TREND MICRO™

6.0 TREND MICRO™ Control Manager

Service Pack 3

Tour d'horizon des défenses contre les menaces connectées

Gestion centralisée de la sécurité pour l'entreprise

N° de référence du document : CMFM67185/150909

Date de publication : juillet 2015

Protégé par les brevets américains n° 5,623,600; 5,889,943; 5,951,698 et 6,119,165

La documentation utilisateur pour Trend Micro Control Manager présente les fonctions principales du logiciel et les instructions d'installation pour votre environnement de production. Lisez attentivement ce manuel avant d'installer ou d'utiliser le logiciel.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du logiciel dans le fichier d'aide en ligne et dans la Base de connaissances en ligne sur le site Web de Trend Micro.

Trend Micro cherche toujours 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.

Veuillez évaluer cette documentation sur le site Web suivant :

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

À propos de la défense contre les menaces connectées

DÉFENSE CONTRE LES MENACES CONNECTÉES

Control Manager rassemble un grand nombre de produits et solutions Trend Micro pour vous aider à détecter, à analyser et à répondre aux attaques ciblées et aux menaces avancées avant qu'elles ne provoquent des dommages durables.

En savoir plus :

Intégration de produits relatifs à la défense contre les menaces connectées

Objets suspects et fichiers IOC

Les attaques ciblées et les menaces avancées sont conçues pour contourner la protection de votre réseau en évitant les défenses de sécurité existantes.

Control Manager facilite l'investigation des attaques ciblées et des menaces avancées à l'aide de :

- **Objets suspects** : fichiers, adresses IP, domaines ou URL pouvant potentiellement exposer des systèmes au danger ou à des pertes
- **Fichiers IOC** : décrivent des indicateurs de compromis (IOC) identifiés sur un hôte ou un réseau. Les fichiers IOC aident les administrateurs et les investigateurs à analyser et à interpréter les données de menaces de façon cohérente.

En savoir plus :

- *Processus de gestion et de traitement des objets suspects*
- *Gestion des IOC*

Isolation d'endpoint

Vous pouvez isoler les endpoints menacés pour exécuter une investigation et résoudre les problèmes de sécurité.

En savoir plus :

Isolation des endpoints

Surveillance améliorée des menaces de sécurité

Utilisez les widgets suivants sous l'onglet **Résumé** pour surveiller la sécurité du réseau et pour répondre aux menaces les plus critiques :

- Menaces critiques
- Utilisateurs avec des menaces
- Endpoints présentant des menaces

Ces widgets fournissent des liens vers un écran Menaces de sécurité. Cet écran trace les menaces (par **utilisateur** ou **endpoint**) pendant une certaine période.

À partir de l'écran Menaces de sécurité, vous pouvez concentrer votre attention sur une menace particulière pour afficher si elle a récemment **affecté** d'autres utilisateurs et endpoints. Lancez l'**évaluation d'impact** pour voir si la même menace a affecté plus d'utilisateurs et d'endpoints sur une longue période.

Ces vues globales vous permettent de voir une chaîne des événements, à l'échelle de l'entreprise, susceptibles de conduire à une attaque, y compris les endpoints menacés utilisés pour préparer ou mener une attaque.

En savoir plus :

- *Écran Menaces de sécurité (utilisateur)*
- *Écran Menaces de sécurité (endpoint)*
- *Écran Utilisateurs affectés*
- *Évaluation de l'impact*

Intégration des produits relatifs à la défense contre les menaces connectées

Produits principaux

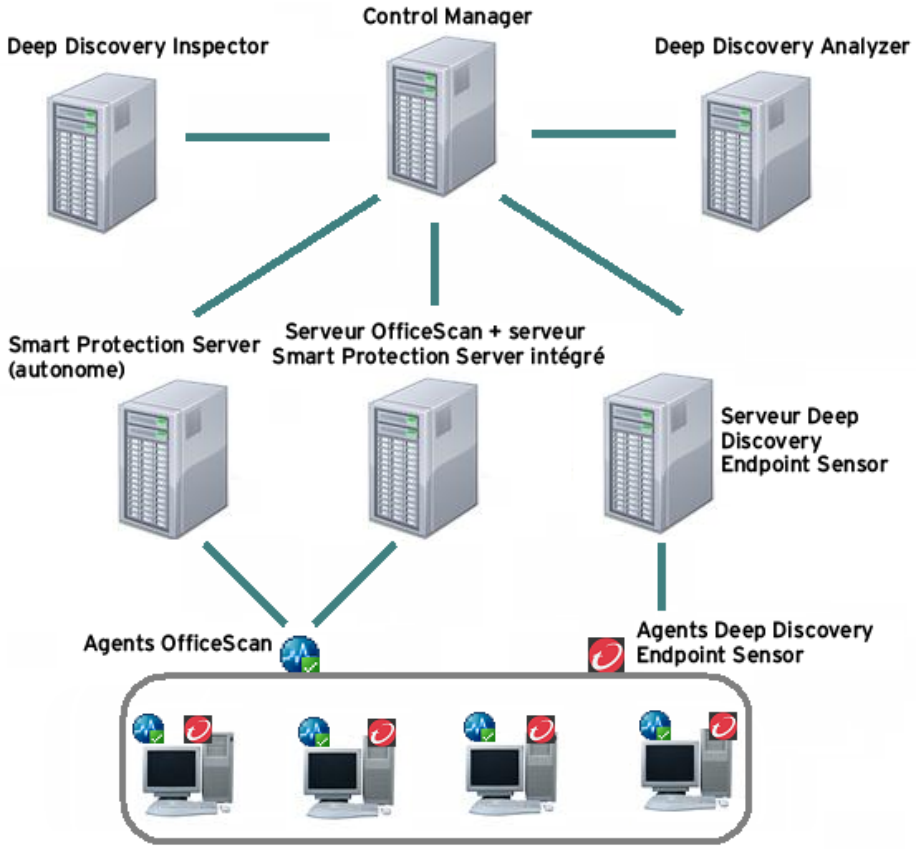
La défense contre les menaces connectées nécessite les produits Trend Micro suivants :

- Control Manager
- Deep Discovery Inspector
- OfficeScan
- Smart Protection Server (autonome) ou intégré à OfficeScan

Autres produits pris en charge

Les produits Trend Micro suivants peuvent également être intégrés à Control Manager pour la défense contre les menaces connectées :

- Deep Discovery Endpoint Sensor
- Deep Discovery Analyzer



Le rôle de chaque produit dans la stratégie de défense contre les menaces connectées est présenté en détail dans *Processus de gestion et de traitement des objets suspects à la page 10* et dans *Gestion des IOC à la page 18*.

Installez ces produits et enregistrez-les sur Control Manager. Les tableaux ci-dessous répertorient les références et les ressources nécessaires pour installer et enregistrer les produits.

Important

Enregistrez Deep Discovery Inspector et/ou Deep Discovery Analyzer **avant** d'enregistrer OfficeScan. Si OfficeScan est enregistré en premier, il ne sera pas en mesure d'obtenir des objets suspects dans les produits Deep Discovery.

Control Manager	
Version minimale	6.0 SP3
Installation	Références : • Guide d'installation de la version 6.0 pour installer le produit • Fichier Lisez-moi pour installer le Service Pack http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx

Informations Control Manager	Certains produits gérés nécessitent les informations suivantes relatives à Control Manager : • **Nom d'hôte** (nom de domaine complet (FQDN) de préférence) ou **adresse IP** : requis par Deep Discovery Inspector et à OfficeScan pour l'enregistrement. L'enregistrement est effectué sur la console de ces produits. **Remarque** L'enregistrement des autres produits de défense contre les menaces connectées est effectué sur la console Control Manager. • **Clé API** : requis par Deep Discovery Inspector, OfficeScan et Smart Protection Server pour la synchronisation des objets suspects. Déployez manuellement la clé API sur Deep Discovery Inspector 3.8 ou version ultérieure, OfficeScan 11 SP1 et Smart Protection Server 3.0 Patch 1. Pour obtenir la clé API, ouvrez la console d'administration de Control Manager et accédez à **Administration** > **Objets suspects** > **Paramètres de distribution**. Dans le cas des versions ultérieures d'OfficeScan et de Smart Protection Server, la clé API est automatiquement déployée après l'enregistrement de Control Manager, si un produit Deep Discovery a déjà été enregistré auprès de Control Manager.

Deep Discovery Inspector	
Version minimale	3.8
Installation et déploiement	Références : • Carte de démarrage rapide • Guide de déploiement et d'installation http://docs.trendmicro.com/en-us/enterprise/deep-discovery-inspector.aspx

Enregistrement et synchronisation de l'objet suspect	Terminez l'enregistrement et activez la synchronisation de l'objet suspect dans la console d'administration de Deep Discovery Inspector. Vous pouvez facilement lancer la console d'administration de Deep Discovery Inspector dans l'écran Serveurs gérés de Control Manager. Instructions d'enregistrement et de synchronisation : http://docs.trendmicro.com/all/ent/ddi/v3.8/en-us/ddi_3.8_olh/admin_int-prods-srvcs_tmcm_register.html

Deep Discovery Analyzer	
Version minimale	5.1
Installation et déploiement	Références : • Carte de démarrage rapide • Guide d'installation et de mise à niveau http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx
Enregistrement	Terminez l'enregistrement dans la console d'administration de Control Manager. Accédez à **Administration** > **Serveurs gérés** et sélectionnez Deep Discovery Analyzer dans la liste des produits.

OfficeScan	
Version minimale	11 SP1

Installation	Références : • Guide d'installation et de mise à niveau de la version 11 pour installer le programme serveur • Fichier Lisez-moi du Service Pack pour installer le Service Pack sur le serveur • Aide en ligne ou Guide de l'administrateur de la version 11 ou ultérieure pour installer les agents et utiliser le serveur Smart Protection Server intégré http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx
Enregistrement et synchronisation de l'objet suspect	Avant l'enregistrement d'OfficeScan, assurez-vous que vous avez enregistré au moins un produit Deep Discovery sur Control Manager. Terminez l'enregistrement et activez la synchronisation de l'objet suspect dans la console Web du serveur OfficeScan. Vous pouvez facilement lancer la console Web du serveur OfficeScan dans l'écran Serveurs gérés de Control Manager. • Instructions d'enregistrement : http://docs.trendmicro.com/fr-fr/enterprise/officescan-110-sp1-server/managing-the-product/osce-company_name-co/osce-registering-pro.aspx • Instructions de synchronisation (OfficeScan 11 SP1 uniquement) : http://docs.trendmicro.com/fr-fr/enterprise/officescan-110-sp1-server/managing-the-product/suspicious-objects-c/configuring-suspicio.aspx **Remarque** Des versions ultérieures d'OfficeScan ou des versions non anglaises d'OfficeScan 11 SP1 ont été améliorées pour synchroniser automatiquement des objets suspects avec Control Manager après l'enregistrement.

Smart Protection Server (autonome)	
Version minimale	3.0 Patch 1
Installation	Références : • Guide d'installation et de mise à niveau de la version 3.0 pour installer le produit • Fichier Lisez-moi pour installer le correctif http://docs.trendmicro.com/fr-fr/enterprise/smart-protection-server.aspx
Synchronisation de l'objet suspect	Instructions de synchronisation (Smart Protection Server 3.0 Patch 1 uniquement) : http://docs.trendmicro.com/all/ent/sps/v3.0p1/fr-fr/sps_3.0p1_olh/using_smart_prot_ccca_configure.html **Remarque** Seules les versions Smart Protection Server ultérieures à la version 3.0 Patch 1 prennent en charge l'enregistrement avec Control Manager. Une fois l'enregistrement terminé, Smart Protection Server synchronise automatiquement les objets suspects avec Control Manager.

Deep Discovery Endpoint Sensor	
Version minimale	1.5 (version d'évaluation)
Installation	Référence : Guide d'installation (pour les instructions d'installation du serveur et de l'agent) http://docs.trendmicro.com/en-us/enterprise/deep-discovery-endpoint-sensor.aspx

Enregistrement	Terminez l'enregistrement dans la console d'administration de Control Manager. Accédez à **Administration** > **Serveurs gérés** et sélectionnez Deep Discovery Endpoint Sensor dans la liste des produits.

Processus de gestion et de traitement des objets suspects

Le processus de traitement des objets suspects peut être décomposé en plusieurs phases, les voici :

Envoi d'un échantillon

Virtual Analyzer intégré dans les échantillons envoyés de processus de produits gérés suivants :

- **Deep Discovery Inspector 3.8** : Utilise des règles d'envoi de fichiers configurées par l'administrateur pour déterminer les échantillons à envoyer à son Virtual Analyzer
- **Deep Discovery Analyzer 5.1** : Reçoit les échantillons chargés par les administrateurs du produit ou envoyés par d'autres produits Trend Micro

Analyse

Virtual Analyzer dans les produits gérés recueille et analyse les échantillons envoyés. Virtual Analyzer repère les **objets suspects** en fonction du risque qu'ils présentent en termes de danger ou de perte. Les objets pris en charge comprennent les fichiers (valeurs de hachage SHA-1), les adresses IP, les domaines et les URL.

Distribution

Control Manager rassemble les objets suspects et les actions de scan par rapport aux objets et les distribue ensuite aux autres produits.

3.1. Objets suspects de Virtual Analyzer Les produits gérés avec Virtual Analyzer envoient une liste d'objets suspects à Control Manager. Control Manager affiche les objets suspects dans **Administration** > **Objets suspects** > **Objets Virtual Analyzer**, dans l'onglet **Objets**.	**3.3. Objets suspects définis par l'utilisateur** Les administrateurs de Control Manager peuvent ajouter des objets qu'ils estiment suspects, mais qui ne figurent pas actuellement dans la liste d'objets suspects de Virtual Analyzer en accédant à **Administration** > **Objets suspects** > **Objets définis par l'utilisateur**.
3.2. Exceptions aux objets suspects de Virtual Analyzer Dans la liste d'objets suspects de Virtual Analyzer (**Administration** > **Objets suspects** > **Objets Virtual Analyzer**), les administrateurs de Control Manager peuvent sélectionner des objets qui sont considérés comme sûrs, puis les ajouter à la liste d'exceptions. La liste d'exceptions s'affiche sous l'onglet **Exceptions** à côté de l'onglet **Objets**. Control Manager renvoie la liste d'exceptions aux produits gérés avec Virtual Analyzer. Si un objet suspect à partir d'un produit géré correspond à un objet figurant dans la liste d'exceptions, le produit ne l'envoie plus à Control Manager.	**3.4. Distribution de l'objet suspect** Control Manager rassemble Virtual Analyzer et les objets suspects définis par l'utilisateur (à l'exclusion des exceptions) et les envoie à certains produits gérés. Ces produits synchronisent et utilisent tout ou partie de ces objets. Voici les produits gérés pris en charge et les versions minimales requises : • **Deep Discovery Inspector 3.8** : Développe sa liste d'**objets suspects** pour inclure les objets définis par l'utilisateur et ceux détectés par d'autres produits de Deep Discovery • **OfficeScan 11 SP1** : Recherche les **fichiers**, **adresses IP** et **URL** suspects au cours de scans de routine • **Smart Protection Server 3.0 Patch 1 (autonome) ou intégré à OfficeScan 11 SP1** : Transmet les informations sur les **URL suspectes** aux produits Trend Micro (comme les agents OfficeScan, ScanMail et Deep Security) qui envoient des requêtes Web Reputation

3.5. Actions de scan

Configurez des actions de scan (journaliser, bloquer ou mettre en quarantaine) par rapport aux objets suspects qui affectent les endpoints.

Les actions Bloquer et Mettre en quarantaine sont considérées comme des actions « actives », tandis que l'action « journaliser » est considérée comme une action « passive ». Si les produits exécutent une action active, Control Manager déclare les endpoints affectés comme **atténués**. Si l'action est passive, les endpoints sont déclarés **menacés**.

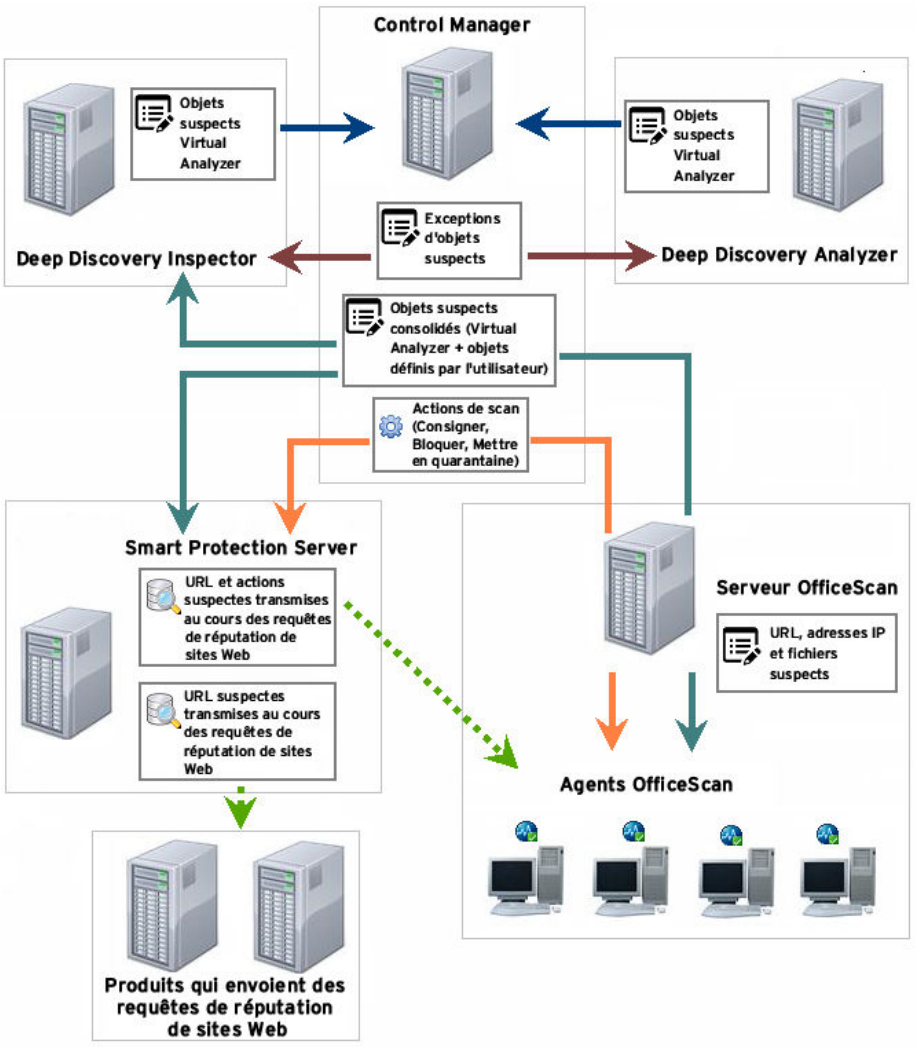
Les actions de scan sont configurées séparément pour Virtual Analyzer et les objets suspects définis par l'utilisateur.

- **Administration** > **Objets suspects** > **Objets Virtual Analyzer**
- **Administration** > **Objets suspects** > **Objets définis par l'utilisateur**

Control Manager déploie automatiquement les actions sur certains produits gérés.

Voici les produits gérés pris en charge et les versions minimales requises :

- **OfficeScan 11 SP1** : Exécute des actions contre les **fichiers**, **adresses IP** et **URL** suspects de Virtual Analyzer (les actions contre les objets définis par l'utilisateur ne sont pas prises en charge)
- **Smart Protection Server 3.0 Patch 1 (autonome) ou intégré à OfficeScan 11 SP1** : Transmet les actions contre les URL suspectes aux agents OfficeScan qui envoient des requêtes Web Reputation.

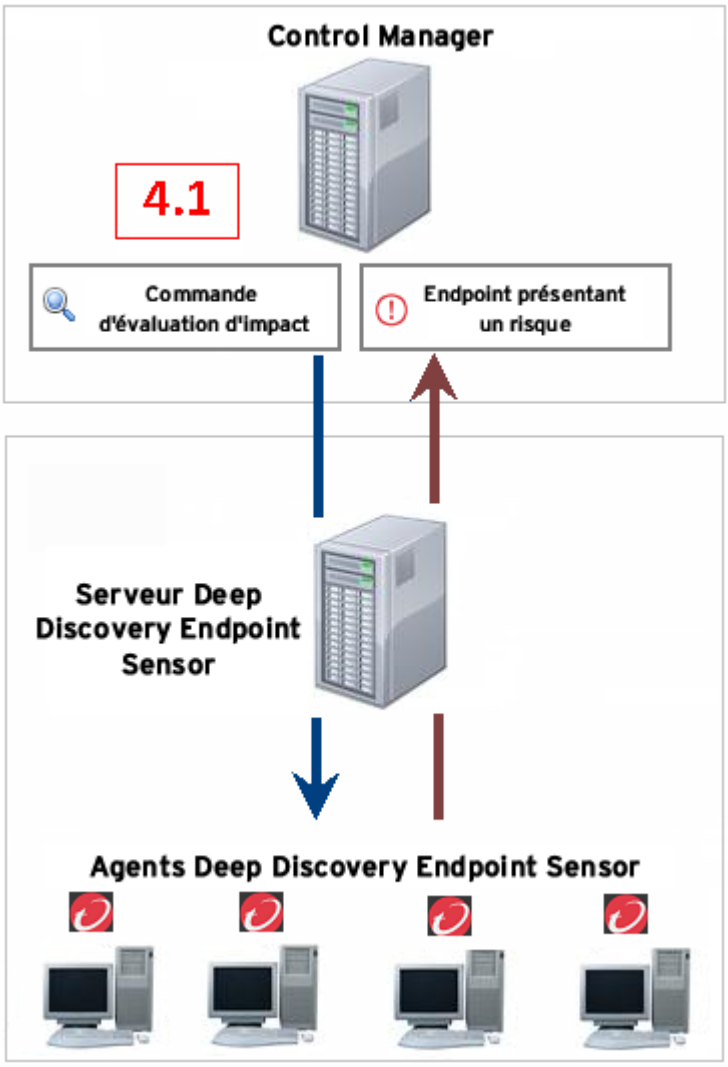

Control Manager
Objets suspects Virtual Analyzer
Objets suspects Virtual Analyzer
Deep Discovery Inspector
Exceptions d'objets suspects
Deep Discovery Analyzer
Objets suspects consolidés (Virtual Analyzer + objets définis par l'utilisateur)
Actions de scan (Consigner, Bloquer, Mettre en quarantaine)
Smart Protection Server
URL et actions suspectes transmises au cours des requêtes de réputation de sites Web
URL suspectes transmises au cours des requêtes de réputation de sites Web
Serveur OfficeScan
URL, adresses IP et fichiers suspects
Agents OfficeScan
Produits qui envoient des requêtes de réputation de sites Web

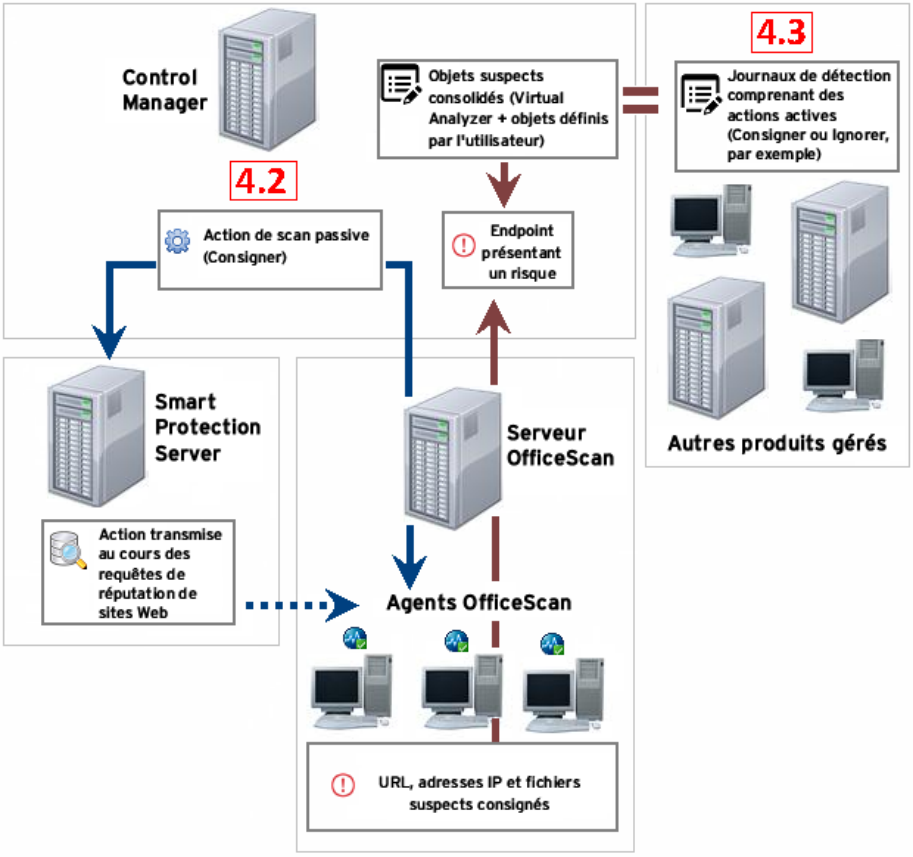
Évaluation d'impact

L'évaluation de l'impact vérifie les endpoints des activités suspectes associées à des objets suspects. Les endpoints avec activités suspectes confirmées sont considérés comme **menacés**.

Control Manager considère également les endpoints comme menacés si les produits exécutent des actions « passives » par rapport à des objets suspects.

4.1. Évaluation de l'impact À partir de la liste des objets suspects de Virtual Analyzer, dans **Administration** > **Objets suspects** > **Objets Virtual Analyzer**, exécutez l'évaluation de l'impact pour déterminer les endpoints menacés. L'évaluation de l'impact requiert **Deep Discovery Endpoint Sensor**. La version minimale requise est la version **1.5**. Ce produit n'effectue que l'évaluation et n'exécute aucune action sur les endpoints menacés.	**4.3. Correspondance de la détection** Control Manager vérifie également la Web Reputation, le filtrage d'URL, l'inspection de contenu réseau ainsi que les journaux de détection des règles de base reçus de tous les produits gérés, puis les compare à sa liste d'objets suspects. Si une correspondance est détectée à partir d'un endpoint spécifique et que le produit géré entreprend une action « passive » (par exemple, Consigner, Ignorer, ou Avertir et Continuer), l'endpoint est également considéré comme menacé.
4.2. Action de Scan « passive » Lorsque l'action de scan configurée dans Control Manager et déployée sur les agents OfficeScan est « passive » (journal), les endpoints affectés sont considérés comme menacés.	**Endpoints menacés** Pour afficher le nombre d'endpoints menacés, accédez à**Administration** > **Objets suspects** > **Objets Virtual Analyzer** et consultez la colonne **Terminaux menacés**. Pour afficher les informations détaillées sur les endpoints menacés, accédez à la colonne **Objet**, puis cliquez sur l'icône en forme de flèche (si disponible) devant le nom de l'objet suspect. L'écran s'agrandit et affiche un tableau des détails sur l'objet suspect et les terminaux menacés.


Control Manager
4.1
Commande d'évaluation d'impact
Endpoint présentant un risque
Serveur Deep Discovery Endpoint Sensor
Agents Deep Discovery Endpoint Sensor



5

Mitigation

L'agent OfficeScan et d'autres produits gérés exécutent des actions de scan « actives » par rapport aux objets suspects.

5.1. Actions de scan de Control Manager

Lorsque vous déployez une action de scan « active » (bloquer ou mettre en quarantaine) à partir de Control Manager sur les agents OfficeScan, les menaces dirigées vers les endpoints affectés sont considérées comme atténuées.

5.2. Actions de scan de produits gérés

Les produits gérés peuvent effectuer des actions de scan spécifiques au produit (telles que bloquer, supprimer, mettre en quarantaine ou bloquer avec écrasement) sur les menaces détectées. Si Control Manager établit une correspondance avec un objet suspect dans les journaux (réputation de sites Web, filtrage des URL, inspection du contenu réseau et détection basée sur des règles) d'un produit géré, une évaluation des menaces est effectuée. Control Manager considère toutes les menaces visant les endpoints comme atténuées si le produit géré a exécuté une action « active » sur l'objet suspect.

Remarque

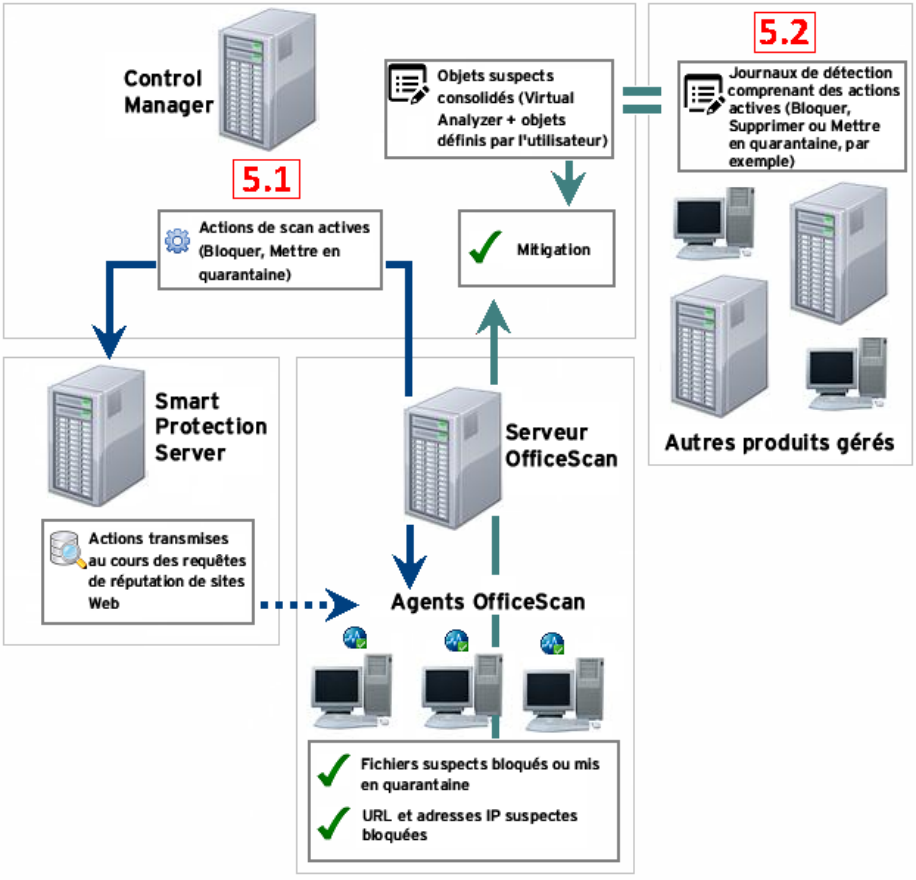
Consultez le manuel de l'administrateur de vos produits gérés pour plus d'informations sur les types d'actions que les produits spécifiques peuvent exécuter sur les menaces détectées.

Isolation d'endpoint

Une autre action consiste en l'isolation des endpoints menacés. Effectuez cette action si vous devez effectuer une investigation détaillée.

Seuls les endpoints comportant des **agents OfficeScan** peuvent être isolés. La version minimale requise est la version **11 SP1**. Le pare-feu des agents doit être activé.

Pour plus d'informations, consultez la section *Isolation des endpoints et restauration de la connexion à la page 34*.



Gestion des IOC

La gestion des IOC (Indicateurs de compromission) comprend les tâches suivantes :

1

Génération de fichiers IOC

Procurez-vous des fichiers IOC auprès de vos homologues et d'autres experts en sécurité. Ouvrez la console d'administration de Control Manager et accédez à **Administration** > **Indicateurs de compromission** pour ajouter les fichiers IOC.

Si, pour une raison quelconque, un objet suspect de Deep Discovery Analyzer 5.1 ou Deep Discovery Inspector 3.8 ne s'affiche pas dans l'écran des objets suspects de l'analyseur virtuel (**Administration** > **Objets suspects** > **Objets Virtual Analyzer**), téléchargez le package d'enquête sur les objets suspects correspondant dans la console du produit géré. Ce package d'enquête (disponible sous la forme d'un seul fichier compressé) contient des fichiers conformes à IOC et à d'autres ressources d'enquête.

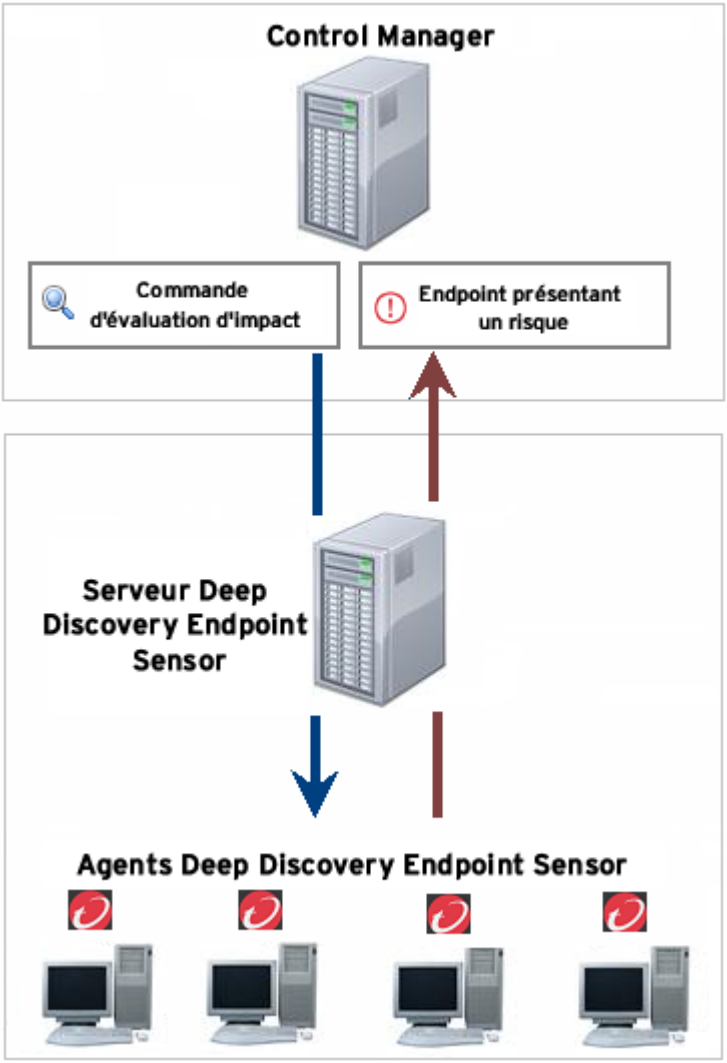
Control Manager ne nécessite que les fichiers IOC pour l'évaluation de l'impact, extrayez les fichiers .ioc du fichier compressé, puis ajoutez-les à Control Manager. Il n'est pas possible d'ajouter le fichier compressé.

Important

Après l'extraction et l'ajout des fichiers .ioc, supprimez le fichier compressé de l'ordinateur, car il contient des fichiers potentiellement malveillants.

Évaluation d'impact

Lancez l'évaluation d'impact afin de vérifier les activités suspectes selon les indicateurs répertoriés dans les fichiers IOC. Les endpoints contenant des activités suspectes sont considérés comme **menacés**.



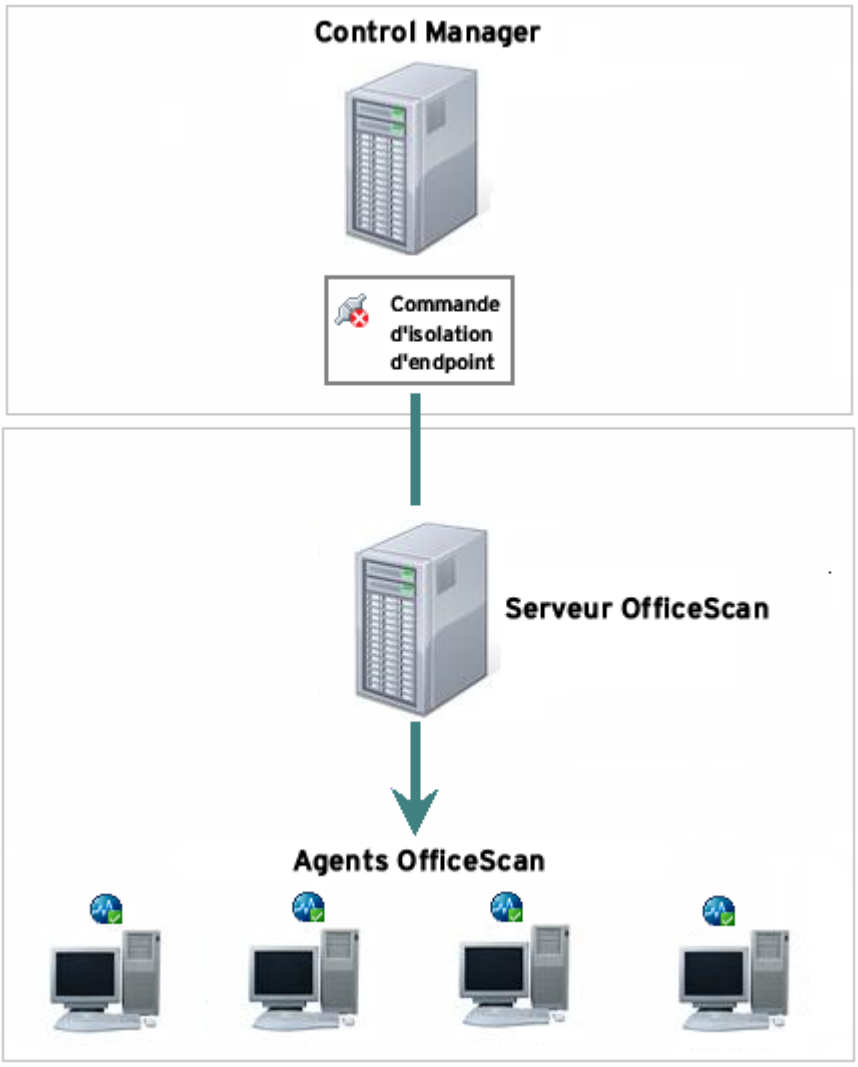
Accédez à **Administration** > **Indicateurs de compromission** et exécutez une évaluation de l'impact sur un ou plusieurs fichiers IOC afin de déterminer les endpoints menacés.

L'évaluation de l'impact requiert **Deep Discovery Endpoint Sensor**. La version minimale requise est la version **1.5**.

Ce produit n'effectue que l'évaluation et n'exécute aucune action sur les endpoints menacés.

Isolation d'endpoint

Isolez un endpoint affecté pour mener une enquête détaillée. Pour ce faire, accédez à **Administration** > **Indicateurs de compromission**, allez dans la colonne **Menacé**, puis cliquez sur un nombre représentant le nombre d'endpoints menacés.



Seuls les endpoints comportant des **agents OfficeScan** peuvent être isolés. La version minimale requise est la version **11 SP1**. Le pare-feu des agents doit être activé.

Pour plus d'informations, consultez la section *Isolation des endpoints et restauration de la connexion à la page 34*.

Surveillance améliorée des menaces de sécurité

Utilisez les widgets suivants sous l'onglet **Résumé** pour surveiller la sécurité du réseau et pour répondre aux menaces les plus critiques :

- Menaces critiques
- Utilisateurs avec des menaces
- Endpoints présentant des menaces

Ces widgets fournissent des liens vers un écran Menaces de sécurité. Cet écran trace les menaces (par **utilisateur** ou **endpoint**) pendant une certaine période.

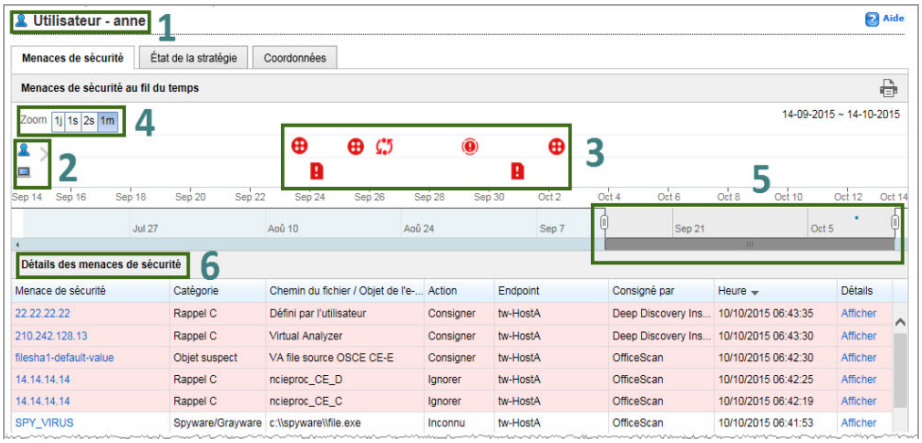
À partir de l'écran Menaces de sécurité, vous pouvez concentrer votre attention sur une menace particulière pour afficher si elle a récemment **affecté** d'autres utilisateurs et endpoints. Lancez l'**évaluation d'impact** pour voir si la même menace a affecté plus d'utilisateurs et d'endpoints sur une longue période.

Ces vues globales vous permettent de voir une chaîne des événements, à l'échelle de l'entreprise, susceptibles de conduire à une attaque, y compris les endpoints menacés utilisés pour préparer ou mener une attaque.

Menaces de sécurité (utilisateur)

Affichez les menaces de sécurité détectées sur tous les endpoints appartenant à un utilisateur.

Il existe plusieurs façons d'accéder à cet écran. Il est recommandé d'accéder au widget **Utilisateurs avec des menaces** sur le tableau de bord et de cliquer sur une valeur qui représente le nombre de menaces détectées sur tous les endpoints appartenant à un utilisateur.



Les principaux éléments d'interface utilisateur figurant dans l'écran sont les suivants :

NOMBRE	DESCRIPTION
1	Un utilisateur avec des endpoints qui présentent des menaces de sécurité
2	Les endpoints que possède l'utilisateur (représentés par une icône de moniteur) et l'utilisateur (représenté par une icône de personne) Par défaut, le nom d'hôte d'un endpoint et le nom de domaine de l'utilisateur s'affichent en regard des icônes. Cliquez sur la flèche grise pour afficher ou masquer les noms d'hôte et de domaine.

<table>
<tr><th>Nombre</th><th colspan="3">Description</th></tr>
<tr><td rowspan="6">3</td><td colspan="3">Menaces de sécurité détectées sur les endpoints, représentées par des icônes

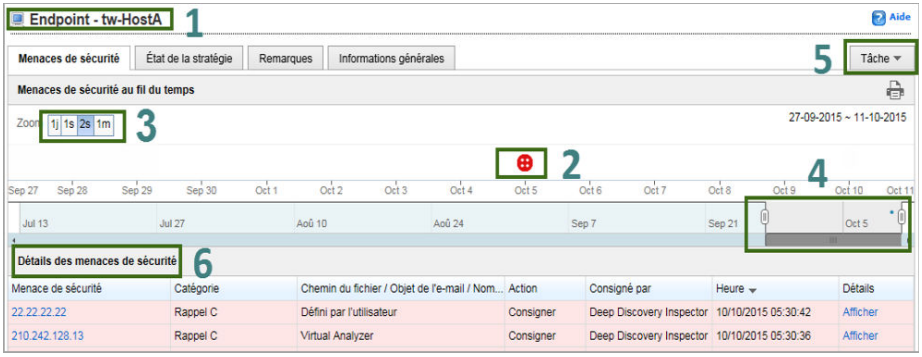
Passez la souris sur une icône pour afficher les détails de la menace.</td></tr>
<tr><td> 
Violation de l'application</td><td> 
Violation de la surveillance des comportements</td><td> 
Rappel C&C</td></tr>
<tr><td> 
Incident DLP</td><td> 
Violation de contenu</td><td> 
Violation du pare-feu</td></tr>
<tr><td> 
Événement de prévention des intrusions</td><td> 
Violation de contenu réseau</td><td> 
E-mail d'hameçonnage</td></tr>
<tr><td> 
Spam</td><td> 
Spyware/Grayware</td><td> 
Objet suspect</td></tr>
<tr><td> 
Virus/Malware</td><td> 
Violation Web</td><td> 
Plusieurs événements</td></tr>
<tr><td>4 et 5</td><td colspan="3">Filtre utilisé pour contrôler le nombre de menaces de sécurité détectées au cours d'une certaine période</td></tr>
</table>

NOMBRE	DESCRIPTION
6	Tableau contenant des détails sur les menaces de sécurité Les menaces critiques sont en rouge dégradé pour une meilleure visibilité. Si ce n'est pas le cas, choisissez l'une des options suivantes : • Cliquez sur une valeur dans la colonne **Menace de sécurité** pour afficher les *utilisateurs affectés par la menace*. • Cliquez sur une valeur dans la colonne **Détails** pour afficher une entrée de journal.

Menaces de sécurité (endpoint)

Affichez les menaces de sécurité détectées sur un endpoint particulier.

Il existe plusieurs façons d'accéder à cet écran. Il est recommandé d'accéder au widget **Endpoints présentant des menaces** dans le tableau de bord, puis de cliquer sur une valeur représentant le nombre de menaces détectées sur un endpoint.



Les principaux éléments d'interface utilisateur figurant dans l'écran sont les suivants :

<table>
<tr><th>Nombre</th><th>Description</th></tr>
<tr><td>1</td><td>Endpoint affecté par les menaces de sécurité

Une icône s'affiche après le nom du Endpoint (comme illustré ci-dessous) si Control Manager a isolé l'endpoint ou est sur le point de restaurer sa connexion réseau.

  </td></tr>
<tr><td>2</td><td>Les menaces de sécurité détectées sur les endpoints, représentées par des icônes

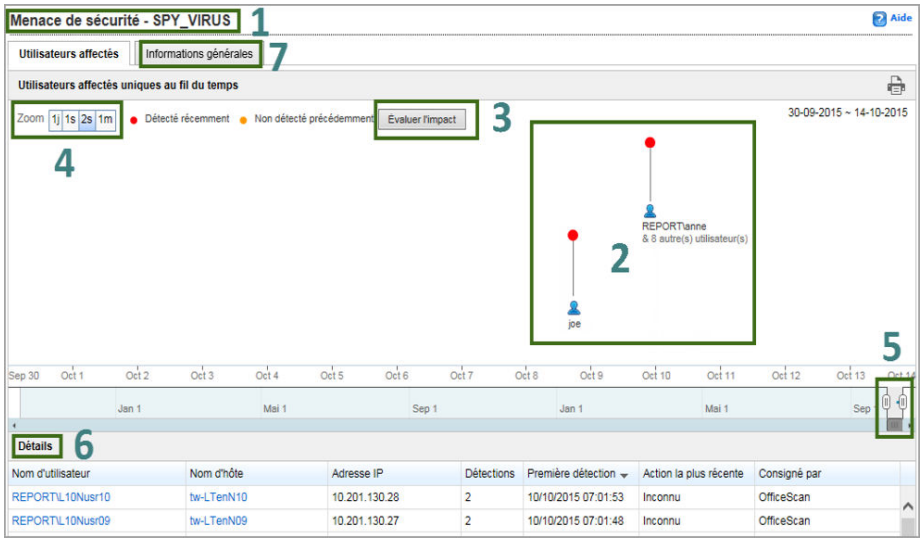
Passez la souris sur une icône pour afficher les détails de la menace.

<table>
<tr><td> 
Violation de l'application</td><td> 
Violation de la surveillance des comportements</td><td> 
Rappel C&C</td></tr>
<tr><td> 
Incident DLP</td><td> 
Violation de contenu</td><td> 
Violation du pare-feu</td></tr>
<tr><td> 
Événement de prévention des intrusions</td><td> 
Violation de contenu réseau</td><td> 
E-mail d'hameçonnage</td></tr>
<tr><td> 
Spam</td><td> 
Spyware/Grayware</td><td> 
Objet suspect</td></tr>
<tr><td> 
Virus/Malware</td><td> 
Violation Web</td><td> 
Plusieurs événements</td></tr>
</table>
</td></tr>
<tr><td>3 et 4</td><td>Filtre utilisé pour contrôler le nombre de menaces de sécurité détectées au cours d'une certaine période</td></tr>
</table>

NOMBRE	DESCRIPTION
5	Les tâches suivantes peuvent être effectuées sur l'endpoint : • Affecter des balises • *Isoler l'endpoint*
6	Tableau contenant des détails sur les menaces de sécurité Les menaces critiques sont en rouge dégradé pour une meilleure visibilité. Si ce n'est pas le cas, choisissez l'une des options suivantes : • Cliquez sur une valeur dans la colonne **Menace de sécurité** pour afficher les *utilisateurs affectés par la menace*. • Cliquez sur une valeur dans la colonne **Détails** pour afficher une entrée de journal.

Utilisateurs affectés

Le fait de cliquer sur le nom de la menace dans l'écran *Menaces de sécurité (utilisateur)* ou *Menaces de sécurité (endpoint)* permet d'ouvrir l'écran Utilisateurs affectés dans lequel s'affiche la liste d'utilisateurs uniques concernés par la menace.



Les principaux éléments d'interface utilisateur figurant dans l'écran sont les suivants :

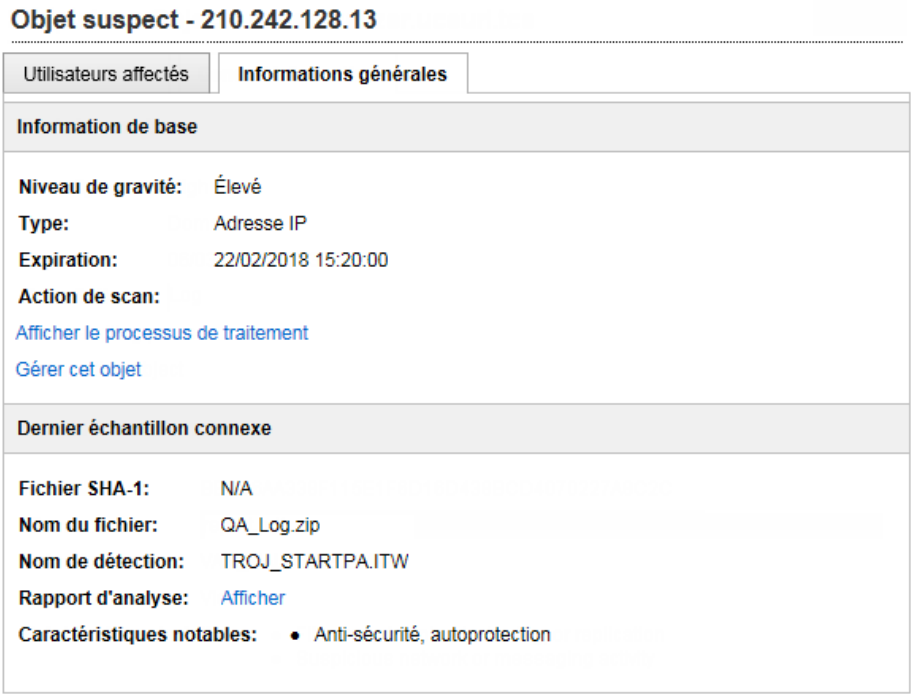
Nombre	Description
1	Menace de sécurité qui affecte un ou plusieurs utilisateurs

NOMBRE	DESCRIPTION
2	Utilisateurs affectés et nature de la détection (**Détecté récemment** ou**Non détecté précédemment**), représentés par des icônes La nature de la détection est représentée par une couleur spécifique. Reportez-vous à la légende avant le bouton **Évaluer l'impact** afin d'afficher la signification de chaque couleur. Si un utilisateur présente les mêmes détections que d'autres utilisateurs, un numéro s'affiche sous le nom d'utilisateur. Passez la souris sur le nom d'utilisateur pour afficher tous les utilisateurs affectés.
3	Bouton de lancement de l'évaluation de l'impact sur les menaces de sécurité L'évaluation de l'impact sur les menaces de sécurité requiert **Deep Discovery Endpoint Sensor** et **Deep Discovery Inspector**. Ces deux produits utilisent *Scan rétro* pour procéder à l'évaluation. Si un seul de ces produits est enregistré sur Control Manager, une évaluation partielle de l'impact sera effectuée. Après l'évaluation, le graphique sera mis à jour avec une liste des menaces non encore détectées. Il s'agit de menaces discrètes et sophistiquées qui ont échappé à la détection.
4 et 5	Filtre temporel utilisé pour contrôler le nombre d'utilisateurs affectés affiché
6	Tableau comportant des informations sur les utilisateurs affectés Cliquez sur une valeur de la colonne **Nom d'utilisateur** ou **Nom d'hôte** pour afficher les *menaces de sécurité sur l'endpoint de l'utilisateur*.
7	Onglet comportant des *informations générales* concernant la menace de sécurité

Informations générales sur les menaces de sécurité

Affichez les informations sur une menace de sécurité particulière.

Les informations affichées varient en fonction du type de menace et des informations liées aux menaces reçues des produits gérés.



Évaluation d'impact

Il existe plusieurs façons de lancer une évaluation d'impact.

Évaluation d'impact sur les objets suspects

Lancez l'évaluation d'impact afin de vérifier les activités suspectes associées aux objets suspects. Les endpoints contenant des activités suspectes sont considérés comme **menacés**.

L'évaluation de l'impact sur les objets suspects nécessite un produit Trend Micro appelé **Deep Discovery Endpoint Sensor**.

Pour lancer l'évaluation, accédez à **Administration** > **Objets suspects** > **Objets Virtual Analyzer**.

Évaluation d'impact sur les fichiers IOC

Lancez l'évaluation d'impact afin de vérifier les activités suspectes selon les indicateurs répertoriés dans les fichiers IOC. Les endpoints contenant des activités suspectes sont considérés comme **menacés**.

L'évaluation d'impact sur les fichiers IOC nécessite un produit Trend Micro appelé **Deep Discovery Endpoint Sensor**.

Pour lancer l'évaluation, accédez à **Administration** > **Indicateurs de compromission**.

Évaluation d'impact sur les menaces de sécurité

Lancez l'évaluation d'impact sur les menaces de sécurité afin de vérifier les endpoints affectés. Cela est particulièrement utile pour vérifier les menaces discrètes et sophistiquées qui ont échappé à la détection.

L'évaluation d'impact sur les menaces de sécurité requiert **Deep Discovery Endpoint Sensor** et **Deep Discovery Inspector**. Ces produits utilisent **Scan rétro** pour procéder à l'évaluation.

Si un seul de ces produits est enregistré sur Control Manager, une évaluation partielle de l'impact sera effectuée.

Pour lancer l'évaluation :

1. Accédez à l'écran *Menaces de sécurité (utilisateur)* ou *menaces de sécurité (endpoint)*.
2. Cliquez sur un nom de menace. S'affiche alors l'écran *Utilisateurs affectés*, avec l'option **Évaluer l'impact**.

En savoir plus :

Scan rétro

Scan rétro

Scan rétro de Deep Discovery Inspector

Scan rétro est un service cloud permettant de scanner les journaux d'historique d'accès Web pour les tentatives de rappel des serveurs C&C et d'autres activités liées à votre réseau. Les journaux d'accès Web peuvent inclure des connexions non détectées et débloquées aux serveurs C&C n'ayant été découverts que récemment. L'examen de ces journaux constitue une partie importante des investigations judiciaires pour déterminer si votre réseau est affecté par des attaques.

Scan rétro stocke les informations du journal suivantes dans Smart Protection Network :

- Adresses IP des endpoints surveillés par Deep Discovery Inspector
- URL accessibles via des endpoints
- GUID de Deep Discovery Inspector

Scan rétro scanne ensuite périodiquement les entrées du journal stockées pour vérifier les tentatives de rappel aux serveurs C&C dans les listes suivantes :

- Liste de Trend Micro Intelligence globale : Trend Micro compile la liste à partir de plusieurs sources, puis évalue le niveau de risque de chaque adresse de rappel C&C. La liste C&C est mise à jour et envoyée aux produits activés quotidiennement.
- Liste définie par l'utilisateur : Scan rétro peut également scanner des journaux par rapport à votre propre liste de serveurs C&C. Les adresses doivent être stockées dans un fichier texte.

Important

L'écran Scan rétro dans Deep Discovery Inspector affiche uniquement les informations pour les scans qui utilisent la liste Trend Micro Intelligence globale.

Scan rétro dans Deep Discovery Endpoint Sensor

Scan rétro examine les événements de l'historique et leur chaîne d'activité en fonction d'une condition de recherche spécifiée. Les résultats peuvent être affichés sous forme de mindmap montrant le flux d'exécution de toute activité suspecte. Cela facilite l'analyse de la chaîne d'événements, à l'échelle de l'entreprise, qui sont impliqués dans une attaque ciblée.

Scan rétro utilise les types d'objets suivants pour son investigation :

- Enregistrement DNS

- Adresse IP
- Nom du fichier
- Dossier du fichier
- Valeurs de hachage SHA-1
- Valeurs de hachage MD5
- Compte utilisateur

Scan rétro interroge une base de données normalisée contenant les événements de l'historique d'un endpoint. Par rapport à un fichier journal traditionnel, cette méthode utilise moins d'espace disque et consomme moins de ressources.

Isolation des endpoints et restauration de la connexion

Isolez les endpoints menacés pour exécuter une investigation et résoudre les problèmes de sécurité. Restaurez rapidement la connexion lorsque tous les problèmes ont été résolus.

L'isolation des endpoints et la restauration de la connexion nécessitent l'**agent OfficeScan**. La version minimale requise est la version **11 SP1**. En outre, le **pare-feu** de l'agent OfficeScan doit être activé.

Mise en place de l'isolation d'un endpoint

L'option **Isoler** est disponible dans les écrans suivants :

1.1. Écran Endpoint

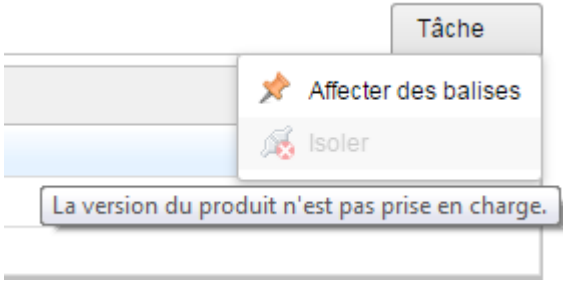
Remarque

Tous les onglets de l'écran Endpoint contiennent l'option **Isoler**.

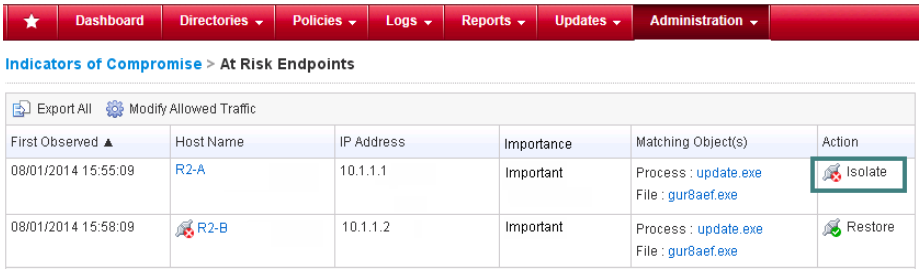
Il existe plusieurs façons d'accéder à cet écran. Il est recommandé d'accéder à **Répertoires** > **Utilisateurs/Endpoints**, d'utiliser la fonction de recherche dans l'écran pour trouver l'endpoint à isoler, puis de cliquer sur le nom du Endpoint lors de l'affichage des résultats de la recherche.

Si l'isolation ne peut pas être effectuée, un message s'affiche sous l'option **Isoler** afin d'indiquer l'un des problèmes suivants :

- L'agent sur l'endpoint exécute une version non prise en charge.
- Le compte utilisateur servant à se connecter à Control Manager ne dispose pas des autorisations nécessaires.



1.2. Écran Endpoints menacés



Remarque

Pour atteindre cet écran, accédez à **Administration** > **Indicateurs de compromis**, allez dans la colonne **Menacé**, puis cliquez sur un nombre représentant le nombre d'endpoints menacés.

2

Surveillance de l'état d'isolation

Un message s'affiche en haut de l'écran Endpoint ou Endpoints menacés pendant l'isolation d'un endpoint, vous informant que celle-ci est en cours d'exécution.

Le message disparaît lorsque l'isolation est terminée. Sur l'endpoint, un message de notification s'affiche pour informer l'utilisateur de l'isolation.

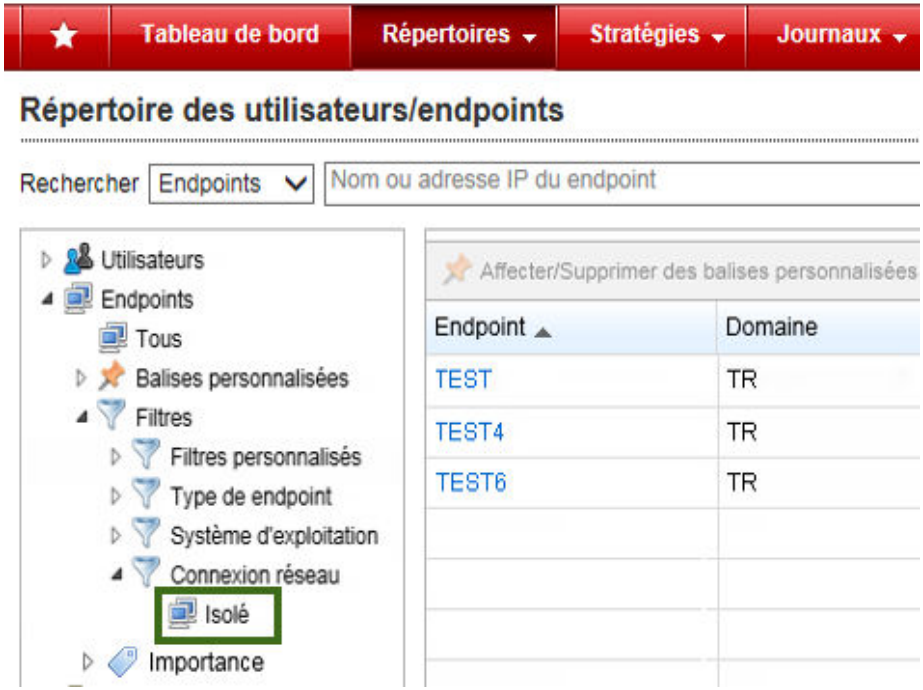
En cas de problème, le message change. Les problèmes sont les suivants :

- Le pare-feu de l'agent OfficeScan a été désactivé par l'administrateur du serveur OfficeScan ou par l'utilisateur, qui dispose de privilèges pour configurer les paramètres du pare-feu. Il est également possible que le pare-feu ne fonctionne plus.
- Pas de connexion entre l'agent OfficeScan sur l'endpoint et son serveur parent.
- Le serveur OfficeScan et l'agent sont tous deux installés sur l'endpoint. L'isolation de l'endpoint provoquera des perturbations des fonctions du serveur OfficeScan.
- Une erreur inattendue est survenue.

Actualisez l'écran pour obtenir l'état le plus récent.

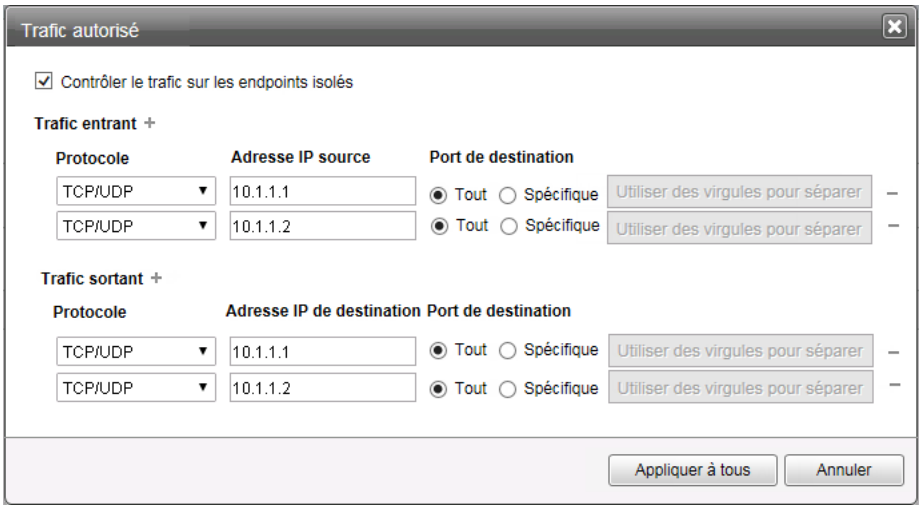
Surveillance des endpoints isolés

Une liste des endpoints isolés est disponible dans l'arborescence Endpoint, lorsque vous sélectionnez le filtre par défaut, **Isolé**.



Configuration du trafic autorisé

Par défaut, l'isolation des endpoints bloque tout le trafic entrant et sortant, excepté le trafic entre l'agent OfficeScan et son serveur parent.



Vous pouvez configurer le trafic entrant et sortant que vous souhaitez autoriser sur les endpoints isolés. Ces paramètres s'appliquent à **tous** les endpoints isolés et ne peuvent pas être configurés pour chaque endpoint.

Si d'autres agents Trend Micro sont installés sur les endpoints, veillez à configurer le trafic autorisé de sorte que les agents puissent continuer à communiquer avec leurs serveurs parents.

Agent	Trafic entrant	Trafic sortant	Autres éléments requis
Vulnerability Protection	**Protocole** : TCP **Adresse IP source** : Adresse IP du serveur parent **Port de destination** : 4118	**Protocole** : TCP **Adresse IP de destination** : Adresse IP du serveur parent **Port de destination** : 4120	Si le serveur Vulnerability Protection est installé à l'aide des paramètres DNS, ajoutez le protocole, l'adresse IP et les ports de destination du serveur DNS.
Endpoint Encryption	**Protocole** : TCP **Adresse IP source** : Adresse IP du serveur parent **Port de destination** : 80, 8080	**Protocole** : TCP **Adresse IP de destination** : Adresse IP du serveur parent **Port de destination** : 80, 8080	Si le serveur Endpoint Encryption est installé à l'aide des paramètres DNS, ajoutez le protocole, l'adresse IP et les ports de destination du serveur DNS.

AGENT	TRAFIC ENTRANT	TRAFIC SORTANT	AUTRES ÉLÉMENTS REQUIS
Deep Discovery Endpoint Sensor	**Protocole** : TCP **Adresse IP source** : Adresse IP du serveur parent **Port de destination** : 8081	**Protocole** : TCP **Adresse IP de destination** : Adresse IP du serveur parent **Port de destination** : 8002, 8003	Paramètres DNS (trafic entrant) : **Protocole** : UDP **Adresse IP source** : Adresse IP du serveur DNS **Port de destination** : 53 Paramètres DNS (trafic sortant) : **Protocole** : UDP **Adresse IP de destination** : Adresse IP du serveur DNS **Port de destination** : 53
Endpoint Application Control	**Protocole** : TCP **Adresse IP source** : Adresse IP du serveur parent **Port de destination** : 80, 443, 8080, 4343	**Protocole** : TCP **Adresse IP de destination** : Adresse IP du serveur parent **Port de destination** : 8085, 8443	Si le serveur Endpoint Application Control est installé à l'aide des paramètres DNS, ajoutez le protocole, l'adresse IP et les ports de destination du serveur DNS.

Cliquez sur **Appliquer à tous** pour déployer les paramètres sur les serveurs OfficeScan avec les agents qui ont isolé ou qui sont sur le point d'isoler des endpoints.

Restauration de la connexion des endpoints

Après que vous avez terminé votre investigation et confirmé la fiabilité de l'endpoint, restaurez la connexion au réseau de l'endpoint. L'option **Restaurer** est disponible sur l'écran Endpoint ou l'écran Endpoints menacés.

Une fois que vous avez cliqué sur **Restaurer**, un message s'affiche en haut de l'écran, vous informant que la restauration de la connexion est en cours d'exécution. Le message disparaît une fois la restauration terminée.

En cas de problème, le message change. Les problèmes sont les suivants :

- Le pare-feu de l'agent OfficeScan a été désactivé par l'administrateur du serveur OfficeScan ou par l'utilisateur, qui dispose de privilèges pour configurer les paramètres du pare-feu. Il est également possible que le pare-feu ne fonctionne plus. Par conséquent, la connexion réseau a été automatiquement restaurée, mais l'endpoint reste dans le filtre **Isolé** dans l'arborescence Control Manager Endpoint.

  Activez le pare-feu de l'agent ou vérifiez qu'il fonctionne correctement, puis déclenchez l'isolation des endpoints dans Control Manager (pour maintenir l'endpoint isolé) ou la restauration de la connexion (pour supprimer l'endpoint du filtre **Isolé** dans l'arborescence des endpoints).

- Pas de connexion entre l'agent OfficeScan sur l'endpoint et son serveur parent.

- Une erreur inattendue est survenue.

Actualisez l'écran pour obtenir l'état le plus récent.

Historique des isolations d'endpoints et des restaurations de la connexion

Control Manager conserve un enregistrement de toutes les tâches d'isolation et de restauration de connexion effectuées sur un endpoint. Pour afficher ces enregistrements, accédez à l'écran Endpoint, puis cliquez sur l'onglet **Notes**.


Tableau de bord
Répertoires
Stratégies
Journaux
Rapports
Mises à jour
Administration
< Précédent
Endpoint - FR-PC
Aide
Menaces de sécurité
État de la stratégie
Remarques
Informations générales
Tâche
Remarque:
Ajouter
Heure
Remarque
Utilisateur
10/10/2015 04:28:26
Restaurer
root
08/10/2015 07:06:07
Isoler
root

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: CMFM67185/150909