants et tente de les mettre en quarantaine : 1. processus non reconnu comme sans danger qui tente de modifier, supprimer ou renommer trois fichiers dans un certain intervalle de temps. 2. processus ayant tenté de modifier un type d'extension de fichier protégé En outre, activez **Sauvegarder automatiquement les fichiers modifiés par des programmes suspects** pour créer des copies de fichiers chiffrés sur des endpoints. Après la fin du processus de chiffrement et la détection d'une menace de ransomware par OfficeScan, ce dernier invite les utilisateurs finaux à restaurer les fichiers concernés sans subir de perte de données. **Remarque** La sauvegarde automatique des fichiers nécessite au moins 100 Mo d'espace disque sur l'endpoint de l'agent et ne sauvegarde que les fichiers d'une taille inférieure à 10 Mo. L'emplacement du dossier de sauvegarde sur les endpoints de l'agent est :<Dossier d'installation de l'agent>`\CCSF \module\DRE\data`. **AVERTISSEMENT!** Si **Sauvegarder automatiquement les fichiers modifiés par des programmes suspects** n'est pas activé, OfficeScan ne peut pas récupérer les premiers fichiers affectés par une menace de ransomware.

OPTION	DESCRIPTION
Bloquer les processus généralement associés à des ransomwares	Les ransomwares distribuent généralement les fichiers exécutables dans des emplacements spécifiques sur des endpoints avant de tenter de pirater des fichiers. Le blocage des processus démarrés à partir de ces emplacements peut contribuer à empêcher les ransomwares de pirater des fichiers.
Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis	L'inspection des programmes surveille les processus et effectue un accrochage aux API pour déterminer si un programme se comporte de façon inattendue. Bien que cette procédure augmente le taux de détection globale de fichiers exécutables compromis, cela peut entraîner une diminution des performances système. **Conseil** L'inspection des programmes fournit une meilleure sécurité si vous sélectionnez **Menaces connues et potentielles** dans la liste déroulante **Menaces à bloquer**. **Important** Non pris en charge sur les plates-formes Windows Server 2003 sans SP2 (ou version ultérieure) et Windows XP 64 bits.

Protection contre les exploitations

La protection contre les exploitations fonctionne en binôme avec l'inspection des programmes pour surveiller le comportement des programmes et détecter un comportement anormal pouvant indiquer qu'un pirate a exploité la vulnérabilité d'un programme. Après détection, la surveillance des comportements met fin au processus du programme.

Important

La protection contre les exploitations impose la sélection de l'option **Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis**.

Protection de programme récemment trouvé

La surveillance des comportements fonctionne en binôme avec les services de Web Reputation et le scan en temps réel pour vérifier la prévalence des fichiers téléchargés via des canaux Web, des applications de messagerie ou des scripts de macros de Microsoft Office. Après avoir détecté un nouveau fichier, les administrateurs peuvent afficher un message à l'attention des utilisateurs qui s'apprêtent à l'exécuter. Trend Micro classe le programme comme nouveau en fonction du nombre de détections ou de l'ancienneté du fichier, tels qu'ils sont déterminés par Smart Protection Network.

La surveillance des comportements scanne les types de fichiers suivants pour chaque canal :

- Web (HTTP/HTTPS) : scanne les fichiers `.exe`.
- Applications de messagerie électronique :scanne les fichiers `.exe`, ainsi que les fichiers `.exe` compressés dans des fichiers `.zip` et `.rar` non chiffrés.

Remarque

- Les administrateurs doivent activer les services Web Reputation sur l'agent pour autoriser l'Agent OfficeScan à scanner le trafic HTTP ou HTTPS avant de pouvoir afficher cette invite.
- L'Agent OfficeScan fait correspondre les noms des fichiers téléchargés via des applications de messagerie lors du processus d'exécution. Si le nom de fichier a été modifié, l'utilisateur ne reçoit pas d'invite.

Surveillance des événements

La surveillance des événements fournit une approche plus générique de la protection contre les logiciels non autorisés et les attaques de programmes malveillants. Elle surveille les zones du système pour certains événements, permettant aux administrateurs de gérer les programmes qui déclenchent ces événements. Utilisez la surveillance des événements si vous avez des exigences de protection du système spécifiques différentes de la protection fournie par le blocage du comportement des programmes malveillants.

Le tableau suivant répertorie les événements du système surveillés.

TABLEAU 13-1. Événements du système surveillés

ÉVÉNEMENTS	DESCRIPTION
Fichier système dupliqué	De nombreux programmes malveillants créent des copies d'eux-mêmes ou d'autres programmes malveillants à l'aide de noms de fichiers utilisés par les fichiers système Windows. Cette opération vise généralement à remplacer les fichiers système, à éviter la détection ou à décourager les utilisateurs de supprimer les fichiers malveillants.
Modification du fichier d'hôtes	Le fichier d'hôtes fait correspondre les noms de domaines aux adresses IP. De nombreux programmes malveillants modifient le fichier Hosts de telle sorte que le navigateur Web soit redirigé vers des sites Web infectés, inexistants ou contrefaits.
Comportement suspect	Un comportement suspect peut être une action spécifique ou une série d'actions rarement effectuées par des programmes légitimes. Les programmes présentant un comportement suspect doivent être utilisés avec prudence.
Nouveau plug-in Internet Explorer	Les spywares/graywares installent souvent des plug-ins Internet Explorer indésirables tels que des barres d'outils et des Browser Helper Objects.
Modification des paramètres d'Internet Explorer	De nombreux virus/programmes malveillants modifient les paramètres d'Internet Explorer, notamment la page d'accueil, les sites Web de confiance, les paramètres de serveur proxy et les extensions de menu.
Modification de la stratégie de sécurité	Les modifications de la stratégie de sécurité Windows peuvent permettre à des applications indésirables de s'exécuter ou de modifier les paramètres système.
Injection de la bibliothèque de programmes	De nombreux programmes malveillants configurent Windows pour que toutes les applications chargent automatiquement une bibliothèque de programmes (DLL). Les routines malveillantes de la DLL peuvent ainsi s'exécuter à chaque fois qu'une application démarre.

ÉVÉNEMENTS	DESCRIPTION
Modification du shell	De nombreux programmes malveillants modifient les paramètres du shell Windows de manière à s'associer eux-mêmes à certains types de fichiers. Cette routine leur permet de se lancer automatiquement si les utilisateurs ouvrent les fichiers associés dans l'Explorateur Windows. La modification des paramètres du shell Windows peut aussi permettre à des programmes malveillants de suivre les programmes utilisés et de s'exécuter conjointement avec les applications légitimes.
Nouveau service	Les services Windows sont des processus dotés de fonctions spéciales qui s'exécutent généralement en continu à l'arrière plan, avec un accès administratif total. Les programmes malveillants s'installent parfois sous forme de services pour rester cachés.
Modification de fichiers système	Certains fichiers système de Windows déterminent le comportement du système et notamment les paramètres relatifs aux programmes de démarrage et aux économiseurs d'écran. De nombreux programmes malveillants modifient les fichiers système de manière à s'exécuter automatiquement au démarrage et contrôler le comportement du système.
Modification de la stratégie de pare-feu	La stratégie de pare-feu Windows détermine quelles applications ont accès au réseau, quels ports sont ouverts à la communication et quelles adresses IP peuvent communiquer avec l'ordinateur. De nombreux programmes malveillants modifient la stratégie de manière à s'octroyer à eux-mêmes l'accès au réseau et à Internet.
Modification de processus système	De nombreux programmes malveillants effectuent diverses actions sur les processus intégrés à Windows Ces actions peuvent consister à interrompre ou modifier des processus en cours d'exécution.
Nouveau programme de démarrage	En règle générale, les applications malveillantes ajoutent ou modifient les entrées du démarrage automatique dans le registre Windows pour se lancer automatiquement à chaque démarrage de l'ordinateur.

Lorsque la surveillance des événements détecte un événement du système surveillé, elle exécute l'action configurée pour l'événement.

Le tableau suivant répertorie les éventuelles mesures que les administrateurs peuvent prendre sur les événements du système surveillés.

TABLEAU 13-2. Actions sur les événements du système surveillés

ACTION	DESCRIPTION
Évaluer	L'Agent OfficeScan autorise toujours l'exécution des programmes associés à un événement et consigne l'événement pour évaluation. Il s'agit de l'action par défaut pour tous les événements du système surveillés. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Autoriser	L'Agent OfficeScan autorise toujours l'exécution des programmes associés à un événement.
Demander si nécessaire	L'Agent OfficeScan invite les utilisateurs à autoriser ou refuser les programmes associés à un événement et ajoute les programmes à la liste d'exceptions Si l'utilisateur ne répond pas dans le délai imparti, l'Agent OfficeScan autorise automatiquement l'exécution du programme. La valeur par défaut de la période est 30 secondes. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Refuser	L'Agent OfficeScan bloque toujours l'exécution des programmes associés à un événement et consigne l'événement. Après le blocage d'un programme dont les notifications sont activées, l'Agent OfficeScan affiche une notification sur l'Endpoint.

Liste d'exceptions de la surveillance des comportements

La liste d'exceptions de la surveillance des comportements contient les programmes que l'Agent OfficeScan ne surveille pas avec la surveillance des comportements.

- **Programmes approuvés** : l'Agent OfficeScan permet à tous les programmes de la liste des programmes approuvés d'ignorer le scan de surveillance des comportements.

Remarque

Bien que la surveillance des comportements ne prenne aucune mesure sur les programmes ajoutés à la liste des programmes approuvés, d'autres fonctions de scan (par exemple, le scan basé sur les fichiers) continuent à scanner le programme avant de permettre l'exécution du programme.

- **Programmes bloqués** : l'Agent OfficeScan bloque tous les programmes figurant dans la liste des programmes bloqués. Pour configurer la liste des programmes bloqués, activez la surveillance des événements.

Configurez la liste d'exceptions depuis la console Web. Vous pouvez également accorder aux utilisateurs le privilège de configurer leur propre liste d'exceptions depuis la console de l'Agent OfficeScan.

Pour plus d'informations, voir *Configuration des privilèges d'agent à la page 12-4*.

Prise en charge des caractères génériques de la liste d'exceptions

La liste approuvée de surveillance des comportements d'OfficeScan prend en charge l'utilisation des caractères génériques lors de la définition de chemins d'accès aux fichiers, de noms de fichiers et de types d'exceptions d'extension. Utilisez les tableaux suivants pour correctement formater vos listes d'exceptions afin de vous assurer qu'OfficeScan exclut les fichiers et dossiers appropriés du scan.

Caractères génériques pris en charge :

- Astérisque (*) : représente n'importe quel caractère ou n'importe quelle chaîne de caractères.
- Point d'interrogation (?) : représente un seul caractère.

Important

La liste approuvée de surveillance des comportements d'OfficeScan ne prend pas en charge l'utilisation des caractères génériques pour remplacer des dénominations de lecteur système ou des adresses UNC.

TYPE D'EXCEPTION	UTILISATION DE CARACTÈRES GÉNÉRIQUES	CORRESPONDENT	NE CORRESPONDENT PAS
Répertoires	`C:\*` Exclut tous les fichiers et dossiers sur le lecteur spécifié	• `C:\sample.exe` • `C:\folder\test.doc`	• `D:\sample.exe` • `E:\folder\test.doc`
Certains fichiers dans une couche de dossier spécifique	`C:\*\Sample.exe` Exclut le fichier `Sample.exe` uniquement si celui-ci se trouve dans un sous-dossier du répertoire `C:\`	• `C:\files\Sample.exe` • `C:\temp\files\Sample.exe`	• `C:\sample.exe`
Chemins UNC	`\\<chemin UNC>\*\Sample.exe` Exclut le fichier `Sample.exe` uniquement si celui-ci se trouve dans un sous-dossier du chemin UNC spécifié	• `\\<chemin UNC>\files\Sample.exe` • `\\<chemin UNC>\temp\files\Sample.exe`	• `R:\files\Sample.exe` Motif : les lecteurs mappés ne sont pas pris en charge. • `\\<chemin UNC>\Sample.exe` Motif : le fichier n'existe pas dans un sous-dossier du chemin d'accès UNC.

TYPE D'EXCEPTION	UTILISATION DE CARACTÈRES GÉNÉRIQUES	CORRESPONDENT	NE CORRESPONDENT PAS
Noms de fichiers et extensions	`C:\*.*` Exclut tous les fichiers avec extensions dans tous les dossiers et sous-dossiers du répertoire `C:\`	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\test.doc`	• `D:\sample.exe` • `C:\Sample` **Remarque** `C:\Sample` n'a pas d'extension de fichier et n'est donc pas exclu du scan.
Noms de fichiers	`C:\*.exe` Exclut tous les fichiers ayant l'extension `.exe` dans tous les dossiers et sous-dossiers du répertoire `C:\`	• `C:\Sample.exe` • `C:\temp\test.exe`	• `C:\Sample.doc` • `C:\temp\test.bat` • `C:\Sample` **Remarque** `C:\Sample` n'a pas d'extension de fichier et n'est donc pas exclu du scan.

TYPE D'EXCEPTION	UTILISATION DE CARACTÈRES GÉNÉRIQUES	CORRESPONDENT	NE CORRESPONDENT PAS
Extensions de fichier	`C:\Sample.*` Exclut tous les fichiers portant le nom `Sample` et n'importe quelle extension dans tous les dossiers et sous-dossiers du répertoire `C:\`	• `C:\Sample.exe` • `C:\temp\Sample.doc`	• `C:\Sample1.doc` • `C:\temp\Samples.bat` • `C:\Sample` **Remarque** `C:\Sample` n'a pas d'extension de fichier et n'est donc pas exclu du scan.
Fichiers dans des structures de répertoires spécifiques	`C:\*\*\Sample.exe` Exclut tous les fichiers situés dans la deuxième couche de sous-dossier ou dans n'importe quel sous-dossier subséquent du répertoire `C:\` portant le nom de fichier et l'extension `Sample.exe`	• `C:\files\temp\Sample.exe` • `C:\files\temp\test\Sample.exe`	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\files\temp\Sample.doc`

TYPE D'EXCEPTION	UTILISATION DE CARACTÈRES GÉNÉRIQUES	CORRESPONDENT	NE CORRESPONDENT PAS
Chemins ou noms de fichiers complexes	`C:\Sam*e??.exe` Exclut tous les fichiers dont les noms remplissent les conditions suivantes : • Commencent par les caractères « Sam » • Le troisième avant-dernier caractère du nom de fichier doit être « e ». • Au moins 1 caractère existe entre la chaîne « Sam » de début et la chaîne de fin « e?? » du nom de fichier • Exactement 2 caractères existent avant l'extension de fichier et après le « e » dans le nom de fichier • L'extension de fichier est `.exe` Si un fichier répond à toutes les conditions requises et se trouve dans n'importe quel sous-dossier du répertoire `C:\`, OfficeScan exclut ce fichier des scans.	• `C:\Sample12.exe` • `C:\test\SametimeAA.exe` • `C:\SamSamSample12.exe`	• `C:\SaSmple12.exe` Motif : ne commence pas par « Sam » • `C:\SamSamSam12.exe` Motif : ne contient pas de « e » comme troisième avant-dernier caractère • `C:\Same12.exe` Motif : n'inclut pas de caractères entre la chaîne de début « Sam » et le troisième avant-dernier caractère « e » • `C:\Sample1.exe` Motif : n'inclut pas 2 caractères avant l'extension et après le « e » • `C:\Sample12.doc` Motif : extension incorrecte

Configuration des règles et des exceptions de surveillance des comportements

Configurez les stratégies de surveillance des comportements pour protéger les Endpoints contre les logiciels de rançon, les attaques par exploitation et les menaces émergentes. Utilisez la fonction de surveillance des événements pour évaluer ou bloquer les comportements couramment associés aux programmes malveillants.

Remarque

- La surveillance des comportements ne prend pas en charge les plates-formes 64 bits Windows XP ou Windows 2003.
- Par défaut, la surveillance des comportements est désactivée sur toutes les versions des plates-formes Windows Server.

Procédure

1. Dans la section **Blocage du comportement des programmes malveillants** :
   a. Sélectionnez **Activer le blocage du comportement des programmes malveillants** et spécifiez les types de menaces à bloquer :
      - **Menaces connues** : bloque les comportements associés à des menaces connues liées à des programmes malveillants
      - **Menaces connues et potentielles** : bloque les comportements associés à des menaces connues et entreprend une action sur les comportements potentiellement malveillants
   b. Sélectionner les fonctionnalités de protection contre les logiciels de rançon que vous souhaitez activer pour vous protéger contre les menaces des logiciels de rançon.
      - **Protéger des documents contre toute opération de chiffrement ou de modification non autorisée** : Empêche les menaces potentielles de logiciels de rançon de chiffrer ou de modifier le contenu de documents
        - **Sauvegarder et restaurer automatiquement les fichiers modifiés par des programmes suspects** : crée des copies de

sauvegarde de fichiers chiffrés sur des Endpoints afin d'éviter toute perte de données après détection d'une menace de logiciel de rançon

Remarque

La sauvegarde automatique des fichiers nécessite au moins 100 Mo d'espace disque sur l'endpoint de l'agent et ne sauvegarde que les fichiers d'une taille inférieure à 10 Mo.

- **Bloquer les processus généralement associés à des logiciels de rançon** : Bloque les processus associés à des menaces de logiciels de rançon avant qu'ils ne puissent effectuer un chiffrement ou une modification de documents
- **Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis** : L'inspection des programmes surveille les processus et effectue un accrochage aux API pour déterminer si un programme se comporte de façon inattendue. Bien que cette procédure augmente le taux de détection globale de fichiers exécutables compromis, cela peut entraîner une diminution des performances système.

Conseil

L'inspection des programmes fournit une meilleure sécurité si vous sélectionnez **Menaces connues et potentielles** dans la liste déroulante **Menaces à bloquer**.

Pour plus de détails, voir *Protection contre les ransomwares à la page 13-3*.

c. Sous **Protection contre les exploitations**, activez **Arrêter les programmes qui présentent un comportement anormal associé à des attaques par exploitation** pour protéger contre les programmes potentiellement exploités.

Remarque

La protection contre les exploitations impose la sélection de l'option **Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis**.

Pour obtenir des informations détaillées, consultez la section *Protection contre les exploitations à la page 13-5*.

2. Dans la section **Programmes récemment trouvés**, activez **Surveiller les programmes récemment trouvés téléchargés via le Web ou les canaux d'application de messagerie** et sélectionnez s'il convient d'**Inviter l'utilisateur** avant d'exécuter le programme téléchargé ou de demander à OfficeScan de consigner uniquement les détections.

3. Dans la section **Surveillance des événements** :

   a. Sélectionnez **Activer la surveillance des événements**.

   b. Cliquez sur **Spécifier des paramètres détaillés** pour sélectionner les types d'événements à surveiller.

   c. Choisissez les événements du système à surveiller et sélectionnez une action pour chacun de ces événements.

      Pour des informations relatives aux événements du système surveillés et aux actions, voir *Surveillance des événements à la page 13-6*.

4. Cliquez sur l'onglet **Exceptions** pour configurer les listes d'exceptions.

   a. Sous **Saisissez le chemin d'accès complet du programme**, entrez le chemin d'accès complet du programme à approuver ou à bloquer.

      Séparez les entrées multiples par des points virgules (;).

   b. Cliquez sur **Ajouter à la liste des URL approuvées** ou **Ajouter à la liste des URL bloquées**.

   c. Pour supprimer de la liste un programme approuvé ou bloqué, cliquez sur l'icône de la corbeille ( ) en regard du programme.

Remarque

OfficeScan accepte un maximum de 1 024 programmes approuvés et programmes bloqués au total.

Chapitre 14

Paramètres de stratégie de protection contre les programmes malveillants

Cette section décrit comment configurer la détection des programmes malveillants sur les Agents OfficeScan.

Les rubriques sont les suivantes :

- *Types de méthodes de scan à la page 14-2*
- *Scan manuel à la page 14-5*
- *Scan en temps réel à la page 14-13*
- *Scan immédiat à la page 14-22*
- *Scan programmé à la page 14-29*
- *Actions de scan à la page 14-38*
- *Support d'exclusion de scan à la page 14-49*

Types de méthodes de scan

Les Agents OfficeScan peuvent utiliser l'une des deux méthodes de scan disponibles pour rechercher des risques de sécurité. Les méthodes de scan sont le Smart Scan et le scan traditionnel.

- **Smart Scan**

  Les Agents OfficeScan qui utilisent Smart Scan sont appelés **agents Smart Scan** dans ce document. Ces agents bénéficient de scans locaux et de requêtes en ligne fournis par les services de File Reputation.

- **Scan traditionnel**

  Les Agents qui n'utilisent pas Smart Scan sont appelés **agents de scan traditionnel**. Un agent de scan traditionnel stocke tous les composants d'Agent OfficeScan sur l'Endpoint et scanne tous les fichiers localement.

Instructions relatives au changement de méthode de scan

Le tableau suivant présente des remarques que vous devez prendre en compte avant de changer la méthode de scan que les Agents OfficeScan utilisent.

TABLEAU 14-1. Éléments à prendre en compte lorsque vous basculez vers Smart Scan

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Licence du produit	Assurez-vous que vous avez activé toutes les licences requises pour la nouvelle méthode de scan.

Éléments à prendre en compte	Détails
serveur OfficeScan	Vérifiez que les agents peuvent se connecter au serveur OfficeScan. OfficeScan demande uniquement aux agents en ligne de changer de méthode de scan. Les agents hors ligne sont notifiés lorsqu'ils sont en ligne. Les agents indépendants sont notifiés lorsqu'ils sont en ligne ou, dans le cas des agents disposant des privilèges de mise à jour programmée, lors de l'exécution d'une mise à jour programmée. Vérifiez également que le serveur OfficeScan dispose des tout derniers composants pour s’assurer que Agents OfficeScan peut télécharger les bonnes signatures du serveur.
Nombre d'Agents OfficeScan à basculer	Le basculement simultané d'un nombre relativement réduit d'Agents OfficeScan à la fois permet d’utiliser efficacement les ressources du serveur OfficeScan et du serveur Smart Protection Server. Ces serveurs peuvent effectuer d'autres tâches critiques lorsque les Agents OfficeScan changent de méthode de scan.
Synchronisation	Lors de changement de méthode de scan, les Agents OfficeScan doivent télécharger des versions complètes des fichiers de signatures pour la nouvelle méthode de scan. Prévoyez d’effectuer le changement pendant les heures creuses pour minimiser l’impact sur la bande passante réseau et l’interruption des opérations quotidiennes des utilisateurs. Trend Micro recommande de désactiver « Mettre à jour » sur les Agents OfficeScan pendant le processus de conversion.

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Paramètres d'arborescence des agents	La méthode de scan est un paramètre détaillé que vous pouvez appliquer au niveau de la racine, du domaine ou d'un Agent OfficeScan individuel. Lorsque vous changez de méthode de scan, vous pouvez : • Créer un nouveau domaine d'arborescence des agents et attribuer la nouvelle méthode de scan. Tout agent que vous déplacez vers le domaine applique la méthode de scan. Lorsque vous déplacez l'agent, activez le paramètre **Appliquer les paramètres du nouveau domaine aux agents sélectionnés**. • Sélectionner un domaine et configurer la nouvelle méthode de scan. Tous les Agents OfficeScan appartenant au domaine qui n'utilisent pas déjà la méthode de scan basculent vers la nouvelle méthode de scan. • Sélectionner un ou plusieurs Agents OfficeScan d'un domaine et changer la méthode de scan. **Remarque** Tout changement de méthode de scan du domaine remplace la méthode que vous avez configurée pour des agents individuels.

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Prise en charge d'IPv6	Les agents Smart Scan envoient des requêtes de scan aux sources Smart Protection. Un agent Smart Scan IPv6 pur ne peut pas envoyer directement de requêtes à des sources IPv4 pures, telles que : • Smart Protection Server 2.0 (intégré ou autonome) **Remarque** IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5. • Trend Micro Smart Protection Network De même, un agent Smart Scan IPv4 pur ne peut pas envoyer de requêtes à des serveurs Smart Protection IPv6 purs. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents Smart Scan de se connecter aux sources.
Services Smart Protection	Si vous faites basculer les Agents OfficeScan du scan traditionnel vers Smart Scan, assurez-vous d'avoir configuré Smart Protection Services.

Scan manuel

Le scan manuel est un scan à la demande qui démarre immédiatement après avoir été lancé par un utilisateur depuis la console de l'Agent OfficeScan. La durée du scan dépend du nombre de fichiers spécifiés pour le scan et des ressources matérielles du endpoint de l'Agent OfficeScan.

Configurez et appliquez des paramètres de scan manuel à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan manuel

Configurez les paramètres de scan manuel en utilisant les onglets suivants :

- *Scan manuel : onglet Cible à la page 14-6*
- *Scan manuel : onglet Action à la page 14-8*
- *Scan manuel : onglet Exclusion de scan à la page 14-11*

Scan manuel : onglet Cible

Procédure

1. Dans la section **Fichiers à scanner**, sélectionnez l'un des éléments suivants :

   - **Tous les fichiers scannables** inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

     Remarque

     Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

   - **Types de fichiers scannés par IntelliScan** scanne les fichiers d'après le véritable type de fichier.
   - **Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :** spécifie manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

Remarque

Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

- **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

2. Dans la section **Paramètres de scan**, configurez les paramètres requis.

PARAMÈTRE	DESCRIPTION
Scanner les dossiers cachés	Permet à l'Agent OfficeScan de détecter, puis de scanner les dossiers marqués sur l'Endpoint
Scanner les lecteurs de réseau	Scanne les répertoires physiquement situés sur d'autres Endpoints, mais mappés sur l'Endpoint local
Scanner les fichiers compressés	Scanne le nombre spécifié de couches de compression au sein d'un fichier archivé **Remarque** Le scan sur plusieurs couches peut détecter des programmes malveillants intentionnellement enfouis dans une archive compressée, cependant le scan peut affecter les performances du système.

PARAMÈTRE	DESCRIPTION
Scanner les objets OLE	Scanne le nombre spécifié de couches Object Linking and Embedding (OLE) dans un fichier **Détecter le code d'exploitation dans les fichiers OLE** : la détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office. **Remarque** Le nombre de couches spécifié s'applique aux options **Scanner les objets OLE** et **Détecter le code d'exploitation dans les fichiers OLE**.
Scanner la zone d'amorçage	Scanne le secteur d'amorçage du disque dur de l'Endpoint à la recherche de virus/programmes malveillants

3. Dans la section **Utilisation du processeur**, sélectionnez l'un des éléments suivants :

   - **Élevé** : aucune interruption entre les scans
   - **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50% et pas d'interruption si elle est de 50% ou moins
   - **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Scan manuel : onglet Action

Procédure

1. Dans la section **Virus/programmes malveillants**, configurez les paramètres requis.

   a. Sélectionnez le type d'action que l'Agent OfficeScan entreprend après la détection d'une menace pour la sécurité.

- **Utiliser ActiveAction** : cette fonction utilise un ensemble d'actions de scan pré-configurées destinées à lutter contre les virus et les programmes malveillants.

  Pour plus d'informations, voir *ActiveAction à la page 14-38*.

  - **Personnaliser l'action pour les virus/programmes malveillants probables** : sélectionnez et spécifiez l'action que l'Agent OfficeScan entreprend en cas de programmes malveillants probables

- **Utiliser la même action pour tous les types de virus/programmes malveillants** : spécifiez l'action que l'Agent OfficeScan entreprend sur toutes les menaces de programmes malveillants

- **Utiliser une action spécifique pour chaque type de virus/programme malveillant** : spécifiez l'action que l'Agent OfficeScan entreprend en cas de menaces de sécurité spécifiques

  Pour plus d'informations, voir *Actions de scan personnalisées à la page 14-40*.

b. Sélectionnez **Sauvegarder les fichiers avant nettoyage** pour créer une copie chiffrée du fichier infecté sur l'Endpoint dans le dossier `<dossier d'installation de l'agent>\Backup`.

   La création d'une copie de sauvegarde du fichier vous permet de restaurer la version d'origine du fichier, si nécessaire.

c. Spécifiez l'emplacement du répertoire de quarantaine.

   - **Mettre en quarantaine sur le serveur gérant l'agent OfficeScan** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine au serveur de gestion OfficeScan

   - **Répertoire de quarantaine** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine à l'emplacement spécifié

   Pour plus d'informations, voir *Quarantine Directory à la page 14-41*.

d. Dans la section **Damage Cleanup Services**, configurez les éléments suivants :

- **Type de nettoyage**
  - **Nettoyage standard** : l'Agent OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
    - Détecte et supprime les chevaux de Troie actifs
    - Élimine les processus créés par les chevaux de Troie
    - Répare les fichiers système modifiés par les chevaux de Troie
    - Supprime les fichiers et les applications laissés par les chevaux de Troie
  - **Nettoyage avancé** : outre les actions de nettoyage standard, l'Agent OfficeScan interrompt les activités de logiciels de sécurité non autorisés, connus également sous le nom de « FakeAV », et certaines variantes de rootkits.
- **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté** : effectue le type de nettoyage configuré sur de probables menaces de programmes malveillants

Remarque

Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**.

2. Dans la section **Spyware/Grayware**, sélectionnez l'action que l'Agent OfficeScan entreprend après la détection de spywares/graywares.
   - **Nettoyer** : termine tous les processus liés et supprime les valeurs de registre, fichiers, cookies et raccourcis associés

Remarque

Après avoir nettoyé des spywares/graywares, les Agents OfficeScan sauvegardent les données concernant ces programmes. Vous pouvez restaurer ces données si vous estimez que l'accès à ces spywares/graywares est sans danger.

- **Ignorer** : consigne la détection mais permet l'exécution du programme

Scan manuel : onglet Exclusion de scan

Procédure

1. Sélectionnez **Activer l'exclusion de scan**.
2. Dans la section **Liste des exclusions de scan (répertoires)**, configurez les paramètres requis.
   a. Sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** pour automatiquement exclure les répertoires associés à d'autres produits Trend Micro.

      Pour plus d'informations, voir *Exclusions du répertoire des produits Trend Micro à la page 14-49*.

   b. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   c. Saisissez un chemin d'accès à un répertoire à exclure des scans, puis cliquez sur le bouton **+**.

      L'Agent OfficeScan ne scanne pas les fichiers situés dans le répertoire spécifié (et ses sous-répertoires).

Remarque

- Vous pouvez spécifier un maximum de 256 répertoires à exclure du scan.
- Les exclusions de répertoires prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

3. Dans la section **Liste des exclusions de scan (fichiers)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
   - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Saisissez un nom de fichier ou le nom de fichier avec un chemin d'accès à un répertoire complet à exclure des scans, puis cliquez sur le bouton **+**.

Remarque

- Vous pouvez spécifier un maximum de 256 fichiers à exclure du scan.
- Les exclusions de fichiers prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

4. Dans la section **Liste des exclusions de scan (extensions de fichier)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent

- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

b. Sélectionnez ou saisissez une extension de fichier à exclure des scans, puis cliquez sur le bouton **Ajouter >**.

Remarque

- Vous pouvez spécifier au maximum 256 extensions de fichier à exclure du scan.
- Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) pour remplacer un seul caractère ou un astérisque (*) pour remplacer plusieurs caractères comme caractères génériques. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*` ou `D??`.

Scan en temps réel

Le scan en temps réel s'effectue en continu. Lors de la réception, de l'ouverture, du téléchargement, de la copie ou de la modification d'un fichier, le scan en temps réel recherche les risques pour la sécurité. Si l'Agent OfficeScan ne détecte pas de risque de sécurité, les utilisateurs peuvent accéder au fichier. Si l'Agent OfficeScan détecte un risque de sécurité ou un virus/programme malveillant probable, un message de notification s'affiche indiquant le nom du fichier infecté et le risque de sécurité spécifique.

Le scan en temps réel dispose d'une mémoire cache persistante rechargée à chaque démarrage de l'Agent OfficeScan. Si des fichiers ou des dossiers ont été modifiés depuis le dernier déchargement de l'Agent OfficeScan, ce dernier les supprime de la mémoire cache.

Configuring Real-time Scan Settings

Procédure

1. Sélectionnez les options suivantes :
   - **Activer le scan antivirus/programme malveillant**
   - **Activer le scan antispyware/grayware**

   Remarque

   Vous devez activer le scan de virus/programmes malveillants avant que vous puissiez activer le scan anti-spyware et anti-grayware. Au cours d'une épidémie virale, l'Agent OfficeScan active automatiquement le scan en temps réel et vous ne pouvez pas désactiver le scan avant la fin de l'épidémie. Le scan en temps réel contribue à empêcher les virus de modifier ou de supprimer des fichiers et des dossiers sur les Endpoints.

2. Configurez les paramètres **Cible**.

   Pour plus d'informations, voir *Scan en temps réel : onglet cible à la page 14-14*.

3. Configurez les paramètres **Action**.

   Pour plus d'informations, voir *Scan en temps réel : onglet Action à la page 14-17*.

4. Configurez les paramètres **Exclusion de scan**.

   Pour plus d'informations, voir *Scan en temps réel : onglet Exclusion de scan à la page 14-20*.

Scan en temps réel : onglet cible

Procédure

1. Dans la section **Action des utilisateurs sur les fichiers**, sélectionnez les opérations de fichiers déclenchant un scan dans la liste déroulante **Scanner les fichiers en cours de**.

- **Création/modification et récupération** : scanne tous les fichiers créés, modifiés ou ouverts sur l'Endpoint
- **Création/modification** : scanne tous les fichiers créés ou modifiés sur l'Endpoint
- **Récupération** : scanne tous les fichiers ouverts sur l'Endpoint

2. Dans la section **Fichiers à scanner**, sélectionnez l'un des éléments suivants :

   - **Tous les fichiers scannables** inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

     Remarque

     Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

   - **Types de fichiers scannés par IntelliScan** scanne les fichiers d'après le véritable type de fichier.
   - **Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :** spécifie manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

     Remarque

     Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

     - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
     - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

3. Dans la section **Paramètres de scan**, configurez les paramètres requis.

PARAMÈTRE	DESCRIPTION
Scanner les disquettes pendant l'arrêt	Scanne les disquettes pendant l'arrêt
Scanner les lecteurs de réseau	Scanne les répertoires physiquement situés sur d'autres Endpoints, mais mappés sur l'Endpoint local
Scanner le secteur d'amorçage du dispositif de stockage USB après sa connexion	Ne scanne automatiquement que le secteur d'amorçage d'un dispositif de stockage USB chaque fois que l'utilisateur le connecte
Scanner tous les fichiers des périphériques de stockage amovibles lors de leur connexion	Scanne automatiquement tous les fichiers d'un dispositif de stockage USB chaque fois que l'utilisateur le connecte
Mettre en quarantaine les variantes de programmes malveillants détectées en mémoire	La surveillance des comportements recherche dans la mémoire système des processus suspects, tandis que le scan en temps réel mappe le processus et y recherche la présence de menaces de programmes malveillants. S'il existe une menace de programme malveillant, le scan en temps réel met le processus et/ou le fichier en quarantaine.
Scanner les fichiers compressés	Scanne le nombre spécifié de couches de compression au sein d'un fichier archivé **Remarque** Le scan sur plusieurs couches peut détecter des programmes malveillants intentionnellement enfouis dans une archive compressée, cependant le scan peut affecter les performances du système.

PARAMÈTRE	DESCRIPTION
Scanner les objets OLE	Scanne le nombre spécifié de couches Object Linking and Embedding (OLE) dans un fichier **Détecter le code d'exploitation dans les fichiers OLE** : la détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office. **Remarque** Le nombre de couches spécifié s'applique aux options **Scanner les objets OLE** et **Détecter le code d'exploitation dans les fichiers OLE**.
Activer IntelliTrap	Détecte les codes malveillants, tels que les logiciels robots, dans les fichiers compressés
Activer le scan de l'exploitation CVE pour les fichiers téléchargés via Web et e-mail	Bloque les processus qui tentent d'exploiter des failles connues dans des produits disponibles dans le commerce, sur la base du système CVE (Common Vulnerabilities and Exposures)

Scan en temps réel : onglet Action

Procédure

1. Dans la section **Virus/programmes malveillants**, configurez les paramètres requis.

   a. Sélectionnez le type d'action que l'Agent OfficeScan entreprend après la détection d'une menace pour la sécurité.

   - **Utiliser ActiveAction** : cette fonction utilise un ensemble d'actions de scan pré-configurées destinées à lutter contre les virus et les programmes malveillants.

     Pour plus d'informations, voir *ActiveAction à la page 14-38*.

- **Personnaliser l'action pour les virus/programmes malveillants probables** : sélectionnez et spécifiez l'action que l'Agent OfficeScan entreprend en cas de programmes malveillants probables

- **Utiliser la même action pour tous les types de virus/programmes malveillants** : spécifiez l'action que l'Agent OfficeScan entreprend sur toutes les menaces de programmes malveillants

- **Utiliser une action spécifique pour chaque type de virus/programme malveillant** : spécifiez l'action que l'Agent OfficeScan entreprend en cas de menaces de sécurité spécifiques

  Pour plus d'informations, voir *Actions de scan personnalisées à la page 14-40*.

b. Sélectionnez les types de notification qui s'affichent pour les utilisateurs finaux.

- **Afficher une notification lorsqu'un virus/programme malveillant est détecté** : choisissez d'afficher une notification informant l'utilisateur de l'Agent OfficeScan de la détection d'un programme malveillant

- **Afficher une notification lorsqu'un virus/programme malveillant est détecté** : choisissez d'afficher une notification informant l'utilisateur de l'Agent OfficeScan de la détection d'un probable programme malveillant

c. Sélectionnez **Sauvegarder les fichiers avant nettoyage** pour créer une copie chiffrée du fichier infecté sur l'Endpoint dans le dossier `<dossier d'installation de l'agent>\Backup`.

   La création d'une copie de sauvegarde du fichier vous permet de restaurer la version d'origine du fichier, si nécessaire.

d. Spécifiez l'emplacement du répertoire de quarantaine.

- **Mettre en quarantaine sur le serveur gérant l'agent OfficeScan** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine au serveur de gestion OfficeScan

- **Répertoire de quarantaine** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine à l'emplacement spécifié

Pour plus d'informations, voir *Quarantine Directory à la page 14-41*.

e. Dans la section **Damage Cleanup Services**, configurez les éléments suivants :

- **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté** : effectue le type de nettoyage configuré sur de probables menaces de programmes malveillants

Remarque

Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**.

2. Dans la section **Spyware/Grayware**, sélectionnez l'action que l'Agent OfficeScan entreprend après la détection de spywares/graywares.

- **Nettoyer** : termine tous les processus liés et supprime les valeurs de registre, fichiers, cookies et raccourcis associés

Remarque

Après avoir nettoyé des spywares/graywares, les Agents OfficeScan sauvegardent les données concernant ces programmes. Vous pouvez restaurer ces données si vous estimez que l'accès à ces spywares/graywares est sans danger.

- **Refuser l'accès** : empêche l'utilisateur final d'ouvrir ou de copier les composants du spyware/grayware
- **Afficher une notification sur les Endpoints lorsqu'un spyware/grayware est détecté** : sélectionnez cette option pour afficher une notification informant l'utilisateur de l'Agent OfficeScan lorsqu'une détection de spyware/grayware se produit

Scan en temps réel : onglet Exclusion de scan

Procédure

1. Sélectionnez **Activer l'exclusion de scan**.

2. Dans la section **Liste des exclusions de scan (répertoires)**, configurez les paramètres requis.

   a. Sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** pour automatiquement exclure les répertoires associés à d'autres produits Trend Micro.

   Pour plus d'informations, voir *Exclusions du répertoire des produits Trend Micro à la page 14-49*.

   b. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
   - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   c. Saisissez un chemin d'accès à un répertoire à exclure des scans, puis cliquez sur le bouton **+**.

   L'Agent OfficeScan ne scanne pas les fichiers situés dans le répertoire spécifié (et ses sous-répertoires).

   Remarque

   - Vous pouvez spécifier un maximum de 256 répertoires à exclure du scan.
   - Les exclusions de répertoires prennent en charge l'utilisation de caractères génériques.

     Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

3. Dans la section **Liste des exclusions de scan (fichiers)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Saisissez un nom de fichier ou le nom de fichier avec un chemin d'accès à un répertoire complet à exclure des scans, puis cliquez sur le bouton **+**.

   Remarque

   - Vous pouvez spécifier un maximum de 256 fichiers à exclure du scan.
   - Les exclusions de fichiers prennent en charge l'utilisation de caractères génériques.

     Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

4. Dans la section **Liste des exclusions de scan (extensions de fichier)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Sélectionnez ou saisissez une extension de fichier à exclure des scans, puis cliquez sur le bouton **Ajouter >**.

Remarque

- Vous pouvez spécifier au maximum 256 extensions de fichier à exclure du scan.
- Le scan en temps réel ne prend pas en charge l'utilisation de caractères génériques pour les exclusions d'extension.

Scan immédiat

Le scan immédiat est lancé à distance par des administrateurs via la console Web et peut être ciblé sur un ou plusieurs Endpoints de l'Agent OfficeScan.

Configurez et appliquez des paramètres de scan immédiat à un ou plusieurs Agents OfficeScan et domaines, ou à tous les Agents OfficeScan gérés par le serveur.

Configuration des paramètres de scan immédiat

Procédure

1. Sélectionnez les options suivantes :
   - **Activer le scan antivirus/programme malveillant**
   - **Activer le scan antispyware/grayware**

   Remarque

   Vous devez activer le scan de virus/programmes malveillants avant que vous puissiez activer le scan anti-spyware et anti-grayware.

2. Configurez les paramètres **Cible**.

   Pour plus d'informations, voir *Scan immédiat : onglet cible à la page 14-23*.

3. Configurez les paramètres **Action**.

   Pour plus d'informations, voir *Scan immédiat : onglet Action à la page 14-25*.

4. Configurez les paramètres **Exclusion de scan**.

   Pour plus d'informations, voir *Scan immédiat : onglet Exclusion du scan à la page 14-27*.

Scan immédiat : onglet cible

Procédure

1. Dans la section **Fichiers à scanner**, sélectionnez l'un des éléments suivants :

   - **Tous les fichiers scannables** inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

     Remarque

     Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

   - **Types de fichiers scannés par IntelliScan** scanne les fichiers d'après le véritable type de fichier.

   - **Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :** spécifie manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

     Remarque

     Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

     - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
     - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

2. Dans la section **Paramètres de scan**, configurez les paramètres requis.

PARAMÈTRE	DESCRIPTION
Scanner les fichiers compressés	Scanne le nombre spécifié de couches de compression au sein d'un fichier archivé **Remarque** Le scan sur plusieurs couches peut détecter des programmes malveillants intentionnellement enfouis dans une archive compressée, cependant le scan peut affecter les performances du système.
Scanner les objets OLE	Scanne le nombre spécifié de couches Object Linking and Embedding (OLE) dans un fichier **Détecter le code d'exploitation dans les fichiers OLE** : la détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office. **Remarque** Le nombre de couches spécifié s'applique aux options **Scanner les objets OLE** et **Détecter le code d'exploitation dans les fichiers OLE**.
Scanner la zone d'amorçage	Scanne le secteur d'amorçage du disque dur de l'Endpoint à la recherche de virus/programmes malveillants

3. Dans la section **Utilisation du processeur**, sélectionnez l'un des éléments suivants :

   - **Élevé** : aucune interruption entre les scans
   - **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50% et pas d'interruption si elle est de 50% ou moins
   - **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Scan immédiat : onglet Action

Procédure

1. Dans la section **Virus/programmes malveillants**, configurez les paramètres requis.

   a. Sélectionnez le type d'action que l'Agent OfficeScan entreprend après la détection d'une menace pour la sécurité.

      - **Utiliser ActiveAction** : cette fonction utilise un ensemble d'actions de scan pré-configurées destinées à lutter contre les virus et les programmes malveillants.

        Pour plus d'informations, voir *ActiveAction à la page 14-38*.

        - **Personnaliser l'action pour les virus/programmes malveillants probables** : sélectionnez et spécifiez l'action que l'Agent OfficeScan entreprend en cas de programmes malveillants probables

      - **Utiliser la même action pour tous les types de virus/programmes malveillants** : spécifiez l'action que l'Agent OfficeScan entreprend sur toutes les menaces de programmes malveillants

      - **Utiliser une action spécifique pour chaque type de virus/programme malveillant** : spécifiez l'action que l'Agent OfficeScan entreprend en cas de menaces de sécurité spécifiques

        Pour plus d'informations, voir *Actions de scan personnalisées à la page 14-40*.

   b. Sélectionnez **Sauvegarder les fichiers avant nettoyage** pour créer une copie chiffrée du fichier infecté sur l'Endpoint dans le dossier `<dossier d'installation de l'agent>\Backup`.

      La création d'une copie de sauvegarde du fichier vous permet de restaurer la version d'origine du fichier, si nécessaire.

   c. Spécifiez l'emplacement du répertoire de quarantaine.

- **Mettre en quarantaine sur le serveur gérant l'agent OfficeScan** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine au serveur de gestion OfficeScan
- **Répertoire de quarantaine** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine à l'emplacement spécifié

Pour plus d'informations, voir *Quarantine Directory à la page 14-41*.

d. Dans la section **Damage Cleanup Services**, configurez les éléments suivants :

- **Type de nettoyage**
  - **Nettoyage standard** : l'Agent OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
    - Détecte et supprime les chevaux de Troie actifs
    - Élimine les processus créés par les chevaux de Troie
    - Répare les fichiers système modifiés par les chevaux de Troie
    - Supprime les fichiers et les applications laissés par les chevaux de Troie
  - **Nettoyage avancé** : outre les actions de nettoyage standard, l'Agent OfficeScan interrompt les activités de logiciels de sécurité non autorisés, connus également sous le nom de « FakeAV », et certaines variantes de rootkits.
- **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté** : effectue le type de nettoyage configuré sur de probables menaces de programmes malveillants

Remarque

Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**.

2. Dans la section **Spyware/Grayware**, sélectionnez l'action que l'Agent OfficeScan entreprend après la détection de spywares/graywares.

- **Nettoyer** : termine tous les processus liés et supprime les valeurs de registre, fichiers, cookies et raccourcis associés

Remarque

Après avoir nettoyé des spywares/graywares, les Agents OfficeScan sauvegardent les données concernant ces programmes. Vous pouvez restaurer ces données si vous estimez que l'accès à ces spywares/graywares est sans danger.

- **Ignorer** : consigne la détection mais permet l'exécution du programme

Scan immédiat : onglet Exclusion du scan

Procédure

1. Sélectionnez **Activer l'exclusion de scan**.
2. Dans la section **Liste des exclusions de scan (répertoires)**, configurez les paramètres requis.
   a. Sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** pour automatiquement exclure les répertoires associés à d'autres produits Trend Micro.

      Pour plus d'informations, voir *Exclusions du répertoire des produits Trend Micro à la page 14-49*.

   b. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   c. Saisissez un chemin d'accès à un répertoire à exclure des scans, puis cliquez sur le bouton **+**.

L'Agent OfficeScan ne scanne pas les fichiers situés dans le répertoire spécifié (et ses sous-répertoires).

Remarque

- Vous pouvez spécifier un maximum de 256 répertoires à exclure du scan.
- Les exclusions de répertoires prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

3. Dans la section **Liste des exclusions de scan (fichiers)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
   - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Saisissez un nom de fichier ou le nom de fichier avec un chemin d'accès à un répertoire complet à exclure des scans, puis cliquez sur le bouton **+**.

Remarque

- Vous pouvez spécifier un maximum de 256 fichiers à exclure du scan.
- Les exclusions de fichiers prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

4. Dans la section **Liste des exclusions de scan (extensions de fichier)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

- **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

b. Sélectionnez ou saisissez une extension de fichier à exclure des scans, puis cliquez sur le bouton **Ajouter >**.

Remarque

- Vous pouvez spécifier au maximum 256 extensions de fichier à exclure du scan.
- Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) pour remplacer un seul caractère ou un astérisque (*) pour remplacer plusieurs caractères comme caractères génériques. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*` ou `D??`.

Scan programmé

Un scan programmé démarre automatiquement aux date et heure programmées. Utilisez le scan programmé pour automatiser les scans de routine sur l'agent et gérer plus efficacement vos scans.

Configurez et appliquez des paramètres de scan programmé à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan programmé

Procédure

1. Sélectionnez les options suivantes :

- **Activer le scan antivirus/programme malveillant**
- **Activer le scan antispyware/grayware**

Remarque

Vous devez activer le scan de virus/programmes malveillants avant que vous puissiez activer le scan anti-spyware et anti-grayware.

2. Configurez les paramètres **Cible**.

   Pour plus d'informations, voir *Scan programmé : onglet Cible à la page 14-30*.

3. Configurez les paramètres **Action**.

   Pour plus d'informations, voir *Scan programmé : onglet Action à la page 14-33*.

4. Configurez les paramètres **Exclusion de scan**.

   Pour plus d'informations, voir *Scan programmé : onglet Exclusion de scan à la page 14-36*.

Scan programmé : onglet Cible

Procédure

1. Dans la section **Programmation**, spécifiez la fréquence du scan programmé :

   - **Quotidien** : scanne chaque jour à l'heure spécifiée
   - **Hebdomadaire, tous les <jour de semaine>** : scanne une fois par semaine le jour spécifié à l'heure indiquée
   - **Mensuelle, le <nombre>** : scanne une fois par mois le jour spécifié à l'heure indiquée
   - **Mensuelle, le <ordinal> <jour de semaine>** : scanne une fois par mois le jour de semaine spécifié à l'heure indiquée

Important

Si vous sélectionnez un jour qui n'existe pas dans un mois spécifique (par exemple, jour « 30 » n'existe pas en février), le scan programmé se produit le dernier jour de ce mois.

Remarque

Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

- **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
- **Sont personnalisables**: D'autres administrateurs peuvent configurer des stratégies enfant différentes des paramètres de stratégie parent.

2. Dans la section **Fichiers à scanner**, sélectionnez l'un des éléments suivants :

- **Tous les fichiers scannables** inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

  Remarque

  Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

- **Types de fichiers scannés par IntelliScan** scanne les fichiers d'après le véritable type de fichier.
- **Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :** spécifie manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

Remarque

Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

- **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

3. Dans la section **Paramètres de scan**, configurez les paramètres requis.

PARAMÈTRE	DESCRIPTION
Scanner les fichiers compressés	Scanne le nombre spécifié de couches de compression au sein d'un fichier archivé **Remarque** Le scan sur plusieurs couches peut détecter des programmes malveillants intentionnellement enfouis dans une archive compressée, cependant le scan peut affecter les performances du système.
Scanner les objets OLE	Scanne le nombre spécifié de couches Object Linking and Embedding (OLE) dans un fichier **Détecter le code d'exploitation dans les fichiers OLE** : la détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office. **Remarque** Le nombre de couches spécifié s'applique aux options **Scanner les objets OLE** et **Détecter le code d'exploitation dans les fichiers OLE**.
Scanner la zone d'amorçage	Scanne le secteur d'amorçage du disque dur de l'Endpoint à la recherche de virus/programmes malveillants

4. Dans la section **Utilisation du processeur**, sélectionnez l'un des éléments suivants :

- **Élevé** : aucune interruption entre les scans
- **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50% et pas d'interruption si elle est de 50% ou moins
- **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Scan programmé : onglet Action

Procédure

1. Dans la section **Virus/programmes malveillants**, configurez les paramètres requis.

   a. Sélectionnez le type d'action que l'Agent OfficeScan entreprend après la détection d'une menace pour la sécurité.

   - **Utiliser ActiveAction** : cette fonction utilise un ensemble d'actions de scan pré-configurées destinées à lutter contre les virus et les programmes malveillants.

     Pour plus d'informations, voir *ActiveAction à la page 14-38*.

     - **Personnaliser l'action pour les virus/programmes malveillants probables** : sélectionnez et spécifiez l'action que l'Agent OfficeScan entreprend en cas de programmes malveillants probables

   - **Utiliser la même action pour tous les types de virus/programmes malveillants** : spécifiez l'action que l'Agent OfficeScan entreprend sur toutes les menaces de programmes malveillants
   - **Utiliser une action spécifique pour chaque type de virus/programme malveillant** : spécifiez l'action que l'Agent OfficeScan entreprend en cas de menaces de sécurité spécifiques

     Pour plus d'informations, voir *Actions de scan personnalisées à la page 14-40*.

   b. Sélectionnez les types de notification qui s'affichent pour les utilisateurs finaux.

- **Afficher une notification lorsqu'un virus/programme malveillant est détecté** : choisissez d'afficher une notification informant l'utilisateur de l'Agent OfficeScan de la détection d'un programme malveillant
- **Afficher une notification lorsqu'un virus/programme malveillant est détecté** : choisissez d'afficher une notification informant l'utilisateur de l'Agent OfficeScan de la détection d'un probable programme malveillant

c. Sélectionnez **Sauvegarder les fichiers avant nettoyage** pour créer une copie chiffrée du fichier infecté sur l'Endpoint dans le dossier `<dossier d'installation de l'agent>\Backup`.

La création d'une copie de sauvegarde du fichier vous permet de restaurer la version d'origine du fichier, si nécessaire.

d. Spécifiez l'emplacement du répertoire de quarantaine.

- **Mettre en quarantaine sur le serveur gérant l'agent OfficeScan** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine au serveur de gestion OfficeScan
- **Répertoire de quarantaine** : l'Agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine à l'emplacement spécifié

Pour plus d'informations, voir *Quarantine Directory à la page 14-41*.

e. Dans la section **Damage Cleanup Services**, configurez les éléments suivants :

- **Type de nettoyage**
  - **Nettoyage standard** : l'Agent OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
    - Détecte et supprime les chevaux de Troie actifs
    - Élimine les processus créés par les chevaux de Troie
    - Répare les fichiers système modifiés par les chevaux de Troie
    - Supprime les fichiers et les applications laissés par les chevaux de Troie

- **Nettoyage avancé** : outre les actions de nettoyage standard, l'Agent OfficeScan interrompt les activités de logiciels de sécurité non autorisés, connus également sous le nom de « FakeAV », et certaines variantes de rootkits.

- **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté** : effectue le type de nettoyage configuré sur de probables menaces de programmes malveillants

Remarque

Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**.

2. Dans la section **Spyware/Grayware**, sélectionnez l'action que l'Agent OfficeScan entreprend après la détection de spywares/graywares.

   - **Nettoyer** : termine tous les processus liés et supprime les valeurs de registre, fichiers, cookies et raccourcis associés

Remarque

Après avoir nettoyé des spywares/graywares, les Agents OfficeScan sauvegardent les données concernant ces programmes. Vous pouvez restaurer ces données si vous estimez que l'accès à ces spywares/graywares est sans danger.

   - **Ignorer** : consigne la détection mais permet l'exécution du programme

   - **Afficher une notification sur les Endpoints lorsqu'un spyware/grayware est détecté** : sélectionnez cette option pour afficher une notification informant l'utilisateur de l'Agent OfficeScan lorsqu'une détection de spyware/grayware se produit

Scan programmé : onglet Exclusion de scan

Procédure

1. Sélectionnez **Activer l'exclusion de scan**.

2. Dans la section **Liste des exclusions de scan (répertoires)**, configurez les paramètres requis.

   a. Sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** pour automatiquement exclure les répertoires associés à d'autres produits Trend Micro.

   Pour plus d'informations, voir *Exclusions du répertoire des produits Trend Micro à la page 14-49*.

   b. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
   - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   c. Saisissez un chemin d'accès à un répertoire à exclure des scans, puis cliquez sur le bouton **+**.

   L'Agent OfficeScan ne scanne pas les fichiers situés dans le répertoire spécifié (et ses sous-répertoires).

Remarque

- Vous pouvez spécifier un maximum de 256 répertoires à exclure du scan.
- Les exclusions de répertoires prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

3. Dans la section **Liste des exclusions de scan (fichiers)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Saisissez un nom de fichier ou le nom de fichier avec un chemin d'accès à un répertoire complet à exclure des scans, puis cliquez sur le bouton **+**.

   Remarque

   - Vous pouvez spécifier un maximum de 256 fichiers à exclure du scan.
   - Les exclusions de fichiers prennent en charge l'utilisation de caractères génériques.

     Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 14-50*.

4. Dans la section **Liste des exclusions de scan (extensions de fichier)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Sélectionnez ou saisissez une extension de fichier à exclure des scans, puis cliquez sur le bouton **Ajouter >**.

Remarque

- Vous pouvez spécifier au maximum 256 extensions de fichier à exclure du scan.
- Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) pour remplacer un seul caractère ou un astérisque (*) pour remplacer plusieurs caractères comme caractères génériques. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*` ou `D??`.

Actions de scan

Vous pouvez configurer les Agents OfficeScan pour utiliser un ensemble d'actions de scan prédéfinies ou des actions personnalisées basées sur le type de programme malveillant détecté.

Important

Certains fichiers ne sont pas nettoyables.

Pour plus d'informations, consultez :

- *ActiveAction à la page 14-38*
- *Actions de scan personnalisées à la page 14-40*
- *Fichiers non nettoyables à la page 14-43*

ActiveAction

À chaque type de virus/programme malveillant correspond une action de scan différente. Pour personnaliser les actions de scan, vous devez posséder les connaissances nécessaires sur les virus/programmes malveillants. Cette tâche peut être fastidieuse. L'Agent OfficeScan utilise ActiveAction pour pallier à ces problèmes.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et les programmes malveillants. Si les actions de scan ne vous sont pas familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus ou programme malveillant, l'utilisation de l'outil ActiveAction est recommandée.

ActiveAction offre les avantages suivants :

- ActiveAction applique les actions de scan recommandées par Trend Micro. Vous ne perdez plus votre temps à configurer vous-même les actions de scan.
- Les créateurs de virus/programmes malveillants modifient en permanence la manière dont leurs virus attaquent les Endpoints. Les paramètres d'ActiveAction sont mis à jour pour assurer une protection contre les menaces et les méthodes d'attaques les plus récentes des virus /programmes malveillants.

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/ programme malveillant.

TABLEAU 14-2. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Exploitation CVE	Ignorer	N/A	N/A	N/A
Canular	Quarantaine	N/A	Quarantaine	N/A
Chevaux de Troie	Quarantaine	N/A	Quarantaine	N/A
Virus	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus de test	Refuser l'accès	N/A	Ignorer	N/A
Utilitaire de compression	Quarantaine	N/A	Quarantaine	N/A
Autres	Nettoyer	Quarantaine	Nettoyer	Quarantaine

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Virus/programmes malveillants probables	Refuser l'accès ou action configurée par l'utilisateur	N/A	Ignorer ou action configurée par l'utilisateur	N/A

Remarque

- Pour les virus et programmes malveillants probables, l'action par défaut est « Refuser l'accès » pendant le scan en temps réel et « Ignorer » pendant le scan manuel et le scan programmé. S'il ne s'agit pas des actions que vous souhaitez effectuer, vous pouvez les modifier par « Mettre en quarantaine », « Supprimer » ou « Renommer ».
- Certains fichiers ne sont pas nettoyables.
- ActiveAction n'est pas disponible pour le scan anti-spywares/graywares.

Actions de scan personnalisées

ACTION	DESCRIPTION
Supprimer	Supprime un fichier infecté.
Mise en quarantaine	Renomme, puis déplace le fichier infecté vers un répertoire de quarantaine temporaire sur l'Endpoint. L'Agent OfficeScan envoie ensuite les fichiers en quarantaine vers le répertoire de quarantaine spécifié, qui se trouve par défaut sur le serveur de gestion. L'Agent OfficeScan chiffre les fichiers en quarantaine envoyés à ce répertoire. Pour plus d'informations, voir *Quarantine Directory à la page 14-41*.

ACTION	DESCRIPTION
Nettoyer	Nettoie le fichier infecté avant d'autoriser l'accès complet au fichier. Si le fichier est impossible à nettoyer, l'Agent OfficeScan effectue une deuxième action, pouvant être l'une des actions suivantes : « Mettre en quarantaine », « Supprimer », « Renommer » et « Ignorer ». Cette action peut être exécutée sur tous les types de menaces liées à la sécurité, à l'exception des virus/programmes malveillants probables. **Remarque** Certains fichiers ne sont pas nettoyables. Pour obtenir des informations détaillées, consultez la section *Fichiers non nettoyables à la page 14-43*.
Renommer	Remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier renommé. Ils peuvent l'ouvrir s'ils associent le fichier à une application déterminée. Le virus/programme malveillant peut s'exécuter lors de l'ouverture du fichier infecté renommé.
Ignorer	N'effectue aucune action sur les menaces détectées, mais consigne la détection dans les journaux.
Refuser l'accès	Lorsque l'Agent OfficeScan détecte une tentative d'ouverture ou d'exécution d'un fichier infecté, il bloque immédiatement l'opération. Les utilisateurs peuvent supprimer manuellement le fichier infecté.

Quarantine Directory

Si l'action concernant un fichier infecté est « Mettre en quarantaine », Agent OfficeScan chiffre le fichier et le déplace vers un dossier de quarantaine temporaire sous <Dossier d'installation de l'agent>\SUSPECT, puis l'envoie vers le répertoire de quarantaine désigné.

Remarque

Vous pouvez restaurer des fichiers encodés en quarantaine si vous devez y accéder par la suite.

Acceptez le répertoire de quarantaine par défaut, qui se trouve sur l'ordinateur du serveur OfficeScan. Le répertoire est au format URL. Il contient le nom d'hôte du serveur ainsi que l'adresse IP.

- Si le serveur gère simultanément des agents IPv4 et IPv6, utilisez le nom d'hôte de façon à ce que tous les Agents OfficeScan puissent envoyer des fichiers mis en quarantaine au serveur.
- Si le serveur dispose uniquement d'une adresse IPv4 ou s'il est identifié par celle-ci, seuls les Agents OfficeScan IPv4 purs et à double pile peuvent lui envoyer des fichiers mis en quarantaine.
- Si le serveur dispose uniquement d'une adresse IPv6 ou s'il est identifié par celle-ci, seuls les Agents OfficeScan IPv6 purs et à double pile peuvent lui envoyer des fichiers mis en quarantaine.

Vous pouvez également définir un répertoire de quarantaine alternatif en saisissant son URL, chemin UNC ou chemin de fichier absolu. Les agents doivent être en mesure de se connecter à ce répertoire. Par exemple, le répertoire alternatif doit disposer d'une adresse IPv6 si des Agents OfficeScan iPv6 purs ou à double pile sont censés lui envoyer des fichiers mis en quarantaine. Trend Micro vous recommande de désigner comme répertoire alternatif un répertoire à double pile, qui sera identifié par son nom d'hôte et dont vous saisirez le chemin UNC.

Reportez-vous au tableau suivant pour obtenir de l'aide sur l'utilisation d'une URL, d'un chemin UNC ou d'un chemin de fichier absolu :

TABLEAU 14-3. Répertoire de quarantaine

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Répertoire installé sur l'ordinateur serveur de gestion	URL	`http://<osceserver>`	Il s'agit du répertoire par défaut. Configurez les paramètres de ce répertoire, comme la taille du dossier de quarantaine.
	Chemin UNC	`\\<osceserver>\ofcscan\Virus`	

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Répertoire sur un autre ordinateur serveur OfficeScan (si vous avez d'autres serveurs OfficeScan sur le réseau)	URL	`http://<osceserver2>`	Vérifiez que les Agents OfficeScan peuvent se connecter à ce répertoire. Si vous spécifiez un répertoire non valide, l'Agent OfficeScan conserve les fichiers en quarantaine dans le dossier SUSPECT jusqu'à ce que vous indiquiez un répertoire de quarantaine valide. Dans les journaux de virus/programmes malveillants du serveur, le résultat de scan est «Impossible d'envoyer le fichier en quarantaine vers le dossier de quarantaine spécifié». Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
	Chemin UNC	`\\<osceserver2>\ofcscan\Virus`	
Autre Endpoint sur le réseau	Chemin UNC	`\\<nom_ordinateur>\temp`	
Autre répertoire se trouvant sur l'Agent OfficeScan	Chemin de fichier absolu	`C:\temp`	

Fichiers non nettoyables

Le moteur de scan antivirus ne nettoie pas les fichiers suivants :

TABLEAU 14-4. Solutions aux fichiers non nettoyables

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés par des chevaux de Troie	Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement malveillantes, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas. Solution : le moteur Damage Cleanup et le modèle de nettoyage des dommages suppriment les chevaux de Troie.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés par des vers	Un ver est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes de endpoint. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome. Solution : Trend Micro recommande de supprimer les vers.
Fichiers infectés protégés en écriture	Solution : supprimez la protection en écriture pour permettre le nettoyage du fichier.
Fichiers protégés par mot de passe	Les fichiers protégés par mot de passe incluent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe. Solution : supprimez la protection par mot de passe pour permettre le nettoyage du fichier.
Fichiers de sauvegarde	Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. Le processus de nettoyage crée une sauvegarde du fichier infecté au cas où le virus/programme malveillant l'endommagerait au cours du processus de nettoyage. Solution : si le nettoyage réussit, vous n'avez pas besoin de conserver la copie de sauvegarde du fichier infecté. Si le endpoint fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.
Fichiers infectés dans la corbeille	Il peut arriver que le système n'autorise pas la suppression des fichiers infectés présents dans la corbeille, car le système est en cours d'exécution.
	Solution sous Windows XP ou Windows Server 2003 avec le système de fichiers NTFS : 1. Connectez-vous au endpoint avec des privilèges d'administrateur.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION

	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Ouvrez l'invite de commande.
	4. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.
	5. Vérifiez si les fichiers ont été supprimés.

	Solution sous d'autres systèmes d'exploitation (ou ceux sans NTFS) :
	1. Redémarrez le endpoint en mode MS-DOS.
	2. Ouvrez l'invite de commande.
	3. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.

Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer	Il peut arriver que le système n'autorise pas le nettoyage des fichiers infectés présents dans le dossier Temp de Windows ou dans le dossier temporaire d'Internet Explorer, car le endpoint les utilise. Les fichiers à nettoyer sont peut-être des fichiers temporaires nécessaires au fonctionnement de Windows.
	Solution sous Windows XP ou Windows Server 2003 avec le système de fichiers NTFS :

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION

	1. Connectez-vous au endpoint avec des privilèges d'administrateur.
	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les endpoints Windows XP ou Windows Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd temp`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	4. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	a. Ouvrez l'invite de commande et accédez au dossier Temp d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files` pour les endpoints Windows XP ou Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
	c. Vérifiez si les fichiers ont été supprimés.

	Solution sous d'autres systèmes d'exploitation (ou ceux sans NTFS) :
	1. Redémarrez le endpoint en mode MS-DOS.
	2. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les endpoints Windows XP ou Windows Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd temp`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	c. Redémarrez le endpoint en mode normal.
	3. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	a. Ouvrez l'invite de commande et accédez au dossier Temp d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files` pour les endpoints Windows XP ou Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer. c. Redémarrez le endpoint en mode normal.
Fichiers compressés à l'aide d'un format de compression non pris en charge	Solution : décompressez les fichiers.
Fichiers verrouillés ou en cours d'exécution	Solution : déverrouillez les fichiers ou attendez qu'ils aient été exécutés.
Fichiers corrompus	Solution : supprimez les fichiers.

Fichiers infectés par des chevaux de Troie

Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement nuisibles, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas.

Solution : l'Agent OfficeScan utilise le moteur Damage Cleanup et le modèle Damage Cleanup pour supprimer les chevaux de Troie.

Fichiers infectés par des vers

Un ver informatique est un programme (ou ensemble de programmes) autonome qui peut répandre des copies opérationnelles de lui-même ou de ses segments au sein d'autres endpoints. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome.

Solution : Trend Micro recommande de supprimer les vers.

Fichiers infectés protégés en écriture

Solution : retirez la protection en écriture pour autoriser l'Agent OfficeScan à nettoyer le fichier.

Fichiers protégés par mot de passe

Comprennent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe.

Solution : supprimez la protection par mot de passe pour autoriser l'Agent OfficeScan à nettoyer ces fichiers.

Fichiers de sauvegarde

Les fichiers portant les extensions RB0~RB9 sont des copies de sauvegarde des fichiers infectés. L'Agent OfficeScan crée une sauvegarde du fichier infecté en prévision d'éventuels dommages générés par le virus/programme malveillant pendant le nettoyage.

Solution : si l'Agent OfficeScan a réussi à nettoyer le fichier infecté, vous n'avez pas besoin de conserver la copie de sauvegarde. Si l'Endpoint fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.

Support d'exclusion de scan

Lors de l'exclusion de répertoires et de noms de fichiers du scan anti-programmes malveillants, consultez les informations d'assistance technique suivantes :

- *Exclusions du répertoire des produits Trend Micro à la page 14-49*
- *Exceptions avec caractères génériques à la page 14-50*

Exclusions du répertoire des produits Trend Micro

Si vous sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** dans la section **Liste des exclusions de scan (répertoires)**, l'Agent OfficeScan exclut automatiquement les répertoires de produits suivants :

- <Dossier d'installation du serveur>
- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11 et 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

Exceptions avec caractères génériques

Les listes d'exclusion de scan pour les fichiers et les répertoires prennent en charge l'utilisation des caractères génériques. Utilisez le caractère « ? » pour remplacer un caractère et « * » pour en remplacer plusieurs.

Utilisez les caractères génériques avec précaution. L'utilisation d'un caractère erroné peut exclure des fichiers ou des répertoires incorrects. Par exemple, l'ajout de `C:\*` à la liste des exclusions de scan (fichiers) exclut l'intégralité du lecteur `C:\`.

TABLEAU 14-5. Exclusions de scan avec des caractères génériques

VALEUR	EXCLUS	NON EXCLUS

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Tous les fichiers `.txt` du répertoire `C:\`	Tous les autres types de fichiers du répertoire `C:\`
`[]`	Non pris en charge	Non pris en charge

Chapitre 15

Paramètres de stratégie de Web Reputation

Cette section décrit comment configurer les stratégies de Web Reputation sur les Agents OfficeScan.

Les rubriques sont les suivantes :

- *Web Reputation à la page 15-2*
- *Configuration de Stratégie de Web Reputation à la page 15-2*

Web Reputation

La technologie Web Reputation suit la crédibilité de domaines Web en attribuant une note de réputation en fonction de facteurs tels que l'âge du site Web, les changements d'emplacement historiques et des indications d'activités suspectes découvertes par une analyse des comportements des programmes malveillants. Trend Micro analyse continuellement les sites Web et met à jour les notes de réputation de sites Web pour empêcher les utilisateurs d'accéder à du contenu potentiellement malveillant.

Lorsqu'un utilisateur tente d'accéder à un site Web, l'Agent OfficeScan interroge une source Smart Protection pour déterminer le niveau de risque du contenu. La stratégie de Web Reputation pour l'Agent OfficeScan détermine s'il convient d'autoriser ou non l'accès au site Web.

Web Reputation vous permet d'ajouter des sites Web que vous considérez sûrs ou dangereux aux listes Approuvés ou Bloqués. L'Agent OfficeScan n'interroge pas les notes de réputation des sites Web pour les sites Web ajoutés aux listes, mais autorise ou bloque plutôt l'accès automatiquement.

Configuration de Stratégie de Web Reputation

Spécifiez les informations d'authentification du serveur proxy si vous avez défini un serveur proxy pour gérer la communication HTTP dans votre entreprise et si une authentification est requise avant que l'accès au Web ne soit autorisé.

Procédure

1. Pour configurer une stratégie applicable aux agents externes, cliquez sur l'onglet **Agents externes** ; pour configurer une stratégie applicable aux agents internes, cliquez sur **Agents internes**.

2. Sous **Activer Web Reputation sur les systèmes d'exploitation suivants**, sélectionnez les types de plates-formes Windows à protéger (**Plates-formes de postes de travail Windows** et **Plates-formes Windows Server**).

Conseil

Trend Micro vous recommande de désactiver la stratégie de Web Reputation pour les agents internes si vous utilisez déjà un produit Trend Micro doté de la fonction de Web Reputation, tel qu'InterScan Web Security Virtual Appliance.

3. Sélectionnez **Activer le mode d'évaluation**.

Remarque

En mode d'évaluation, les Agents OfficeScan autorisent l'accès à tous les sites Web. Pour tout site Web qui enfreint le paramètre **Niveau de sécurité** configuré, l'Agent OfficeScan consigne l'événement. Le mode d'évaluation vous permet de contrôler l'accès au site Web et d'évaluer la sécurité de ce dernier avant d'en bloquer activement l'accès aux utilisateurs. En fonction de l'évaluation des journaux d'accès, vous pouvez ajouter des sites Web approuvés à la liste des URL approuvées avant de désactiver le mode d'évaluation.

4. Sélectionnez **Vérifier les URL HTTPS**.

Important

Avant que Web Reputation puisse vérifier les URL HTTPS, vous devez configurer certains paramètres prérequis pour différents navigateurs.

Pour plus d'informations, voir *Prise en charge du scan d'URL HTTPS à la page 15-6*.

5. Sélectionnez **Ne scanner que les ports HTTP courants** pour restreindre le scan de Web Reputation au trafic à travers les ports 80, 81, et 8080. Par défaut, Web Reputation scanne tout le trafic sur tous les ports.

Remarque

Non pris en charge sous Windows 7, 8, 8.1, 10 ou Windows Server 2008 R2, 2012 ou plates-formes ultérieures.

6. Pour les Agents OfficeScan internes, sélectionnez **Envoyer les requêtes aux serveurs Smart Protection** si vous souhaitez que les Agents OfficeScan envoient des requêtes aux serveurs Smart Protection.

   - Si vous activez cette option :

- Les agents consultent la liste des sources Smart Protection pour savoir à quels serveurs Smart Protection Server envoyer les requêtes.
- Assurez-vous que des serveurs Smart Protection Servers sont disponibles. Si aucun serveur Smart Protection Server n'est disponible, les agents n'envoient pas de requête à Smart Protection Network. Les seules sources restantes de données de Web Reputation pour les agents sont les listes des URL approuvées et bloquées.
- Les agents ne bloquent pas les sites Web non testés. Les serveurs Smart Protection Servers ne stockent pas les données de Web Reputation de ces sites Web.

- Si vous désactivez cette option :
  - Les agents envoient des requêtes de Web Reputation à Smart Protection Network. Les Endpoints doivent disposer d'une connexion Internet pour envoyer des requêtes.
  - Les agents peuvent bloquer des sites Web non testés si vous sélectionnez l'option **Bloquer les pages qui n'ont pas été testées par Trend Micro**.

Remarque

Les agents externes envoient des requêtes de Web Reputation à Smart Protection Network.

7. Sélectionnez l'un des niveaux de sécurité de la fonction de Web Reputation : **Élevé**, **Moyen** ou **Faible**

Remarque

Les niveaux de sécurité déterminent si Web Reputation autorise ou bloque l'accès à une URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, Web Reputation ne bloque que les URL qui constituent des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de faux positifs augmente également.

8. Si vous désactivez l'option **Envoyer les requêtes aux serveurs Smart Protection Server**, vous pouvez sélectionner **Bloquer les pages qui n'ont pas été testées par Trend Micro**.

Remarque

Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés. Le blocage de l'accès aux pages non testées peut améliorer la sécurité, mais il peut également empêcher l'accès à des pages sûres.

9. Sélectionnez **Bloquer les pages contenant un script malveillant** afin d'identifier les exploitations de navigateur Web et les scripts malveillants, tout en empêchant que l'utilisation de ces menaces ne compromette le navigateur Internet.

   Web Reputation utilise à la fois le fichier de signatures de prévention contre l'exploitation du navigateur et le fichier de signatures de l'analyseur de script pour identifier et bloquer les pages Web avant que le système ne soit exposé à une menace.

Important

- La fonction Prévention contre l'exploitation du navigateur est uniquement prise en charge sur Internet Explorer 7.0 et versions ultérieures.
- La fonction de prévention de l'exploitation des failles du navigateur requiert l'activation du service de protection avancé.

10. Configurez les listes d'approbation et de blocage.

Remarque

La liste approuvée est prioritaire sur la liste bloquée. Lorsqu'une URL correspond à une entrée de la liste des URL approuvées, les agents autorisent toujours l'accès à cette URL, même si elle figure dans la liste des URL bloquées.

   a. Sélectionnez **Activer la liste des URL approuvées/bloquées**.

   b. Entrez une URL.

Vous pouvez ajouter un caractère générique (*) à tout emplacement dans l'URL.

Par exemple :

- La saisie de `www.trendmicro.com/*` signifie que Web Reputation approuve toutes les pages dans le site Web Trend Micro.
- La saisie de `*.trendmicro.com/*` signifie que Web Reputation approuve toutes les pages sur tout sous-domaine de `trendmicro.com`.

Vous pouvez également entrer des URL contenant des adresses IP. Si une URL contient une adresse IPv6, précisez l'adresse entre parenthèses.

c. Cliquez sur **Ajouter à la liste des URL approuvées** ou **Ajouter à la liste des URL bloquées**.

Important

La Web Reputation n'effectue aucun scan des adresses des listes des éléments bloqués et approuvés.

11. Pour soumettre des commentaires relatifs à l'évaluation de Web Reputation, cliquez sur **Réévaluer l'URL**. Le système de requête du service d'évaluation de la Web Reputation de Trend Micro s'ouvre dans une fenêtre de navigateur.

12. Choisissez d'autoriser ou non l'envoi par l'Agent OfficeScan de journaux de Web Reputation au serveur. Autorisez les agents à envoyer des journaux si vous souhaitez analyser les URL bloquées par Web Reputation et entreprendre les actions appropriées à l'encontre des URL auxquelles vous estimez pouvoir accéder en toute sécurité.

Prise en charge du scan d'URL HTTPS

La communication HTTPS utilise des certificats pour identifier les serveurs Web. Les données sont chiffrées pour éviter le vol et l'espionnage. Bien que plus sécurisés, l'accès aux site Web utilisant HTTPS entraîne toujours des risques. Les site compromis, même ceux disposant de certificats valides, peuvent héberger des programmes malveillants et volent des informations personnelles. En outre, les certificats sont assez simples à obtenir, ce qui facilite l'installation de serveurs Web malveillants utilisant HTTPS.

Important

Le scan HTTPS ne prend en charge que les plates-formes Windows 8, Windows 8.1, Windows 10 ou Windows 2012 en mode poste de travail.

Activez la vérification des URL HTTPS afin de réduire les risques d'exposition aux sites compromis et malveillants qui utilisent HTTPS. Web Reputation peut surveiller le trafic HTTPS sur les navigateurs suivants :

TABLEAU 15-1. Navigateurs pris en charge pour le trafic HTTPS

NAVIGATEUR	VERSION	PRÉREQUIS
Microsoft Internet Explorer	8.x	Dernière version
	9.x	Pour les Agents OfficeScan fonctionnant sous Windows 7, 8, 8.1, 10, Server 2008 R2 ou Server 2012, les utilisateurs doivent activer le module complémentaire `Trend Micro Osprey Plugin Class` dans la fenêtre contextuelle du navigateur. Pour les Agents OfficeScan fonctionnant sous Windows XP, Server 2003 ou Server 2008, les utilisateurs doivent activer le module complémentaire `TmIEPlugInBHO Class` dans la fenêtre contextuelle du navigateur.
	10.x	
	11.x	
Mozilla Firefox	3.5 ou ultérieure	Vous devez activer la fonction **Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis** du service de prévention des modifications non autorisées et de la surveillance des comportements sur les agents pour scanner le trafic HTTPS. **Remarque** Le scan HTTPS sur ces navigateurs n'est pas pris en charge sur les plates-formes Windows XP, Server 2003/2003 R2 ou Server 2008.
Chrome	Dernière version	
Microsoft Edge	Dernière version	

Pour plus d'informations sur la configuration des paramètres d'Internet Explorer pour Web Reputation, consultez les articles suivants de la base de connaissances :

- http://esupport.trendmicro.com/solution/en-us/1060643.aspx
- http://esupport.trendmicro.com/solution/en-us/1095350.aspx

Chapitre 16

Protection contre les menaces inconnues

Cette section décrit comment configurer les Agents OfficeScan pour détecter des menaces précédemment non identifiées, ciblées ou à faible prévalence, ou pour s'en protéger.

Les rubriques sont les suivantes :

- *Apprentissage automatique prédictif à la page 16-2*
- *Configuration des paramètres de soumission d'échantillons à la page 16-6*
- *Configuration des paramètres de connexion suspecte à la page 16-6*

Apprentissage automatique prédictif

L'apprentissage automatique prédictif de Trend Micro utilise des technologies d'apprentissage automatique avancées pour mettre en corrélation des informations liées aux menaces et exécuter des analyses approfondies afin de détecter l'apparition de risques inconnus liés à la sécurité, grâce à l'empreinte digitale numérique, à la correspondance des API et à d'autres fonctions liées aux fichiers. L'apprentissage automatique prédictif effectue également une analyse comportementale sur des processus inconnus ou de faible prévalence afin de détecter les tentatives d'infection de votre réseau par une menace émergente ou inconnue.

L'apprentissage automatique prédictif est un outil puissant qui contribue à protéger votre environnement contre les menaces non identifiées et les attaques émergentes.

TYPE DE DÉTECTION	DESCRIPTION
Fichier	Après la détection d'un fichier inconnu ou à faible prévalence, l'Agent OfficeScan analyse le fichier à l'aide du Moteur de scan de menaces avancées (ATSE) pour extraire des caractéristiques de fichiers et envoie le rapport au moteur d'apprentissage automatique prédictif, hébergé sur le réseau Trend Micro Smart Protection Network. Grâce à l'utilisation de la modélisation de programmes malveillants, l'apprentissage automatique prédictif compare l'exemple au modèle de programme malveillants, affecte un score de probabilité et détermine le type de programme malveillant potentiel contenant le fichier. Selon la configuration d'apprentissage automatique prédictif, l'Agent OfficeScan peut tenter de « mettre en quarantaine » le fichier affecté pour éviter que la menace ne continue à se propager sur votre réseau.

Type de détection	Description
Processus	Après la détection d'un processus inconnu ou à faible prévalence, l'Agent OfficeScan surveille le processus en utilisant le moteur d'intelligence contextuelle et envoie le rapport comportemental au moteur d'apprentissage automatique prédictif. Grâce à l'utilisation de la modélisation de programmes malveillants, l'apprentissage automatique prédictif compare le comportement du processus au modèle de programme, affecte un score de probabilité et détermine le type de programme malveillant potentiel contenant le fichier. La détection de processus surveille également l'exécution de script. Si le moteur d'intelligence contextuelle détecte l'exécution d'un script suspect, l'apprentissage automatique prédictif entreprend l'action configurée. L'apprentissage automatique prédictif exécute le blocage de script sur les types de scripts suivants : • cscript • jar • powershell • vbs • wscript Selon la configuration de l'apprentissage automatique prédictif, l'Agent OfficeScan peut « Interrompre » le processus concerné et tenter de nettoyer le fichier ayant exécuté le processus ou le script.

Configuration des paramètres de l'apprentissage automatique prédictif

Remarque

L'apprentissage automatique prédictif nécessite que vous activiez les services suivants :

- Prévention des modifications non autorisées
- Service de protection avancé

Procédure

1. Sélectionnez **Activer l'apprentissage automatique prédictif**.
2. Sous **Paramètres de détection**, sélectionnez le type de détection et l'action associée qu'effectue l'apprentissage automatique prédictif.

TYPE DE DÉTECTION	ACTIONS
Fichier	• **Mettre en quarantaine** : Sélectionnez cette option pour mettre automatiquement en quarantaine les fichiers qui présentent des fonctionnalités associées aux programmes malveillants sur la base de l'analyse d'apprentissage automatique prédictif • **Consigner uniquement** : Sélectionnez cette option pour scanner les fichiers inconnus et consigner l'analyse de l'apprentissage automatique prédictif pour un examen interne plus poussé de la menace

TYPE DE DÉTECTION	ACTIONS
Processus	• **Interrompre** : Sélectionnez cette option pour arrêter automatiquement les processus ou les scripts qui présentent des comportements de programmes malveillants sur la base de l'analyse de l'apprentissage automatique prédictif **Important** L'apprentissage automatique prédictif tente de nettoyer les fichiers exécutés par les processus ou les scripts malveillants. Si l'action de nettoyage a échoué, l'apprentissage automatique prédictif met les fichiers concernés en quarantaine. • **Consigner uniquement** : Sélectionnez cette option pour scanner les processus ou les scripts inconnus et consigner l'analyse de l'apprentissage automatique prédictif pour un examen interne plus poussé de la menace

3. Sous **Exceptions,** configurez les exceptions globales du fichier d'apprentissage automatique prédictif pour empêcher que tous les agents ne détectent un fichier comme étant malveillant.

   a. Cliquez sur **Ajouter le hachage du fichier**.

      L'écran **Ajouter un fichier à la liste des exceptions** s'ouvre.

   b. Spécifiez la valeur de hachage du fichier SHA-1 à exclure du scan.

   c. Fournissez éventuellement une remarque sur la raison de l'exception ou pour décrire le ou les noms de fichiers associés à la valeur de hachage.

   d. Cliquez sur **Ajouter**.

      L'apprentissage automatique prédictif ajoute le hachage du fichier à la liste d'exceptions.

Configuration des paramètres de soumission d'échantillons

Vous pouvez configurer les Agents OfficeScan pour soumettre des objets de fichiers pouvant contenir des menaces précédemment non identifiées dans un analyseur Virtual Analyzer pour y effectuer une analyse plus poussée. Après l'évaluation des objets, Virtual Analyzer ajoute les objets trouvés contenant des menaces inconnues dans la liste des objets suspects de Virtual Analyzer et distribue les listes aux autres Agents OfficeScan dans tout le réseau.

Les fichiers suspects incluent les éléments suivants :

- Programmes non connus de Trend Micro (téléchargés via les navigateurs Web ou les canaux de messagerie pris en charge)
- Détections heuristiques de processus (téléchargés via les navigateurs Web ou les canaux de messagerie pris en charge)
- Programmes d'exécution automatique à faible prévalence sur le stockage amovible

Important

Agents OfficeScan peut envoyer des fichiers d'échantillons d'une taille pouvant aller jusqu'à 50 Mo à l'analyseur Virtual Analyzer pour analyse.

Procédure

1. Sélectionnez **Activer l'envoi de fichiers suspects à Virtual Analyzer**.

Configuration des paramètres de connexion suspecte

Les Agents OfficeScan peuvent consigner toutes les connexions établies entre des endpoints et des adresses de la liste d'adresses IP C&C globale. Vous pouvez également consigner les adresses IP configurées dans la liste des adresses IP bloquées définie par l'utilisateur, mais toujours y autoriser l'accès.

Agents OfficeScan peut également surveiller les connexions dues à un botnet ou à une autre menace liée à un programme malveillant. Lorsqu'une menace liée à un programme malveillant a été détectée, Agents OfficeScan peut tenter de nettoyer l'infection.

Procédure

1. Activez le paramètre **Détecter les connexions vers les adresses de la liste d'adresses IP C&C globale** pour surveiller les connexions établies vers les serveurs C&C confirmés par Trend Micro et choisissez de **Consigner uniquement** ou de **Bloquer** les connexions.

   - Pour permettre aux agents de se connecter à des adresses de la liste des adresses IP bloquées définie par l'utilisateur, activez le paramètre **Consigner les accès à des adresses de la liste des adresses IP bloquées définie par l'utilisateur et autoriser l'accès à ces adresses**.

   Remarque

   Vous devez activer la consignation des connexions réseau pour qu'Agents OfficeScan puisse autoriser l'accès aux adresses de la liste des adresses IP bloquées définie par l'utilisateur.

2. Activez le paramètre **Détecter les connexions à l'aide de reconnaissance réseau des programmes malveillants** et choisissez de **Consigner uniquement** ou de **Bloquer** les connexions.

   - Pour autoriser Agents OfficeScan à tenter de nettoyer les connexions effectuées vers des serveurs C&C, activez le paramètre **Nettoyer les connexions suspectes lorsqu'un rappel C&C est détecté**. Les Agents OfficeScan utilisent GeneriClean pour nettoyer la menace liée à un programme malveillant et mettre fin à la connexion au serveur C&C.

   Remarque

   Vous devez activer **Consigner les connexions à l'aide du système de reconnaissance réseau des programmes malveillants** pour qu'Agents OfficeScan puisse tenter de nettoyer les connexions effectuées vers des serveurs C&C détectées par la mise en correspondance de structure des paquets.

Chapitre 17

Paramètres de stratégie de contrôle des dispositifs

Cette section décrit comment configurer les stratégies de contrôle des dispositifs sur les Agents OfficeScan.

Les rubriques sont les suivantes :

- *Contrôle des dispositifs à la page 17-2*
- *Configuration des paramètres de contrôle des dispositifs à la page 17-2*

Contrôle des dispositifs

Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.

Vous pouvez configurer des stratégies de contrôle des dispositifs pour les agents internes et externes. Les administrateurs configurent généralement une stratégie plus stricte pour les agents externes.

Control Manager fournit une configuration de stratégie de contrôle de dispositifs basée sur les Endpoints et sur l'utilisateur.

Configuration des paramètres de contrôle des dispositifs

Procédure

1. Sélectionnez **Activer le contrôle des dispositifs**.
   - Si vous êtes sur l'onglet **Agents externes**, vous pouvez appliquer des paramètres aux agents internes en sélectionnant **Appliquer tous les paramètres aux agents internes**.
   - Si vous êtes sur l'onglet **Agents internes**, vous pouvez appliquer des paramètres aux agents externes en sélectionnant **Appliquer tous les paramètres aux agents externes**.
2. Ajoutez ou modifiez une règle de contrôle des dispositifs :
   - Pour les règles basées sur l'utilisateur :
     - Pour créer une règle basée sur des comptes d'utilisateurs ou de groupes Active Directory, cliquez sur **Ajouter**.

- Pour modifier une règle basée sur des comptes d'utilisateurs ou de groupes Active Directory, cliquez sur le lien dans la colonne **Comptes utilisateurs**.

Important

Les règles de contrôle des dispositifs basées sur l'utilisateur sont uniquement disponibles après l'intégration d'Active Directory à Control Manager.

- Pour modifier la règle par défaut basée sur l'Endpoint :
  - Cliquez sur le lien **Tous les utilisateurs (par défaut)** dans la colonne **Comptes utilisateurs**.

Remarque

Vous ne pouvez pas supprimer la règle par défaut basée sur l'Endpoint.

L'écran **Règles de contrôle des dispositifs** s'ouvre.

3. Dans la section **Comptes utilisateurs**, saisissez et sélectionnez le ou les comptes utilisateurs ou groupes Active Directory auxquels s'applique la règle.

Remarque

Vous ne pouvez pas spécifier des comptes d'utilisateurs ou de groupes lors de l'édition de la règle par défaut basée sur l'Endpoint **Tous les utilisateurs (par défaut)**.

4. Dans la section **Périphériques de stockage** :
   a. Sélectionnez une autorisation pour chaque périphérique de stockage.

Important

- Seuls les agents OfficeScan pour lesquels la protection des données est activée peuvent entreprendre l'action de « blocage ». Si vous déployez une stratégie auprès d'agents OfficeScan pour lesquels la protection des données n'est pas activée, OfficeScan applique l'action configurée dans la zone de la liste déroulante.
- OfficeScan applique automatiquement l'autorisation d'accès configurée pour tous les dispositifs USB présents dans la **Liste des dispositifs USB autorisés**, même si vous n'activez pas la protection des données.

Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques à la page 17-6*.

Si vous avez choisi de restreindre l'accès à un périphérique de stockage, le bouton **Programmes autorisés** apparaît. Pour les **périphériques de stockage USB**, si vous avez sélectionné **Bloquer (protection des données)**, le bouton **Périphérique USB autorisés** apparaît.

b. (Facultatif) Cliquez sur **Programmes autorisés** pour configurer une liste de programmes auxquels le contrôle des dispositifs ne restreint pas l'accès sur aucun type de périphérique.

   L'écran **Programmes autorisés** s'ouvre.

   i. Saisissez le chemin d'accès complet ou les informations du fournisseur de signature numérique approuvé des programmes auquel le contrôle des dispositifs donne accès aux utilisateurs.

Remarque

- Lorsque vous spécifiez un fournisseur de signature numérique, le contrôle des dispositifs autorise uniquement les programmes signés par l'éditeur à **s'exécuter**.

  Pour plus d'informations, consultez la section *Spécification d'un fournisseur Digital Signature à la page 17-10*.

- Lorsque vous spécifiez le chemin complet d'un programme, la liste des programmes autorisés du contrôle des dispositifs prend en charge l'utilisation des caractères génériques.

  Pour plus d'informations, consultez la section *Prise en charge des caractères génériques pour la liste des programmes autorisés du contrôle des dispositifs à la page 17-9*.

ii. Cliquez sur **Ajouter**.

Le chemin d'accès complet du programme ou les informations du fournisseur de signature numérique figurent dans la liste.

iii. Indiquez si vous souhaitez autoriser le programme à **S'exécuter** ou **Lire/Écrire**.

iv. Cliquez sur **OK**.

c. (Facultatif) Cliquez sur **Dispositifs USB autorisés** pour configurer une liste de dispositifs USB que le contrôle des dispositifs ne bloque pas.

L'écran **Dispositifs USB autorisés** s'affiche.

i. Saisissez le nom du fournisseur du dispositif, son modèle et son numéro de série dans la liste.

ii. Pour ajouter plusieurs périphériques, cliquez sur l'icône plus (+).

iii. Dans la liste déroulante **Autorisations**, spécifiez le niveau d'accès qu'octroie le contrôle des dispositifs aux utilisateurs accédant aux dispositifs USB spécifiés.

iv. Cliquez sur **OK**.

d. Sélectionnez **Bloquer la fonction AutoRun sur les périphériques de stockage USB** pour empêcher des programmes enregistrés sur les dispositifs USB de s'exécuter automatiquement.

e. Sélectionnez **Afficher un message de notification sur l'Endpoint lorsqu'OfficeScan détecte un accès non autorisé à un dispositif** pour informer les utilisateurs finaux que le contrôle des dispositifs a restreint l'accès à un dispositif.

5. Pour les Agents OfficeScan sur lesquels la fonction Protection des données est installée, choisissez d'**Autoriser** ou de **Bloquer** l'accès aux dispositifs répertoriés sous **Appareils mobiles** et **Périphériques qui ne sont pas destinés au stockage**.

6. Cliquez sur **OK**.

Remarque

Le contrôle des dispositifs attribue automatiquement à toutes les règles basées sur l'utilisateur une priorité plus élevée que la règle basée sur l'Endpoint par défaut (**Tous les utilisateurs (par défaut)**).

7. (Facultatif) Gérer la liste des règles du contrôle des dispositifs.

   - **Priorité** : cliquez sur les flèches pour modifier la priorité des règles basées sur l'utilisateur.
   - **Copier** : sélectionnez une règle, cliquez sur **Copier**, puis modifiez le contenu de la règle.
   - **Supprimer** : sélectionnez une règle et cliquez sur **Supprimer** pour supprimer définitivement la règle de la liste.

Autorisations pour les périphériques

Les autorisations du contrôle des dispositifs pour les périphériques de stockage sont utilisées dans les cas suivants :

- Lorsque vous autorisez l'accès aux périphériques de stockage USB, CD/DVD, disquettes et lecteurs de réseau. Vous pouvez accorder un accès complet ou limiter le niveau d'accès à ces périphériques.
- Configurez la liste des périphériques de stockage USB approuvés. Le contrôle des dispositifs vous permet de bloquer l'accès à tous les périphériques de stockage USB, sauf ceux qui ont été ajoutés à la liste des périphériques approuvés. Vous pouvez accorder un accès complet aux périphériques approuvés ou limiter le niveau d'accès.

Le tableau suivant répertorie les autorisations d'accès aux périphériques de stockage.

TABLEAU 17-1. Autorisations de contrôle des dispositifs pour les périphériques de stockage

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Accès complet	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier En d'autres termes, un fichier peut être enregistré, déplacé et copié sur le périphérique.
Modifier	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer Opérations interdites : Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier
Lire et exécuter	Opérations autorisées : Copier, Ouvrir, Exécuter Opérations interdites : Enregistrer, Déplacer, Supprimer	Opérations interdites : Enregistrer, Déplacer, Copier
Lire	Opérations autorisées : Copier, Ouvrir Opérations interdites : Enregistrer, Déplacer, Supprimer, Exécuter	Opérations interdites : Enregistrer, Déplacer, Copier

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Répertorier le contenu des dispositifs uniquement	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient sont visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier
Bloquer (disponible après l'installation de la protection des données)	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient ne sont pas visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier

La fonction de scan de fichiers complète et peut annuler les autorisations relatives aux périphériques. Si, par exemple, l'une d'entre elles autorise l'ouverture d'un fichier mais que l'Agent OfficeScan détecte que celui-ci est infecté par un programme malveillant, une action de scan spécifique est exécutée sur le fichier pour éliminer ce programme. Si l'action de scan est Nettoyer, le fichier s'ouvre une fois le nettoyage effectué. Si, en revanche l'action de scan est Supprimer, le fichier est supprimé.

Le tableau suivant répertorie les autorisations pour les périphériques mobiles et non destinés au stockage gérées par le service de protection des données.

TABLEAU 17-2. Autorisations de contrôle des dispositifs pour périphériques mobiles et non destinés au stockage

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Autoriser	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier En d'autres termes, un fichier peut être enregistré, déplacé et copié sur le périphérique.

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Bloquer	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient ne sont pas visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier

Conseil

Le contrôle des dispositifs pour la protection des données prend en charge toutes les plates-formes 64 bits. Pour assurer la surveillance de la prévention des modifications non autorisées sur les systèmes non pris en charge par l'Agent OfficeScan, définissez les autorisations pour les dispositifs sur **Bloquer** pour limiter l'accès à ces dispositifs.

Prise en charge des caractères génériques pour la liste des programmes autorisés du contrôle des dispositifs

Le nome et le chemin d'accès d'un programme doivent compter 259 caractères au maximum et ne peuvent contenir que des caractères alphanumérique (A-Z, a-z, 0-9). Il est impossible de spécifier uniquement le nom du programme.

Vous pouvez utiliser des caractères génériques pour remplacer la lettre d'un lecteur et le nom d'un programme. Utilisez un point d'interrogation (?) pour remplacer un seul caractère, comme la lettre d'un lecteur. Utilisez un astérisque (*) pour remplacer plusieurs caractères, comme un nom de programme.

Remarque

Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.

Les caractères génériques peuvent être utilisés dans les exemples suivants :

TABLEAU 17-3. Utilisation correcte des caractères génériques

EXEMPLE	DONNÉES CORRESPONDANTES
?:\Password.exe	Le fichier «Password.exe» situé dans n'importe quel lecteur
C:\Program Files\Microsoft *.exe	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files*.*	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files\a**?**c.exe	Tout fichier .exe sous C:\Program Files dont le nom est composé de 3 caractères, commençant par la lettre « a » et se terminant par la lettre « c »
C:*	Tout fichier se trouvant directement sous C:\drive, qu'il possède ou non une extension de fichier

Les caractères génériques ne peuvent pas être utilisés dans les exemples suivants :

TABLEAU 17-4. Utilisation incorrecte des caractères génériques

EXEMPLE	CAUSE
??:\Buffalo\Password.exe	?? représente deux caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.
***:\Buffalo\Password.exe	* représente plusieurs caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.
C:*\Password.exe	Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.
C:**?**\Password.exe	

Spécification d'un fournisseur Digital Signature

Spécifiez un fournisseur de signature digitale si vous faites confiance aux programmes de ce fournisseur. Par exemple, entrez Microsoft Corporation ou Trend Micro, Inc. Vous pouvez obtenir le fournisseur de signature digitale en vérifiant les propriétés d'un

programme (par exemple, en cliquant avec le bouton droit sur le programme et en sélectionnant **Propriétés**).

Chapitre 18

Liste des exclusions de scan

Cette section décrit comment configurer les listes d'exclusion de scan qui s'appliquent à plusieurs fonctions de scan.

Les rubriques sont les suivantes :

- *Liste des spywares/graywares approuvés à la page 18-2*
- *Liste des programmes approuvés à la page 18-3*

Liste des spywares/graywares approuvés

L'Agent OfficeScan fournit une liste des spywares/graywares « approuvés », qui contient les fichiers ou les applications que vous ne souhaitez pas voir considérés comme des spywares ou des graywares. Lorsqu'un spyware/grayware particulier est détecté lors d'un scan, l'Agent OfficeScan vérifie la liste des spywares/graywares approuvés et n'effectue aucune action si une correspondance est trouvée dans cette liste.

Appliquez la liste approuvée à un ou plusieurs Agents OfficeScan et domaines, ou à tous les Agents OfficeScan gérés par le serveur. La liste des spywares/graywares approuvés s'applique à tous les types de scan, ce qui signifie que la même liste approuvée sera utilisée lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat.

Managing the Spyware/Grayware Approved List

Procédure

1. Dans le tableau **Noms des spywares/graywares**, sélectionnez un nom de spyware/grayware. Pour sélectionner plusieurs noms, maintenez enfoncée la touche CTRL lors de la sélection.

   - Vous pouvez également entrer un mot-clé dans le champ **Rechercher** et cliquer sur **Rechercher**. Le tableau est actualisé avec les noms correspondant au mot-clé.

2. Cliquez sur **Ajouter**.

   Les noms se déplacent dans le tableau **Liste approuvée**.

3. Pour supprimer les noms dans la liste des spywares/graywares approuvés, sélectionnez les noms et cliquez sur **Supprimer**. Pour sélectionner plusieurs noms, maintenez enfoncée la touche CTRL lors de la sélection.

Liste des programmes approuvés

Vous pouvez configurer Agents OfficeScan pour qu'il ignore les processus sécurisés lors des scans en temps réel et des scans de surveillance des comportements. Lorsqu'un programme a été ajouté à la liste des programmes approuvés, l'Agent OfficeScan n'effectue pas de scan en temps réel sur le programme ou tout processus lancé par ce programme. L'ajout de programmes à la liste des programmes approuvés améliore les performances de scan sur les endpoints.

Remarque

Vous pouvez ajouter des fichiers à la liste des programmes approuvés dans les cas suivants :

- Le fichier ne se trouve pas dans le répertoire système de Windows.
- Le fichier comporte une signature numérique valide.

Lorsqu'un programme a été ajouté à la liste des programmes approuvés, l'Agent OfficeScan l'exclut automatiquement des scans suivants :

- Scan en temps réel pour la vérification de fichiers
- Surveillance des comportements
- Scan en temps réel de processus

Configuration de la liste des programmes approuvés

La liste des programmes approuvés exclut les programmes et tous les processus enfant appelés par le programme du scan en temps réel et du scan de surveillance des comportements.

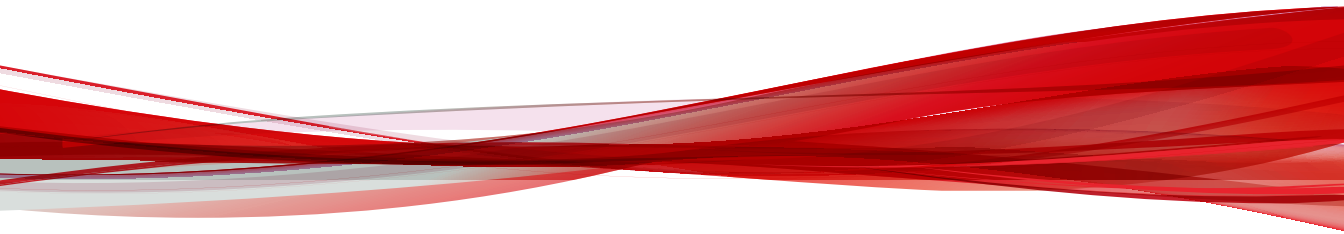
Procédure

1. Saisissez le chemin complet du programme à exclure de la liste.
2. Cliquez sur **Ajouter à la liste des programmes approuvés**.

3. Pour supprimer un programme de la liste, cliquez sur l'icône **Supprimer**.

Partie VII

Widgets de Prévention contre la perte de données OfficeScan



Chapitre 19

Paramètres de la stratégie de prévention contre la perte de données OfficeScan

Cette section décrit comment configurer les stratégies de prévention contre la perte de données pour les Agents OfficeScan.

Les rubriques sont les suivantes :

- *Prévention contre la perte de données (DLP) à la page 19-2*
- *Configuration d'une stratégie de prévention contre la perte de données à la page 19-3*

Prévention contre la perte de données (DLP)

Les solutions de sécurité classiques sont destinées à empêcher les menaces de sécurité externes d'atteindre le réseau. Dans l'environnement de sécurité actuel, elles s'avèrent incomplètes. Les failles de sécurité sont désormais monnaie courante et exposent les données sensibles et confidentielles d'une organisation (appelées des actifs numériques) à des entités externes non autorisées. Une faille de sécurité peut résulter d'erreurs ou de négligences des employés internes, de l'externalisation des données, d'ordinateurs volés ou égarés, ou d'attaques malveillantes.

Les violations de données peuvent :

- Porter préjudice à la réputation de la marque
- Diminuer la confiance des clients envers l'organisation
- Entraîner des coûts supplémentaires pour couvrir la réparation et le paiement d'amandes pour violation des règles de conformité
- Mener à la perte d'opportunités commerciales et de chiffre d'affaires lorsque la propriété intellectuelle est volée

Du fait de la fréquence et des effets dramatiques des violations de données, les organisations considèrent dorénavant la protection des actifs numériques comme un composant décisif de leur infrastructure de sécurité.

La prévention contre la perte de données protège les données sensibles de l'entreprise contre toute fuite accidentelle ou délibérée. La prévention contre la perte des données permet ce qui suit :

- Identifiez les informations sensibles exigeant une protection à l'aide d'identificateurs de données
- La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes.
- Le renforcement de la conformité à des normes de confidentialité établies

Avant de pouvoir contrôler une perte potentielle des informations sensibles, vous devez être en mesure de répondre aux questions suivantes :

- Quelles données doivent être protégées des utilisateurs non autorisés ?
- Où se trouvent les données sensibles ?
- Comment sont transmises les données sensibles ?
- Quels sont les utilisateurs autorisés à accéder ou transmettre les données sensibles ?
- Quelle action doit être entreprise en cas de violation de la sécurité ?

Cet audit primordial implique en général plusieurs départements et membres du personnel au courant des informations sensibles de votre entreprise.

Si vous avez déjà défini les informations sensibles et les stratégies de sécurité, vous pouvez commencer à définir les identificateurs de données ainsi que les stratégies d'entreprise.

Configuration d'une stratégie de prévention contre la perte de données

Procédure

1. Cliquez sur l'onglet **Agents externes** pour configurer une stratégie applicable aux agents externes et sur **Agents internes** pour configurer une stratégie applicable aux agents internes.

   Remarque

   Au besoin, configurez les paramètres d'emplacement des agents. Les agents utiliseront ces paramètres pour appliquer la stratégie de prévention contre la perte de données appropriée.

   Pour plus de détails, reportez-vous au *Manuel de l'administrateur OfficeScan*.

2. Sélectionnez **Activer la prévention contre la perte de données**.
3. Choisissez l'un des éléments suivants :

- Si vous êtes sur l'onglet **Agents externes**, vous pouvez appliquer tous les paramètres de prévention contre la perte de données aux agents internes en sélectionnant **Appliquer tous les paramètres aux agents internes**.
- Si vous êtes sur l'onglet **Agents internes**, vous pouvez appliquer tous les paramètres de prévention contre la perte de données aux agents externes en sélectionnant **Appliquer tous les paramètres aux agents externes**.

4. Gérez les règles que la prévention contre la perte de données applique à la stratégie dans l'onglet **Règles**.

TÂCHE	DESCRIPTION
Ajouter une nouvelle règle	Cliquez sur **Ajouter** pour créer une règle qui s'applique à la stratégie. Pour plus d'informations, voir *Configuration de règles de prévention contre la perte de données à la page 19-5*.
Copier les paramètres d'une règle existante	Sélectionnez une règle existante et cliquez sur **Copier** pour ouvrir l'écran **Paramètres de la stratégie de prévention contre la perte de données**. Modifiez les paramètres de la règle selon les besoins.
Supprimer des règles existantes	Sélectionnez une règle existante, puis cliquez sur **Supprimer** pour supprimer la règle de la liste.
Modifier des règles existantes	Cliquez sur le nom **Règle** d'une règle existante pour en modifier les paramètres.
Activer/ désactiver des règles existantes	Cliquez sur le bouton sous la colonne **Activer** afin d'activer ou de désactiver une règle pour la stratégie.

Remarque

Une stratégie peut contenir jusqu'à 40 règles.

5. Cliquez sur l'onglet **Exceptions** et configurez les paramètres d'exception nécessaires.

Pour plus d'informations, voir *Exceptions de prévention contre la perte de données à la page 19-14*.

Configuration de règles de prévention contre la perte de données

Remarque

La prévention contre la perte de données traite les règles et les modèles selon leur ordre de priorité. Si une règle est définie sur « Ignorer », la prévention contre la perte de données traite la règle suivante de la liste. Si une règle est définie sur « Bloquer » ou « Justification de l'utilisateur », la prévention contre la perte de données bloque ou accepte l'action de l'utilisateur et interrompt le traitement de cette règle ou de ce modèle.

Procédure

1. Sélectionnez **Activer cette règle**.
2. Indiquez un nom pour la règle.

   Configurez les paramètres du modèle :

3. Cliquez sur l'onglet **Modèle**.
4. Dans la liste **Modèles disponibles**, sélectionnez des modèles, puis cliquez sur **Ajouter**.

   Lorsque vous sélectionnez des modèles :

   - Sélectionnez plusieurs entrées en cliquant sur les noms de modèle, ce qui met leur nom en surbrillance.
   - Si vous recherchez un modèle spécifique, utilisez la fonction de recherche. Vous pouvez y saisir tout ou partie du nom du modèle.

   Remarque

   Chaque règle contient un maximum de 200 modèles.

Configurez les paramètres du canal :

5. Cliquez sur l'onglet **Canal**.

6. Sélectionnez les canaux pour la règle.

   Pour plus d'informations sur les canaux, voir *Canaux réseau à la page 19-7* et *Canaux système et application à la page 19-10*.

7. Si vous avez sélectionné l'un des canaux réseau, sélectionnez la portée de transmission :

   - **Toutes les transmissions**
   - **Uniquement les transmissions hors du réseau local**

   Pour plus d'informations sur l'étendue de transmission, l'influence de l'étendue de transmission sur les cibles et la manière de définir des cibles correctement, voir *Étendue et cibles de transmission pour les canaux réseau à la page 19-7*.

8. Si vous avez sélectionné **Clients de messagerie** :

   a. Cliquez sur **Exceptions**.

   b. Indiquez les domaines de messagerie internes contrôlés et non contrôlés.

      Pour plus d'informations sur les domaines de messagerie contrôlés et non contrôlés, voir *Clients de messagerie à la page 19-8*.

9. Si vous avez sélectionné **Stockage amovible** :

   a. Cliquez sur **Exceptions**.

   b. Ajoutez des périphériques de stockage amovibles non contrôlés en les identifiant par leurs fournisseurs. Le modèle et l'ID de série du dispositif sont facultatifs.

      La liste approuvée pour les périphériques USB prend en charge l'utilisation de l'astérisque (*) comme caractère générique. Remplacez tout champ avec l'astérisque (*) pour inclure tous les périphériques répondant aux autres champs.

Par exemple, [vendeur]-[modèle]-* place tous les dispositifs USB du vendeur et du type de modèle spécifiés dans la liste approuvée, peu importe l'ID de série.

c. Pour ajouter plusieurs périphériques, cliquez sur l'icône plus (**+**).

Configurez les paramètres de l'action :

10. Cliquez sur l'onglet **Action**.

11. Sélectionnez une action principale et toute action complémentaire applicable. Pour plus d'informations sur les actions, voir *Mesures de prévention contre la perte de données à la page 19-11*.

12. Après avoir configuré les paramètres de **Modèle**, **Canal** et **Action**, cliquez sur **Enregistrer**.

Étendue et cibles de transmission pour les canaux réseau

L'étendue et les cibles de transmission définissent les transmissions de données sur les canaux réseau que Prévention contre la perte de données doit contrôler. Pour les transmissions qui doivent être contrôlées, Prévention contre la perte de données vérifie la présence d'identificateurs de données avant d'autoriser ou de bloquer la transmission. Pour les transmissions qui ne doivent pas être contrôlées, Prévention contre la perte de données ne vérifie pas la présence d'identificateurs de données et autorise directement la transmission.

Canaux réseau

La prévention contre la perte de données peut contrôler les transmissions de données via les canaux réseau suivants :

- Clients de messagerie
- FTP
- HTTP et HTTPS
- Applications de messagerie instantanée

- Protocole SMB
- Webmail

Pour déterminer les transmissions de données à contrôler, la prévention contre la perte de données vérifie l'étendue de transmission que vous devez configurer. En fonction de l'étendue sélectionnée, la prévention contre la perte de données contrôlera toutes les transmissions de données ou uniquement les transmissions effectuées en dehors du réseau local (LAN).

Clients de messagerie

Le module de prévention contre la perte de données surveille les e-mails transmis via divers clients de messagerie. La prévention contre la perte de données recherche des identificateurs de données dans l'objet, le corps et les pièces jointes du courrier électronique. Pour obtenir la liste des clients de messagerie pris en charge, consultez le document *Listes de protection des données* à l'adresse :

Le contrôle s'effectue lorsqu'un utilisateur tente d'envoyer un e-mail. Si l'e-mail contient des identificateurs de données, la prévention contre la perte de données autorise ou bloque l'e-mail.

Vous pouvez définir les domaines de messagerie internes non contrôlés et des sous-domaines contrôlés.

- **Domaines de messagerie non contrôlés** : la prévention contre la perte de données autorise immédiatement la transmission d'e-mails envoyés à des domaines non contrôlés.

Remarque

Des transmissions de données effectuées vers des domaines de messagerie non contrôlés et vers des sous-domaines de messagerie contrôlés pour lesquels l'action est définie sur « Contrôler » ont le même résultat, À savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les domaines de messagerie non contrôlés, la prévention contre la perte de données n'enregistre pas la transmission alors que pour les sous-domaines de messagerie contrôlés, la transmission est toujours enregistrée.

- **Sous-domaines de messagerie contrôlés** : quand la prévention contre la perte de données détecte un courrier électronique transmis à un sous-domaine contrôlé, elle vérifie l'action définie par la stratégie. Selon l'action définie, la transmission est autorisée ou bloquée.

Remarque

Si vous définissez les clients de messagerie comme des canaux contrôlés, un e-mail doit correspondre à une stratégie pour être contrôlé. Par contre, un courrier électronique envoyé À un sous-domaine de messagerie contrôlé est automatiquement vérifié, même s'il ne correspond pas À une stratégie.

Spécifiez des domaines en utilisant l'un des formats suivants en prenant soin de séparer les domaines par des virgules :

- format X400, tel que /O=Trend/OU=USA, /O=Trend/OU=China
- Domaines de messagerie, comme `example.com`

Pour les e-mails envoyés via le protocole SMTP, la prévention contre la perte de données vérifie si le serveur SMTP cible figure dans les listes suivantes :

1. Cibles contrôlées
2. Cibles non contrôlées
3. Domaines de messagerie non contrôlés
4. Sous-domaines de messagerie contrôlés

Cela signifie que si un courrier électronique est envoyé vers un serveur SMTP se trouvant dans la liste des cibles contrôlées, le courrier est vérifié. Si le serveur SMTP ne se trouve pas dans la liste des cibles contrôlées, la prévention contre la perte de données vérifie les autres listes.

Pour les courriers électroniques envoyés via d'autres protocoles, la prévention contre la perte de données ne vérifie que les listes suivantes :

1. Domaines de messagerie non contrôlés
2. Sous-domaines de messagerie contrôlés

Canaux système et application

La prévention contre la perte de données peut contrôler les canaux système et application suivants :

- Cloud Storage Service
- Enregistreurs de données (CD/DVD)
- Applications pair-À-pair
- Cryptage PGP
- Imprimante
- Stockage amovible
- Logiciel de synchronisation (ActiveSync)
- Presse-papiers Windows

Outil Liste de dispositifs

Exécutez localement l'outil Liste de dispositifs sur chaque endpoint pour interroger les dispositifs externes qui y sont connectés. L'outil scanne un endpoint à la recherche de dispositifs externes, puis affiche les informations relatives à ce dispositif dans une fenêtre de navigateur. Vous pouvez ensuite utiliser les informations lors de la configuration des paramètres des dispositifs pour la prévention contre la perte de données et le contrôle des dispositifs.

Exécution de l'outil Liste de dispositifs

Procédure

1. Sur l'ordinateur serveur OfficeScan, accédez au répertoire `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Copiez `listDeviceInfo.exe` sur le endpoint cible.

3. Sur le endpoint, double-cliquez sur `listDeviceInfo.exe`.

4. Les informations relatives au dispositif s'affichent dans la fenêtre de navigation qui s'ouvre. La prévention contre la perte de données et le contrôle des dispositifs utilisent les informations suivantes :

   - Revendeur (obligatoire)
   - Modèle (facultatif)
   - ID de série (facultatif)

Mesures de prévention contre la perte de données

Lorsque la prévention contre la perte de données détecte la transmission d'identificateurs de données, elle vérifie la stratégie DLP pour les identificateurs de données détectés, puis effectue l'action configurée pour la stratégie.

Le tableau suivant répertorie les actions Prévention contre la perte de données.

TABLEAU 19-1. Mesures de prévention contre la perte de données

ACTION	DESCRIPTION
Actions	
Ignorer	La prévention contre la perte de données autorise et consigne la transmission.
Bloquer	La prévention contre la perte de données bloque et consigne la transmission.
Actions supplémentaires	
Notifier l'utilisateur de l'agent	La prévention contre la perte de données affiche un message de notification pour informer l'utilisateur de la transmission de données et si cette dernière est autorisée ou bloquée.
Données d'enregistrement	Indépendamment de l'action principale, la prévention contre la perte de données enregistre les informations sensibles dans le répertoire `<dossier d'installation du client>\DLPLite\Forensic`. Sélectionnez cette

ACTION	DESCRIPTION
	action pour évaluer les informations sensibles en cours de marquage par Prévention contre la perte de données. Les informations sensibles enregistrées utilisent trop d'espace disque. De ce fait, Trend Micro recommande fortement de choisir cette option uniquement pour les informations hautement sensibles.
Chiffrer les canaux pris en charge À l'aide de la clé / du mot de passe spécifié(e) (uniquement disponible si Endpoint Encryption est installé) **Remarque** Cette option est disponible uniquement pour les canaux de service de stockage amovible et de Cloud Storage lors de la sélection de l'action **Ignorer**.	Si Trend Micro Endpoint Encryption est installé avec l'agent OfficeScan, la prévention contre la perte de données peut chiffrer automatiquement les fichiers avant d'autoriser un utilisateur À les déplacer. Si Endpoint Encryption n'est pas installé, la prévention contre la perte de données bloque les fichiers. Choisissez l'une des clés de chiffrement suivantes ou un mot de passe fixe : • **Clé utilisateur** :également dénommée **clé locale**, cette clé est unique pour chaque utilisateur et limite l'accès au fichier chiffré À son créateur. • **Clé partagée** : cette clé fait référence À la **clé de groupe** ou **clé d'entreprise**. L'administrateur Endpoint Encryption en configure le type À l'aide de la console PolicyServer MMC. • **Mot de passe fixe** : les utilisateurs fournissent manuellement un mot de passe fixe par le biais d'une invite À l'écran. Endpoint Encryption crée un package auto-extractible auquel les utilisateurs peuvent accéder depuis n'importe quel endpoint après avoir fourni le mot de passe de déchiffrement.

Action	Description
	Important • Endpoint Encryption doit être installé sur le endpoint cible et l'utilisateur doit se connecter À Endpoint Encryption pour chiffrer les données. • Les fichiers chiffrés se trouvant sur des périphériques USB font l'objet d'un scan de la prévention contre la perte de données lorsque des utilisateurs tentent de déchiffrer ces fichiers. Le déchiffrage de fichiers contenant des données sensibles sur un périphérique USB déclenche le protocole de chiffrement ; par conséquent, le système demande (À nouveau) le chiffrement des données sensibles. Pour empêcher le module de prévention contre la perte de données de tenter de chiffrer à nouveau les données, déplacez les fichiers chiffrés vers un lecteur local avant toute tentative d'accès aux données. • La prévention contre la perte de données bloque les tentatives de téléchargement de fichiers sur le stockage en ligne avec un client Web. Chiffrez manuellement les fichiers avant de les télécharger avec un client Web.
Justification de l'utilisateur **Remarque** Cette option est uniquement disponible lorsque l'action **Bloquer** a été sélectionnée.	La prévention contre la perte de données affiche une boîte de dialogue supplémentaire avant d'exécuter l'action « Bloquer ». L'utilisateur peut forcer le contournement de l'action « Bloquer » en fournissant une explication quant À la sûreté du transfert des données sensibles. Les motifs de justification disponibles sont les suivants : • **Cette action est effectuée dans le cadre d'un processus d'entreprise établi.** • **Ce transfert a été approuvé par mon responsable.** • **Les données contenues dans ce fichier ne sont pas confidentielles.**

ACTION	DESCRIPTION
	• **Autre** : les utilisateurs peuvent fournir une autre explication dans ce champ.

Exceptions de prévention contre la perte de données

Les exceptions DLP s'appliquent à l'intégralité de la stratégie, y compris aux règles définies au sein de la stratégie. La prévention contre la perte de données applique les paramètres d'exception à toutes les transmissions avant de scanner les actifs numériques. Si une transmission correspond à l'une des règles d'exception, la prévention contre la perte de données autorise ou scanne immédiatement cette transmission, selon le type d'exception.

Définition des cibles contrôlées et non contrôlées

Définissez les cibles non contrôlées et contrôlées en fonction de la portée de transmission configurée dans l'onglet **Canal**. Pour obtenir plus d'informations sur la manière de définir des cibles contrôlées et non contrôlées pour **Toutes les transmissions**, consultez *Étendue de transmission :Toutes les transmissions à la page 19-15*. Pour obtenir plus d'informations sur la manière de définir des cibles contrôlées et non contrôlées pour **Uniquement les transmissions effectuées hors du réseau local**, consultez *étendue de transmission:uniquement les transmissions hors du réseau local à la page 19-17*.

Suivez ces instructions lors de la définition de cibles contrôlées ou non contrôlées :

1. Définir chaque cible par :
   - Adresse IP
   - Nom d'hôte
   - FQDN
   - Adresse réseau et masque de sous-réseau, par exemple 10.1.1.1/32

Remarque

Pour le masque de sous-réseau, la prévention contre la perte de données ne prend en charge que les ports de type CIDR (Classless Inter-Domain Routing). Cela signifie que vous pouvez ne saisir qu'un numéro comme 32 au lieu de 255.255.255.0.

2. Pour cibler des canaux spécifiques, incluez la valeur par défaut ou les numéros de port définis par l'entreprise pour ces canaux. Par exemple, le port 21 est généralement utilisé pour le trafic FTP, le port 80 pour HTTP et le port 443 pour HTTPS. Utilisez le signe deux-points pour séparer la cible des numéros de port.
3. Vous pouvez également inclure des plages de ports. Pour inclure tous les ports, ignorez la plage de ports.

   Vous trouverez ci-dessous des exemples de cibles avec des numéros et des plages de ports :

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. Séparez les cibles par des virgules.

Étendue de transmission :Toutes les transmissions

La prévention contre la perte de données surveille les données transmises hors de l'ordinateur hôte.

Remarque

Trend Micro recommande de choisir cette étendue pour les agents externes.

Si vous ne souhaitez pas contrôler les transmissions de données vers certaines cibles hors de l'ordinateur hôte, définissez les points suivants :

- **Cibles non contrôlées** : la prévention de perte de données ne surveille pas les données transmises vers ces cibles.

Remarque

Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, À savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, la prévention contre la perte de données ne consigne pas la transmission, tandis que pour les cibles contrôlées, la transmission est toujours consignée.

- **Cibles contrôlées** : il s'agit de cibles spécifiques, au sein des cibles non contrôlées, qui doivent être contrôlées. Les cibles contrôlées sont :
  - facultatives si vous avez défini des cibles non contrôlées.
  - non configurables si vous n'avez pas défini de cibles non contrôlées.

Par exemple :

Les adresses IP suivantes sont attribuées au département juridique de votre entreprise :

- `10.201.168.1` À `10.201.168.25`

Vous créez une stratégie qui contrôle la transmission des contrats de travail à tous les employés à l'exception du personnel travaillant à plein-temps dans le département juridique. Vous devez donc sélectionner **Toutes les transmissions** comme étendue de transmission et ensuite :

OPTION	ÉTAPES
Option 1	1. Ajouter `10.201.168.1` À `10.201.168.25` aux cibles non contrôlées. 2. Ajouter les adresses IP du personnel travaillant à temps partiel dans le département juridique aux cibles contrôlées. Il y aurait 3 adresses IP : `10.201.168.21` À `10.201.168.23`.
Option 2	Ajouter les adresses IP du personnel travaillant à temps plein dans le département juridique aux cibles non contrôlées. • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 19-14*.

étendue de transmission:uniquement les transmissions hors du réseau local

La prévention contre la perte de données contrôle les données transmises vers une cible à l'extérieur du réseau local.

Remarque

Trend Micro recommande de choisir cette étendue pour les agents internes.

« Réseau » se rapporte À l'entreprise ou au réseau local. Cela comprend le réseau actuel (adresse IP du endpoint et masque de réseau) et les adresses IP privées standards suivantes :

- Classe A :`10.0.0.0` À `10.255.255.255`
- Classe B :`172.16.0.0` À `172.31.255.255`
- Classe C :`192.168.0.0` À `192.168.255.255`

Si vous sélectionnez cette étendue de transmission, vous pouvez définir ce qui suit :

- **Cibles non contrôlées** : cibles situées hors du réseau local que vous considérez comme inoffensives et qui ne doivent donc pas être contrôlées.

  Remarque

  Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, À savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, la prévention contre la perte de données ne consigne pas la transmission, tandis que pour les cibles contrôlées, la transmission est toujours consignée.

- **Cibles contrôlées** : définit les cibles dans le réseau local que vous souhaitez contrôler.

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 19-14*.

Règles de décompression

Les fichiers contenus dans des fichiers compressés peuvent être scannés pour déceler la présence d'actifs numériques. Pour déterminer les fichiers à scanner, la prévention contre la perte de données applique les règles suivantes à un fichier compressé :

- **dlp_compressed_size**
- **dlp_compressed_layers**
- **dlp_compressed_file_count**

Chapitre 20

Widgets Data Discovery

Cette section contient des rubriques d'aide concernant tous les widgets du tableau de bord de Data Discovery qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget Principales détections de stratégies de fichiers sensibles à la page 20-2*
- *Widget Principaux endpoints sur lesquels se trouvent des fichiers sensibles à la page 20-4*
- *Widget Principales correspondances de modèles Data Discovery à la page 20-6*
- *Widget Principaux fichiers sensibles à la page 20-7*

Widget Principales détections de stratégies de fichiers sensibles

Ce widget affiche des informations sur les détections de violations de stratégie Data Discovery et les fichiers sensibles qui ont déclenché les règles.

Remarque

Par défaut, le widget affiche les données de tous les produits gérés pour lesquels le compte utilisateur dispose de privilèges d'affichage.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

- Pour définir une plage de temps ou un intervalle personnalisé, cliquez sur l'icône Paramètres (>) et sélectionnez **Personnalisé** pour la **Plage**.

Utilisez la liste déroulante **Règle** pour spécifier la règle ayant déclenché la détection.

- Pour définir le nombre de règles qui s'affichent, cliquez sur l'icône Paramètres (>) et sélectionnez une valeur dans la liste déroulante **Règles à afficher**.
- Pour regrouper les données restantes, cliquez sur l'icône Paramètres (>) et sélectionnez **Afficher les données restantes comme « Autres »**.

Vous pouvez choisir d'afficher les données dans une table, un graphique à barres, un graphique circulaire ou un graphique linéaire en cliquant sur les icônes d'affichage ( ).

L'affichage par défaut présente les informations suivantes dans une table.

Nom de la colonne	Description
Rule Name	Affiche les règles déclenchées par les fichiers sensibles.

Nom de la colonne	Description
Détections	Affiche le nombre de fois où la règle est déclenchée Cliquez sur le nom de la colonne **Détections** pour trier la table en fonction du nombre de détections. Cliquez sur le nombre pour afficher des informations détaillées sur la détection (moment auquel la détection se produit, fichiers sensibles détectés).
Pourcentage	Affiche le nombre de fois où la règle est déclenchée en pourcentage du nombre total de détections

Cliquez sur un nombre dans la colonne **Détections** ou cliquez sur une section de graphique pour afficher des informations détaillées.

Données	Description
Reçu	Heure et date auxquelles Control Manager a reçu les données
Généré	Heure et date auxquelles la détection s'est produite
Règle	Règle déclenchée
Endpoint	Endpoint ayant déclenché la règle
Domaine	Domaine ayant déclenché la règle
Utilisateur	Utilisateur ayant déclenché la règle
Domaine de l'utilisateur	Domaine auquel appartient l'utilisateur
Chemin d'accès au fichier	Chemin d'accès au fichier sensible
Fichier	Nom du fichier sensible
Modèle	Modèle auquel appartient la règle
Action	Action entreprise sur le fichier sensible

Widget Principaux endpoints sur lesquels se trouvent des fichiers sensibles

Ce widget affiche des informations sur les endpoints avec des fichiers sensibles qui ont déclenché des violations de stratégie Data Discovery.

Remarque

Par défaut, le widget affiche les données de tous les produits gérés pour lesquels le compte utilisateur dispose de privilèges d'affichage.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

- Pour définir une plage de temps ou un intervalle personnalisé, cliquez sur l'icône Paramètres (>) et sélectionnez **Personnalisé** pour la **Plage**.

Utilisez la liste déroulante **Règle** pour spécifier la règle ayant déclenché la détection.

- Pour définir le nombre de modèles qui s'affichent, cliquez sur l'icône Paramètres (>) et sélectionnez une valeur dans la liste déroulante **Endpoints à afficher**.
- Pour regrouper les données restantes, cliquez sur l'icône Paramètres (>) et sélectionnez **Afficher les données restantes comme « Autres »**.

Vous pouvez choisir d'afficher les données dans une table, un graphique à barres ou un graphique circulaire en cliquant sur les icônes d'affichage ( ).

L'affichage par défaut présente les informations suivantes dans une table.

Nom de la colonne	Description
Endpoints	Affiche l'endpoint avec des fichiers sensibles qui ont déclenché la règle

Nom de la colonne	Description
Détections	Affiche le nombre de fois où la règle est déclenchée Cliquez sur le nom de la colonne **Détections** pour trier la table en fonction du nombre de détections.
Pourcentage	Affiche le nombre de fois où la règle est déclenchée en pourcentage du nombre total de détections

Cliquez sur un nombre dans la colonne **Détections** ou cliquez sur une section de graphique pour afficher des informations détaillées.

Données	Description
Reçu	Heure et date auxquelles Control Manager a reçu les données
Généré	Heure et date auxquelles la détection s'est produite
Règle	Règle déclenchée
Endpoint	Endpoint ayant déclenché la règle
Domaine	Domaine ayant déclenché la règle
Utilisateur	Utilisateur ayant déclenché la règle
Domaine de l'utilisateur	Domaine auquel appartient l'utilisateur
Chemin d'accès au fichier	Chemin d'accès au fichier sensible
Fichier	Nom du fichier sensible
Modèle	Modèle auquel appartient la règle
Action	Action entreprise sur le fichier sensible

Widget Principales correspondances de modèles Data Discovery

Ce widget affiche des informations sur les principales violations de stratégie de modèles Data Discovery au fil du temps.

Remarque

Par défaut, le widget affiche les données de tous les produits gérés pour lesquels le compte utilisateur dispose de privilèges d'affichage.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

- Pour définir une plage de temps ou un intervalle personnalisé, cliquez sur l'icône Paramètres (>) et sélectionnez **Personnalisé** pour la **Plage**.

Utilisez la liste déroulante **Règle** pour spécifier la règle ayant déclenché la détection.

- Pour définir le nombre de modèles qui s'affichent, cliquez sur l'icône Paramètres (>) et sélectionnez une valeur dans la liste déroulante **Modèle à afficher**.
- Pour regrouper les données restantes, cliquez sur l'icône Paramètres (>) et sélectionnez **Afficher les données restantes comme « Autres »**.

Vous pouvez choisir d'afficher les données dans une table, un graphique à barres ou un graphique circulaire en cliquant sur les icônes d'affichage ( ).

L'affichage par défaut présente les informations suivantes dans une table.

NOM DE LA COLONNE	DESCRIPTION
Modèles	Affiche les modèles déclenchés par les fichiers sensibles
Détections	Affiche le nombre de fois où le modèle est déclenché Cliquez sur le nom de la colonne **Détections** pour trier la table en fonction du nombre de détections.

Nom de la colonne	Description
Pourcentage	Affiche le nombre de fois où le modèle est déclenché en pourcentage du nombre total de détections

Cliquez sur un nombre dans la colonne **Détections** ou cliquez sur une section de graphique pour afficher des informations détaillées.

Données	Description
Reçu	Heure et date auxquelles Control Manager a reçu les données
Généré	Heure et date auxquelles la détection s'est produite
Règle	Règle déclenchée
Endpoint	Endpoint ayant déclenché la règle
Domaine	Domaine ayant déclenché la règle
Utilisateur	Utilisateur ayant déclenché la règle
Domaine de l'utilisateur	Domaine auquel appartient l'utilisateur
Chemin d'accès au fichier	Chemin d'accès au fichier sensible
Fichier	Nom du fichier sensible
Modèle	Modèle auquel appartient la règle
Action	Action entreprise sur le fichier sensible

Widget Principaux fichiers sensibles

Ce widget affiche des informations sur les principaux fichiers sensibles qui ont déclenché des violations de stratégie Data Discovery au fil du temps.

Remarque

Par défaut, le widget affiche les données de tous les produits gérés pour lesquels le compte utilisateur dispose de privilèges d'affichage.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

- Pour définir une plage de temps ou un intervalle personnalisé, cliquez sur l'icône Paramètres (>) et sélectionnez **Personnalisé** pour la **Plage**.

Utilisez la liste déroulante **Règle** pour spécifier la règle ayant déclenché la détection.

- Pour définir le nombre de détections qui s'affichent, cliquez sur l'icône Paramètres (>) et sélectionnez une valeur dans la liste déroulante **Fichiers sensibles à afficher**.
- Pour regrouper les données restantes, cliquez sur l'icône Paramètres (>) et sélectionnez **Afficher les données restantes comme « Autres »**.

Vous pouvez choisir d'afficher les données dans une table, un graphique à barres ou un graphique circulaire en cliquant sur les icônes d'affichage ( ).

L'affichage par défaut présente les informations suivantes dans une table.

Nom de la colonne	Description
Fichier	Affiche les fichiers sensibles ayant potentiellement échappé
Détections	Affiche le nombre de fois où les fichiers sensibles ont potentiellement échappé Cliquez sur le nom de la colonne **Détections** pour trier la table en fonction du nombre de détections.
Pourcentage	Affiche le nombre de fois où les fichiers sensibles ont potentiellement échappé en pourcentage du nombre total de détections

Cliquez sur un nombre dans la colonne **Détections** ou cliquez sur une section de graphique pour afficher des informations détaillées.

DONNÉES	DESCRIPTION
Reçu	Heure et date auxquelles Control Manager a reçu les données
Généré	Heure et date auxquelles la détection s'est produite
Règle	Règle déclenchée
Endpoint	Endpoint ayant déclenché la règle
Domaine	Domaine ayant déclenché la règle
Utilisateur	Utilisateur ayant déclenché la règle
Domaine de l'utilisateur	Domaine auquel appartient l'utilisateur
Chemin d'accès au fichier	Chemin d'accès au fichier sensible
Fichier	Nom du fichier sensible
Modèle	Modèle auquel appartient la règle
Action	Action entreprise sur le fichier sensible

Chapitre 21

Paramètres de stratégie d'OfficeScan Data Discovery

Cette section explique comment configurer les paramètres de stratégie d'OfficeScan Data Discovery dans Control Manager.

Les rubriques sont les suivantes:

- *Création de stratégies de découverte des données à la page 21-2*

Création de stratégies de découverte des données

Data Discovery permet de rechercher des informations sensibles dans les bases de données, les endpoints et les systèmes de gestion des documents. Les widgets Découverte des données affichent l'état de conformité avec une stratégie de la société en termes de prévention contre la perte de données. L'utilisation de stratégies et de widgets Data Discovery permet aux administrateurs de réaliser des actions de correction sur leur réseau.

Remarque

L'exécution d'un scan complet sur un répertoire ou un lecteur de endpoint peut considérablement ralentir le système pour les utilisateurs finaux.

Procédure

1. Sélectionnez **Activer Data Discovery**.
2. Cliquez sur **Ajouter**.

   L'écran **Paramètres de la stratégie Data Discovery** s'affiche.
3. Sélectionnez **Activer cette règle**.
4. Spécifiez un nom pour la règle.
5. Configurez les paramètres du dossier cible :

   a. Cliquez sur l'onglet **Dossier cible**.

   Remarque

   Le dossier racine ne peut être ni un dossier partagé de Windows, ni un dispositif amovible (dispositif USB ou DVD).

   b. Dans la section **Chemin d'accès au fichier**, indiquez l'emplacement pour le scan des fichiers.

Remarque

Data Discovery ne scanne pas les fichiers `autoexec.bat` situés dans les répertoires suivants :

- `\Documents and Settings\*\Application Data\`
- `\Documents and Settings\*\Local Settings\`
- `\Documents and Settings\*\Cookies\`
- `\Program Files\`
- `\Windows\`
- `\Winnt\`
- `\Users\*\AppData\`
- `\ProgramData\`

c. Dans la section **Exceptions de types de fichiers**, indiquez les exceptions de scan.

- **Scanner** : indiquez les fichiers ou types de fichiers à scanner.
- **Ne pas scanner** : indiquez les fichiers, types de fichiers ou dossiers que Découverte des données ne scannera pas.

Remarque

- Découverte des données prend en charge les caractères génériques suivants :
  - * : remplace tout caractère ou toute suite de caractères situés avant ou après le signe *
  - ? : remplace un caractère unique ou un caractère unique codé sur deux octets
- Si vous avez plusieurs entrées, séparez-les par une barre verticale (|), selon le format suivant :
  - Pour les fichiers : *.<extension du fichier> (par exemple : *.exe|*.doc)
  - Pour les dossiers : indiquez un chemin de fichier (par exemple : *\Test*|C:\My-Docs\)

Configurez les paramètres du modèle :

6. Configurez les paramètres du modèle :

   a. Cliquez sur l'onglet **Modèle**.

   b. Dans la liste **Modèles disponibles**, sélectionnez des modèles, puis cliquez sur **Ajouter**.

      Lorsque vous sélectionnez des modèles :

      - Sélectionnez plusieurs entrées en cliquant sur les noms de modèle, ce qui met leur nom en surbrillance.
      - Si vous recherchez un modèle spécifique, utilisez la fonction de recherche. Vous pouvez y saisir tout ou partie du nom du modèle.

      Remarque

      - Chaque règle contient un maximum de 500 modèles.
      - Si votre modèle favori ne se ne trouve pas dans la liste **Modèles disponibles**, accédez à **Stratégies** > **Ressources de stratégies** > **Modèles DLP** et créez un nouveau modèle.

7. Configurez les paramètres de l'action :

   a. Cliquez sur l'onglet **Action**.

   b. Sélectionnez **Surveiller** pour enregistrer les détections à des fins d'analyse.

   c. (Facultatif) Sélectionnez **Chiffrer** pour chiffrer les fichiers sensibles en utilisant l'une des méthodes suivantes :

      - **Clé utilisateur**
      - **Clé de groupe**
      - **Mot de passe de chiffrement** : il s'agit d'un mot de passe global qui sert à tous les serveurs OfficeScan. Cliquez sur **Créer un mot de passe de chiffrement** pour configurer un mot de passe.

8. Programmez l'exécution du scan :

   a. Cliquez sur l'onglet **Programmation**.

   b. Indiquez la fréquence du scan.

   c. Indiquez l'heure de début du scan.

9. Cliquez sur **Enregistrer** pour appliquer les paramètres.

Partie VIII

Widgets Endpoint Application Control

Chapitre 22

Widgets du tableau de bord d'Endpoint Application Control

Cette section contient des rubriques d'aide concernant tous les widgets du tableau de bord d'Endpoint Application Control qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget Indicateurs de performance clés de Endpoint Application Control à la page 22-2*
- *Gestion des règles de Endpoint Application Control à la page 22-7*
- *Widget Récapitulatif des utilisateurs et des endpoints de Endpoint Application Control à la page 22-8*
- *Principales applications lancées à la page 22-13*
- *Widget Événements d'application, de règle et de stratégie de Endpoint Application Control à la page 22-14*
- *Principales stratégies Endpoint Application Control déclenchées à la page 22-23*
- *Principaux utilisateurs déclenchant des règles de blocage Endpoint Application Control à la page 22-23*

Widget Indicateurs de performance clés de Endpoint Application Control

Ce widget affiche les indicateurs de performance clés d'Endpoint Application Control en fonction des critères sélectionnés. Il comprend des modèles personnalisables pour les applications détectées pour la première fois, les applications ne figurant pas dans la liste Certified Safe Software, le nombre moyen d'agents arrêtés, le nombre moyen d'endpoints non connectés et la règle de blocage et de verrouillage.

FIGURE 22-1. Exemple de widget Indicateurs de performance clés

Par défaut, le widget attribue l'indicateur « Important » ( ) aux événements dont le nombre d'occurrences s'élève à 5 et l'indicateur « Critique » ( ) aux événements dont le nombre d'occurrences s'élève à 10. Si vous le souhaitez, vous pouvez marquer des événements comme importants ou critiques en personnalisant les seuils d'événement.

Voir le tableau *Tâches d'ajout ou de modification d'indicateur*.

Accédez au **Tableau de bord**, puis sélectionnez **Paramètres du widget** dans le menu en haut à droite du widget pour effectuer les tâches suivantes :

TABLEAU 22-1. Tâches de configuration du widget Indicateurs de performance clés

TÂCHE	ÉTAPES
Modifier le calcul des tendances des indicateurs utilisé par le widget.	Le widget affiche les tendances dans la colonne **Modifier**. Le widget calcule les tendances des indicateurs en comparant la période actuelle avec la moyenne des périodes précédentes. Sous **Calculs de tendance**, saisissez un nombre de périodes précédentes pour obtenir une moyenne. La valeur par défaut est fixée à **1**.

Accédez au **Tableau de bord**, localisez ce widget, puis cliquez sur **Modifier** pour exécuter les tâches suivantes liées aux indicateurs. Après avoir exécuté les tâches, cliquez sur **OK**.

TABLEAU 22-2. Tâches associées aux indicateurs dans le widget Indicateurs de performance clés

TÂCHE	ÉTAPES
Ajouter un nouvel indicateur.	1. Cliquez sur **Ajouter un indicateur**. L'écran **Ajouter un indicateur** s'affiche. 2. Sélectionnez un modèle, personnalisez les paramètres (facultatif), puis cliquez sur **Enregistrer**. Voir le tableau *Tâches d'ajout ou de modification d'indicateur*.
Modifier un indicateur.	1. Cliquez sur l'indicateur dans la liste. L'écran **Modifier l'indicateur** s'affiche. 2. Personnalisez les paramètres, puis cliquez sur **Enregistrer**. Voir le tableau *Tâches d'ajout ou de modification d'indicateur*.
Supprimer un indicateur.	Cliquez sur à gauche de l'indicateur, puis cliquez sur **Supprimer**.

TABLEAU 22-3. Tâches d'ajout ou de modification d'indicateur

TÂCHE	ÉTAPES
Nommer un indicateur.	Sous **Titre**, saisissez un nom. **Conseil** Laissez ce champ vide pour permettre à Control Manager de nommer l'indicateur en fonction de votre configuration.
Sélectionner un modèle.	Sous **Modèle**, sélectionnez un modèle. Voir *À propos des modèles*.
Modifier la période.	Sous **Période**, sélectionnez une période pour les données de l'indicateur.
Afficher les icônes de seuil.	Cochez la case **Activer les seuils**.
Masquer les icônes de seuil.	Décochez la case **Activer les seuils**.
Définir le seuil « Important » ( ).	Sous **Marquer les événements comme importants**, saisissez le nombre minimal d'occurrences des événements. L'icône s'affiche dans la colonne **Occurrences** si les conditions suivantes sont réunies : • Le nombre d'occurrences d'un événement qui correspondent à cet indicateur est égal ou supérieur au seuil. • La case **Activer les seuils** est cochée.

TÂCHE	ÉTAPES
Définir le seuil « Critique » ( ).	Sous **Marquer les événements comme critiques**, saisissez le nombre minimal d'occurrences des événements. L'icône s'affiche dans la colonne **Occurrences** si les conditions suivantes sont réunies : • Le nombre d'occurrences d'un événement qui correspondent à cet indicateur est égal ou supérieur au seuil. • La case **Activer les seuils** est cochée.

Ce widget inclut des modèles personnalisables pour les indicateurs suivants :

« MODÈLE »	« TYPE DE JOURNAL »	« PAR » COLONNE DES OCCURRENCES REGROUPÉES PAR TYPE DE DONNÉES	« PÉRIODE » (PAR DÉFAUT)
Applications détectées pour la première fois	Applications approuvées **Important** Ces données correspondent au type de journal « Applications connues ».		7 jours
Applications ne figurant pas dans la liste Certified Safe Software	Actions de stratégie		7 jours

« Modèle »	« Type de journal »	« Par » Colonne des occurrences regroupées par type de données	« Période » (par défaut)
Nombre moyen d'agents arrêtés	Échantillons de clients **Important** Ces données correspondent à la source de données « Utilisateurs et endpoints ».		1 jour
Nombre moyen d'endpoints non connectés	Échantillons de clients **Important** Ces données correspondent à la source de données « Utilisateurs et endpoints ».		Plusieurs fois au cours du dernier jour
Événements d'application de règles de blocage et de verrouillage	Actions de stratégie	• Nom de l'endpoint • Nom (par défaut) • Nom d'utilisateur	7 jours

« Modèle »	« Type de journal »	« par » Colonne des occurrences regroupées par type de données	« Période » (par défaut)
Événements d'application de règles de blocage	Actions de stratégie	• Nom de l'endpoint • Nom (par défaut) • Nom d'utilisateur	7 jours
Événements d'application de règles de verrouillage	Actions de stratégie	• Nom de l'endpoint • Nom (par défaut) • Nom d'utilisateur	7 jours
Applications non catégorisées détectées	Actions de stratégie		7 jours

Gestion des règles de Endpoint Application Control

Ce widget fournit la liste des types et des noms des règles contenues dans Endpoint Application Control.

Pour ajouter des règles à Endpoint Application Control, cliquez sur **Ajouter une règle** afin de sélectionner des types de règles spécifiques à ajouter.

RÈGLE	DESCRIPTION
Autoriser	Utilisez la règle d'**autorisation** pour étendre les droits d'autorisation des applications approuvées.
Bloquer	Utilisez la règle de **blocage** pour bloquer les applications avant ou après l'exécution.
Verrouillage	Utilisez la règle de **verrouillage** pour autoriser toutes les applications actuellement installées. Un inventaire d'endpoint complet et à jour est alors requis.

Widget Récapitulatif des utilisateurs et des endpoints de Endpoint Application Control

Ce widget affiche un récapitulatif de la distribution des utilisateurs et des endpoints de Endpoint Application Control en fonction des critères sélectionnés. Il comprend des modèles personnalisables pour les connexions d'agent, les versions d'agent, les versions Windows des endpoints, les stratégies, les mises à jour de stratégie et les règles. Modifiez les modèles à l'aide des paramètres personnalisés.

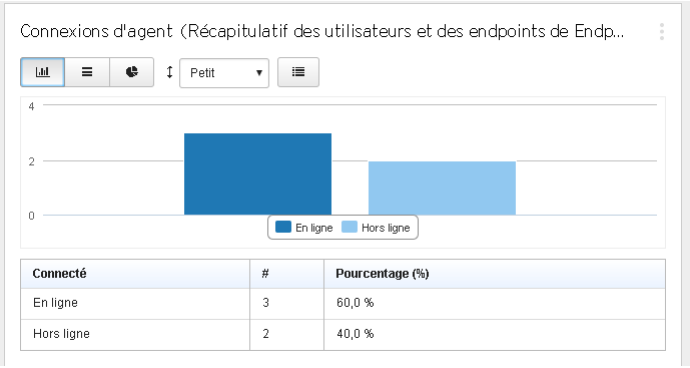


FIGURE 22-2. Exemple sur le widget Récapitulatif des utilisateurs et des endpoints

Accédez au **Tableau de bord**, puis sélectionnez **Paramètres du widget** dans le menu en haut à droite du widget pour effectuer les tâches suivantes :

TABLEAU 22-4. Tâches de configuration du widget Récapitulatif des utilisateurs et des endpoints

TÂCHE	ÉTAPES
Nommer le widget.	Sous **Titre**, saisissez un nom. **Conseil** Laissez ce champ vide pour permettre à Control Manager de nommer le widget en fonction de votre configuration.
Sélectionner un modèle.	Sous **Modèle**, sélectionnez un modèle.
Modifier la source de données.	Sélectionnez **Avancé**. Sous **Source de données**, sélectionnez une source de données pour les données affichées par le widget. **FIGURE 22-3. Source de données**
Réduisez le nombre de résultats qui s'affichent.	Sélectionnez **Avancé**. Sous **Limiter les résultats à ce qui suit**, utilisez la recherche dynamique.

TÂCHE	ÉTAPES
Modifier le type de graphique.	Sous **Affichage**, sélectionnez l'un des types de graphique suivants : • Sélectionnez pour un graphique linéaire avec points de données. • Sélectionnez pour un histogramme horizontal. • Sélectionnez pour un graphique circulaire. (par défaut) • Sélectionnez pour une table de données. **Remarque** Ce contrôle n'est pas disponible si (affichage d'une table de données sous le graphique) est sélectionné.

TÂCHE	ÉTAPES
Modifier la taille du graphique.	À droite des types de graphique, sélectionnez l'une des tailles de graphique suivantes : • Sélectionnez **Petit** pour un graphique d'une hauteur de 1 unité environ. • Sélectionnez **Moyen** pour un graphique d'une hauteur de 2 unités environ. (par défaut) • Sélectionnez **Grand** pour un graphique d'une hauteur de 4 unités environ. **FIGURE 22-4. Taille du graphique**
Modifier l'emplacement de la légende.	Sous **Légende**, sélectionnez l'un des emplacements suivants : • **Aucun** • **En bas** (par défaut) • **À droite** • **En haut** • **À gauche** **Remarque** Ce contrôle n'est pas disponible si (affichage des données sous forme de graphique circulaire) est sélectionné.
Afficher les contrôles graphiques sur le widget.	Cochez la case **Barre d'outils**. (par défaut)
Masquer les contrôles graphiques sur le widget.	Décochez la case **Barre d'outils**.

TÂCHE	ÉTAPES
Afficher la table de résumé des données sous le graphique.	Cochez la case **Table de résumé des données sous le graphique**.
Masquer la table de résumé des données sous le graphique.	Décochez la case **Table de résumé des données sous le graphique**. (par défaut)
Enregistrer la configuration en tant que nouveau modèle.	Sous **Modèle**, sélectionnez + **Enregistrer les paramètres actuels en tant que modèle**.
Supprimer le widget.	Sélectionnez **Fermer le widget** dans le menu en haut à droite du widget. Le widget et toutes les personnalisations apportées aux paramètres du widget sont supprimées.

Ce widget inclut les modèles personnalisables suivants :

Remarque

Un seul modèle peut être affiché à la fois.

« MODÈLE »	« SOURCE DE DONNÉES »	ÉTENDUE	« AVANCÉ » COLONNE DE DONNÉES (PAR DÉFAUT)
Connexions d'agent	Utilisateurs et endpoints	Tous (non configurable par l'utilisateur)	Connecté
Versions d'agent	Utilisateurs et endpoints	3 premiers	Version de l'agent
Versions Windows des endpoints	Utilisateurs et endpoints	3 premiers	Version de Windows
Stratégies	Utilisateurs et endpoints	3 premiers	Stratégie

« Modèle »	« Source de données »	Étendue	« Avancé » Colonne de données (par défaut)
Mises à jour de stratégie	Utilisateurs et endpoints	Tous (non configurable par l'utilisateur)	Mises à jour de stratégie
Règles	Utilisateurs et endpoints	3 premiers	règles

Principales applications lancées

Ce widget affiche les applications les plus lancées signalées par Endpoint Application Control.

Utilisez l'icône d'**affichage** pour sélectionner le format des données.

Remarque

Ce widget prend uniquement en charge Endpoint Application Control 1.0

Widget Événements d'application, de règle et de stratégie de Endpoint Application Control

Utilisez ce widget pour afficher un récapitulatif de distribution des événements d'application de Endpoint Application Control en fonction des critères sélectionnés.

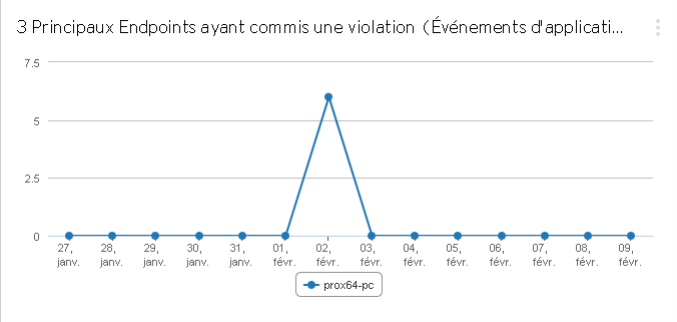
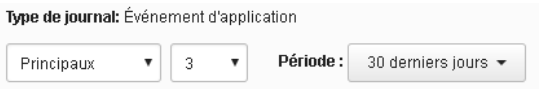


FIGURE 22-5. Exemple de widget Événements d'application, de règle et de stratégie

Accédez au **Tableau de bord**, puis sélectionnez **Paramètres du widget** dans le menu en haut à droite du widget pour effectuer les tâches suivantes :

TABLEAU 22-5. Tâches de configuration du widget Événements d'application, de règle et de stratégie

TÂCHE	ÉTAPES
Nommer le widget.	Sous **Titre**, saisissez un nom. **Conseil** Laissez ce champ vide pour permettre à Control Manager de nommer le widget en fonction de votre configuration.
Sélectionner un modèle.	Sous **Modèle**, sélectionnez un modèle. Voir **À propos des modèles**.

TÂCHE	ÉTAPES
Modifier la portée des données.	Sous **Type de journal**, sélectionnez une portée pour les données affichées par le widget.  **FIGURE 22-6. Portée des données**
Modifier la période.	Sous **Période**, sélectionnez une période pour les données du widget.
Modifier la source de données.	1. Sélectionnez **Avancé**. Le widget affiche les paramètres complémentaires. 2. Sous **Type de journal**, sélectionnez une source de données pour les données affichées par le widget. **FIGURE 22-7. Source de données**
Réduisez le nombre de résultats qui s'affichent.	Sélectionnez **Avancé**. Sous **Limiter les résultats à ce qui suit**, utilisez la recherche dynamique.

TÂCHE	ÉTAPES
Modifier le type de graphique.	Sous **Affichage**, sélectionnez l'un des types de graphique suivants : • Sélectionnez pour un graphique linéaire avec points de données. (par défaut) • Sélectionnez pour un histogramme vertical. • Sélectionnez pour un histogramme horizontal. • Sélectionnez pour un graphique circulaire. • Sélectionnez pour une table de données. **Remarque** Ce contrôle n'est pas disponible si (affichage d'une table de données sous le graphique) est sélectionné.

TÂCHE	ÉTAPES
Modifier la taille du graphique.	À droite des types de graphique, sélectionnez l'une des tailles de graphique suivantes : • Sélectionnez **Petit** pour un graphique d'une hauteur de 1 unité environ. • Sélectionnez **Moyen** pour un graphique d'une hauteur de 2 unités environ. (par défaut) • Sélectionnez **Grand** pour un graphique d'une hauteur de 4 unités environ. **FIGURE 22-8. Taille du graphique** **Remarque** Ce contrôle n'est pas disponible si (affichage des données sous forme de table) est sélectionné.

TÂCHE	ÉTAPES
Modifier l'emplacement de la légende.	Sous **Légende**, sélectionnez l'un des emplacements suivants : • **Aucun** • **En bas** (par défaut) • **À droite** • **En haut** • **À gauche** **Remarque** Ce contrôle n'est pas disponible si (affichage des données sous forme de graphique circulaire) ou (affichage des données sous forme de table) est sélectionné.
Afficher les contrôles graphiques sur le widget.	Cochez la case **Barre d'outils**.
Masquer les contrôles graphiques sur le widget.	Décochez la case **Barre d'outils**. (par défaut)
Afficher la table de résumé des données sous le graphique.	Cochez la case **Table de résumé des données sous le graphique**.
Masquer la table de résumé des données sous le graphique.	Décochez la case **Table de résumé des données sous le graphique**. (par défaut)
Enregistrer la configuration en tant que nouveau modèle.	Sous **Modèle**, sélectionnez **Enregistrer les paramètres actuels en tant que modèle**.

Ce widget inclut les modèles personnalisables suivants :

Remarque

Un seul modèle peut être affiché à la fois.

« Modèle »	« Type de journal »	Portée (par défaut)	« Période » (par défaut)	« Avancé » Colonne de données (par défaut)	« Avancé » Recherche dynamique (par défaut)
Applications sans règles	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom	La règle est vide
Stratégies appliquées	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Stratégie	La stratégie n'est pas vide

« Modèle »	« Type de journal »	Portée (par défaut)	« Période » (par défaut)	« Avancé » Colonne de données (par défaut)	« Avancé » Recherche dynamique (par défaut)
Applications bloquées	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom	L'action entreprise est bloquée
Applications utilisées	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom	L'action entreprise est autorisée

« Modèle »	« Type de journal »	Portée (par défaut)	« Période » (par défaut)	« Avancé » Colonne de données (par défaut)	« Avancé » Recherche dynamique (par défaut)
Stratégies non respectées	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Stratégie	La stratégie n'est pas vide ET L'action entreprise est bloquée
Règles non respectées	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom	La règle n'est pas vide ET L'action entreprise est bloquée

« Modèle »	« Type de journal »	Portée (par défaut)	« Période » (par défaut)	« Avancé » Colonne de données (par défaut)	« Avancé » Recherche dynamique (par défaut)
Endpoints ayant commis une violation	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom de l'endpoint	L'action entreprise est bloquée
Utilisateurs ayant commis une violation	Événement d'application **Important** Ces données correspondent au type de journal « Actions de stratégie ».	3 premiers	14 derniers jours	Nom d'utilisateur	L'action entreprise est bloquée

Principales stratégies Endpoint Application Control déclenchées

Ce widget affiche les stratégies Endpoint Application Control comportant le plus de correspondances.

Utilisez l'icône d'**affichage** pour sélectionner le format des données.

Remarque

Ce widget prend uniquement en charge Endpoint Application Control 1.0

Principaux utilisateurs déclenchant des règles de blocage Endpoint Application Control

Ce widget affiche les utilisateurs qui déclenchent le plus les règles de blocage et de verrouillage d'Endpoint Application Control.

Utilisez l'icône d'**affichage** pour sélectionner le format des données.

Remarque

Ce widget prend uniquement en charge Endpoint Application Control 1.0

Chapitre 23

Widget Paramètres de stratégie de Endpoint Application Control

Utilisez les widgets Endpoint Application Control suivants pour gérer vos agents Endpoint Application Control depuis Control Manager.

- *Règles de stratégie à la page 23-2*
- *Journalisation de stratégie à la page 23-3*
- *Déploiement de stratégies à la page 23-5*
- *Connexion au serveur PolicyServer à la page 23-6*
- *Expérience utilisateur – Stratégies à la page 23-7*

Règles de stratégie

Développez la section **Règles** afin d'exécuter les tâches suivantes :

TÂCHE	ÉTAPES
Afficher la liste des règles attribuées à cette stratégie.	Les règles attribuées à la stratégie s'affichent dans le tableau sous le bouton **Attribuer une règle**. **Conseil** Les applications de système d'exploitation considérées comme sûres par Certified Safe Software sont autorisées sauf si elles sont spécifiquement bloquées par une règle.
Attribuer une règle à cette stratégie.	Cliquez sur **Attribuer une règle**, puis effectuez l'une des actions suivantes : • Pour sélectionner des règles existantes à attribuer à la stratégie, sélectionnez **Existant**. L'écran **Attribuer des règles existantes à la stratégie** s'affiche. Sélectionnez la ou les règles à attribuer, puis cliquez sur **Attribuer les règles**.
Supprimer les règles sélectionnées de cette stratégie.	Sélectionnez la ou les règles dans la liste, cliquez sur **Supprimer la sélection**, puis cliquez de nouveau sur **Supprimer la sélection**.

Le tableau suivant décrit les options de configuration supplémentaires.

PARAMÈTRE DE STRATÉGIE	DÉTAILS
Autoriser systématiquement toutes les applications du répertoire Windows (ignorer les règles de blocage et de verrouillage)	Par défaut, Endpoint Application Control autorise toutes les applications situées dans le répertoire Windows. Cela fonctionne comme une règle d'**autorisation** pour le chemin par défaut de Windows, en supprimant toutes les règles de **blocage** ou de **verrouillage**.

Paramètre de stratégie	Détails
Appliquer automatiquement les règles de verrouillage aux endpoints lorsqu'ils sont déconnectés	Les endpoints déconnectés ne peuvent pas recevoir ou appliquer de nouvelles stratégies. Par défaut, cela signifie qu'un endpoint déconnecté continue d'appliquer sa stratégie actuelle.
Activer la protection contre les objets suspects (nécessite un abonnement à Control Manager)	Endpoint Application Control protège les endpoints correspondants contre les objets suspects.
Utiliser la méthode de blocage au niveau utilisateur la plus compatible et la moins riche en fonctions	Le blocage au niveau du noyau empêche les applications de démarrer en bloquant l'accès aux fichiers. Cela permet de renforcer la sécurité, mais peut, de manière inattendue, bloquer ou retarder momentanément l'accès à certains fichiers dont les applications autorisées ont besoin. Cette fonction est uniquement prise en charge dans les stratégies définies pour correspondre en premier aux critères « Utilisateur et groupe » (hors compte « SYSTÈME »). Le blocage au niveau utilisateur permet aux applications de démarrer, puis les arrête au niveau tâche. Ce blocage risque de ne pas être en mesure d'arrêter certaines applications après leur démarrage et ne prend pas en charge la fonction Source sécurisée ni le blocage des bibliothèques de liaison (DLL) et des applications associées à l'interpréteur Java.

Journalisation de stratégie

Développez la section **Journalisation** afin de configurer les paramètres de stratégie suivants pour les utilisateurs et les endpoints correspondants :

Paramètre de stratégie	Détails
Journaliser les actions suivantes	Sélectionnez l'une des restrictions de journalisation suivantes : • Choisissez **Aucune** pour ne journaliser aucune action. • Choisissez **Blocage** pour journaliser tout démarrage ou accès à une application bloquée qui n'est pas issue d'un répertoire exclu. Il s'agit du paramètre par défaut pour une nouvelle stratégie. • Choisissez **Sélection** pour journaliser tout démarrage ou accès à une application sélectionnée qui n'est pas issue d'un répertoire exclu. Utilisez la liste qui s'affiche pour sélectionner les règles à respecter. • Choisissez **N'importe quelle action** pour journaliser tout démarrage ou accès à une application qui n'est pas issue d'un répertoire exclu. **Remarque** La sélection de cette option peut générer des fichiers journaux volumineux et considérablement augmenter le transfert de données sur le réseau.
Exclure les répertoires suivants des journaux	Sélectionnez **Exclure les répertoires suivants des journaux**, puis saisissez les chemins des applications à exclure. Séparez chaque chemin par un retour chariot. Les chemins par défaut sont `%SYSTEMROOT%` et `%WINDIR%`.
Collecter les journaux agrégés tou(te)s les	Sélectionnez l'intervalle de collecte des journaux agrégés par endpoints. La valeur par défaut est fixée à **2 heures**. La valeur suggérée dépend du nombre d'agents déployés.

Déploiement de stratégies

Développez la section **Déploiement** afin de configurer les paramètres de stratégie suivants pour les utilisateurs et les endpoints correspondants :

Paramètre de stratégie	Détails
Envoyer les mises à jour de stratégie toutes les	Sélectionnez l'intervalle de temps de mise à jour de stratégie. La valeur par défaut est fixée à **15 minutes**. L'intervalle suggéré dépend du nombre d'agents déployés. Par défaut, pour réduire le transfert de données sur le réseau et les besoins en stockage à l'échelle locale, les stratégies déployées incluent uniquement les applications correspondantes déjà détectées dans l'inventaire d'un endpoint. À chaque intervalle de déploiement de stratégie, Endpoint Application Control inclut les éventuelles applications récemment ajoutées sur l'endpoint qui correspondent aux règles contenues dans la stratégie déployée.
Déployer la stratégie complète dans les cas suivants **Remarque** La sélection de ces options peut considérablement augmenter le transfert de données sur le réseau.	Si vous le souhaitez, vous pouvez déployer la « stratégie complète », qui inclut toutes les applications correspondantes et ignore la correspondance des inventaires d'endpoint. • Sélectionnez **L'endpoint se connecte pour moins de** et indiquez un nombre d'heures par semaine si les endpoints correspondants ne se connectent pas régulièrement au serveur. • Sélectionnez **L'endpoint commence à appliquer les règles de verrouillage** si les endpoints correspondants doivent être autorisés à installer et exécuter les applications indiquées dans les règles d'**autorisation** après l'application de règles de verrouillage.

Connexion au serveur PolicyServer

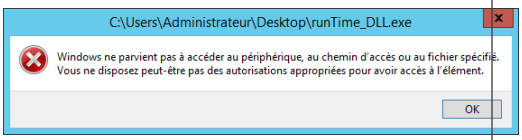
Développez la section **Connexion au serveur** afin de configurer les paramètres de stratégie suivants pour les utilisateurs et les endpoints correspondants :

PARAMÈTRE DE STRATÉGIE	DÉTAILS
Se connecter au serveur suivant	Votre réseau comporte peut-être plusieurs serveurs Endpoint Application Control, ou un serveur a peut-être été déplacé vers une nouvelle adresse IP. Indiquez le serveur auquel l'endpoint doit se connecter une fois cette stratégie appliquée. • Sélectionnez **Par défaut** pour utiliser le même serveur que celui qui héberge la console Web. Il s'agit du paramètre par défaut pour une nouvelle stratégie. • Sélectionnez **Spécifié**, puis saisissez l'adresse et le port du serveur pour indiquer un serveur.
Utiliser le protocole HTTPS	Par défaut, Endpoint Application Control utilise la configuration HTTP ou HTTPS sélectionnée pendant l'installation du serveur. Sélectionnez **Utiliser le protocole HTTPS** pour définir en permanence l'utilisation d'HTTPS par les utilisateurs ou les endpoints correspondants. **Conseil** L'utilisation de cette option nécessite que vous importiez l'autorité de certificat du serveur vers les endpoints de l'agent. Pour obtenir la procédure détaillée, consultez la page https://success.trendmicro.com/solution/1115573

Expérience utilisateur – Stratégies

Développez la section **Expérience utilisateur** afin de configurer les paramètres de stratégie suivants pour les utilisateurs et les endpoints correspondants :

PARAMÈTRE DE STRATÉGIE	DÉTAILS
Afficher l'icône de la barre d'état système	L'icône de la barre d'état système de Endpoint Application Control ( ) peut afficher les notifications, permettre à l'utilisateur de demander un accès à des applications et permettre à l'utilisateur de mettre à jour manuellement les paramètres et les journaux d'Endpoint Application Control. • Sélectionnez **Oui** pour afficher l'icône dans les barres d'état système Windows des utilisateurs correspondants. • Sélectionnez **Non** pour masquer l'icône.

PARAMÈTRE DE STRATÉGIE	DÉTAILS
Afficher les messages de notification	Il peut s'avérer inapproprié de présenter des notifications à certains utilisateurs. Par exemple, les utilisateurs d'endpoints à usage spécifique tels que des DAB, des dispositifs médicaux, des kiosques et des pompes à essence peuvent être perturbés par les notifications et les demandes d'interactions associées. • Sélectionnez **Oui** pour présenter les notifications d'Endpoint Application Control aux utilisateurs correspondants. • Sélectionnez **Non** pour bloquer la présentation des notifications et désactiver les interactions associées avec l'utilisateur. **Important** Une fois qu'Endpoint Application Control a bloqué ou retardé le démarrage d'une application en utilisant la méthode du blocage au niveau du noyau, Windows peut présenter la notification suivante aux utilisateurs finaux :  **FIGURE 23-1. Notification de blocage de Windows** Endpoint Application Control n'est pas en mesure de masquer cette notification. Vous pouvez éviter cette notification en appliquant le blocage au niveau de l'utilisateur.

Paramètre de stratégie	Détails
Générer un nouvel inventaire	Les endpoints génèrent des inventaires pour effectuer le suivi des applications nouvelles et supprimées. Endpoint Application Control recueille régulièrement les inventaires d'applications auprès des endpoints. Sélectionnez un intervalle de temps (par exemple, quotidien ou hebdomadaire).
Heure de début	Sélectionnez une heure de début pour le scan d'inventaire.

Partie IX

Widgets ScanMail for Microsoft Exchange

Chapitre 24

Configuration de la prévention contre la perte de données

Ce chapitre explique comment configurer la prévention contre la perte de données afin de protéger l'environnement Exchange.

Les rubriques sont les suivantes:

- *Configuration d'une stratégie de prévention contre la perte de données à la page 24-2*

Configuration d'une stratégie de prévention contre la perte de données

Les stratégies de prévention contre la perte de données régissent les actions entreprises par Control Manager lorsqu'il détecte des informations sensibles dans des messages électroniques.

Créez une nouvelle stratégie en cliquant sur **Prévention contre la perte de données** > **Stratégies DLP** > **Ajouter**.

Modifiez une stratégie existante en cliquant sur **Prévention contre la perte de données** > **Stratégies DLP** > **[nom de la stratégie DLP]**.

Configurez les stratégies de prévention contre la perte de données à l'aide du processus en cinq étapes ci-dessous :

1. *Sélection de comptes à la page 24-2*
2. *Configuration de cibles DLP à la page 24-4*
3. *Configuration d'actions DLP à la page 24-5*
4. *Configuration de notifications DLP à la page 24-6*
5. *Activation d'une stratégie DLP à la page 24-7*

Sélection de comptes

Procédure

1. Accédez à l'écran **Stratégies de prévention contre la perte de données** en accédant à **Prévention contre la perte de données** > **Stratégies DLP**.
2. Ajoutez ou modifiez une stratégie ou une exception :
   - Dans le cas de nouvelles stratégies ou exceptions :

     Cliquez sur **Ajouter**.
   - Dans le cas de stratégies ou exceptions pré-existantes :

a. Cliquez sur le nom de la stratégie ou de l'exception.

b. Cliquez sur l'onglet **Comptes**.

3. Sélectionnez les expéditeurs ou les destinataires associés au scan de stratégie.

- En cas de création d'une nouvelle stratégie :

  a. Sélectionnez le type de compte :

     - **Depuis n'importe quel expéditeur vers n'importe quel destinataire**.
     - **Depuis un ou des expéditeurs spécifiques vers n'importe quel destinataire**.
     - **Depuis n'importe quel expéditeur vers un ou des destinataires spécifiques**.
     - **Depuis un ou des expéditeurs spécifiques vers un ou des destinataires spécifiques** .

  b. Cliquez sur le lien **expéditeur(s) spécifique(s)** ou **destinataire(s) spécifique(s)** (le cas échéant).

- En cas de modification de stratégie :

  a. Sélectionnez le type de compte :

     - **Tout**
     - **Expéditeur(s) spécifique(s)**
     - **Destinataire(s) spécifique(s)**
     - **Expéditeur(s) et destinataire(s) spécifique(s)**

     Control Manager applique uniquement la stratégie aux comptes sélectionnés pour le type de **Comptes** indiqué. Si vous sélectionnez des comptes pour un autre type de comptes, Control Manager n'applique pas la stratégie aux précédents comptes sélectionnés.

  b. Cliquez sur le lien **Modifier** dans les tableaux afin de modifier les comptes inclus et les comptes exclus pour cette stratégie.

4. Choisissez l'une des options suivantes :

   - **Tout le monde** : permet d'appliquer cette stratégie ou exception à tous les utilisateurs.
   - **Comptes spécifiques** : sélectionnez des éléments dans les groupes Active Directory ou les groupes spéciaux Control Manager.

5. Recherchez et sélectionnez des utilisateurs AD/groupes/contacts/groupes spéciaux et ajoutez-les à la liste des comptes sélectionnés.

6. Recherchez et sélectionnez des utilisateurs AD/groupes/contacts/groupes spéciaux et ajoutez-les à la liste des comptes sélectionnés dans l'écran **Exclure des comptes**.

Configuration de cibles DLP

Procédure

1. Accédez à l'écran **Stratégies de prévention contre la perte de données** en accédant aux éléments suivants :

   - Pour les scans en temps réel : **Prévention contre la perte de données** > **Stratégies DLP**
   - Pour les scans manuels : **Scan manuel** > **Prévention contre la perte de données**
   - Pour les scans programmés : **Scan programmé** > **[Ajouter ou Modifier]** > **Prévention contre la perte de données**

2. Ajoutez ou modifiez une stratégie ou une exception :

   - Dans le cas de nouvelles stratégies ou exceptions :

     a. Cliquez sur **Ajouter**.

     b. Accédez à l'écran **Spécifier une règle**.

   - Dans le cas de stratégies ou exceptions pré-existantes :

a. Cliquez sur le nom de la stratégie ou de l'exception.

b. Cliquez sur l'onglet **Cible**.

3. Cochez la ou les cases correspondant à la ou aux zones cibles du message électronique à scanner.

   Les cibles disponibles sont les suivantes :

   - **En-tête** (**De**, **À** et **Cc**)
   - **Objet**
   - **Corps**
   - **Pièce jointe**

4. Sélectionnez des modèles dans la liste des modèles disponibles, puis cliquez sur **Ajouter >>** pour appliquer les modèles à la stratégie.

   Remarque

   Une stratégie de prévention contre la perte de données nécessite de sélectionner au moins un modèle avant de pouvoir être activée.

5. Dans la barre d'outils Modèle(s) DLP disponible(s), cliquez sur **Ajouter** pour créer un nouveau modèle ou sur **Importer** pour importer un fichier de modèle.

Configuration d'actions DLP

Procédure

1. Accédez à l'écran **Stratégies de prévention contre la perte de données** en accédant aux éléments suivants :

   - Pour les scans en temps réel : **Prévention contre la perte de données** > **Stratégies DLP**
   - Pour les scans manuels : **Scan manuel** > **Prévention contre la perte de données**

- Pour les scans programmés : **Scan programmé** > **[Ajouter ou Modifier]** > **Prévention contre la perte de données**

2. Ajoutez ou modifiez une stratégie ou une exception :
   - Dans le cas de nouvelles stratégies ou exceptions :
     a. Cliquez sur **Ajouter**.
     b. Accédez à l'écran **Spécifier une action**.
   - Dans le cas de stratégies ou exceptions pré-existantes :
     a. Cliquez sur le nom de la stratégie ou de l'exception.
     b. Cliquez sur l'onglet **Action**.
3. Sélectionnez une action que Control Manager devra entreprendre s'il détecte du contenu indésirable.
4. Pour envoyer des notifications à des personnes spécifiques :
   - Cochez la case **Transférer au supérieur de l'expéditeur**.
   - Cochez la case **Transférer vers des adresses électroniques spécifiques** et saisissez l'adresse électronique des destinataires.
5. Indiquez si des notifications doivent être envoyées lorsqu'une action est entreprise en sélectionnant **Notifier** ou **Ne pas notifier**.
6. Configurez les **Options avancées** selon les besoins.

Configuration de notifications DLP

Procédure

1. Accédez à l'écran **Stratégies de prévention contre la perte de données** en accédant aux éléments suivants :
   - Pour les scans en temps réel : **Prévention contre la perte de données** > **Stratégies DLP**

- Pour les scans manuels : **Scan manuel** > **Prévention contre la perte de données**
- Pour les scans programmés : **Scan programmé** > **[Ajouter ou Modifier]** > **Prévention contre la perte de données**

2. Ajoutez ou modifiez une stratégie ou une exception :
   - Dans le cas de nouvelles stratégies ou exceptions :
     a. Cliquez sur **Ajouter**.
     b. Accédez à l'écran **Spécifier une notification**.
   - Dans le cas de stratégies ou exceptions pré-existantes :
     a. Cliquez sur le nom de la stratégie ou de l'exception.
     b. Cliquez sur l'onglet **Notification**.
3. Cochez les cases correspondant aux personnes que Control Manager devra informer.
4. Cliquez sur **Afficher les détails** afin de personnaliser la notification pour ce destinataire.
5. Sélectionnez des options de notification.
6. Cliquez sur **Écrire dans le journal des événements Windows** pour que Control Manager inscrive la notification dans un journal des événements Windows.

Activation d'une stratégie DLP

Procédure

1. Accédez à l'écran **Stratégies de prévention contre la perte de données** en accédant aux éléments suivants :
   - Pour les scans en temps réel : **Prévention contre la perte de données** > **Stratégies DLP**

- Pour les scans manuels : **Scan manuel** > **Prévention contre la perte de données**
- Pour les scans programmés : **Scan programmé** > **[Ajouter ou Modifier]** > **Prévention contre la perte de données**

2. Ajoutez ou modifiez une stratégie avant l'activation :
   - Dans le cas de nouvelles stratégies :
     a. Cliquez sur **Ajouter**.
     b. Accédez à l'écran **Nom et priorité**.
   - Pour les stratégies déjà existantes :

     Cliquez sur le nom de la stratégie.
3. Sélectionnez l'élément pour activer la stratégie ou l'exception.
4. Saisissez le nom de votre stratégie dans la zone **Nom de la stratégie**.
5. Spécifiez la priorité.
   - Dans le cas de nouvelles stratégies :

     Saisissez la priorité de votre stratégie dans la zone **Priorité**.
   - Dans le cas de stratégies pré-existantes :
     a. Cochez la case en regard du nom de la stratégie ou de l'exception dans la liste.
     b. Cliquez sur **Réorganiser**.
     c. Saisissez la valeur de la priorité dans le champ **Priorité**.
     d. Cliquez sur **Enregistrer la réorganisation**.
6. Cliquez sur **Enregistrer**.

Partie X

Widgets Trend Micro Security (for Mac)

Chapitre 25

Widgets Trend Micro Security (for Mac)

Cette section contient des rubriques d'aide concernant tous les widgets Trend Micro Security (for Mac) qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget Indicateurs de performance de Security (for Mac) à la page 25-2*

Widget Indicateurs de performance de Security (for Mac)

Ce widget affiche les indicateurs de performance clés de Trend Micro Security (for Mac) en fonction des critères sélectionnés. Ce widget comprend des seuils d'événement et des modèles personnalisables.

Remarque

Par défaut, le widget attribue l'indicateur « Important » ( ) aux événements dont le nombre d'occurrences s'élève à 15 et l'indicateur « Critique » ( ) aux événements dont le nombre d'occurrences s'élève à 30. Si vous le souhaitez, vous pouvez marquer des événements comme importants ou critiques en personnalisant les seuils d'événement.

Configurez l'heure de mise à jour quotidienne en cliquant sur le menu déroulant et en sélectionnant l'heure de génération des données. Mettez à jour manuellement les données en cliquant sur l'icone Actualiser (>).

Modifiez les serveurs gérés utilisés en tant que sources par le widget en cliquant sur l'icône Paramètres (>). Dans la boîte de dialogue qui s'affiche, sélectionnez le ou les serveurs gérés à utiliser en tant que sources, puis cliquez sur **Enregistrer**.

Ajoutez un indicateur en cliquant sur **Ajouter un indicateur**. Dans la boîte de dialogue qui s'affiche, sélectionnez un **Nom** et spécifiez les paramètres facultatifs. Cliquez sur **Enregistrer** lorsque vous avez terminé.

Modifiez un indicateur en cliquant sur l'indicateur dans la liste. Dans la boîte de dialogue qui s'affiche, modifiez les paramètres. Cliquez sur **Enregistrer** lorsque vous avez terminé.

Supprimez et modifiez un indicateur en cliquant sur l'indicateur dans la liste. Dans la boîte de dialogue qui s'affiche, cliquez sur **Supprimer** puis sur **OK**.

Configurez les paramètres des seuils d'événement dans l'écran **Ajouter un indicateur** ou **Modifier un indicateur**.

Remarque

L'icône « Important » ou « Critique » s'affiche dans la colonne **Occurrences** si les deux conditions suivantes sont réunies :

- Le nombre d'occurrences d'un événement qui correspondent à cet indicateur est égal ou supérieur au seuil.
- L'option **Activer les alertes aux seuils suivants** est sélectionnée.

Chapitre 26

Paramètres de stratégie de Trend Micro Security (for Mac)

Cette section explique comment configurer les paramètres de stratégie de Trend Micro Security (for Mac) dans Control Manager.

Les rubriques sont les suivantes:

- *Types de méthode de scan à la page 26-2*
- *Types de scan à la page 26-8*
- *Paramètres de cache des scans à la page 26-31*
- *Exclusions de scan à la page 26-32*
- *Autoprotection de l'agent à la page 26-36*
- *Mises à jour des agents à la page 26-37*
- *Réputation de sites Web à la page 26-41*

Types de méthode de scan

Les agents Trend Micro Security (for Mac) peuvent utiliser l'une des deux méthodes de scan pour rechercher les risques de sécurité. Les méthodes de scan sont le Smart Scan et le scan traditionnel.

- **Smart scan**

  Les agents qui utilisent Smart Scan sont appelés « Agents Smart Scan » dans ce document. Les agents Smart Scan bénéficient des scans locaux et des requêtes en ligne effectuées par les services File Reputation.

  Il s'agit du type de méthode de scan par défaut.

- **Scan traditionnel**

  Les agents n'utilisant pas le Smart Scan sont appelés les « agents de scan traditionnel ». Un agent de scan traditionnel stocke tous les composants Trend Micro Security (for Mac) sur l'endpoint de l'agent et scanne tous les fichiers localement.

Comparaison entre les méthodes de scan

Le tableau suivant établit une comparaison entre les deux méthodes de scan :

TABLEAU 26-1. Comparaison entre Scan traditionnel et Smart Scan

BASE DE COMPARAISON	SCAN TRADITIONNEL	SMART SCAN
Comportement du scan	L'agent Scan traditionnel procède au scan sur l'endpoint local.	• L'agent Smart Scan procède au scan sur l'endpoint local. • Si l'agent ne peut pas déterminer le risque que présente le fichier durant le scan, l'agent vérifie le risque en envoyant une requête de scan à une source Smart Protection. • L'agent « met en mémoire cache » le résultat de la requête de scan pour améliorer les performances du scan.
Composants utilisés et mis à jour	Tous les composants disponibles sur la source de mise à jour, hormis le Smart Scan Agent Pattern.	Tous les composants disponibles sur la source de mise à jour, hormis le fichier de signatures de virus et le fichier de signatures de surveillance active des spywares.
Source de mise à jour par défaut	Serveur Trend Micro Security (for Mac)	Serveur Trend Micro Security (for Mac)

Modification de la méthode de scan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine ( ) afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Méthodes de scan**.
4. Sélectionnez **Scan traditionnel** ou **Smart Scan**.

5. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône racine, choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment où vous configurez les paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Basculement de Smart Scan vers le scan traditionnel

Le tableau suivant indique les autres éléments à prendre en compte lorsque vous faites passer les agents en mode de scan traditionnel.

TABLEAU 26-2. Éléments à prendre en compte lors du basculement vers le scan traditionnel

ÉLÉMENT	DÉTAILS
Nombre d'agents à basculer	Le fait de basculer simultanément un nombre relativement faible d'agents permet une utilisation optimale du serveur Trend Micro Security (for Mac) et des ressources Smart Protection Server. Ces serveurs peuvent effectuer d'autres tâches critiques lorsque les agents changent de méthode de scan.

Élément	Détails
Opportunité du moment	Lors du retour au mode de scan traditionnel, les agents téléchargeront probablement la version complète du fichier de signatures de virus et du fichier de signatures de surveillance active des spywares à partir du serveur Trend Micro Security (for Mac). Ces fichiers de signatures ne sont utilisés que par les agents de scan traditionnel. Pensez à effectuer le basculement pendant les heures creuses afin que le processus de téléchargement se fasse plus rapidement. Pensez également à effectuer le basculement lorsqu'aucun agent n'est programmé pour la mise à jour depuis le serveur.
Paramètres de l'arborescence des agents	La méthode de scan est un paramètre granulaire qui peut être configuré au niveau de la racine, du domaine ou de l'agent. Lors du basculement vers le mode de scan traditionnel, vous pouvez : • Créez un nouveau groupe et définissez le scan traditionnel comme méthode de scan. Tout agent que vous déplacez vers ce groupe utilisera le scan traditionnel. Lorsque vous déplacez l'agent, activez le paramètre **Appliquer les paramètres du nouveau groupe au(x) client(s) sélectionné(s)**. • Sélectionnez un groupe et configurez-le pour utiliser le scan traditionnel. Les agents smart scan appartenant au groupe basculeront vers le scan traditionnel. • Sélectionnez un ou plusieurs agents smart scan dans un groupe et faites-les basculer vers le scan traditionnel. **Remarque** Toutes les modifications apportées à la méthode de scan du groupe remplaceront la méthode de scan configurée pour les agents individuels.

Basculement du scan traditionnel vers Smart Scan

Si vous faites passer les agents du scan traditionnel à Smart Scan, assurez-vous d'avoir installé Smart Protection Services sur le serveur OfficeScan. Pour obtenir des informations détaillées, consultez la documentation relative à OfficeScan.

Le tableau suivant montre les autres éléments dont il faut tenir compte lorsque les agents passent en mode Smart Scan.

TABLEAU 26-3. Éléments à prendre en compte lors du passage en mode Smart Scan

ÉLÉMENT	DÉTAILS
Licence du produit	Pour utiliser Smart Scan, assurez-vous d'avoir activé les licences des services suivants sur le serveur OfficeScan et que les licences n'ont pas expiré : • Antivirus • Réputation de sites Web et Anti-spyware
Serveur Trend Micro Control Manager	Vérifiez que les agents peuvent se connecter au serveur Trend Micro Security (for Mac). Seuls les agents en ligne seront invités à basculer vers smart scan. Les agents hors ligne sont notifiés lorsqu'ils passent en mode en ligne. Les agents itinérants sont notifiés lorsqu'ils passent en mode en ligne ou, si l'agent dispose de privilèges de mise à jour programmée, lorsque la mise à jour programmée s'exécute.
Nombre d'agents à basculer	Le fait de basculer simultanément un nombre relativement faible d'agents permet une utilisation optimale des ressources du serveur Trend Micro Security (for Mac). Le serveur Trend Micro Security (for Mac) peut effectuer d'autres tâches critiques lorsque les agents changent de méthode de scan.

Élément	Détails
Opportunité du moment	Lors du premier basculement vers smart scan, les agents doivent télécharger la version complète de Smart Scan Agent Pattern à partir du serveur Trend Micro Security (for Mac). Le fichier Smart Scan Pattern n'est utilisé que par les agents smart scan. Pensez à effectuer le basculement pendant les heures creuses afin que le processus de téléchargement se fasse plus rapidement. Pensez également à effectuer le basculement lorsqu'aucun agent n'est programmé pour la mise à jour depuis le serveur.
Paramètres de l'arborescence des agents	La méthode de scan est un paramètre granulaire qui peut être défini au niveau racine, groupe ou individuel de l'agent. En passant en mode Smart Scan, vous pouvez : • Créer un groupe et lui attribuer Smart Scan comme méthode de scan. Tous les agents que vous déplacerez dans ce groupe utiliseront Smart Scan. Lorsque vous déplacez un agent, activez le paramètre **Appliquer les paramètres du nouveau groupe aux agents sélectionnés**. • Sélectionner un groupe et le configurer pour qu'il utilise Smart Scan. Les agents de scan traditionnel appartenant à ce groupe basculeront en mode Smart Scan. • Sélectionner un ou plusieurs agents de scan traditionnel d'un groupe et les basculer en mode Smart Scan. **Remarque** Toutes les modifications apportées à la méthode de scan du groupe remplaceront la méthode de scan configurée pour les agents individuels.

ÉLÉMENT	DÉTAILS
Prise en charge IPv6	Les agents Smart Scan envoient des requêtes de scan aux sources Smart Protection. Un agent Smart Scan IPv6 pur ne peut pas directement envoyer de requête à des sources IPv4 pures telles que : • Smart Protection Server 3.0 (intégré ou autonome) • Trend Micro Smart Protection Network De même, un agent Smart Scan IPv4 pur ne peut pas envoyer de requête à des serveurs Smart Protection Server IPv6. Un serveur proxy à double pile, tel que DeleGate, capable de convertir les adresses IP est requis pour la connexion des agents Smart Scan aux sources.

Types de scan

Trend Micro Security (for Mac) fournit les types de scan suivants afin de protéger les endpoints contre les risques de sécurité :

TYPE DE SCAN	DESCRIPTION
Scan en temps réel	Scanne automatiquement un fichier reçu, ouvert, téléchargé, copié ou modifié Consultez la section *Scan en temps réel à la page 26-9*.
Scan manuel	Lancé par l'utilisateur : scanne un fichier ou un ensemble de fichiers Consultez la section *Scan manuel à la page 26-16*.
Scan programmé	Scanne automatiquement les fichiers du Endpoint en fonction de la programmation configurée par l'administrateur Consultez la section *Scan programmé à la page 26-23*.
Scanner maintenant	Lancé par l'administrateur : scanne les fichiers sur un ou plusieurs Endpoints cible

Scan en temps réel

Le scan en temps réel s'effectue en continu. À chaque réception, ouverture, téléchargement, copie ou modification d'un fichier, le scan en temps réel scanne le fichier afin de détecter d'éventuels risques de sécurité. Si Control Manager ne détecte aucun risque de sécurité, le fichier demeure à son emplacement et les utilisateurs peuvent continuer à accéder au fichier. Si Control Manager détecte un risque de sécurité, il affiche un message de notification contenant le nom du fichier infecté et le risque spécifique lié à la sécurité.

Configurez et appliquez les paramètres de scan en temps réel à un ou à plusieurs agents et groupes, ou bien à tous les agents gérés par le serveur.

Configuration des paramètres de scan en temps réel

Procédure

1. Configurez les critères de scan suivants :
   - *Action des utilisateurs sur les fichiers à la page 26-9*
   - *Paramètres de scan à la page 26-10*
2. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés.

   Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 26-13*.

Action des utilisateurs sur les fichiers

Choisissez des actions sur les fichiers qui déclencheront le scan en temps réel. Sélectionnez l'une des options suivantes :

- **Scanner les fichiers en cours de création/modification** :Scanne les nouveaux fichiers présents sur le Endpoint (par exemple, après leur téléchargement) ou les fichiers en cours de modification

- **Scanner les fichiers en cours de récupération/d'exécution** :Scanne les fichiers lors de leur ouverture
- **Scanner les fichiers en cours de création/modification et de récupération/exécution**
- **Scanner les fichiers en cours de création/modification/exécution**

Par exemple, si la troisième option est sélectionnée, un nouveau fichier téléchargé sur le Endpoint sera scanné et ne sera pas déplacé si aucun risque de sécurité n'est détecté. Le fichier sera scanné lors de son ouverture ou, s'il a été modifié, avant l'enregistrement des modifications.

Paramètres de scan

Sélectionnez une ou plusieurs options parmi les suivantes :

- **Scanner les fichiers compressés** : permet à Trend Micro Security (pour Mac) de scanner des fichiers individuels dans les fichiers compressés. Trend Micro Security (pour Mac) prend en charge les types de compression suivants :

Extension	Type
.zip	Archive créée avec Pkzip
.rar	Archive créée avec RAR
.tar	Archive créée avec Tar
.arj	Archive compressée ARJ
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Fichiers compressés 16 bits
.bin	MacBinary
.cab	Fichier Microsoft Cabinet
Microsoft Compressed/MSCOMP	

Extension	Type
.eml; .mht	MIME
.td0	Format Teledisk
.bz2	Fichier compressé avec Unix BZ2 et Bzip
.uu	UUEncode
.ace	WinAce

- **Scanner les lecteurs réseau** : Scanne les lecteurs réseau ou les dossiers mappés à l'Endpoint.

Actions de scan

Spécifiez l'action effectuée par Trend Micro Security (pour Mac) lorsqu'un type de scan particulier détecte un risque de sécurité.

L'action que Trend Micro Security (pour Mac) effectue dépend du type de scan qui a détecté le risque de sécurité. Par exemple, lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan manuel (type de scan), il nettoie (action) le fichier infecté.

Les actions suivantes contre les risques de sécurité peuvent être effectuées par Trend Micro Security (pour Mac) :

Actions de scan	Détails
Supprimer	Trend Micro Security (pour Mac) supprime le fichier infecté du Endpoint.

ACTIONS DE SCAN	DÉTAILS
Quarantaine	Trend Micro Security (pour Mac) renomme, puis déplace le fichier infecté vers le répertoire de quarantaine de l'Endpoint situé sous `<Dossier d'installation de l'agent>/common/lib/vsapi/quarantine`. Une fois dans le répertoire de quarantaine, Trend Micro Security (pour Mac) peut effectuer une action supplémentaire sur le fichier en quarantaine, en fonction de l'action spécifiée par l'utilisateur. Trend Micro Security (pour Mac) peut supprimer, nettoyer ou restaurer le fichier. L'opération de restauration correspond au déplacement du fichier vers son emplacement d'origine sans effectuer d'action. Les utilisateurs peuvent restaurer le fichier s'il est réellement inoffensif. Le nettoyage correspond à la suppression du risque de sécurité du fichier en quarantaine, puis à son transfert vers son emplacement d'origine si le nettoyage est réussi.
Nettoyer	Trend Micro Security (pour Mac) supprime le risque de sécurité d'un fichier infecté avant d'autoriser les utilisateurs à y accéder. Si le fichier n'est pas nettoyable, Trend Micro Security (pour Mac) effectue une seconde action qui peut être l'une des actions suivantes : Quarantaine, Supprimer et Ignorer. Pour configurer la deuxième action, accédez à **Gestion des agents** > **Paramètres** > **{Type de scan}** et cliquez sur l'onglet **Action**.

Actions de scan	Détails
Ignorer	Trend Micro Security (pour Mac) n'effectue pas d'action sur le fichier infecté, mais consigne le risque de sécurité détecté dans les journaux. Le fichier reste à son emplacement. Trend Micro Security (pour Mac) « ignore » toujours les fichiers infectés de type virus/programmes malveillants potentiels, afin de réduire le risque de faux positifs. Si une analyse plus poussée confirme que le virus/programme malveillant potentiel constitue effectivement un risque de sécurité, un nouveau fichier de signatures est publié pour permettre à Trend Micro Security (pour Mac) d'entreprendre l'action de scan appropriée. S'il se révèle inoffensif, le virus/programme malveillant potentiel ne sera plus détecté. Par exemple, Trend Micro Security (pour Mac) détecte « virus_potentiel_x » sur un fichier nommé « 123.pdf » et n'entreprend aucune action au moment de la détection. Trend Micro confirme ensuite que « virus_potentiel_x » est un cheval de Troie et publie une nouvelle version du fichier de signatures. Après le chargement du nouveau fichier de signatures, Trend Micro Security (pour Mac) détectera « virus_potentiel_x » en tant que cheval de Troie et, si l'action contre un tel programme est « Supprimer », supprimera « 123.pdf ».

Options d'action de scan et paramètres supplémentaires

Lors de la configuration de l'action de scan, sélectionnez l'une des options suivantes :

Option	Détails
Utiliser ActiveAction	ActiveAction est un ensemble d'actions de scan préconfigurées pour différents types de risques de sécurité. Si vous ignorez quelle action est la mieux adaptée à un type de risque de sécurité, l'utilisation de l'outil ActiveAction est recommandée. Les paramètres ActiveAction sont constamment mis à jour dans les fichiers de signatures pour protéger les Endpoints contre les risques de sécurité et les méthodes d'attaques les plus récents.

OPTION	DÉTAILS
Utiliser la même action pour tous les types de risques de sécurité	Sélectionnez cette option si vous voulez que la même action soit effectuée sur tous les types de risques de sécurité, sauf les virus/programmes malveillants potentiels. Pour les virus/programmes malveillants potentiels, l'action est toujours « Ignorer ». Si vous choisissez « Nettoyer » comme première action, sélectionnez une seconde action que Trend Micro Security (pour Mac) effectue en cas d'échec du nettoyage. Si la première action n'est pas « Nettoyer », aucune seconde action n'est configurable. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Actions de scan à la page 26-11*.

Paramètres supplémentaires de scan en temps réel

PARAMÈTRE	DÉTAILS
Afficher une notification lorsqu'un risque de sécurité est détecté	Lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan en temps réel, il peut afficher un message de notification informant l'utilisateur de la détection.

Privilèges du scan programmé

Si un scan programmé est activé sur le Endpoint, les utilisateurs peuvent reporter et ignorer/arrêter le scan programmé.

Privilège	Détails
Différer le scan programmé	Les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes : • Différer le scan programmé avant son exécution, puis indiquer la durée du report. Un scan programmé ne peut être différé qu'une seule fois. • Si un scan programmé est en cours, les utilisateurs peuvent arrêter le scan et le redémarrer ultérieurement. Les utilisateurs peuvent alors indiquer la durée d'attente avant le redémarrage du scan. Lorsque le scan redémarre, tous les fichiers précédemment scannés sont à nouveau scannés. Un scan programmé ne peut être arrêté et redémarré qu'une seule fois. Configurer le nombre d'heures et de minutes, ce qui correspond à : • La durée maximale de report • La durée d'attente maximale avant le redémarrage du scan
Ignorer ou arrêter le scan programmé	Ce privilège permet aux utilisateurs d'effectuer les actions suivantes : • Ignorer le scan programmé, avant son exécution • Arrêter le scan programmé, lorsqu'il est en cours

Paramètres supplémentaires de scan programmé

Paramètre	Détails
Afficher une notification avant l'exécution du scan programmé	Lorsque vous activez cette option, un message de notification s'affiche sur le Endpoint quelques minutes avant l'exécution du scan programmé. Les utilisateurs sont informés de la programmation du scan (date et heure) et des privilèges de scan programmé dont ils disposent, tels que reporter, ignorer ou arrêter un scan programmé. Configurez le moment de l'affichage du message de notification, en minutes.

PARAMÈTRE	DÉTAILS
Arrêter automatiquement le scan programmé lorsque celui-ci dure plus de __ heures et __ minutes	L'agent arrête le scan lorsque la durée indiquée s'est écoulée, même si le scan n'est pas terminé. L'agent avertit immédiatement les utilisateurs de tout risque de sécurité détecté lors du scan.

Scan manuel

Le scan manuel est un scan à la demande qui démarre immédiatement après avoir été lancé dans la console de l'agent. Sa durée dépend du nombre de fichiers à scanner et des ressources matérielles du Endpoint.

Configurez et appliquez les paramètres de scan manuel à un ou plusieurs agents et groupes, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan manuel

Procédure

1. Configurez les critères de scan suivants :
   - *Paramètres de scan à la page 26-16*
   - *Utilisation du processeur à la page 26-18*
2. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés.

   Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 26-13*.

Paramètres de scan

Sélectionnez une ou plusieurs options parmi les suivantes :

- **Scanner les fichiers compressés** : permet à Trend Micro Security (pour Mac) de scanner des fichiers individuels dans les fichiers compressés. Trend Micro Security (pour Mac) prend en charge les types de compression suivants :

Extension	Type
.zip	Archive créée avec Pkzip
.rar	Archive créée avec RAR
.tar	Archive créée avec Tar
.arj	Archive compressée ARJ
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Fichiers compressés 16 bits
.bin	MacBinary
.cab	Fichier Microsoft Cabinet
Microsoft Compressed/MSCOMP	
.eml; .mht	MIME
.td0	Format Teledisk
.bz2	Fichier compressé avec Unix BZ2 et Bzip
.uu	UUEncode
.ace	WinAce

- **Scanner Time Machine** : permet à Trend Micro Security (pour Mac) de détecter et de scanner les lecteurs Time Machine.

Remarque

Après avoir activer l'option **Scanner Time Machine** pour les scans manuels et programmés, Trend Micro Security (pour Mac) peut détecter les menaces malveillantes, mais ne peut prendre aucune mesure (nettoyage, mise en quarantaine ou suppression) à cause d'une limitation liée aux autorisations sur Mac OS. Toutes les actions de scan configurées sont affichées comme ayant échoué dans les journaux du produit.

- **Scanner les lecteurs réseau** : Scanne les lecteurs réseau ou les dossiers mappés à l'Endpoint.

Utilisation du processeur

Trend Micro Security (pour Mac) peut s'interrompre entre chaque fichier scanné. Ce paramètre est utilisé lors du scan manuel, du scan programmé et du scan immédiat.

Sélectionnez l'une des options suivantes :

- **Élevé** :Aucune interruption entre les fichiers lors des scans
- **Faible** :Interruption entre les fichiers lors des scans

Actions de scan

Spécifiez l'action effectuée par Trend Micro Security (pour Mac) lorsqu'un type de scan particulier détecte un risque de sécurité.

L'action que Trend Micro Security (pour Mac) effectue dépend du type de scan qui a détecté le risque de sécurité. Par exemple, lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan manuel (type de scan), il nettoie (action) le fichier infecté.

Les actions suivantes contre les risques de sécurité peuvent être effectuées par Trend Micro Security (pour Mac) :

Actions de scan	Détails
Supprimer	Trend Micro Security (pour Mac) supprime le fichier infecté du Endpoint.
Quarantaine	Trend Micro Security (pour Mac) renomme, puis déplace le fichier infecté vers le répertoire de quarantaine de l'Endpoint situé sous `<Dossier d'installation de l'agent>/common/lib/vsapi/quarantine`. Une fois dans le répertoire de quarantaine, Trend Micro Security (pour Mac) peut effectuer une action supplémentaire sur le fichier en quarantaine, en fonction de l'action spécifiée par l'utilisateur. Trend Micro Security (pour Mac) peut supprimer, nettoyer ou restaurer le fichier. L'opération de restauration correspond au déplacement du fichier vers son emplacement d'origine sans effectuer d'action. Les utilisateurs peuvent restaurer le fichier s'il est réellement inoffensif. Le nettoyage correspond à la suppression du risque de sécurité du fichier en quarantaine, puis à son transfert vers son emplacement d'origine si le nettoyage est réussi.
Nettoyer	Trend Micro Security (pour Mac) supprime le risque de sécurité d'un fichier infecté avant d'autoriser les utilisateurs à y accéder. Si le fichier n'est pas nettoyable, Trend Micro Security (pour Mac) effectue une seconde action qui peut être l'une des actions suivantes : Quarantaine, Supprimer et Ignorer. Pour configurer la deuxième action, accédez à **Gestion des agents** > **Paramètres** > **{Type de scan}** et cliquez sur l'onglet **Action**.

ACTIONS DE SCAN	DÉTAILS
Ignorer	Trend Micro Security (pour Mac) n'effectue pas d'action sur le fichier infecté, mais consigne le risque de sécurité détecté dans les journaux. Le fichier reste à son emplacement. Trend Micro Security (pour Mac) « ignore » toujours les fichiers infectés de type virus/programmes malveillants potentiels, afin de réduire le risque de faux positifs. Si une analyse plus poussée confirme que le virus/programme malveillant potentiel constitue effectivement un risque de sécurité, un nouveau fichier de signatures est publié pour permettre à Trend Micro Security (pour Mac) d'entreprendre l'action de scan appropriée. S'il se révèle inoffensif, le virus/programme malveillant potentiel ne sera plus détecté. Par exemple, Trend Micro Security (pour Mac) détecte « virus_potentiel_x » sur un fichier nommé « 123.pdf » et n'entreprend aucune action au moment de la détection. Trend Micro confirme ensuite que « virus_potentiel_x » est un cheval de Troie et publie une nouvelle version du fichier de signatures. Après le chargement du nouveau fichier de signatures, Trend Micro Security (pour Mac) détectera « virus_potentiel_x » en tant que cheval de Troie et, si l'action contre un tel programme est « Supprimer », supprimera « 123.pdf ».

Options d'action de scan et paramètres supplémentaires

Lors de la configuration de l'action de scan, sélectionnez l'une des options suivantes :

OPTION	DÉTAILS
Utiliser ActiveAction	ActiveAction est un ensemble d'actions de scan préconfigurées pour différents types de risques de sécurité. Si vous ignorez quelle action est la mieux adaptée à un type de risque de sécurité, l'utilisation de l'outil ActiveAction est recommandée. Les paramètres ActiveAction sont constamment mis à jour dans les fichiers de signatures pour protéger les Endpoints contre les risques de sécurité et les méthodes d'attaques les plus récents.

Option	Détails
Utiliser la même action pour tous les types de risques de sécurité	Sélectionnez cette option si vous voulez que la même action soit effectuée sur tous les types de risques de sécurité, sauf les virus/programmes malveillants potentiels. Pour les virus/programmes malveillants potentiels, l'action est toujours « Ignorer ». Si vous choisissez « Nettoyer » comme première action, sélectionnez une seconde action que Trend Micro Security (pour Mac) effectue en cas d'échec du nettoyage. Si la première action n'est pas « Nettoyer », aucune seconde action n'est configurable. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Actions de scan à la page 26-11*.

Paramètres supplémentaires de scan en temps réel

Paramètre	Détails
Afficher une notification lorsqu'un risque de sécurité est détecté	Lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan en temps réel, il peut afficher un message de notification informant l'utilisateur de la détection.

Privilèges du scan programmé

Si un scan programmé est activé sur le Endpoint, les utilisateurs peuvent reporter et ignorer/arrêter le scan programmé.

Privilège	Détails
Différer le scan programmé	Les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes : • Différer le scan programmé avant son exécution, puis indiquer la durée du report. Un scan programmé ne peut être différé qu'une seule fois. • Si un scan programmé est en cours, les utilisateurs peuvent arrêter le scan et le redémarrer ultérieurement. Les utilisateurs peuvent alors indiquer la durée d'attente avant le redémarrage du scan. Lorsque le scan redémarre, tous les fichiers précédemment scannés sont à nouveau scannés. Un scan programmé ne peut être arrêté et redémarré qu'une seule fois. Configurer le nombre d'heures et de minutes, ce qui correspond à : • La durée maximale de report • La durée d'attente maximale avant le redémarrage du scan
Ignorer ou arrêter le scan programmé	Ce privilège permet aux utilisateurs d'effectuer les actions suivantes : • Ignorer le scan programmé, avant son exécution • Arrêter le scan programmé, lorsqu'il est en cours

Paramètres supplémentaires de scan programmé

Paramètre	Détails
Afficher une notification avant l'exécution du scan programmé	Lorsque vous activez cette option, un message de notification s'affiche sur le Endpoint quelques minutes avant l'exécution du scan programmé. Les utilisateurs sont informés de la programmation du scan (date et heure) et des privilèges de scan programmé dont ils disposent, tels que reporter, ignorer ou arrêter un scan programmé. Configurez le moment de l'affichage du message de notification, en minutes.

PARAMÈTRE	DÉTAILS
Arrêter automatiquement le scan programmé lorsque celui-ci dure plus de __ heures et __ minutes	L'agent arrête le scan lorsque la durée indiquée s'est écoulée, même si le scan n'est pas terminé. L'agent avertit immédiatement les utilisateurs de tout risque de sécurité détecté lors du scan.

Scan programmé

Le scan programmé démarre automatiquement aux date et heure programmées. Il permet d'automatiser les scans de routine sur l'agent et d'améliorer l'efficacité de votre gestion des scans.

Configurez et appliquez les paramètres de scan programmé à un ou plusieurs clients agents et groupes, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan programmé

Procédure

1. Cochez la case pour activer le scan programmé.
2. Configurez les critères de scan suivants :
   - *Programmation à la page 26-24*
   - *Cible du scan à la page 26-24*
   - *Paramètres de scan à la page 26-25*
   - *Utilisation du processeur à la page 26-18*
3. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés.

   Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 26-13*.

Programmation

Configurez la fréquence (quotidienne, hebdomadaire ou mensuelle) ainsi que l'heure d'exécution du scan programmé.

Si vous avez sélectionné le 29, le 30 ou le 31 pour les scans programmés mensuels, Trend Micro Security (pour Mac) exécute le scan programmé le dernier jour du mois lorsque le mois est plus court.

Cible du scan

Sélectionnez l'une des options suivantes :

- **Tous les fichiers scannables** : Scanne tous les fichiers
- **Types de fichier scannés par IntelliScan** : Scanne uniquement les fichiers susceptibles de contenir du code malveillant, y compris ceux dissimulés sous une extension inoffensive.
- **Nom du fichier ou du dossier accompagné du chemin complet** : Scanne uniquement le ou les fichiers se trouvant dans un dossier spécifique.

    1. Saisissez un chemin d'accès complet à un fichier ou à un répertoire, puis cliquez sur **Ajouter**.

        - Exemple de chemin d'accès complet à un fichier : `/Users/username/temp.zip`
        - Exemple de chemin d'accès à un répertoire : `/Users/username`

    2. Pour supprimer un chemin d'accès complet à un fichier ou à un répertoire, sélectionnez-le, puis cliquez sur **Supprimer**.

IntelliScan

IntelliScan est une méthode d'identification des fichiers à scanner. Pour les fichiers exécutables (par exemple, `.exe`), le véritable type du fichier est déterminé en fonction de son contenu. Pour les fichiers non exécutables (au format `.txt` par exemple), le véritable type du fichier est déterminé en fonction de son en-tête.

IntelliScan offre les avantages suivants :

- Optimisation des performances : IntelliScan n'affecte pas les applications du Endpoint car il exploite au minimum les ressources système de l'ordinateur.
- Durée de scan réduite : comme IntelliScan est capable d'identifier le type réel des fichiers, il ne scanne que les fichiers réellement vulnérables aux infections. La durée du scan s'en trouve considérablement réduite, puisque tous les fichiers ne sont pas concernés.

Paramètres de scan

Sélectionnez une ou plusieurs options parmi les suivantes :

- **Scanner les fichiers compressés** : permet à Trend Micro Security (pour Mac) de scanner des fichiers individuels dans les fichiers compressés. Trend Micro Security (pour Mac) prend en charge les types de compression suivants :

Extension	Type
.zip	Archive créée avec Pkzip
.rar	Archive créée avec RAR
.tar	Archive créée avec Tar
.arj	Archive compressée ARJ
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Fichiers compressés 16 bits
.bin	MacBinary
.cab	Fichier Microsoft Cabinet
Microsoft Compressed/MSCOMP	
.eml; .mht	MIME
.td0	Format Teledisk
.bz2	Fichier compressé avec Unix BZ2 et Bzip

Extension	Type
.uu	UUEncode
.ace	WinAce

- **Scanner Time Machine** : permet à Trend Micro Security (pour Mac) de détecter et de scanner les lecteurs Time Machine.

  Remarque

  Après avoir activer l'option **Scanner Time Machine** pour les scans manuels et programmés, Trend Micro Security (pour Mac) peut détecter les menaces malveillantes, mais ne peut prendre aucune mesure (nettoyage, mise en quarantaine ou suppression) à cause d'une limitation liée aux autorisations sur Mac OS. Toutes les actions de scan configurées sont affichées comme ayant échoué dans les journaux du produit.

- **Ignorer le scan programmé lorsque la durée de la batterie d'un Endpoint est inférieure à __ % et que son adaptateur secteur est débranché** : Trend Micro Security (pour Mac) ignore le scan programmé s'il détecte que la durée de la batterie d'un Endpoint est faible et que l'adaptateur secteur n'est pas branché. Si la durée de la batterie est faible, mais que l'adaptateur secteur est branché, le scan est effectué. Si un scan est en cours lorsque la durée de la batterie devient faible, il n'est pas terminé.

Utilisation du processeur

Trend Micro Security (pour Mac) peut s'interrompre entre chaque fichier scanné. Ce paramètre est utilisé lors du scan manuel, du scan programmé et du scan immédiat.

Sélectionnez l'une des options suivantes :

- **Élevé** :Aucune interruption entre les fichiers lors des scans
- **Faible** :Interruption entre les fichiers lors des scans

Actions de scan

Spécifiez l'action effectuée par Trend Micro Security (pour Mac) lorsqu'un type de scan particulier détecte un risque de sécurité.

L'action que Trend Micro Security (pour Mac) effectue dépend du type de scan qui a détecté le risque de sécurité. Par exemple, lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan manuel (type de scan), il nettoie (action) le fichier infecté.

Les actions suivantes contre les risques de sécurité peuvent être effectuées par Trend Micro Security (pour Mac) :

ACTIONS DE SCAN	DÉTAILS
Supprimer	Trend Micro Security (pour Mac) supprime le fichier infecté du Endpoint.
Quarantaine	Trend Micro Security (pour Mac) renomme, puis déplace le fichier infecté vers le répertoire de quarantaine de l'Endpoint situé sous `<Dossier d'installation de l'agent>/common/lib/vsapi/quarantine`. Une fois dans le répertoire de quarantaine, Trend Micro Security (pour Mac) peut effectuer une action supplémentaire sur le fichier en quarantaine, en fonction de l'action spécifiée par l'utilisateur. Trend Micro Security (pour Mac) peut supprimer, nettoyer ou restaurer le fichier. L'opération de restauration correspond au déplacement du fichier vers son emplacement d'origine sans effectuer d'action. Les utilisateurs peuvent restaurer le fichier s'il est réellement inoffensif. Le nettoyage correspond à la suppression du risque de sécurité du fichier en quarantaine, puis à son transfert vers son emplacement d'origine si le nettoyage est réussi.
Nettoyer	Trend Micro Security (pour Mac) supprime le risque de sécurité d'un fichier infecté avant d'autoriser les utilisateurs à y accéder. Si le fichier n'est pas nettoyable, Trend Micro Security (pour Mac) effectue une seconde action qui peut être l'une des actions suivantes : Quarantaine, Supprimer et Ignorer. Pour configurer la deuxième action, accédez à **Gestion des agents** > **Paramètres** > **{Type de scan}** et cliquez sur l'onglet **Action**.

Actions de scan	Détails
Ignorer	Trend Micro Security (pour Mac) n'effectue pas d'action sur le fichier infecté, mais consigne le risque de sécurité détecté dans les journaux. Le fichier reste à son emplacement. Trend Micro Security (pour Mac) « ignore » toujours les fichiers infectés de type virus/programmes malveillants potentiels, afin de réduire le risque de faux positifs. Si une analyse plus poussée confirme que le virus/programme malveillant potentiel constitue effectivement un risque de sécurité, un nouveau fichier de signatures est publié pour permettre à Trend Micro Security (pour Mac) d'entreprendre l'action de scan appropriée. S'il se révèle inoffensif, le virus/programme malveillant potentiel ne sera plus détecté. Par exemple, Trend Micro Security (pour Mac) détecte « virus_potentiel_x » sur un fichier nommé « 123.pdf » et n'entreprend aucune action au moment de la détection. Trend Micro confirme ensuite que « virus_potentiel_x » est un cheval de Troie et publie une nouvelle version du fichier de signatures. Après le chargement du nouveau fichier de signatures, Trend Micro Security (pour Mac) détectera « virus_potentiel_x » en tant que cheval de Troie et, si l'action contre un tel programme est « Supprimer », supprimera « 123.pdf ».

Options d'action de scan et paramètres supplémentaires

Lors de la configuration de l'action de scan, sélectionnez l'une des options suivantes :

Option	Détails
Utiliser ActiveAction	ActiveAction est un ensemble d'actions de scan préconfigurées pour différents types de risques de sécurité. Si vous ignorez quelle action est la mieux adaptée à un type de risque de sécurité, l'utilisation de l'outil ActiveAction est recommandée. Les paramètres ActiveAction sont constamment mis à jour dans les fichiers de signatures pour protéger les Endpoints contre les risques de sécurité et les méthodes d'attaques les plus récents.

Option	Détails
Utiliser la même action pour tous les types de risques de sécurité	Sélectionnez cette option si vous voulez que la même action soit effectuée sur tous les types de risques de sécurité, sauf les virus/programmes malveillants potentiels. Pour les virus/programmes malveillants potentiels, l'action est toujours « Ignorer ». Si vous choisissez « Nettoyer » comme première action, sélectionnez une seconde action que Trend Micro Security (pour Mac) effectue en cas d'échec du nettoyage. Si la première action n'est pas « Nettoyer », aucune seconde action n'est configurable. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Actions de scan à la page 26-11*.

Paramètres supplémentaires de scan en temps réel

Paramètre	Détails
Afficher une notification lorsqu'un risque de sécurité est détecté	Lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan en temps réel, il peut afficher un message de notification informant l'utilisateur de la détection.

Privilèges du scan programmé

Si un scan programmé est activé sur le Endpoint, les utilisateurs peuvent reporter et ignorer/arrêter le scan programmé.

Privilège	Détails
Différer le scan programmé	Les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes : • Différer le scan programmé avant son exécution, puis indiquer la durée du report. Un scan programmé ne peut être différé qu'une seule fois. • Si un scan programmé est en cours, les utilisateurs peuvent arrêter le scan et le redémarrer ultérieurement. Les utilisateurs peuvent alors indiquer la durée d'attente avant le redémarrage du scan. Lorsque le scan redémarre, tous les fichiers précédemment scannés sont à nouveau scannés. Un scan programmé ne peut être arrêté et redémarré qu'une seule fois. Configurer le nombre d'heures et de minutes, ce qui correspond à : • La durée maximale de report • La durée d'attente maximale avant le redémarrage du scan
Ignorer ou arrêter le scan programmé	Ce privilège permet aux utilisateurs d'effectuer les actions suivantes : • Ignorer le scan programmé, avant son exécution • Arrêter le scan programmé, lorsqu'il est en cours

Paramètres supplémentaires de scan programmé

Paramètre	Détails
Afficher une notification avant l'exécution du scan programmé	Lorsque vous activez cette option, un message de notification s'affiche sur le Endpoint quelques minutes avant l'exécution du scan programmé. Les utilisateurs sont informés de la programmation du scan (date et heure) et des privilèges de scan programmé dont ils disposent, tels que reporter, ignorer ou arrêter un scan programmé. Configurez le moment de l'affichage du message de notification, en minutes.

PARAMÈTRE	DÉTAILS
Arrêter automatiquement le scan programmé lorsque celui-ci dure plus de __ heures et __ minutes	L'agent arrête le scan lorsque la durée indiquée s'est écoulée, même si le scan n'est pas terminé. L'agent avertit immédiatement les utilisateurs de tout risque de sécurité détecté lors du scan.

Paramètres de cache des scans

À chaque scan, l'agent contrôle le cache des fichiers modifiés pour vérifier si un fichier a été modifié depuis le dernier démarrage de l'agent.

- Si un fichier a été modifié, l'agent le scanne et l'ajoute au cache des fichiers scannés.
- Si aucune modification n'a été apportée à un fichier, l'agent vérifie si le fichier fait partie du cache des fichiers scannés.
  - Si tel est le cas, l'agent ne scanne pas le fichier en question.
  - Dans le cas contraire, l'agent vérifie le cache des fichiers approuvés.

Remarque

Le cache des fichiers approuvés contient les fichiers qui sont considérés comme fiables par Trend Micro Security (for Mac). Un fichier fiable est un fichier ayant été scanné successivement à l'aide de plusieurs versions du fichier de signatures et pour qui chaque scan a donné un résultat positif (aucune menace), ou un fichier ne présentant aucune menace n'ayant pas été modifié pendant une longue période.

  - Si le fichier se trouve dans le cache des fichiers approuvés, l'agent ne scanne pas le fichier en question.
  - Dans le cas contraire, l'agent scanne le fichier en question et l'ajoute au cache des fichiers scannés.

L'ensemble ou une partie des caches sont effacés à chaque mise à jour du fichier de signatures ou du moteur de scan.

Si l'exécution de scans est fréquente et que beaucoup de fichiers sont présents dans les caches, la durée de scan est réduite de façon significative.

Si l'exécution de scans est peu fréquente, désactivez les caches afin que chaque fichier soit contrôlé à la recherche de menaces à chaque scan.

Exclusions de scan

Configurez les exclusions de scan afin d'accroître les performances du scan et d'ignorer les fichiers inoffensifs.. Lorsqu'un type de scan spécifique s'exécute, Trend Micro Security (pour Mac) vérifie la liste d'exclusion de scan pour déterminer les fichiers du Endpoint qui seront exclus du scan.

LISTE DES EXCLUSIONS DE SCAN	DÉTAILS
Fichiers	Trend Micro Security (pour Mac) ne scanne pas un fichier si : • Ce fichier se trouve dans le répertoire indiqué dans la liste des exclusions de scan • Ce fichier correspond au chemin de fichier complet (chemin du répertoire et nom du fichier) indiqué dans la liste des exclusions de scan
Extensions de fichiers	Trend Micro Security (pour Mac) ne scanne pas un fichier dont l'extension correspond à l'une des extensions incluses dans la liste des exclusions.

Configuration des listes d'exclusion de scan

Pour obtenir des informations détaillées sur les listes des exclusions de scan, consultez la rubrique *Exclusions de scan à la page 26-32*.

Procédure

1. Cochez la case pour activer l'exclusion de scan.

2. Pour configurer la **Liste des exclusions de scan (fichiers)** :

   a. Saisissez un chemin d'accès complet à un fichier ou à un répertoire et cliquez sur **Ajouter**.

   Rappels :

   - Il est impossible de saisir uniquement un nom de fichier.
   - Vous pouvez définir au maximum 64 chemins. Reportez-vous au tableau ci-dessous pour obtenir des exemples.

CHEMIN	DÉTAILS	EXEMPLES
Chemin d'accès complet au fichier	Exclut un fichier spécifique sur le Endpoint	• Exemple 1 : `/file.log` • Exemple 2 : `/System/file.log`

CHEMIN	DÉTAILS	EXEMPLES

Chemin d'accès à un répertoire	Exclut tous les fichiers situés dans un dossier spécifique ainsi que tous ses sous-dossiers	• Exemple 1 :
		`/System/`
		Exemples de fichiers exclus des scans :
		• `/System/file.log`
		• `/System/Library/file.log`
		Exemples de fichiers inclus dans les scans :
		• `/Applications/file.log`
		• Exemple 2 :
		`/System/Library`
		Exemples de fichiers exclus des scans :
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		Exemples de fichiers inclus dans les scans :
		• `/System/file.log`

- Utilisez un astérisque (*) au lieu des noms de dossiers.

  Reportez-vous au tableau ci-dessous pour obtenir des exemples.

CHEMIN	EXEMPLES D'UTILISATION DE CARACTÈRES GÉNÉRIQUES
Chemin d'accès complet au fichier	`/Users/Mac/*/file.log` Exemples de fichiers exclus des scans : • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Exemples de fichiers inclus dans les scans : • `/Users/file.log` • `/Users/Mac/file.log`

Chemin d'accès à un répertoire	• Exemple 1 :
	`/Users/Mac/*`
	Exemples de fichiers exclus des scans :
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Exemples de fichiers inclus dans les scans :
	• `/Users/doc.html`
	• Exemple 2 :
	`/*/Components`
	Exemples de fichiers exclus des scans :
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Exemples de fichiers inclus dans les scans :
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Les correspondances partielles des noms de fichiers ne sont pas prises en charge. Par exemple, il est impossible de saisir `/Users/*user/temp` afin d'exclure les fichiers se trouvant dans des dossiers dont les noms se terminent par « user », tels que « end_user » ou « new_user ».

b. Pour supprimer un chemin, sélectionnez-le, puis cliquez sur **Supprimer**.

3. Pour configurer la **Liste des exclusions de scan (extensions de fichier)** :

a. Saisissez une extension de fichier, sans point (.), et cliquez sur **Ajouter**. Par exemple, saisissez `pdf`. Vous pouvez définir au maximum 64 extensions de fichiers.

b. Pour supprimer une extension de fichier, sélectionnez-la, puis cliquez sur **Supprimer**.

Autoprotection de l'agent

La fonctionnalité d'autoprotection de l'agent Trend Micro Security (pour Mac) empêche d'autres programmes et même l'utilisateur de modifier ou de supprimer les fichiers utilisés par l'agent Trend Micro Security (pour Mac).

Lorsque vous activez l'option **Protéger les fichiers utilisés par l'agent** et que l'agent Trend Micro Security (pour Mac) est en cours d'exécution sur un Endpoint, Trend Micro Security (pour Mac) verrouille les fichiers et les dossiers suivants :

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*

- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

Remarque

Trend Micro Security (pour Mac) autorise l'ajout de fichiers au dossier `/Library/Application Support/TrendMicro/Tools`, mais les fichiers qui s'y trouvent ne peuvent pas en être supprimés.

Mises à jour des agents

Pour garantir le maintien de la protection des agents contre les risques de sécurité les plus récents, procédez à une mise à jour régulière des composants des agents, notamment lorsque les agents possèdent des composants particulièrement obsolètes, ainsi qu'à l'occasion d'une épidémie. Les composants deviennent particulièrement obsolètes lorsque l'agent ne parvient pas à les mettre à jour à partir du serveur Trend Micro Security (pour Mac) ou ActiveUpdate pendant une période prolongée.

Méthodes de mise à jour des agents

Il existe plusieurs méthodes de mise à jour des agents.

MÉTHODE DE MISE À JOUR	DESCRIPTION
Mise à jour manuelle lancée par un administrateur	Lancez une mise à jour à partie de l'un des écrans de la console Web suivants : • écran Gestion des agents. • écran Résumé.

MÉTHODE DE MISE À JOUR	DESCRIPTION
Mise à jour automatique	• Une fois que le serveur a terminé une mise à jour, il notifie immédiatement les agents afin que ceux-ci procèdent également à la mise à jour. • Les mises à jour peuvent être effectuées selon une programmation configurée par vos soins. Vous pouvez configurer et appliquer une programmation concernant un ou plusieurs agents et domaines, ou bien tous les agents gérés par le serveur. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de mise à jour des agents à la page 26-40*.
Mise à jour manuelle lancée par un utilisateur	Les utilisateurs lancent la mise à jour à partir de leurs Endpoints.

Source de mise à jour des agents

Par défaut, les agents téléchargent les composants à partir du serveur Trend Micro Security (pour Mac). Outre ces composants, les agents de Trend Micro Security (pour Mac) reçoivent également des fichiers de configuration mis à jour lors d'une mise à jour depuis le serveur Trend Micro Security (pour Mac). qui leur permettent d'appliquer de nouveaux paramètres. À chaque fois que vous modifiez les paramètres Trend Micro Security (pour Mac) sur la console Web, les fichiers de configuration sont modifiés.

Avant de mettre à jour les agents, vérifiez si le serveur Trend Micro Security (pour Mac) dispose des composants les plus récents.

Configurez un agent, plusieurs d'entre eux ou l'ensemble des agents afin qu'ils effectuent des téléchargements à partir du serveur ActiveUpdate de Trend Micro lorsque le serveur Trend Micro Security (pour Mac) est indisponible.

Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de mise à jour des agents à la page 26-40*.

Remarque

Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives à la mise à jour des agents liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page 26-39*.

Remarques et rappels relatifs à la mise à jour des agents

- Les agents Trend Micro Security (pour Mac) peuvent utiliser des paramètres proxy lors d'une mise à jour. Ceux-ci sont configurés sur la console de l'agent.
- Lors d'une mise à jour, l'icône Trend Micro Security (pour Mac) de la barre des menus du Endpoint indique que le produit est en cours de mise à jour. Si une mise à niveau du programme de l'agent est disponible, les agents procèdent à une mise à jour, puis à une mise à niveau vers la version du programme la plus récente. Les utilisateurs ne peuvent pas exécuter de tâches à partir de la console avant la fin de la mise à jour.
- Accédez à l'écran Résumé pour vérifier que tous les agents ont été mis à jour.

Limitations pour agent en IPv6 pur

La table suivante énumère les limitations qui s'appliquent lorsque les agents ne possèdent qu'une adresse IPv6.

TABLEAU 26-4. Limitations pour agent en IPv6 pur

ÉLÉMENT	LIMITATION
Serveur parent	Les agents en IPv6 pur ne peuvent être gérés par un serveur en IPv4 pur.
Mises à jour	Un agent en IPv6 pur ne peut se mettre à jour depuis des sources de mise à jour en IPv4 pur, telles que : • serveur ActiveUpdate de Trend Micro • Serveur Trend Micro Security (pour Mac) IPv4 pur
Requêtes de l'évaluation de la réputation de sites Web	Un agent en IPv6 pur ne peut envoyer de requêtes de l'évaluation de la réputation de sites Web à Trend Micro Smart Protection Network.

ÉLÉMENT	LIMITATION
Connexion proxy	Un agent en IPv6 pur ne peut se connecter via un serveur proxy en IPv4 pur.
Déploiement de l'agent	Impossible pour Apple Remote Desktop de déployer l'agent vers des Endpoints en IPv6 pur car ces derniers apparaissent constamment hors ligne.

La plupart de ces limitations peuvent être contournées en configurant un serveur proxy à double pile qui peut effectuer des conversions entre adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre les agents et les entités auxquelles ils se connectent.

Configuration des paramètres de mise à jour des agents

Pour obtenir des explications détaillées sur les mises à jour des agents, consultez la rubrique *Mises à jour des agents à la page 26-37*.

Procédure

1. Sélectionnez l'option **Les agents téléchargent les mises à jour depuis le serveur ActiveUpdate de Trend Micro lorsque la connexion au serveur Trend Micro Security (pour Mac) est impossible** afin de permettre aux agents de télécharger les mises à jour depuis le serveur ActiveUpdate de Trend Micro.

   Remarque

   Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives à la mise à jour des agents liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page 26-39*.

2. Sélectionnez **Les agents peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni installer des correctifs de type hotfix** pour autoriser la poursuite des mises à jour des composants, tout en empêchant la mise à niveau de l'agent Trend Micro Security (for Mac).

3. Pour configurer les mises à jour programmées, effectuez les étapes suivantes :

   a. Sélectionnez **Activer la mise à jour programmée**.

   b. Configurez la programmation.

   c. Si vous sélectionnez **Tous les jours** ou **Une fois par semaine**, indiquez l'heure de la mise à jour et la périodicité qu'observera le serveur Trend Micro Security (pour Mac) pour demander aux agents de mettre à jour les composants. Par exemple, si l'heure de début est midi et que la période est de 2 heures, le serveur notifie de manière aléatoire tous les agents en ligne afin qu'ils mettent à jour leurs composants entre midi et 14 h. Ce paramètre évite que tous les agents en ligne se connectent simultanément au serveur à l'heure de début indiquée, ce qui réduit considérablement le trafic en direction du serveur.

Réputation de sites Web

La technologie de réputation de sites Web assure le suivi de la crédibilité des domaines Web en leur attribuant un score de réputation basé sur plusieurs facteurs, dont l'âge du site Web, l'historique des modifications de son emplacement et les indications d'activités suspectes découvertes par le biais d'une analyse de comportement de programmes malveillants. Elle poursuit ensuite le scan des sites et empêche les utilisateurs d'accéder à ceux qui sont infectés.

Les agents envoient des requêtes aux sources Smart Protection afin de déterminer la réputation des sites Web auxquels les utilisateurs tentent d'accéder. La réputation d'un site Web est mise en corrélation avec la stratégie de réputation de sites Web appliquée à l'Endpoint. En fonction de la stratégie utilisée, l'agent bloque ou autorise l'accès au site Web.

Remarque

Cette fonctionnalité prend en charge les dernières versions des navigateurs Safari™, Mozilla™ Firefox™ et Google Chrome™ publiées depuis avril 2014.

Configuration des paramètres de réputation de sites Web

Les paramètres de réputation de sites Web incluent des stratégies qui déterminent si Trend Micro Security (pour Mac) bloque ou autorise l'accès à un site Web. Pour déterminer la stratégie appropriée à utiliser, Trend Micro Security (pour Mac) vérifie l'emplacement de l'agent. L'emplacement de l'agent est « interne » s'il peut se connecter au serveur Trend Micro Security (pour Mac). Dans le cas contraire, l'emplacement de l'agent est « externe ».

Procédure

1. Pour configurer une stratégie pour les agents externes :

   a. Cliquez sur l'onglet **Agents externes**.

   b. Sélectionnez **Activer la stratégie de réputation de sites Web**.

      Lorsque la stratégie est activée, les agents externes envoient des requêtes d'évaluation de la réputation de sites Web au réseau Smart Protection Network.

      Remarque

      Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives aux requêtes d'évaluation de réputation de sites Web liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page 26-39*.

   c. Sélectionnez un niveau de sécurité pour la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**

      Remarque

      Les niveaux de sécurité déterminent si Trend Micro Security (pour Mac) autorise ou bloque l'accès à une URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, Trend Micro Security (pour Mac) ne bloque que les URL constituant des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de détecter des faux positifs augmente également.

d. Pour envoyer des commentaires relatifs à la réputation de sites Web, cliquez sur l'URL fournie. Le système d'évaluation de réputation de sites Web de Trend Micro ouvre une nouvelle fenêtre de navigateur.

2. Pour configurer une stratégie pour les agents internes :

a. Cliquez sur l'onglet **Agents internes**.

b. Sélectionnez **Activer la stratégie de réputation de sites Web**.

Lorsque la stratégie est activée, les agents internes envoient des requêtes d'évaluation de la réputation de sites Web :

- aux serveurs Smart Protection Server si l'option **Envoyer les requêtes aux Smart Protection Servers** est activée.
- au réseau Smart Protection Network si l'option **Envoyer les requêtes aux Smart Protection Servers** est désactivée.

Remarque

Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives aux requêtes d'évaluation de réputation de sites Web liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page 26-39*.

c. Sélectionnez **Envoyer les requêtes aux Smart Protection Servers** si vous souhaitez que les agents internes envoient des requêtes de réputation de sites Web à des serveurs Smart Protection Server.

- Si vous activez cette option, les agents utilisent la même liste de sources Smart Protection que celle utilisée par les agents OfficeScan pour déterminer les serveurs Smart Protection Server auxquels envoyer leurs requêtes.
- Si vous désactivez cette option, les agents envoient des requêtes d'évaluation de la réputation de sites Web au réseau Smart Protection Network. Les Endpoints doivent disposer d'une connexion Internet pour réussir à envoyer des requêtes.

d. Sélectionnez un niveau de sécurité pour la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**

Remarque

Les niveaux de sécurité déterminent si Trend Micro Security (pour Mac) autorise ou bloque l'accès à une URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, Trend Micro Security (pour Mac) ne bloque que les URL constituant des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de détecter des faux positifs augmente également.

Les agents ne bloquent pas les sites Web non testés, quel que soit le niveau de sécurité.

e. Pour envoyer des commentaires relatifs à la réputation de sites Web, cliquez sur l'URL fournie. Le système d'évaluation de réputation de sites Web de Trend Micro ouvre une nouvelle fenêtre de navigateur.

f. Décidez si les agents sont autorisés à envoyer des journaux de réputation de sites Web au serveur. Autorisez les agents à envoyer des journaux si vous souhaitez analyser les URL bloquées par Trend Micro Security (pour Mac), puis effectuez l'action appropriée sur les URL dont vous estimez l'accès sécurisé.

Configuration des listes d'URL approuvées et bloquées

Ajoutez les sites Web que vous considérez comme sûrs ou dangereux à la liste approuvée ou à la liste bloquée. Lorsque Trend Micro Security (for Mac) détecte un accès à l'un de ces sites Web, il autorise ou bloque l'accès automatiquement et cesse d'envoyer une requête aux sources Smart Protection.

Procédure

1. Accédez à la console Web de Trend Micro Security (for Mac).
2. Accédez à **Agents** > **Paramètres généraux de l'agent** > **Liste des URL approuvées/bloquées par réputation de sites Web**.
3. Saisissez une URL dans la zone de texte. Vous pouvez insérer un caractère générique (*) dans l'URL.

   Exemples :

- `www.trendmicro.com/*` signifie toutes les pages du domaine www.trendmicro.com.
- `*.trendmicro.com/*` signifie toutes les pages d'un sous-domaine de trendmicro.com.

Vous pouvez saisir des URL contenant des adresses IP. Si une URL contient une adresse IPv6, placez cette adresse entre crochets.

4. Cliquez sur **Ajouter à la liste approuvée** ou **Ajouter à la liste bloquée**.
5. Pour supprimer une entrée, sélectionnez une option dans la liste déroulante **Afficher** et cliquez sur l'icône en regard d'une URL.
6. Cliquez sur **Enregistrer**.

Partie XI

Widgets Endpoint Sensor

Chapitre 27

Widgets Trend Micro Endpoint Sensor

Cette section contient des rubriques d'aide concernant tous les widgets Trend Micro Endpoint Sensor qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Résumé de surveillance intelligente par hôte à la page 27-2*
- *Investigation Endpoint Sensor à la page 27-2*

Résumé de surveillance intelligente par hôte

Ce widget affiche un récapitulatif des endpoints les plus récents sur lesquels une règle de surveillance a été déclenchée. Les données sont extraites du widget **Résumé de surveillance intelligente par hôte** contenu dans le tableau de bord du serveur Trend Micro Endpoint Sensor.

Nom de la colonne	Description
Nom d'hôte	Nom d'hôte de l'endpoint
Nombre de résultats	Nombre de règles de correspondance déclenchées sur l'endpoint Cliquez pour afficher plus de détails sur les règles déclenchées sur l'endpoint.
Catégorie de la règle	Classification basée sur les six étapes d'une attaque ciblée
Heure de la détection	Date et heure du dernier déclenchement de la règle dans l'endpoint

La valeur par défaut de la période est **Dernières 24 heures**. Modifiez la période selon vos préférences.

Remarque

- Le widget exige la configuration préalable d'une connexion à un serveur Trend Micro Endpoint Sensor. Après avoir ajouté un serveur, actualisez le widget pour commencer à récupérer les données auprès du nouveau serveur.
- Si plusieurs serveurs sont ajoutés, le widget affiche le résultat cumulé des données de tous les serveurs.

Investigation Endpoint Sensor

Le widget **Investigation Endpoint Sensor** se connecte à un serveur à distance Trend Micro Endpoint Sensor pour démarrer une investigation et afficher les résultats de cette investigation directement depuis le tableau de bord de Control Manager.

Cliquez sur **Lancer une nouvelle investigation** pour démarrer une nouvelle investigation, puis sélectionnez une méthode d'investigation :

- Choisissez **Enregistrements historiques** pour enquêter sur des événements historiques basés sur des critères définis par l'utilisateur
- Choisissez **Instantané du système** pour enquêter sur l'état actuel des endpoints sélectionnés

Lorsque la page **Nouvelle investigation** s'affiche, entrez les critères requis. Les types d'investigation suivants sont disponibles :

Type d'investigation	Description
Enregistrements d'historiques - Scan rétroactif	Permet d'enquêter sur des événements historiques basés sur des critères définis par l'utilisateur
Enregistrements d'historiques - Règle d'IOC	Permet d'enquêter sur les événements historiques à l'aide d'une règle d'IOC
Instantané du système - Recherche dans le registre	Permet d'enquêter sur le registre Windows
Instantané du système - Règle YARA	Permet d'enquêter sur les menaces résidant dans la mémoire à l'aide d'une règle YARA
Instantané du système - Règle d'IOC	Permet d'enquêter sur les événements à l'aide d'une règle d'IOC
Instantané du système - Règle de disques IOC	Permet d'enquêter sur les fichiers à l'aide d'une règle d'IOC
Instantané du système - Audit du système	Permet d'enquêter sur tous les processus, services et modules en cours d'exécution

Cliquez sur **Enquêter** pour démarrer l'investigation. Pour arrêter une investigation en cours, cliquez sur **Annuler**.

Le widget s'actualise régulièrement pour afficher la progression de l'investigation. Le widget affiche un graphique circulaire représentant l'ensemble des endpoints classés dans les catégories suivantes :

- **Correspondant** : indique le nombre d'endpoints sur lesquels un objet correspondant a été détecté.
- **Sûr** : indique le nombre d'endpoints sur lesquels aucun objet correspondant n'a été détecté.
- **En attente** : indique le nombre d'endpoints qui n'ont pas encore fait l'objet d'une investigation.
- **Annulé** : indique le nombre d'endpoints qui répondent à l'un des critères suivants :
  - L'investigation effectuée sur l'endpoint a rencontré une erreur
  - L'endpoint n'est pas connecté ou toutes les commandes lui étant envoyées ont expiré
  - L'investigation sur l'endpoint a été interrompue manuellement par l'utilisateur

Une ventilation des totaux est affichée à droite du graphique circulaire. Cliquez sur le nombre de chaque catégorie pour afficher l'écran **Résultat de l'investigation**. Cet écran permet d'obtenir des informations supplémentaires sur les résultats de la dernière investigation démarrée à partir de Control Manager.

Remarque

- Après l'ajout d'un serveur, actualisez le widget pour commencer à récupérer les données du nouveau serveur.
- Si plusieurs serveurs sont ajoutés, le widget affiche le résultat cumulé des données de tous les serveurs.

Chapitre 28

Intégration de Capteur de Endpoint Trend Micro

Le contenu suivant explique comment intégrer Capteur de Endpoint Trend Micro à Control Manager.

Les rubriques sont les suivantes:

- *Intégration de Control Manager dans cette version à la page 28-2*
- *Enregistrement auprès de Control Manager à la page 28-2*
- *Ajout des widgets Endpoint Sensor à la page 28-3*
- *Utilisation de Control Manager pour vérifier l'état à la page 28-5*
- *Utilisation du widget Investigation Endpoint Sensor à la page 28-6*
- *Utilisation des mises à jour automatiques à la page 28-7*
- *Stratégie Trend Micro Endpoint Sensor à la page 28-8*

Intégration de Control Manager dans cette version

Cette version inclut les fonctionnalités suivantes pour la gestion des serveurs Capteur de Endpoint depuis Control Manager :

- Utilisez les fichiers IOC téléchargés dans Control Manager pour lancer des investigations directement sur Capteur de Endpoint depuis la console de Control Manager.
- Enregistrez plusieurs serveurs Capteur de Endpoint. Control Manager peut lancer des investigations simultanées sur plusieurs serveurs Capteur de Endpoint.
- Extrayez les données à partir des résultats d'investigation de Endpoint Sensor. Les données sont alors affichées dans un widget Control Manager.
- Créez et déployez des stratégies sur les serveurs Capteur de Endpoint enregistrés auprès de Control Manager.
- Gérez les règles de surveillance dans Control Manager.
- Configurez et déployez les **Paramètres d'envoi** sur les serveurs Capteur de Endpoint enregistrés auprès de Control Manager.

Enregistrement auprès de Control Manager

Procédure

1. Ouvrez la console d'administration de Control Manager.

   Pour ouvrir la console de Control Manager sur n'importe quel endpoint sur le réseau, ouvrez un navigateur Web et saisissez ce qui suit :

   ```
   https:// <nom du serveur Control Manager> /Webapp/
   index.html
   ```

   Où `<nom du serveur Control Manager>` est l'adresse IP ou le nom d'hôte du serveur Control Manager

2. Accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur**.
3. Dans l'écran qui s'affiche, sélectionnez **Capteur de Endpoint Trend Micro** comme **Type de serveur**, puis cliquez sur **Ajouter**.
4. Dans l'écran **Ajouter un serveur**, indiquez les informations suivantes :
   - Serveur
   - Nom d'affichage
   - Nom d'utilisateur
   - Mot de passe
5. Cliquez sur **Enregistrer** pour ajouter le serveur à la liste. Répétez ces étapes pour ajouter un autre serveur.

Ajout des widgets Endpoint Sensor

Procédure

1. Ouvrez la console d'administration de Control Manager.

   Pour ouvrir la console de Control Manager sur n'importe quel endpoint sur le réseau, ouvrez un navigateur Web et saisissez ce qui suit :

   ```
   https:// <nom du serveur Control Manager> /Webapp/
   index.html
   ```

   Où `<nom du serveur Control Manager>` est l'adresse IP ou le nom d'hôte du serveur Control Manager
2. Accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur**.
3. Dans l'écran qui s'affiche, sélectionnez **Capteur de Endpoint Trend Micro** comme **Type de serveur**, puis cliquez sur **Ajouter**.
4. Indiquez les détails du serveur Control Manager à ajouter, puis cliquez sur **Enregistrer**.

5. Accédez au **Tableau de bord**.

6. Sélectionnez un onglet existant ou créez un onglet.

7. Cliquez sur le bouton **Paramètres** à droite de l'affichage d'onglets.

8. Cliquez sur **Ajouter des widgets**.

9. Dans l'écran qui s'affiche, sélectionnez la catégorie **Endpoint Sensor** dans la liste déroulante.

   Les widgets suivants sont disponibles :

TABLEAU 28-1. Widgets Capteur de Endpoint

NOM DU WIDGET	DESCRIPTION
Résumé de surveillance intelligente par hôte	Permet d'afficher les endpoints qui ont déclenché une règle de surveillance. Actualisez manuellement le widget pour afficher les données les plus récentes. Pour configurer les paramètres du widget, cliquez sur ▼.
Investigation Endpoint Sensor	Exécutez une investigation et affichez un récapitulatif rapide de la dernière investigation Capteur de Endpoint Trend Micro démarrée à partir de Control Manager. Par défaut, le widget s'actualise automatiquement toutes les 2 minutes. Pour configurer les paramètres du widget, cliquez sur ▼. Pour plus d'informations, consultez le *Manuel de l'administrateur Trend Micro Endpoint Sensor*.

10. Sélectionnez un widget ou les deux, puis cliquez sur **Ajouter**.

    Les widgets ajoutés s'affichent dans le **Tableau de bord**. Ces widgets présentent un récapitulatif des investigations les plus récentes et des résultats de surveillance de tous les serveurs enregistrés.

Remarque

Après avoir enregistré un nouveau serveur Endpoint Sensor, actualisez les widgets **Investigation Endpoint Sensor** et **Résumé de surveillance intelligente par hôte** afin de mettre à jour le contenu des widgets avec les données provenant du nouveau serveur.

Utilisation de Control Manager pour vérifier l'état

Utilisez les widgets **État de la connexion du produit** et **État de la connexion de l'agent** pour vérifier l'état des serveurs ou des agents Endpoint Sensor enregistrés. Ces widgets affichent des informations des serveurs Endpoint Sensor ajoutés via l'écran **Administration** > **Serveurs gérés** > **Enregistrement du serveur**.

Procédure

1. Accédez au **Tableau de bord**.
2. Cliquez sur l'onglet **Conformité** pour afficher les widgets suivants :

   Remarque

   l'**État de la connexion du produit** est également disponible dans l'onglet **Résumé**.

   - **État de la connexion du produit** : affiche l'état du serveur dans la colonne **État**

     Cliquez sur **Afficher les détails** pour afficher des informations détaillées sur les serveurs.

   - **État de la connexion de l'agent** : affiche le nombre total d'agents, d'agents en ligne et d'agents hors ligne pour chaque serveur

     Cliquez sur le nombre dans les colonnes **En ligne**, **Hors ligne** ou **Total** pour afficher des informations détaillées sur les agents.

3. Pour ajouter les widgets à un onglet :
   a. Accédez à un onglet existant ou créez un onglet.
   b. Cliquez sur le bouton **Paramètres** à droite de l'affichage d'onglets.
   c. Cliquez sur **Ajouter des widgets**.
   d. Dans l'écran **Ajouter des widgets**, sélectionnez la catégorie **Conformité**.

e. Sélectionnez **État de la connexion de l'agent** ou **État de la connexion du produit**.

f. Cliquez sur **Ajouter**.

Le widget ajouté s'affiche dans l'onglet actuel.

Utilisation du widget Investigation Endpoint Sensor

Procédure

1. Ouvrez la console d'administration de Control Manager
2. Accédez à l'onglet sur lequel le widget Investigation Endpoint Sensor a été ajouté.
3. Dans le widget Investigation Endpoint Sensor, cliquez sur **Lancer une nouvelle investigation** puis sur **Enregistrements historiques** ou **Instantané du système**, selon le type d'investigation que vous prévoyez d'exécuter.
4. Dans l'écran qui s'affiche, indiquez les informations requises.

   Le widget Investigation Endpoint Sensor prend également en charge l'importation des événements de rappel C&C en tant que critères d'investigation.

   a. Dans le widget Investigation Endpoint Sensor, cliquez sur **Lancer une nouvelle investigation** > **Enregistrements historiques**.

   b. Sélectionnez **Scan rétroactif** comme méthode d'investigation.

   c. Cliquez sur **Importer depuis les événements de rappel C&C**.

   d. Dans l'écran qui s'affiche, sélectionnez les événements de rappel C&C nécessitant une investigation, puis cliquez sur **OK**. Les événements sont ajoutés en tant que critères d'investigation.

5. Cliquez sur **Enquêter**.

   L'écran est actualisé et affiche la progression de l'investigation.

Remarque

Pour arrêter une investigation en cours, cliquez sur **Annuler**.

6. Une fois que l'investigation terminée, le widget affiche le nombre d'endpoints classés selon les statuts **Correspondant**, **Sûr**, **En attente** ou **Annulé** au cours de l'investigation. Cliquez sur le résultat de chaque classification pour afficher plus de détails.

Utilisation des mises à jour automatiques

Pour utiliser Control Manager en tant que serveur de mise à jour local pour Endpoint Sensor, procédez comme suit :

Procédure

1. Activez les mises à jour automatiques dans Control Manager.
   a. Ouvrez la console d'administration de Control Manager
   b. Cliquez sur **Mises à jour** > **Téléchargement programmé**
   c. Recherchez les fichiers de signatures suivants :
      - Signature d'exception Endpoint Sensor
      - Signature sécurisée Endpoint Sensor
      - Signature de Attack Discovery
   d. Pour chaque fichier de signatures, cliquez sur le nom du fichier de signatures et sélectionnez **Activer les téléchargements programmés**. Conservez toutes les autres valeurs par défaut.

Remarque

Pour l'intégration de Endpoint Sensor, les **paramètres de déploiement automatique** ne sont pas pris en charge.

e. Cliquez sur **Enregistrer**.

2. Configurez Endpoint Sensor pour utiliser Control Manager comme source de mise à jour.

   a. Ouvrez la console d'administration des serveurs de Endpoint Sensor.

   b. Cliquez sur **Administration** > **Mises à jour**.

   c. Activez **Télécharger les règles de surveillance à partir de la source suivante**.

   d. Sélectionnez **Autre source de mise à jour** et saisissez ce qui suit dans la zone de texte située en dessous :

      ```
      http://<Control Manger server Name>/TVCSDownload/
      Activeupdate
      ```

   e. Cliquez sur **Enregistrer**.

Control Manager inclura les fichiers de signatures de Endpoint Sensor lors de la prochaine mise à jour programmée. Par la suite, Endpoint Sensor téléchargera ces fichiers de signatures à partir de Control Manager lors de la prochaine mise à jour programmée de Endpoint Sensor.

Stratégie Trend Micro Endpoint Sensor

Control Manager comporte une fonction de gestion des stratégies qui permet aux administrateurs de mettre à jour les règles de surveillance à distance et de déployer les paramètres de soumission sur les serveurs enregistrés.

Remarque

Il est possible de créer plusieurs stratégies Endpoint Sensor, mais un serveur ne peut émettre qu'une seule stratégie à la fois.

Préparation du serveur au déploiement des stratégies

Par défaut, les serveurs Endpoint Sensor récemment ajoutés sont placés dans le dossier **Nouvelle entité**. Les serveurs doivent être déplacés vers un autre dossier afin d'être visibles pour le déploiement des stratégies.

Procédure

1. Ouvrez la console d'administration de Control Manager
2. Accédez à **Répertoires** > **Produits**, puis cliquez sur **Gestion des répertoires**.
3. Dans l'arborescence du répertoire, développez le dossier **Nouvelle entité** et localisez le serveur que vous souhaitez gérer.
4. Effectuez l'une des actions suivantes :
   - Faites glisser et déposez le serveur dans un autre dossier.
   - Cliquez sur **Ajouter dossier** pour créer un nouveau dossier, puis faites glisser et déposez le serveur dans le nouveau dossier.

Création et déploiement des stratégies

Procédure

1. Ouvrez la console d'administration de Control Manager
2. Allez à **Stratégies** > **Gestion des stratégies**.
3. Dans la liste déroulante **Produit**, choisissez **Trend Micro Endpoint Sensor**.
4. Cliquez sur **Créer**.
5. Cliquez sur **Spécifier la ou les cibles** et sélectionnez les serveurs Endpoint Sensor sur lesquels vous souhaitez procéder au déploiement.
6. Dans la section **Paramètres de surveillance**, configurer les règles de surveillance et les paramètres de soumission de la nouvelle stratégie.

7. Cliquez sur **Déployer** pour lancer immédiatement le déploiement de stratégie.

   Control Manager applique alors les éventuelles mises à jour ultérieures de la stratégie sur les serveurs Endpoint Sensor cibles, toutes les 24 heures.

Gestion des règles de surveillance

Tenez compte de ce qui suit :

- Gestion des règles de surveillance :

  L'onglet **Règles de surveillance** affiche uniquement les règles définies par l'utilisateur. Les règles de surveillance sont partagées par les stratégies, mais l'état d'une règle de surveillance (activé/désactivé/suppression) est indépendant pour chaque stratégie. Les administrateurs peuvent personnaliser les stratégies en sélectionnant les règles de surveillance à activer, désactiver ou supprimer pour chaque stratégie. Les nouvelles règles de surveillance sont désactivées par défaut.

  Control Manager se limite au contrôle à distance des règles de surveillance dans les serveurs Endpoint Sensor où les règles sont intégrées à une stratégie Endpoint Sensor.

  Si un nouveau serveur Endpoint Sensor est enregistré via **Administration** > **Serveurs gérés**, Control Manager intègre automatiquement ce nouveau serveur Endpoint Sensor à sa planification de déploiement des règles. Lorsqu'arrive l'échéance de planification de déploiement suivante, Control Manager télécharge toutes les règles de surveillance actives sur le serveur récemment enregistré.

- Téléchargement des règles de surveillance :

  Pour télécharger une règle de surveillance, accédez à **Administration** > **Serveurs gérés**. Cliquez sur **Télécharger une règle IOC** > **Choisir un fichier**, puis accédez à l'emplacement de la règle de surveillance. Cliquez sur **Ouvrir** pour télécharger automatiquement la règle de surveillance. Une fois le téléchargement terminé, cliquez sur **Enregistrer** ou sur **Déployer**.

Remarque

- Il est recommandé de spécifier le serveur Endpoint Sensor cible avant de télécharger la règle.
- La fonction **Télécharger une règle IOC** n'est activée que si au moins un serveur Endpoint Sensor est enregistré auprès de Control Manager.

Le fait de télécharger la même règle de surveillance dans Control Manager et sur un serveur Endpoint Sensor enregistré auprès de Control Manager peut générer des conflits. Procédez régulièrement au suivi des règles de surveillance téléchargées via l'écran **Paramètres de surveillance** afin d'éviter les doublons.

Si une règle de surveillance en double est détectée, le message suivant s'affiche : « Impossible de télécharger le fichier. Le fichier existe déjà sur le serveur Endpoint Sensor. Utilisez la console d'administration Endpoint Sensor pour supprimer le fichier, puis essayez de nouveau. »

- Modification de l'état d'une règle de surveillance :

  Pour modifier l'état d'une règle de surveillance, cliquez sur **Changer l'état**, puis sélectionnez **Activer** ou **Désactiver**. Mettez ensuite à jour la règle à distance des serveurs Capteur de Endpoint spécifiés en tant que cibles dans cette stratégie.

  L'état d'une règle de surveillance est indépendant pour chaque stratégie.

- Suppression de règles de surveillance :

  Pour supprimer une règle, sélectionnez la règle, puis cliquez sur **Supprimer**. L'état de la règle supprimée devient **suppression**. Cliquez sur **Enregistrer** ou sur **Déployer** pour terminer la procédure.

AVERTISSEMENT!

- La suppression d'une règle de surveillance supprime également cette règle de surveillance de toutes les autres stratégies Endpoint Sensor.
- Si une règle identique est une nouvelle fois téléchargée dans une nouvelle stratégie, l'ancienne stratégie supprimera à nouveau la règle lors de son exécution programmée.

Si le problème persiste, contactez l'assistance Trend Micro pour obtenir de l'aide.

Gestion des paramètres de soumission

Utilisez l'onglet **Paramètres de soumission** pour indiquer si les fichiers collectés doivent être envoyés à un serveur de fichiers local ou à Deep Discovery Analyzer pour une analyse plus poussée.

Control Manager n'est pas en mesure de configurer une connexion de proxy entre des endpoints Endpoint Sensor et Deep Discovery Analyzer. Pour configurer une connexion de proxy entre des endpoints Endpoint Sensor et Deep Discovery Analyzer, utilisez l'écran **Proxy** de l'ordinateur du serveur Endpoint Sensor.

Partie XII

Widgets Deep Security Manager

Chapitre 29

Widgets Deep Security Manager

Cette section contient des rubriques d'aide concernant tous les widgets Deep Security Manager qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget Deep Security – Historique des événements de la protection anti-programmes malveillants à la page 29-3*
- *Widget Deep Security – État de la protection anti-programmes malveillants (programme malveillant) à la page 29-4*
- *Widget Deep Security – Activité du type d'applications (détection) à la page 29-5*
- *Widget Deep Security – Activité du type d'applications (prévention) à la page 29-6*
- *Widget Résumé des composants Deep Security à la page 29-7*
- *Widget Résumé des fonctions Deep Security à la page 29-9*
- *Widget Deep Security – Activité du pare-feu (détection) à la page 29-10*
- *Widget Deep Security – Activité du pare-feu (prévention) à la page 29-11*
- *Widget Deep Security – Historique des événements du pare-feu à la page 29-12*
- *Widget Deep Security – Activité de surveillance de l'intégrité à la page 29-13*
- *Widget Deep Security – Historique des événements de surveillance de l'intégrité à la page 29-13*

- *Widget Deep Security – Historique des événements de prévention contre les intrusions à la page 29-14*
- *Widget Deep Security – Activité de l'IPS (détection) à la page 29-15*
- *Widget Deep Security – Activité de l'IPS (prévention) à la page 29-16*
- *Widget Deep Security – Activité d'inspection des journaux à la page 29-17*
- *Widget Deep Security – Historique des événements d'inspection des journaux à la page 29-18*
- *Widget Deep Security - Historique des événements du scan de reconnaissance à la page 29-18*
- *Widget Résumé d'état Deep Security à la page 29-19*
- *Widget Deep Security – Historique des événements de la réputation de sites Web à la page 29-21*
- *Widget Deep Security – Activité d'URL de la réputation de sites Web à la page 29-22*

Widget Deep Security – Historique des événements de la protection anti-programmes malveillants

Ce widget affiche le nombre d'événements de la protection anti-programmes malveillants ayant eu lieu pendant une période spécifique.

Cliquez sur une barre pour afficher la page **Événements** de Deep Security Manager, filtrée pour afficher les événements de la protection anti-programmes malveillants correspondant au type d'événements et à la période spécifiés. Vous pouvez également cliquer sur les types d'événements dans la légende pour modifier l'affichage du graphique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Deep Security – État de la protection anti-programmes malveillants (programme malveillant)

Ce widget affiche les cinq menaces de programmes malveillants les plus fréquemment détectées sur vos endpoints.

Cliquez sur un nombre de la colonne **Total** pour afficher des détails supplémentaires sur la console de Deep Security Manager.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Pour mettre une installation Deep Security à la disposition des widgets Deep Security, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Deep Security.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Données	Description
Nom du programme malveillant	Nom de la menace liée à un programme malveillant

Données	Description
Nombre d'éléments non nettoyables	Nombre d'occurrences de la menace que Deep Security n'a pas pu nettoyer
Total	Nombre d'événements dans la plage de temps et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la plage de temps actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Deep Security – Activité du type d'applications (détection)

Ce widget affiche les cinq principaux types d'applications associés aux événements de détection IPS.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de détection IPS associés à un type d'applications spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Données	Description
Nom du type d'application	Nom du type d'application
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Activité du type d'applications (prévention)

Ce widget affiche les cinq principaux types d'applications associés aux événements de prévention IPS.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de prévention IPS associés à un type d'applications spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Données	Description
Nom du type d'application	Nom du type d'application
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Résumé des composants Deep Security

Ce widget affiche les numéros de versions des mises à jour de composants Deep Security disponibles et le pourcentage d'endpoints mis à jour vers la dernière version.

Important

Ce widget ne peut afficher que des données provenant de Deep Security 7.5 ou d'une version ultérieure.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Composants	Nom du composant Deep Security.
Version actuelle	Version actuellement disponible sur Deep Security Manager.
Pourcentage mis à jour	Pourcentage d'ordinateurs gérés mis à jour vers la dernière version. **Remarque** Les mises à jour peuvent ne pas être applicables à tous les ordinateurs gérés.

Le widget affiche les numéros de version des composants suivants.

Composant	Description
Smart Scan Agent Pattern	Fichier de détection de signatures de programmes malveillants de taille réduite envoyé vers Deep Security Virtual Appliance. Si une comparaison avec ces signatures suggère la présence d'un fichier potentiellement malveillant sur un ordinateur, ce fichier est comparé au fichier de signatures plus complet disponible sur le serveur Smart Scan pour confirmation.
Modèle de virus	Fichier qui aide Deep Security Virtual Appliance à identifier les signatures de virus, signatures uniques des bits et des octets qui signalent la présence d'un virus.
Signatures IntelliTrap	IntelliTrap recherche les programmes malveillants susceptibles de se trouver dans les fichiers utilisant la compression en temps réel, ainsi que d'autres caractéristiques de programmes malveillants tels que les packers.
Fichier de signatures de surveillance active des spywares	Signatures de détection de spywares.
Moteur de scan antivirus	Moteur appliquant des fichiers de signatures de virus à un fichier lors d'un scan antivirus.

COMPOSANT	DESCRIPTION
Mise à jour des règles Deep Security	Les règles DPI assurent la détection et la prévention des intrusions (IDS/IPS) en protégeant les failles des attaques connues et inconnues à ce jour.

Widget Résumé des fonctions Deep Security

Ce widget présente l'activité récente de tous les modules Deep Security.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Le widget affiche des informations agrégées provenant de plusieurs serveurs gérés.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Conseil

Pour afficher les données non agrégées provenant de plusieurs serveurs gérés, ajoutez un nouveau widget pour chaque serveur géré.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

DONNÉES	DESCRIPTION
Module	Module Deep Security
Ordinateurs protégés	Nombre actuel d'ordinateurs gérés protégés par ce module et pourcentage de tous les ordinateurs gérés que cela représente
Nombre d'événements	Nombre d'événements générés par le module au cours de la période spécifiée

Données	Description
Tendance	Pourcentage de modification du nombre d'événements depuis la période précédente
Nombre total d'ordinateurs	Nombre total d'ordinateurs gérés par Deep Security

Widget Deep Security – Activité du pare-feu (détection)

Ce widget affiche les cinq principales règles de pare-feu fonctionnant en mode de détection qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de pare-feu déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle

Données	Description
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Activité du pare-feu (prévention)

Ce widget affiche les cinq principales règles de pare-feu fonctionnant en mode de prévention qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de pare-feu déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Historique des événements du pare-feu

Ce widget affiche le nombre d'événements de pare-feu détectés par Deep Security Manager sur la plage de temps spécifiée. Le graphique affiche les événements déclenchés par les règles de pare-feu en mode de détection et de prévention.

Cliquez sur une barre pour afficher des détails supplémentaires sur la console de Deep Security Manager. Vous pouvez également cliquer sur les types d'événements dans la légende pour modifier l'affichage du graphique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Pour mettre une installation Deep Security à la disposition des widgets Deep Security, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Deep Security.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Deep Security – Activité de surveillance de l'intégrité

Ce widget affiche les cinq principales règles de surveillance de l'intégrité qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de surveillance de l'intégrité déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Historique des événements de surveillance de l'intégrité

Ce widget affiche le niveau de gravité des événements consignés par les scans de surveillance de l'intégrité pour la période indiquée.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Deep Security – Historique des événements de prévention contre les intrusions

Ce widget affiche le nombre d'événements de prévention des intrusions détectés par Deep Security Manager sur la plage de temps spécifiée. Le graphique affiche les événements déclenchés par les règles IPS en mode de détection et de prévention.

Cliquez sur une barre pour afficher la page **Événements** de Deep Security Manager, filtrée pour afficher les événements IPS correspondant au mode et à la plage de temps spécifiés. Vous pouvez également cliquer sur un mode (**Détection** ou **Prévention**) dans la légende pour modifier l'affichage du graphique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Deep Security – Activité de l'IPS (détection)

Ce widget affiche les cinq principales règles de l'IPS fonctionnant en mode de détection qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de détection IPS déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente

Données	Description
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Activité de l'IPS (prévention)

Ce widget affiche les cinq principales règles de l'IPS fonctionnant en mode de prévention qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements de prévention IPS déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle

Données	Description
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Activité d'inspection des journaux

Ce widget affiche les cinq principales règles d'inspection des journaux qui ont déclenché le plus grand nombre d'événements.

Cliquez sur une valeur dans la colonne **Totaux** pour afficher l'écran **Événements** de Deep Security Manager, filtré pour afficher les événements d'inspection des journaux déclenchés par une règle spécifique.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Pourcentage de modification entre la période précédente et la période actuelle

Widget Deep Security – Historique des événements d'inspection des journaux

Ce widget affiche le nombre d'événements déclenchés par les règles d'inspection des journaux ayant eu lieu pendant une période spécifique.

Cliquez sur une barre (détection ou prévention) pour afficher la page **Événements** de Deep Security Manager, filtrée pour afficher les événements d'inspection des journaux correspondant au type d'événements et à la période spécifiés. Vous pouvez également cliquer sur les types d'événements dans la légende pour modifier l'affichage du graphique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Deep Security - Historique des événements du scan de reconnaissance

Ce widget affiche le nombre d'événements déclenchés par les paramètres de détection du scan de reconnaissance ayant eu lieu pendant un intervalle de temps spécifié.

Cliquez sur une barre pour afficher la page **Événements** de Deep Security Manager, filtrée pour afficher les événements de détection du scan de reconnaissance

correspondant au type d'événements et à la période spécifiés. Vous pouvez également cliquer sur les types d'événements dans la légende pour modifier l'affichage du graphique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Deep Security. Pour surveiller plusieurs serveurs Deep Security, créez un widget pour chacun d'eux.

Widget Résumé d'état Deep Security

Ce widget affiche le nombre d'alertes critiques et d'alertes d'avertissement, ainsi que l'état des endpoints du réseau.

Le widget affiche des informations agrégées provenant de plusieurs serveurs gérés.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Conseil

Pour afficher les données non agrégées provenant de plusieurs serveurs gérés, ajoutez un nouveau widget pour chaque serveur géré.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

TABLEAU 29-1. Alertes

DONNÉES	DESCRIPTION
Alertes critiques	Nombre d'alertes critiques **Remarque** L'utilisateur détermine si une alerte doit être classée en tant qu'alerte critique ou d'avertissement sur la console Web de Deep Security Manager.
Alertes d'avertissement	Nombre d'alertes d'avertissement **Remarque** L'utilisateur détermine si une alerte doit être classée en tant qu'alerte critique ou d'avertissement sur la console Web de Deep Security Manager.

TABLEAU 29-2. État de l'ordinateur

DONNÉES	DESCRIPTION
Géré (vert)	Protégé et sans erreur ou avertissement.
Non géré (bleu)	Non protégé.
Verrouillé (gris)	Verrouillé. Lorsqu'un ordinateur est à l'état verrouillé, Deep Security Manager ne communique pas avec l'agent/appliance ou ne génère aucune alerte associée à cet ordinateur.
Critique (rouge)	À l'état d'erreur.
Avertissement (jaune)	À l'état d'avertissement.

Widget Deep Security – Historique des événements de la réputation de sites Web

Ce widget affiche le nombre d'événements déclenchés par les services de réputation de sites Web ayant eu lieu pendant une période spécifique.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
Dangereux	L'URL est avérée frauduleuse ou est une source connue de menaces
Très suspect	L'URL est suspectée d'être frauduleuse ou est une source possible de menaces
Suspect	L'URL est associée à du spam ou est potentiellement compromise
Bloqué	L'URL a été bloquée par un administrateur
Non testé	L'URL n'a pas encore été testée par Trend Micro Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés.

Widget Deep Security – Activité d'URL de la réputation de sites Web

Ce widget affiche les cinq principales adresses URL des services de réputation de sites Web qui présentent le plus grand nombre d'événements.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans l'écran qui s'affiche, sélectionnez le serveur géré à utiliser en tant que source, puis cliquez sur **Enregistrer**.

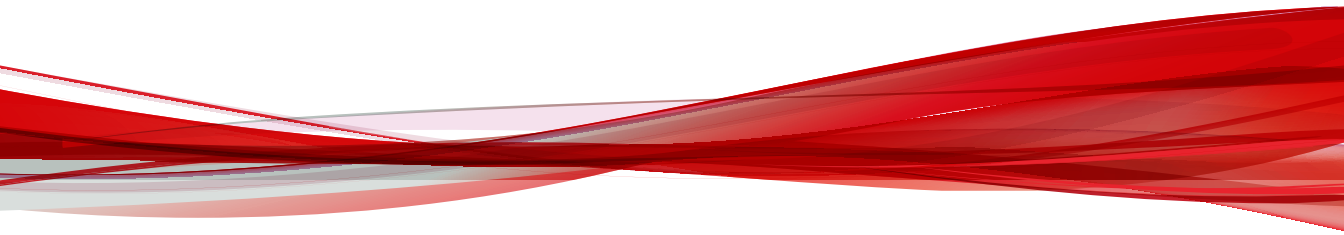
Remarque

Les données affichées dans le widget sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Données	Description
URL	URL
Total	Nombre d'événements dans la période et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la période précédant la période actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Partie XIII

Widgets Control Manager



Chapitre 30

Widgets du tableau de bord de Control Manager

Cette section contient des rubriques d'aide concernant les widgets spécifiques à Control Manager qui sont pris en charge sur le tableau de bord de Control Manager.

Les rubriques sont les suivantes:

- *Widget de vérification de la protection des points finaux à la page 30-2*
- *Widget Principales menaces critiques par durée de résidence à la page 30-3*
- *Widget Hôtes sur lesquels ont été effectuées des tentatives de rappel C&C à la page 30-5*
- *Widget Principales menaces de fichiers de Control Manager à la page 30-6*
- *Widget Hôtes compromis uniques au fil du temps à la page 30-7*
- *État de la stratégie à la page 30-8*
- *Lancement rapide à la page 30-9*

Widget de vérification de la protection des points finaux

Ce widget affiche l'état de protection des endpoints par OfficeScan et Deep Security depuis une structure Active Directory intégrée.

Important

Avant d'utiliser ce widget :

- Synchronisez l'arborescence des clients OfficeScan avec l'arborescence Active Directory.

  Consultez la documentation d'OfficeScan pour obtenir davantage d'instructions.

- Accédez à **Administration** > **Paramètres** > **Vérification de la protection des endpoints** pour activer le widget et configurer les paramètres de connexion des serveurs Active Directory, des serveurs OfficeScan et des serveurs Deep Security.

Cliquez sur l'icône Paramètres (>) pour configurer les options suivantes :

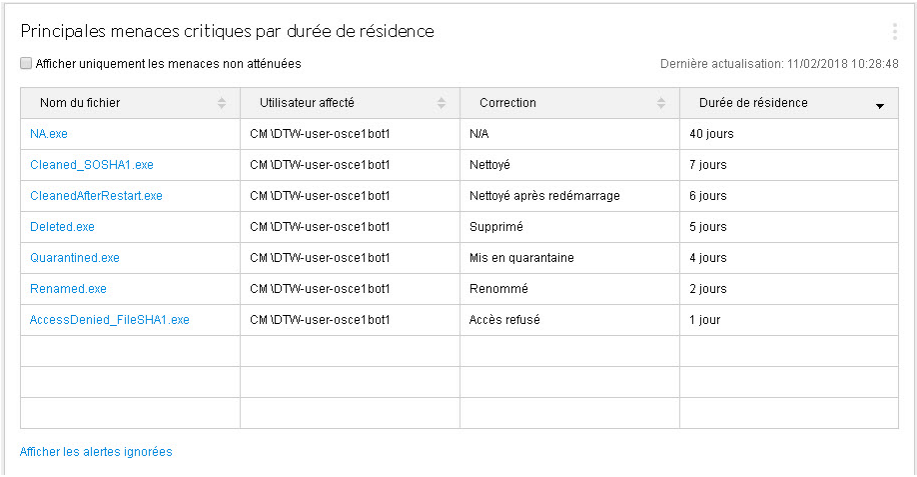
- **Serveurs OfficeScan** : cliquez sur le bouton Parcourir ( ) pour spécifier les serveurs OfficeScan fournissant les données du widget.
- **Serveurs Deep Security** : cliquez sur le bouton Parcourir ( ) pour spécifier les serveurs Deep Security fournissant les données du widget.
- **Colonnes** : spécifiez les colonnes que le widget doit afficher dans la table de données.

Cliquez sur une unité d'organisation dans la structure Active Directory pour visualiser les informations suivantes.

COLONNE	DESCRIPTION
Ordinateur	Affiche le nom de l'endpoint
OfficeScan	Indique si l'endpoint est protégé par un client OfficeScan ou VDI
Deep Security	Indique si l'endpoint est protégé par un agent Deep Security

COLONNE	DESCRIPTION
Hôte physique	Affiche le serveur physique où résident les endpoints virtuels
Fichier de signatures	Affiche la version du fichier de signatures qu'utilise le client OfficeScan ou VDI
Moteur de scan	Affiche la version du moteur de scan qu'utilise le client OfficeScan ou VDI
Version du client	Affiche la version du programme client
Profil Deep Security	Affiche le profil Deep Security en cours d'utilisation
Nom du serveur	Affiche le serveur OfficeScan et/ou Deep Security auquel les endpoints se connectent

Widget Principales menaces critiques par durée de résidence



Ce widget présente les principales menaces critiques en fonction de la durée de présence de la menace sur l'endpoint de l'endpoint de l'utilisateur affecté.

Important

Ce widget nécessite un serveur Trend Micro Endpoint Sensor enregistré. Les widgets affichent les résultats de l'évaluation d'impact effectuée par le serveur Trend Micro Endpoint Sensor, en fonction des valeurs SHA-1 des fichiers considérés comme des menaces critiques.

Vous pouvez sélectionner **Afficher uniquement les menaces non atténuées** pour afficher uniquement les menaces critiques à résoudre.

Cliquez sur les en-têtes de colonnes pour trier les données dans le tableau.

COLONNE	DESCRIPTION
Nom du fichier	Indique le nom de fichier de la menace critique détectée Cliquez sur le **nom du fichier** pour afficher des informations supplémentaires sur les menaces ou effectuer une investigation plus poussée.
Utilisateur affecté	Indique le nom de l'utilisateur affecté
Correction	Affiche l'action de correction effectuée par un produit Trend Micro
Durée de résidence	Indique la durée de présence de la menace sur l'endpoint de l'utilisateur affecté

Cliquez sur **Afficher les alertes ignorées** pour ouvrir l'écran **Alertes ignorées** et afficher des informations sur les alertes de menace critique qui ont été manuellement ignorées par un compte utilisateur Control Manager.

COLONNE	DESCRIPTION
Ignoré	Affiche l'heure à laquelle l'alerte de menace critique a été ignorée
Nom du fichier	Indique le nom de fichier de la menace critique détectée Cliquez sur le **nom du fichier** pour afficher des informations supplémentaires sur les menaces ou effectuer une investigation plus poussée.
Utilisateur affecté	Indique le nom de l'utilisateur affecté

COLONNE	DESCRIPTION
Durée de résidence	Indique la durée de présence de la menace sur l'endpoint de l'utilisateur affecté
Ignoré par	Affiche le compte utilisateur Control Manager qui a ignoré l'alerte de menace critique

Widget Hôtes sur lesquels ont été effectuées des tentatives de rappel C&C

Ce widget affiche le total des hôtes compromis individuels et les regroupe par source de liste C&C.

L'affichage par défaut présente les données du jour en cours.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent. Vous pouvez afficher les données datant d'**Aujourd'hui**, de **1 semaine**, de **2 semaines** ou de **1 mois**.

DONNÉES	DESCRIPTION
Hôtes mis en correspondance avec Intelligence globale	Journaux de rappel C&C détectés par le réseau Trend Micro Intelligence globale, y compris Smart Protection Network.
Hôtes mis en correspondance avec les analyseurs dynamiques	Journaux de rappel C&C détectés par les analyseurs dynamiques, y compris Virtual Analyzer et le moteur d'inspection du contenu réseau. Les analyseurs sont intégrés à des produits tels que Deep Discovery Inspector et OfficeScan.

DONNÉES	DESCRIPTION
Hôtes mis en correspondance avec les listes définies par l'utilisateur dans les produits gérés	Journaux de rappel C&C détectés par les produits à l'aide d'une liste définie par l'utilisateur. La Liste des refus disponible dans Deep Discovery Inspector est un exemple de liste définie par l'utilisateur.

Widget Principales menaces de fichiers de Control Manager

Ce widget effectue un suivi de la répartition des principaux fichiers malveillants détectés sur les endpoints du réseau et affiche les résultats de la répartition détectée par le produit en indiquant les 10/25/50 principales menaces de fichiers (virus et spywares/graywares).

Cliquez sur un nœud du graphique pour ouvrir un écran affichant des informations détaillées. Control Manager effectue une requête ad hoc pour fournir les informations détaillées.

Spécifiez la plage de dates relative aux données affichées par le widget :

- 24 heures
- 1 semaine
- 2 semaines
- 1 mois

Spécifiez la menace que doit afficher le widget. Le widget ne peut afficher des données que pour une menace de fichier à la fois. Par défaut, le widget affiche les données de tous les produits gérés auxquels les privilèges du compte de l'utilisateur donnent accès.

Cliquez sur l'icône des paramètres du widget dans le widget pour accéder aux paramètres supplémentaires.

PARAMÈTRE	DESCRIPTION
Titre	Attribuez un nouveau titre pertinent au widget dans le champ.
Étendue	Spécifiez la portée des données affichée par le widget. L'étendue des données détermine les produits utilisés par le widget pour afficher les données.
Principales menaces	Spécifiez le nombre de menaces à afficher.

Cliquez sur **Enregistrer** pour appliquer les modifications et mettre à jour les données du widget.

Widget Hôtes compromis uniques au fil du temps

Ce widget affiche les hôtes compromis individuels enregistrés par les produits gérés au cours des 30 derniers jours.

Ce widget regroupe et affiche les hôtes compromis individuels sous forme de cercles. La taille du cercle représente le nombre relatif d'hôtes compromis.

- Petit : 1 à 5
- Moyen : 6 à 10
- Grand : 11 ou plus

Déplacez le pointeur de la souris sur une icône d'ordinateur ou un nom d'hôte pour afficher des hôtes compromis supplémentaires.

Utilisez la liste déroulante **Adresse de rappel** pour afficher les hôtes compromis ayant effectué des tentatives de rappel de l'adresse de rappel sélectionnée.

Remarque

La liste déroulante **Adresse de rappel** contient les 25 premières adresses de rappel.

Le widget affiche uniquement la première tentative de rappel de l'adresse de rappel à partir d'un hôte compromis.

Modifiez les produits gérés utilisés en tant que source par le widget en cliquant sur l'icône Paramètres (>). Dans la boîte de dialogue qui s'affiche, spécifiez la **Portée** en cliquant sur >> et en sélectionnant les produits gérés à utiliser en tant que source.

État de la stratégie

Ce widget affiche l'état du déploiement de vos stratégies.

Lorsque vous cliquez sur le nom d'une stratégie ou le nombre de cibles, un nouvel écran **Requête sur le journal** s'ouvre pour fournir des informations détaillées.

DONNÉES	DESCRIPTION
Stratégie	Indique le nom de la stratégie.
État du déploiement	Affiche le pourcentage de cibles qui respectent les paramètres de la stratégie
Déployé	Affiche le nombre de cibles qui ont appliqué les paramètres de la stratégie ou qui possèdent des services produit non activés.
En attente	Affiche le nombre de cibles qui ne respectent pas les paramètres de la stratégie **Remarque** Si le correctif 2575 n'est pas installé, la colonne **En attente** inclut le nombre de cibles qui possèdent des agents hors ligne.

DONNÉES	DESCRIPTION
Hors ligne	Affiche le nombre de cibles qui possèdent des agents hors ligne **Important** Cette fonction nécessite l'installation du correctif 2575. Sinon, la colonne **En attente** inclut le nombre de cibles qui possèdent des agents hors ligne et la colonne **Hors-ligne** ne s'affiche pas.
Avec problèmes	Affiche le nombre de cibles qui n'ont pas appliqué les paramètres de la stratégie pour les raisons suivantes : déploiement de la stratégie non pris en charge, stratégie non configurée, erreurs système, erreurs de communication de l'endpoint avec le serveur du produit, endpoints non pris en charge, paramètres modifiés en local, services des produits désactivés ou déploiement partiel.
Points finaux/ produits sans stratégie	Affiche le nombre d'endpoints ou de produits gérés sans aucune stratégie appliquée
Nombre de points finaux/produits totaux	Affiche le nombre d'endpoints ou de produits gérés que l'administrateur peut gérer

Lancement rapide

Ce widget affiche les raccourcis vers le **Répertoire produits** et la **Gestion des stratégies**.

Partie XIV

Widgets Smart Protection Server

Chapitre 31

Widgets Smart Protection Server

Cette section contient des rubriques d'aide concernant tous les widgets Smart Protection Server qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Utilisateurs actifs pour File Reputation à la page 31-2*
- *Utilisateurs actifs pour la réputation de sites Web à la page 31-2*
- *Rapport sur le trafic HTTP pour File Reputation à la page 31-3*
- *Rapport sur le trafic HTTP pour la réputation de sites Web à la page 31-3*
- *État en temps réel à la page 31-4*
- *10 premiers ordinateurs infectés pour File Reputation à la page 31-5*
- *10 premiers ordinateurs bloqués pour la réputation de sites Web à la page 31-6*

Utilisateurs actifs pour File Reputation

Le widget Utilisateurs actifs affiche le nombre d'utilisateurs ayant envoyé des requêtes File Reputation au serveur Smart Protection Server. Chaque ordinateur client unique est considéré comme un utilisateur actif.

Remarque

Ce widget affiche les informations sous forme de graphique en 2D mis à jour toutes les heures ; vous pouvez également cliquer sur l'icône d'actualisation () à tout moment pour mettre à jour les données.

TABLEAU 31-1. Données du widget

DONNÉES	DESCRIPTION
Utilisateurs	Nombre d'utilisateurs ayant envoyé des requêtes aux ordinateurs Smart Protection Server.
Date	Date de la requête.

Utilisateurs actifs pour la réputation de sites Web

Le widget Utilisateurs actifs indique le nombre d'utilisateurs ayant envoyé des requêtes de Web Reputation au serveur Smart Protection Server. Chaque ordinateur client unique est considéré comme un utilisateur actif.

Remarque

Ce widget affiche les informations sous forme de graphique en 2D mis à jour toutes les 5 minutes ; vous pouvez également cliquer sur l'icône d'actualisation () à tout moment pour mettre à jour les données.

TABLEAU 31-2. Données du widget

DONNÉES	DESCRIPTION
Utilisateurs	Nombre d'utilisateurs ayant envoyé des requêtes aux ordinateurs Smart Protection Server.
Date	Date de la requête.

Rapport sur le trafic HTTP pour File Reputation

Le widget Rapport sur le trafic HTTP affiche le trafic réseau total en kilo-octets (Ko) envoyé vers le serveur Smart Protection Server à partir des requêtes File Reputation générées par les clients. Les informations de ce widget sont mises à jour toutes les heures. Vous pouvez également cliquer sur l'icône d'actualisation ( ) à tout moment pour mettre à jour les données.

TABLEAU 31-3. Données du widget

DONNÉES	DESCRIPTION
Trafic (Ko)	Trafic réseau généré par les requêtes.
Date	Date des requêtes.

Rapport sur le trafic HTTP pour la réputation de sites Web

Le widget Rapport sur le trafic HTTP affiche le trafic réseau total en kilo-octets (Ko) envoyé vers le serveur Smart Protection Server à partir des requêtes de Web Reputation générées par les clients. Les informations de ce widget sont mises à jour toutes les heures. Vous pouvez également cliquer sur l'icône d'actualisation ( ) à tout moment pour mettre à jour les données.

TABLEAU 31-4. Données du widget

DONNÉES	DESCRIPTION
Trafic (Ko)	Trafic réseau généré par les requêtes.
Date	Date des requêtes.

État en temps réel

Le widget État en temps réel permet de surveiller l'état du serveur Smart Protection Server.

Remarque

Lorsque ce widget s'affiche sur l'écran Résumé, la session de la console du produit n'expire pas. L'état de l'ordinateur est mis à jour toutes les minutes ; de ce fait, la session n'expire pas en raison des demandes envoyées au serveur. Cependant, la session arrivera à expiration si l'onglet actuellement affiché ne contient pas ce widget.

TABLEAU 31-5. Données du widget

DONNÉES	DESCRIPTION
Service	Services proposés par Smart Protection Server.
Protocole	Cette option permet d'afficher les protocoles pris en charge par les services. Le service File Reputation prend en charge les protocoles HTTP et HTTPS. Le service de réputation de sites Web prend en charge le protocole HTTP. HTTPS assure une connexion plus sûre alors que HTTP utilise moins de bande passante.
Hôte	Adresses des services de réputation de sites Web et File Reputation. Ces adresses sont utilisées avec les produits Trend Micro qui prennent en charge les ordinateurs Smart Protection Server. Elles permettent de configurer les connexions aux ordinateurs Smart Protection Server.

DONNÉES	DESCRIPTION
État de l'ordinateur	Les éléments suivants s'affichent sous État de fonctionnement : • **Requête File Reputation** : indique si File Reputation fonctionne comme prévu. • **Requête de réputation de sites Web** : indique si le service de réputation de sites Web fonctionne comme prévu. • **ActiveUpdate** : indique si ActiveUpdate fonctionne comme prévu. • **Charge moyenne de l'UC** : indique la charge moyenne de l'ordinateur générée par le noyau pour les 1, 5 et 15 minutes précédentes. • **Mémoire disponible** : indique la quantité de mémoire physique disponible sur l'ordinateur. • **Utilisation du changement de disque** : indique l'utilisation du changement de disque. • **Espace disponible** : indique l'espace disque disponible sur l'ordinateur.

10 premiers ordinateurs infectés pour File Reputation

Ce widget affiche la liste des adresses IP des 10 ordinateurs répertoriés comme étant les plus infectés après que Smart Protection Server a reçu un virus connu à partir d'une requête de réputation de fichiers. Les informations de ce widget sont affichées dans un tableau, qui inclut l'adresse IP des ordinateurs et le nombre total de détections sur chacun d'eux. Ces informations sont mises à jour toutes les heures. Vous pouvez également cliquer sur l'icône d'actualisation ( ) à tout moment pour mettre à jour les données.

Ce widget permet de suivre les ordinateurs les plus infectés de votre réseau.

Remarque

Si vous activez plusieurs serveurs Smart Protection Server dans ce widget, ce dernier calculera le nombre total de détections sur le serveur Smart Protection Server sélectionné et affichera la liste des 10 ordinateurs les plus infectés selon les ordinateurs Smart Protection Server sélectionnés dans la liste.

TABLEAU 31-6. Données du widget

DONNÉES	DESCRIPTION
IP	Adresse IP de l'ordinateur.
Détections	Nombre de menaces de sécurité détectées par cet ordinateur.

10 premiers ordinateurs bloqués pour la réputation de sites Web

Ce widget affiche la liste des adresses IP des 10 ordinateurs répertoriés comme étant les plus bloqués après que Smart Protection Server a reçu une URL pour une requête de réputation de sites Web. Les informations de ce widget sont affichées dans un tableau, qui inclut l'adresse IP des ordinateurs et le nombre total d'URL bloquées sur chacun d'eux. Ces informations sont mises à jour tous les jours. Vous pouvez également cliquer sur l'icône d'actualisation ( ) à tout moment pour mettre à jour les données.

Ce widget permet de suivre les ordinateurs comportant le plus grand nombre d'URL bloquées de votre réseau.

Remarque

Si vous activez plusieurs serveurs Smart Protection Server dans ce widget, ce dernier calculera le nombre total de détections sur le serveur Smart Protection Server sélectionné et affichera la liste des 10 ordinateurs les plus bloqués selon les ordinateurs Smart Protection Server sélectionnés dans la liste.

TABLEAU 31-7. Données du widget

DONNÉES	DESCRIPTION
IP	Adresse IP de l'ordinateur.
Détections	Nombre d'URL bloquées sur cet ordinateur

Partie XV

Widgets Virtual Mobile Infrastructure

Chapitre 32

Widgets Virtual Mobile Infrastructure

Cette section contient des rubriques d'aide concernant tous les widgets Virtual Mobile Infrastructure qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget 5 principales applications lancées d'après Trend Micro Virtual Mobile Infrastructure à la page 32-2*
- *Widget 5 principales applications Web lancées d'après Trend Micro Virtual Mobile Infrastructure à la page 32-2*
- *Widget 5 principaux utilisateurs en ligne d'après Trend Micro Virtual Mobile Infrastructure à la page 32-3*
- *Widget État de l'utilisation des processeurs des serveurs Trend Micro Virtual Mobile Infrastructure à la page 32-3*
- *Widget État de l'utilisation des disques des serveurs Trend Micro Virtual Mobile Infrastructure à la page 32-4*
- *État de l'utilisation de la mémoire des serveurs Trend Micro Virtual Mobile Infrastructure à la page 32-4*
- *Widget État des utilisateurs de Trend Micro Virtual Mobile Infrastructure à la page 32-5*

Widget 5 principales applications lancées d'après Trend Micro Virtual Mobile Infrastructure

Ce widget affiche les cinq applications les plus lancées signalées par les serveurs Trend Micro Virtual Mobile Infrastructure.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom de l'application et l'axe X représente le nombre de lancements de l'application.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget 5 principales applications Web lancées d'après Trend Micro Virtual Mobile Infrastructure

Ce widget affiche les cinq applications Web les plus lancées signalées par les serveurs Trend Micro Virtual Mobile Infrastructure.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom de l'application et l'axe X représente le nombre de lancements de l'application.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget 5 principaux utilisateurs en ligne d'après Trend Micro Virtual Mobile Infrastructure

Ce widget affiche les cinq utilisateurs les plus actifs avec les temps de connexion à l'espace de travail les plus longs selon les serveurs Trend Micro Virtual Mobile Infrastructure.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom d'utilisateur et l'axe X représente le temps de connexion de l'utilisateur à son espace de travail en minutes.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État de l'utilisation des processeurs des serveurs Trend Micro Virtual Mobile Infrastructure

Ce widget affiche l'utilisation des processeurs des serveurs Trend Micro Virtual Mobile Infrastructure.

Les données sont représentées dans un graphique. L'axe Y représente l'utilisation du processeur en pourcentage, tandis que l'axe X représente l'heure à laquelle l'utilisation du processeur a été enregistrée.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État de l'utilisation des disques des serveurs Trend Micro Virtual Mobile Infrastructure

Ce widget affiche l'utilisation des disques des serveurs Trend Micro Virtual Mobile Infrastructure.

Les données suivantes sont représentées dans un graphique circulaire :

- **Disponible** : espace disque disponible sur le serveur géré.
- **Utilisé** : espace disque utilisé sur le serveur géré.
- **Total** : espace disque total sur le serveur géré.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

État de l'utilisation de la mémoire des serveurs Trend Micro Virtual Mobile Infrastructure

Ce widget affiche l'utilisation de la mémoire des serveurs Trend Micro Virtual Mobile Infrastructure.

Les données suivantes sont représentées dans un graphique circulaire :

- **Disponible** : espace mémoire disponible sur le serveur géré.
- **Utilisé** : espace mémoire utilisé sur le serveur géré.
- **Total** : espace mémoire total sur le serveur géré.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État des utilisateurs de Trend Micro Virtual Mobile Infrastructure

Ce widget affiche l'état actuel des utilisateurs indiqué par les serveurs Trend Micro Mobile Virtual Infrastructure.

L'état actuel des utilisateurs est représenté dans un graphique circulaire :

- **Actif** : l'utilisateur est actuellement connecté au serveur et accède à l'espace de travail.
- **Inactif** : l'utilisateur est connecté au serveur et n'accède actuellement pas à l'espace de travail.
- **Hors ligne** : l'utilisateur est déconnecté du serveur.
- **Désactivé** : le compte utilisateur a été désactivé et l'utilisateur ne peut pas accéder au serveur.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Partie XVI

Widgets Vulnerability Protection Manager

Chapitre 33

Widgets Vulnerability Protection

Cette section contient des rubriques d'aide concernant tous les widgets Vulnerability Protection qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget Vulnerability Protection – Activité du type d'applications (détection) à la page 33-2*
- *Widget Vulnerability Protection – Activité du type d'applications (prévention) à la page 33-3*
- *Widget Résumé des fonctions Vulnerability Protection à la page 33-4*
- *Widget Vulnerability Protection – Historique des événements du pare-feu à la page 33-5*
- *Widget Vulnerability Protection – Historique des événements de prévention contre les intrusions à la page 33-6*
- *Widget Vulnerability Protection – Activité de l'IPS (détection) à la page 33-6*
- *Widget Vulnerability Protection – Activité de l'IPS (prévention) à la page 33-7*
- *Widget Vulnerability Protection – Indicateur de performance clé à la page 33-8*
- *Widget Vulnerability Protection – Historique des événements du scan de reconnaissance à la page 33-9*
- *Widget Vulnerability Protection – Récapitulatif de l'état à la page 33-10*
- *Widget Vulnerability Protection – Endpoints vulnérables à la page 33-11*

Widget Vulnerability Protection – Activité du type d'applications (détection)

Ce widget effectue un suivi des types d'application associés aux événements de détection IPS sur l'endpoint.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Vulnerability Protection. Pour surveiller plusieurs serveurs Vulnerability Protection, créez un widget pour chacun d'eux.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de détection IPS associés à un type d'application spécifique, cliquez sur une valeur dans la colonne **Totaux**.

DONNÉES	DESCRIPTION
Nom du type d'application	Nom du type d'application
Total	Nombre d'événements dans la plage de temps et pourcentage du nombre total d'événements de ce type que cela représente

DONNÉES	DESCRIPTION
Total précédent	Nombre d'événements dans la plage de temps précédent la plage de temps actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Vulnerability Protection – Activité du type d'applications (prévention)

Ce widget effectue un suivi des types d'application associés aux événements de prévention IPS sur l'endpoint.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Vulnerability Protection. Pour surveiller plusieurs serveurs Vulnerability Protection, créez un widget pour chacun d'eux.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de prévention IPS associés à un type d'application spécifique, cliquez sur une valeur dans la colonne **Totaux**.

DONNÉES	DESCRIPTION
Nom du type d'application	Nom du type d'application
Total	Nombre d'événements dans la plage de temps et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la plage de temps précédent la plage de temps actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Résumé des fonctions Vulnerability Protection

Ce widget présente l'activité récente de tous les modules Vulnerability Protection.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Conseil

Ce widget peut afficher des données agrégées provenant de plusieurs installations Vulnerability Protection. Les installations Vulnerability Protection représentées dans ce widget sont définies dans l'écran **Enregistrement du serveur**. Pour surveiller plusieurs installations Vulnerability Protection individuellement, créez un widget pour chacune d'elles.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Utilisez la liste déroulante **Intervalle** pour sélectionner la période des données qui s'affichent.

DONNÉES	DESCRIPTION
Module	Nom du module Vulnerability Protection
Ordinateurs protégés	Nombre actuel d'ordinateurs gérés protégés par le module et pourcentage de tous les ordinateurs gérés que cela représente.
Nombre d'événements	Nombre d'événements générés par le module au cours de la période spécifiée
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Vulnerability Protection – Historique des événements du pare-feu

Ce widget affiche le nombre d'événements du pare-feu qui se produisent pendant un intervalle de temps spécifié. Le graphique affiche les événements déclenchés par les règles de pare-feu en mode de détection et de prévention.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de pare-feu (détection ou prévention) dans l'intervalle de temps sélectionné, cliquez sur une section du graphique à barres.

Widget Vulnerability Protection – Historique des événements de prévention contre les intrusions

Ce widget affiche le nombre d'événements IPS ayant eu lieu pendant l'intervalle de temps spécifié. Le graphique affiche les événements déclenchés par les règles IPS en mode de détection et de prévention.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements IPS (détection ou prévention) dans un intervalle de temps spécifique, cliquez sur une section du graphique à barres.

Widget Vulnerability Protection – Activité de l'IPS (détection)

Ce widget affiche les cinq règles de l'IPS fonctionnant en mode de détection qui ont déclenché le plus grand nombre d'événements.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de détection IPS déclenchés par une règle spécifique, cliquez sur une valeur dans la colonne **Totaux**.

Données	Description
Raison	Nom de la règle
Total	Nombre d'événements dans la plage de temps et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la plage de temps précédent la plage de temps actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Vulnerability Protection – Activité de l'IPS (prévention)

Ce widget affiche les cinq règles de l'IPS fonctionnant en mode de prévention qui ont déclenché le plus grand nombre d'événements.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de prévention IPS déclenchés par une règle spécifique, cliquez sur une valeur dans la colonne **Totaux**.

DONNÉES	DESCRIPTION
Raison	Nom de la règle
Total	Nombre d'événements dans la plage de temps et pourcentage du nombre total d'événements de ce type que cela représente
Total précédent	Nombre d'événements dans la plage de temps précédent la plage de temps actuelle
Tendance	Modification du pourcentage entre la période précédente et la période actuelle

Widget Vulnerability Protection – Indicateur de performance clé

Ce widget affiche le nombre d'événements déclenchés par les paramètres de détection du scan de reconnaissance ayant eu lieu pendant un intervalle de temps spécifié.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de détection du scan de reconnaissance dans un intervalle de temps spécifique, cliquez sur une section du graphique à barres.

Widget Vulnerability Protection – Historique des événements du scan de reconnaissance

Ce widget affiche le nombre d'événements déclenchés par les paramètres de détection du scan de reconnaissance ayant eu lieu pendant un intervalle de temps spécifié.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour afficher la page **Événements** de Vulnerability Protection Manager filtrée de façon à afficher les événements de détection du scan de reconnaissance dans un intervalle de temps spécifique, cliquez sur une section du graphique à barres.

Widget Vulnerability Protection – Récapitulatif de l'état

Ce widget affiche le nombre d'alertes critiques et d'alertes d'avertissement, ainsi qu'un graphique circulaire indiquant le pourcentage d'endpoints présentant un état particulier.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Conseil

Ce widget peut afficher des données agrégées provenant de plusieurs installations Vulnerability Protection. Les installations Vulnerability Protection représentées dans ce widget sont définies dans l'écran **Enregistrement du serveur**. Pour surveiller plusieurs installations Vulnerability Protection individuellement, créez un widget pour chacune d'elles.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

ÉTAT DE L'ORDINATEUR	DESCRIPTION
Géré (vert)	Protégé et sans erreurs ou avertissements
Non géré (bleu)	Non protégé
Verrouillé (gris)	Verrouillé. Lorsqu'un ordinateur est à l'état verrouillé, Vulnerability Protection Manager ne communique pas avec l'agent/appliance ou ne génère aucune alerte associée à cet ordinateur.

ÉTAT DE L'ORDINATEUR	DESCRIPTION
Critique (rouge)	À l'état d'erreur
Avertissement (jaune)	À l'état d'avertissement

Widget Vulnerability Protection – Endpoints vulnérables

Utilisez ce widget afin de suivre les endpoints vulnérables.

Vous pouvez choisir l'installation Protection Vulnerability à utiliser comme source de données pour ce widget. Pour sélectionner la source de données, cliquez sur l'icône Paramètres (>) et sélectionnez la source dans la liste prévue à cet effet.

Conseil

Ce widget ne peut afficher que des données provenant d'un seul serveur Vulnerability Protection. Pour surveiller plusieurs serveurs Vulnerability Protection, créez un widget pour chacun d'eux.

Pour mettre une installation Vulnerability Protection à la disposition des widgets Vulnerability Protection, accédez à **Administration** > **Serveurs gérés** > **Enregistrement du serveur** et ajoutez un serveur Vulnerability Protection.

Remarque

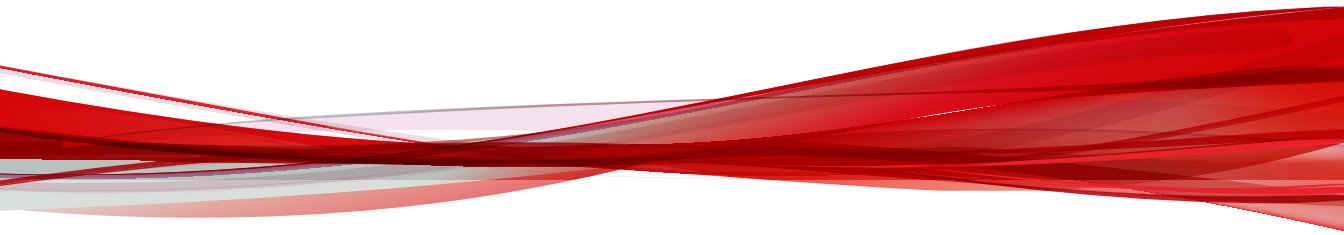
Les données affichées dans les widgets sont restreintes aux actions autorisées par les privilèges du compte utilisateur.

Pour faire apparaître la page des propriétés de règle de Vulnerability Protection Manager, qui affiche les endpoints corrigés virtuellement ou non protégés, cliquez sur une valeur dans les colonnes **Corrigé virtuellement/Non protégé**.

DONNÉES	DESCRIPTION
Nom	Nom de la règle de prévention contre les intrusions
Gravité	Niveau de gravité de la règle de prévention contre les intrusions
CVE	Numéro CVE (failles de sécurité et expositions communes)
Score CVSS	Mesure de la gravité de la faille de sécurité selon la National Vulnerability Database (base de données du gouvernement américain concernant la gestion de données vulnérables)
MS ID	Microsoft Security Patch ID
Corrigé virtuellement	Nombre d'endpoints qui seront assignés à la règle après le scan pour des recommandations
Non protégé	Nombre d'endpoints qui ne seront pas assignés à la règle après le scan pour des recommandations

Partie XVII

Widgets Safe Mobile Workforce



Chapitre 34

Widgets Safe Mobile Workforce

Cette section contient des rubriques d'aide concernant tous les widgets Safe Mobile Workforce qui sont pris en charge dans Control Manager.

Les rubriques sont les suivantes:

- *Widget État de l'utilisation de l'unité centrale des serveurs Safe Mobile Workforce à la page 34-2*
- *Widget État de l'utilisation de la mémoire des serveurs Safe Mobile Workforce à la page 34-2*
- *Widget État de l'utilisation du disque des serveurs Safe Mobile Workforce à la page 34-2*
- *Widget État des utilisateurs Safe Mobile Workforce à la page 34-3*
- *Widget 5 principales applications lancées Safe Mobile Workforce à la page 34-4*
- *Widget 5 principales applications Web lancées Trend Micro Safe Mobile Workforce à la page 34-4*
- *Widget 5 principaux utilisateurs en ligne Safe Mobile Workforce à la page 34-4*

Widget État de l'utilisation de l'unité centrale des serveurs Safe Mobile Workforce

Ce widget indique l'utilisation des processeurs des serveurs Safe Mobile Workforce.

Les données sont représentées dans un graphique. L'axe Y représente l'utilisation du processeur en pourcentage, tandis que l'axe X représente l'heure à laquelle l'utilisation du processeur a été enregistrée.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État de l'utilisation de la mémoire des serveurs Safe Mobile Workforce

Ce widget indique l'utilisation de la mémoire des serveurs Safe Mobile Workforce.

Les données suivantes sont représentées dans un graphique circulaire :

- **Disponible** : espace mémoire disponible sur le serveur géré.
- **Utilisé** : espace mémoire utilisé sur le serveur géré.
- **Total** : espace mémoire total sur le serveur géré.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État de l'utilisation du disque des serveurs Safe Mobile Workforce

Ce widget indique l'utilisation du disque des serveurs Safe Mobile Workforce.

Les données suivantes sont représentées dans un graphique circulaire :

- **Disponible** : espace disque disponible sur le serveur géré.
- **Utilisé** : espace disque utilisé sur le serveur géré.
- **Total** : espace disque total sur le serveur géré.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget État des utilisateurs Safe Mobile Workforce

Ce widget affiche l'état actuel des utilisateurs indiqué par les serveurs Safe Mobile Workforce.

L'état actuel des utilisateurs est représenté dans un graphique circulaire :

- **Actif** : l'utilisateur est actuellement connecté au serveur et accède à l'espace de travail.
- **Inactif** : l'utilisateur est connecté au serveur et n'accède actuellement pas à l'espace de travail.
- **Hors ligne** : l'utilisateur est déconnecté du serveur.
- **Désactivé** : le compte utilisateur a été désactivé et l'utilisateur ne peut pas accéder au serveur.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget 5 principales applications lancées Safe Mobile Workforce

Ce widget affiche les cinq applications les plus lancées signalées par les serveurs Safe Mobile Workforce.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom de l'application et l'axe X représente le nombre de lancements de l'application.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget 5 principales applications Web lancées Trend Micro Safe Mobile Workforce

Ce widget affiche les cinq applications Web les plus lancées signalées par les serveurs Safe Mobile Workforce.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom de l'application et l'axe X représente le nombre de lancements de l'application.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Widget 5 principaux utilisateurs en ligne Safe Mobile Workforce

Ce widget affiche les cinq utilisateurs les plus actifs avec les temps de connexion à l'espace de travail les plus longs selon les serveurs Safe Mobile Workforce.

Les données sont représentées dans un graphique à barres. L'axe Y représente le nom d'utilisateur et l'axe X représente le temps de connexion de l'utilisateur à son espace de travail en minutes.

Modifiez le serveur géré utilisé en tant que source par le widget en cliquant sur le menu déroulant. Dans les options du menu déroulant, sélectionnez l'adresse IP du serveur géré à utiliser en tant que source.

Index

A

actions
    Prévention contre la perte de données, 19-11, 24-5
action sur les événements système surveillés, 13-8
ActiveAction, 14-38
Active Directory
    importer des utilisateurs, 5-8
affichage des autorisations, 2-13
Agent de mise à jour, 12-20
agent OfficeScan
    fichiers, 12-14
Agent OfficeScan
    clés de registre, 12-15
agent OfficeScan agent
    processus, 12-15
à propos de
    authentification, 6-2
attributs de fichier, 2-28, 2-34–2-36
    caractères génériques, 2-35
    création, 2-35
    importation, 2-36
authentification
    à propos de, 6-2
autoprotection de l'agent, 12-14
Autorisations
    nom et chemin d'accès du programme, 17-9
    périphériques de stockage, 17-6

B

Blocage des comportements des programmes malveillants, 13-2

C

Cache de signature numérique, 12-17
canaux réseau, 19-7, 19-8, 19-14, 19-15, 19-17
    cibles contrôlées, 19-14
    cibles non contrôlées, 19-14
    clients de messagerie, 19-8
    étendue de transmission
        toutes les transmissions, 19-15
        transmissions externes, 19-17
    étendue et cible de transmission, 19-7
canaux système et application, 19-10
caractères génériques, 2-35
    attributs de fichier, 2-35
    contrôle des dispositifs, 17-10
changement de la définition des autorisations, 2-13
cibles, 2-23, 6-7
    avec des problèmes, 2-24
    déployé, 2-23
    en attente, 2-23, 6-7
    filtrer par critères, 2-3
    hors ligne, 2-24
    navigation, 2-10
cibles avec problèmes, 2-24
cibles contrôlées, 19-16, 19-17
cibles de la stratégie, 2-23, 6-7
cibles déployées, 2-23
cibles en attente, 2-23, 6-7
cibles hors ligne, 2-24
cibles non contrôlées, 19-15, 19-17
composants
    sur l'agent de mise à jour, 12-20
contrôle des dispositifs, 17-2, 17-6, 17-9, 17-10
    Autorisations, 17-6, 17-9

nom et chemin d'accès du programme, 17-9
caractères génériques, 17-10
configuration requise, 17-2
Fournisseur de Digital Signature, 17-10
périphériques de stockage, 17-6
contrôle des performances, 26-18, 26-26
Control Manager
intégration à Trend Micro Endpoint Sensor, 28-2
stratégies, 6-1
copie des paramètres de stratégie, 2-14
création de stratégies, 2-2, 2-18
copie des paramètres, 2-14
définition des autorisations, 2-13
Paramètres, 2-3
critères
expressions personnalisées, 2-30–2-32
mots-clés, 2-39, 2-40
critères de scan
action des utilisateurs sur les fichiers, 26-9
fichiers à scanner, 26-24
programmation, 26-24
Utilisation du processeur, 26-18, 26-26

D

Data Discovery, 21-2
création de stratégies, 21-2
déclarations de condition, 2-44
définition des autorisations, 2-13
désinstallation
utilisation du programme de désinstallation, 12-9
Digital Signature Pattern, 12-17
documentation, xvi
domaines de messagerie, 19-8
domaines de messagerie non contrôlés, 19-8
DSP, 17-10

E

envoyer une alerte par e-mail, 11-38
événements du système surveillés, 13-6
exclusions de scan, 14-50
expressions, 2-28
personnalisé, 2-30, 2-33
critères, 2-30–2-32
prédéfinies, 2-29
expressions personnalisées, 2-30–2-33
critères, 2-30–2-32
importation, 2-33
Expressions prédéfinies, 2-29
affichage, 2-29
Expressions rationnelles compatibles Perl (PCRE - Perl Compatible Regular Expressions), 2-30

F

fichiers compressés
règles de décompression, 19-18
filtrage des appels
configuration des listes pour le filtrage, 11-19
format des listes pour le filtrage, 11-21
filtrer par critères, 2-3
Fournisseur de Digital Signature, 17-10
spécification, 17-10

G

gestion des stratégies, 2-1, 2-2, 6-7
cibles, 2-23, 6-7
cibles avec problèmes, 2-24
cibles déployées, 2-23
cibles en attente, 2-23, 6-7

cibles hors ligne, 2-24
copie des paramètres de stratégie, 2-14
création de stratégies, 2-2, 2-18
définition, 2-2, 6-7
définition des autorisations, 2-13
liste des stratégies, 2-7, 2-21, 6-6
mise à niveau des modèles de stratégies, 2-26
modification des propriétaires, 2-20
modification des stratégies, 2-16
Paramètres, 2-3
Prévention contre la perte de données, 2-27
priorité de la stratégie, 2-9, 2-22, 6-6, 6-10
propriétaire, 2-24
réorganisation des stratégies, 2-25
stratégies d'ébauche, 2-3, 6-10
stratégies filtrées, 6-10
stratégies spécifiées, 2-3, 6-10
suppression des stratégies, 2-19

I

Identificateurs de données, 2-28
attributs de fichier, 2-28
expressions, 2-28
mots-clés, 2-28
IntelliScan, 26-24

L

liste approuvée, 18-2
liste d'exceptions, 13-9
Surveillance des comportements, 13-9
liste des programmes approuvés, 13-9
liste des programmes bloqués, 13-9
liste des stratégies, 2-7, 2-21, 6-6

M

Mémoire cache du scan, 12-16
Mémoire cache du scan à la demande, 12-18
menaces Web
configuration des listes pour le filtrage, 11-22
contenu réservé aux adultes, 11-23
format des listes pour le filtrage, 11-23, 11-24
sites web spécifiques uniquement, 11-23
méthodes de scan
changement de méthodes de scan, 14-2
scan traditionnel, 14-2
smart scan, 14-2
mise à niveau des modèles de stratégies, 2-26
mises à jour
Agent de mise à jour, 12-20
modèles, 2-42–2-46
déclarations de condition, 2-44
Opérateurs logiques, 2-44
personnalisé, 2-43, 2-45, 2-46
prédéfinies, 2-43
modèles de stratégies, 2-26
modèles personnalisés, 2-43
création, 2-45
importation, 2-46
modèles prédéfinis, 2-43
modification des stratégies, 2-16
mots-clés, 2-28, 2-36
personnalisé, 2-38–2-40, 2-42
prédéfinies, 2-37
mots-clés personnalisés, 2-38
critères, 2-39, 2-40
importation, 2-42
Mots-clés prédéfinis
distance, 2-37
nombre de mots-clés, 2-37

N

navigation dans les cibles, 2-10

O

onglet Conformité, 1-37
onglet détection des menaces, 1-45
onglet Résumé, 1-16
onglets, 1-2
    conformité, 1-37
    détection des menaces, 1-45
    résumé, 1-16
    widgets, 1-2
Opérateurs logiques, 2-44
Outil Liste de dispositifs, 19-10

P

paramètres de stratégie
    copie, 2-14
Paramètres du cache pour les scans, 12-16
PCRE, 2-30
périphériques
    verrouiller, 6-25
    Widget Périphériques Endpoint Encryption, 5-10
périphériques de stockage
    Autorisations, 17-6
portée du produit
    widgets, 1-6
prévention contre la perte de données
    canaux réseau, 19-8, 19-15, 19-17
    canaux système et application, 19-10
Prévention contre la perte de données, 2-27, 2-28, 19-2
    actions, 19-11, 24-5
    attributs de fichier, 2-34–2-36
    canaux réseau, 19-7, 19-14
    expressions, 2-28–2-33
    Identificateurs de données, 2-28
    modèles, 2-42–2-46
    mots-clés, 2-36–2-40, 2-42
    règles de décompression, 19-18
    stratégies, 24-2, 24-4–24-7
        actions, 24-5
        activation, 24-7
        cibles, 24-4
        création, 24-2
        nom et priorité, 24-7
        notification, 24-6
        sélection de comptes, 24-2
Prévention contre la perte de données (DLP), 2-27
priorité de la stratégie, 2-22, 6-6
Prise en charge IPv6
    limitations, 26-39
privilèges
    privilège de déchargement, 12-8
    privilèges du scan de courrier, 12-19
Protection des données, 19-2

R

règles de décompression, 19-18
réorganisation des stratégies, 2-25
répertoire de quarantaine, 14-41
réputation de sites Web, 26-41

S

scan anti-spywares/graywares
    liste approuvée, 18-2
scan de la messagerie, 12-19
Scan en temps réel, 14-13
Scan immédiat, 14-22
Scan manuel, 14-5
Scan programmé, 14-29
scan traditionnel, 26-3, 26-4

basculement vers smart scan, 26-4
sélection de cibles
filtrer par critères, 2-3
smart scan, 26-3, 26-4
basculement du scan traditionnel, 26-4
sous-domaines de messagerie contrôlés, 19-9
spam
SMS, 11-16
configuration des listes pour le filtrage, 11-16
format des listes pour le filtrage, 11-17
WAP Push, 11-18
format de liste approuvée, 11-18
spécifier les cibles
navigation, 2-10
stratégie de conformité
liste de contrôle, 11-35
stratégie générale
fonctions de désinstallation de la protection, 11-5
paramètres de journaux, 11-6
paramètres de mise à jour, 11-6
stratégies, 6-1
commun, 6-22
création, 2-2, 2-18
Data Discovery, 21-2
File Encryption, 6-19
Full Disk Encryption, 6-16
modification, 2-16
réorganisation, 2-25
suppression, 2-19
utilisateur, 6-13
stratégies d'ébauche, 2-3, 6-10
stratégies filtrées, 6-10
réorganisation, 2-25
stratégies spécifiées, 2-3, 6-10
priorité, 2-9, 6-10
suppression des stratégies, 2-19
Surveillance des comportements
action sur les événements système, 13-8
liste d'exceptions, 13-9
Surveillance des événements, 13-6

T

tableau de bord, 5-1
onglets, 1-2
ajout, 1-2
diaporama, 1-2
renommer, 1-2
résumé, 1-16
suppression, 1-3
widgets, 1-2
ajout, 1-4
déplacement, 1-4
modification de la portée du produit, 1-6
terminologie, xviii
types de scan, 26-8
types de stratégies
ébauche, 2-3, 6-10
filtré, 6-10
priorité de la stratégie, 2-22, 6-6
réorganisation des stratégies, 2-25
spécifié, 2-3, 6-10

U

utilisateurs, 6-3
importer depuis AD, 5-8
verrouillage, 6-25
Utilisation du processeur, 26-18, 26-26

W

Web Reputation, 15-2

widgets, 1-2
Connexion d'utilisateur infructueuse à Endpoint Encryption, 5-21
Connexion de périphérique infructueuse à Endpoint Encryption, 5-19
e-mails contenant des menaces avancées, 3-3
État d'Endpoint Encryption, 5-16
principaux destinataires de messages électroniques contenant des menaces avancées, 3-3
Rapport sur les violations de la sécurité d'Endpoint Encryption, 5-25
Verrouillage de périphériques d'Endpoint Encryption, 5-23

TREND MICRO INCORPORATED

Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France

Tél. : +33 (0) 1 76 68 65 00 sales@trendmicro.fr

www.trendmicro.com

Item Code: CMFM78128/171226