TREND MICRO

10.0

Worry-Free™ Business Security Standard e Advanced Edition

Service Pack 1

Guida dell'amministratore

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Trend Micro Incorporated si riserva il diritto di apportare modifiche a questa documentazione e al prodotto in essa descritto senza alcun obbligo di notifica. Prima di installare e utilizzare il prodotto, leggere con attenzione i file readme, le note sulla versione e/o l'ultima edizione della documentazione appropriata, disponibili sul sito Web Trend Micro all'indirizzo:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Trend Micro, il logo della sfera con una T di Trend Micro, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan e ScanMail sono marchi o marchi registrati di Trend Micro Incorporated. Tutti gli altri nomi di prodotti o società potrebbero essere marchi o marchi registrati dei rispettivi proprietari.

Copyright © 2019. Trend Micro Incorporated. Tutti i diritti riservati.

Codice documento: WFEM108677/190617

Data di pubblicazione: Giugno 2019

Protetto da brevetto U.S.: 5.951.698 e 7.188.369

Questa documentazione illustra le caratteristiche principali del prodotto e/o fornisce le istruzioni per l'installazione in un ambiente di produzione. Prima installare o utilizzare il prodotto, leggere attentamente la documentazione.

Informazioni dettagliate sull'utilizzo di caratteristiche specifiche del prodotto sono disponibili nella guida in linea di Trend Micro e nella Knowledge Base di Trend Micro.

Trend Micro si impegna continuamente a migliorare la propria documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, scrivere all'indirizzo docs@trendmicro.com.

È possibile esprimere un giudizio sulla documentazione al seguente indirizzo:

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

Sommario

Prefazione

Prefazione xiii

Documentazione Worry-Free Business Security xiv

Destinatari xiv

Convenzioni utilizzate nella documentazione xv

Capitolo 1: Presentazione di Worry-Free Business Security Standard e Advanced

Panoramica di Trend Micro Worry-Free Business Security 1-2

Novità della versione 1-2

Principali funzioni e vantaggi 1-3

- Trend Micro Smart Protection Network 1-3
- Servizi di reputazione file 1-4
- Servizi di reputazione Web 1-4
- Email Reputation (solo Advanced) 1-5
- Smart Feedback 1-6
- Filtro URL 1-7

Vantaggi della protezione 1-7

Descrizione delle minacce 1-8

- Virus e minacce informatiche 1-9
- Spyware e grayware 1-11
- Spam 1-12
- Intrusioni 1-12
- Comportamento dannoso 1-12
- Falsi punti di accesso 1-12
- Tentativi di phishing 1-13
- Attacchi tramite invii di posta in massa 1-13
- Minacce Web 1-14

Capitolo 2: Informazioni preliminari

Rete Worry-Free Business Security 2-2

Security Server 2-2
Server di scansione 2-2

Agent 2-4

Console Web 2-4
Apertura della console Web 2-5
Navigazione nella console Web 2-8
Icone della console Web 2-10

Capitolo 3: Installazione degli Agent

Installazione di Security Agent 3-2
Requisiti di installazione del Security Agent 3-2
Considerazioni sull'installazione del Security Agent 3-2
Funzioni disponibili per i Security Agent 3-3
Installazione di Security Agent e supporto IPv6 3-5

Metodi di installazione del Security Agent 3-7
Installazione dalla pagina Web interna 3-9
Installazione con Impostazione script di accesso 3-11
Installazione con Client Packager 3-13
Installazione con Installazione remota 3-17
Installazione con Vulnerability Scanner 3-21
Installazione con notifica e-mail 3-32
Migrazione a un Security Agent 3-33
Esecuzione di operazioni post-installazione sui Security Agent 3-34

Installazione di Messaging Security Agent 3-36
Requisiti di installazione di Messaging Security Agent ... 3-36
Installazione del Messaging Security Agent (solo Advanced) 3-36

Rimozione di agent 3-39
Rimozione di agent dalla console Web 3-40
Disinstallazione di agent dalla console Web 3-40
Disinstallazione di Security Agent dall'endpoint 3-41

Disinstallazione del Messaging Security Agent da Microsoft Exchange Server (solo Advanced) 3-42

Capitolo 4: Gestione dei dispositivi

Utilizzo della struttura dei dispositivi 4-2

Utilizzo dei comandi dei dispositivi 4-5

Aggiunta degli agent ai gruppi 4-7

Aggiunta di gruppi 4-8

Personalizzazione delle colonne dell'elenco dispositivi 4-9

Spostamento di agent 4-11

Spostamento di Security Agent tra gruppi 4-12

Spostamento di agent tra Security Server utilizzando la console Web 4-13

Spostamento di un Security Agent tra Security Server con Client Mover 4-14

Replica delle impostazioni 4-16

Replica delle impostazioni del gruppo del Security Agent 4-16

Replica delle impostazioni di Messaging Security Agent (solo Avanzate) 4-17

Importazione ed esportazione delle impostazioni dei gruppi del Security Agent 4-18

Esportazione delle impostazioni 4-19

Importazione delle impostazioni 4-20

Capitolo 5: Gestione delle impostazioni di sicurezza di base per i Security Agent

Riepilogo delle Impostazioni di sicurezza base per i Security Agent 5-2

Metodi di scansione 5-3

Configurazione dei metodi di scansione 5-5

Scansione in tempo reale per i Security Agent 5-7
Configurazione della scansione in tempo reale per i Security Agent 5-7
Intelligenza computazionale predittiva 5-8
Configurazione di Intelligenza computazionale predittiva 5-10
Monitoraggio del comportamento 5-11
Configurazione del monitoraggio del comportamento ... 5-12
Programmi affidabili 5-17
Configurazione di un programmi affidabili 5-17
Directory di quarantena 5-18
Configurazione della directory di quarantena 5-20
Reputazione Web 5-21
Configurazione della reputazione Web per Security Agent 5-23
Filtro URL 5-24
Configurazione del filtro URL 5-24
URL approvati/bloccati 5-25
Configurazione degli URL approvati/bloccati 5-26
Firewall 5-27
Configurazione del firewall 5-30
Utilizzo delle eccezioni Firewall 5-31
Disattivazione del firewall su un gruppo di agent 5-34
Disattivazione del firewall su tutti gli agent 5-34
Controllo dispositivo 5-35
Configurazione del controllo dispositivo 5-35
Strumenti utente 5-37
Configurazione degli strumenti dell'utente 5-38
Privilegi degli agenti 5-38
Configurazione dei privilegi agente 5-39

Capitolo 6: Gestione delle Impostazioni di sicurezza di base per i Messaging Security Agent (solo Advanced)

Messaging Security Agent 6-2
Scansione dei messaggi e-mail da parte di Messaging Security Agent 6-3
Impostazioni predefinite di Messaging Security Agent 6-4

Configurazione della scansione in tempo reale per i Messaging Security Agent 6-5
Configurazione della scansione in tempo reale per Messaging Security Agent 6-6

Anti-Spam 6-6
Servizi Email Reputation 6-8
Scansione dei contenuti 6-10

Filtro dei contenuti 6-16
Gestione delle regole del filtro dei contenuti 6-17
Tipi di regole di filtro dei contenuti 6-21
Aggiunta di regole di filtro dei contenuti per tutte le condizioni di associazione 6-22
Aggiunta di una regola di filtro dei contenuti per le condizioni di associazione 6-25
Aggiunta di una regola di monitoraggio del filtro dei contenuti 6-28
Creazione di eccezioni alle regole per il filtro dei contenuti 6-31

Prevenzione della perdita di dati 6-32
Lavoro di preparazione 6-33
Gestione delle regole per Prevenzione della perdita di dati 6-34
Regole per la Prevenzione della perdita di dati predefinite 6-41
Aggiunta delle regole per Prevenzione della perdita di dati 6-42

Blocco allegati 6-48
Configurazione del blocco degli allegati 6-49

Reputazione Web 6-51
Configurazione della Reputazione Web per Messaging Security Agent 6-53
Mobile Security 6-55
Supporto di Mobile Security 6-56
Configurazione del controllo accesso dispositivo 6-57
Annullamento della cancellazione dei dati di un dispositivo in attesa 6-58
Cancellazione manuale dei dati dai dispositivi 6-59
Configurazione dei criteri di sicurezza 6-59
Quarantena per i Messaging Security Agent 6-65
Consultazione delle directory di quarantena 6-66
Visualizzazione dei risultati della query e azioni correttive 6-68
Gestione delle directory di quarantena 6-70
Configurazione delle directory di quarantena 6-71
Impostazioni di notifica per i Messaging Security Agent 6-72
Configurazione delle impostazioni di notifica per i Messaging Security Agent 6-74
Configurazione di Manutenzione spam 6-74
Gestione della End User Quarantine 6-76
Assistenza Trend Micro/Programma di debug 6-78
Generazione di rapporti del programma di debug di sistema 6-79
Monitoraggio in tempo reale 6-80
Uso del Monitoraggio in tempo reale 6-80
Aggiunta di una declinazione di responsabilità ai messaggi e-mail in uscita 6-81

Capitolo 7: Gestione delle scansioni

Informazioni sulle scansioni 7-2
Scansione in tempo reale 7-3
Scansione manuale 7-3
Esecuzione di scansioni manuali 7-4

Scansione pianificata 7-7
Configurazione delle scansioni pianificate 7-7
Destinazioni di scansione e azioni per i Security Agent 7-10
Destinazioni di scansione e azioni per i Messaging Security Agent 7-18

Capitolo 8: Gestione degli aggiornamenti

Panoramica sugli aggiornamenti 8-2
Componenti da aggiornare 8-4
Hotfix, patch e service pack 8-10
Aggiornamenti del Security Server 8-11
Configurazione dell'origine di aggiornamento del Security Server 8-13
Aggiornamento manuale del Security Server 8-14
Configurazione degli aggiornamenti pianificati per il Security Server 8-15
Rollback dei componenti 8-17
Aggiornamenti di Security Agent e Messaging Security Agent 8-18
Aggiornamenti automatici 8-18
Esecuzione di un aggiornamento manuale 8-18
Suggerimenti e promemoria per l'aggiornamento di un agent 8-19
Update Agent 8-20
Configurazione degli Update Agent 8-22

Capitolo 9: Utilizzo dello stato in tempo reale

Stato in tempo reale 9-2
Centro azioni 9-3
Rilevamenti dei rischi per la sicurezza nel tempo 9-8
Riepilogo ransomware 9-17
Stato della licenza 9-22
Riepilogo server Exchange 9-22
Stato agent 9-22

Capitolo 10: Gestione delle notifiche

Utilizzo delle notifiche 10-2
Configurazione degli eventi per le notifiche 10-4
Variabili token 10-6

Capitolo 11: Gestione delle impostazioni globali

Impostazioni globali 11-2
Configurazione delle impostazioni del proxy Internet 11-3
Configurazione delle impostazioni del server SMTP 11-4
Configurazioni delle impostazioni di desktop/server 11-5
Configurazione delle impostazioni di sistema 11-10
Configurazione delle impostazioni dell'Elenco eccezioni ... 11-14

Capitolo 12: Utilizzo dei registri e dei rapporti

Registri 12-2
Utilizzo delle query del registro 12-4
Rapporti 12-5
Uso dei segnalazioni singole 12-6
Uso dei rapporti pianificati 12-7
Interpretazione dei rapporti 12-11
Operazioni di manutenzione per rapporti e registri 12-14

Capitolo 13: Esecuzione di operazioni di amministrazione

Modifica della password della console Web 13-2
Operazioni relative a Plug-in Manager 13-2
Gestione della licenza di prodotto 13-3
Configurazione delle impostazioni di aggiornamento dei prodotti 13-5
Configurazione delle notifiche di aggiornamento dei prodotti 13-6

Partecipazione al programma Smart Feedback 13-7
Modifica della lingua dell'interfaccia dell'Agent 13-7
Salvataggio e ripristino delle impostazioni del programma .. 13-8
Disinstallazione di Security Server 13-10

Capitolo 14: Uso degli strumenti di gestione

Tipi di strumenti 14-2
Trend Micro Remote Manager Agent 14-3
Installazione di Trend Micro Remote Manager Agent (utenti del portale delle licenze del cliente) 14-4
Installazione di Trend Micro Remote Manager Agent (utenti della piattaforma di gestione delle licenze) 14-6
Gestione degli Agent dal server gestito 14-8
Backup e ripristino delle impostazioni dell'Agent 14-13
Risparmio di spazio su disco 14-15
Esecuzione di Disk Cleaner sul Security Server 14-15
Esecuzione di Disk Cleaner sul Security Server da interfaccia della riga di comando 14-17
Risparmio di spazio su disco sui client 14-17
Spostamento di database Scan Server 14-18
Ripristino dei file crittografati 14-19
Decrittografia e ripristino di file sul Security Agent 14-20
Decrittografia e ripristino di file sul Security Server, directory di quarantena personalizzata o Messaging Security Agent 14-21
Ripristino dei messaggi e-mail Transport Neutral Encapsulation Format 14-23
Utilizzo dello strumento ReGenID 14-23
Gestione dei componenti aggiuntivi di SBS e EBS 14-24
Installazione dei componenti aggiuntivi di SBS e EBS manualmente 14-25
Uso dei componenti aggiuntivi di SBS e EBS 14-25

Appendice A: Icone dei Security Agent

Controllo dello stato dei Security Agent A-2

Visualizzazione delle icone di Security Agent nella barra delle applicazioni di Windows A-4

Accesso al flyover della console A-5

Appendice B: Supporto dell'IPv6 in Worry-Free Business Security

Supporto IPv6 per Worry-Free Business Security e i Security Agent B-2
- Requisiti IPv6 del Security Server B-2
- Requisiti del Messaging Security Agent B-3
- Limitazioni del server IPv6 puro B-3
- Limitazioni del Security Agent IPv6 puro B-4

Configurazione indirizzi IPv6 ..... B-5

Schermate che visualizzano gli indirizzi IP B-6

Appendice C: Assistenza tecnica

Risorse per la risoluzione dei problemi C-2
- Utilizzo del portale di supporto C-2
- Enciclopedia delle minacce C-2

Come contattare Trend Micro C-3
- Semplificazione della chiamata all'assistenza tecnica C-4

Invio di contenuti sospetti a Trend Micro C-4
- Email Reputation Services C-5
- Servizi di reputazione file C-5
- Servizi di reputazione Web C-5

Altre risorse C-6
- Centro di download C-6
- Riscontri sulla documentazione C-6

Appendice D: Nozioni e terminologia prodotti

Patch critica D-2

Hotfix D-2

IntelliScan D-2
IntelliTrap D-3
Sistema di rilevamento anti-intrusione D-3
Parole chiave D-5
Patch D-9
Espressioni regolari D-10
Elenco di esclusione scansione D-18
Service Pack D-25
Porta dei cavalli di Troia D-25
File non disinfettabili D-26

Indice

Indice IN-1

Prefazione

Prefazione

Guida per l'amministratore di Trend Micro™ Worry-Free™ Business Security. Questo documento contiene le informazioni introduttive e illustra le procedure per l'installazione degli agent e per la gestione di agent e Security Server.

Documentazione Worry-Free Business Security

La documentazione di Worry-Free Business Security include:

TABELLA 1. Documentazione Worry-Free Business Security

DOCUMENTAZIONE	DESCRIZIONE
Guida all'installazione e all'aggiornamento	un documento PDF che illustra i requisiti e le procedure di installazione del Security Server e l'aggiornamento del server e degli agenti
Guida dell'amministratore	un documento PDF contenente le informazioni introduttive, le procedure per l'installazione del client e la gestione di Security Server e agente
Guida	File HTML compilati in formato WebHelp o CHM che forniscono procedure, consigli di utilizzo e informazioni specifiche
File Readme	contiene un elenco di problemi noti e la procedura di base per l'installazione. Contiene inoltre le informazioni più recenti sul prodotto che non è stato possibile inserire nella documentazione nel software né in quella stampata
Knowledge Base	Un database online contenente informazioni utili per la risoluzione dei problemi. Fornisce le informazioni più recenti sui problemi noti riscontrati nell'utilizzo dei prodotti. Per accedere alla Knowledge Base, visitare il seguente sito Web: http://esupport.trendmicro.com

Le versioni aggiornate dei documenti PDF e del file Readme sono disponibili per il download alla pagina seguente:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Destinatari

La documentazione di Worry-Free Business Security è destinata agli utenti seguenti:

- **Amministratori della sicurezza**: responsabili della gestione di Worry-Free Business Security, comprese le attività di gestione e installazione di Security Server e agent. Si presuppone che questi utenti abbiano conoscenze avanzate di reti e gestione dei server.
- **Utenti finali**: utenti che hanno il client Security Agent installato nei propri computer. Le conoscenza informatiche di questi utenti variano da principiante a utente esperto.

Convenzioni utilizzate nella documentazione

Per facilitare l'individuazione e l'interpretazione delle informazioni, la documentazione di Worry-Free Business Security segue le convenzioni illustrate di seguito:

TABELLA 2. Convenzioni utilizzate nella documentazione

CONVENZIONE	DESCRIZIONE
TUTTO MAIUSCOLO	Acronimi, abbreviazioni e nomi di alcuni comandi e tasti della tastiera
Grassetto	Menu e comandi dei menu, pulsanti dei comandi, schede, opzioni e attività
Corsivo	Riferimenti ad altra documentazione o a componenti di nuova tecnologia
<Testo>	Indica che il testo all'interno delle parentesi angolari deve essere sostituito da dati effettivi. Ad esempio, `C:\Programmi\<nome_file>` può corrispondere a `C:\Programmi\esempio.jpg`.
Nota	Indica note per la configurazione o raccomandazioni
Suggerimento	Indica informazioni su procedure ottimali e consigli di Trend Micro

Convenzione	Descrizione
AVVERTENZA!	Indica avvisi relativi ad attività che possono comportare danni per i computer della rete

Capitolo 1

Presentazione di Worry-Free™ Business Security Standard e Advanced

In questo capitolo viene fornita una panoramica su Worry-Free Business Security (Worry-Free Business Security).

Panoramica di Trend Micro Worry-Free Business Security

Trend Micro Worry-Free Business Security (Worry-Free Business Security) protegge utenti e risorse delle piccole imprese dal furto di dati e identità, siti pericolosi e spam (solo Advanced).

Questo documento fornisce informazioni per Worry-Free Business Security sia Standard che Advanced. Le sezioni e i capitoli relativi alla versione Advanced sono contrassegnati come "(Solo Advanced)".

Parte di Trend Micro Smart Protection Network, Worry-Free Business Security è:

- **Più sicura**: Blocca virus, spyware, spam (Solo Advanced) e minacce Web prima che raggiungano i client. Il filtro URL blocca l'accesso ai siti Web pericolosi e consente di migliorare la produttività.
- **Più intelligente**: La scansione e gli aggiornamenti rapidi bloccano le nuove minacce, che hanno così un impatto minimo sui client.
- **Più semplice**: Facile da implementare e senza bisogno di amministrazione, Worry-Free Business Security rileva più efficacemente le minacce per consentire di concentrarsi sul lavoro invece che sulla protezione.

Novità della versione

Nella tabella seguente, vengono illustrate le nuove funzionalità e i miglioramenti inclusi in questa versione di Worry-Free Business Security.

Funzionalità/ Miglioramento	Descrizione
Scansione aggressiva	Worry-Free Business Security include ora la funzione Scansione aggressiva per offrire scansione e disinfezione più approfondite degli endpoint infetti. Per ulteriori informazioni, consultare *Utilizzo della struttura dei dispositivi a pagina 4-2* e *Utilizzo dei comandi dei dispositivi a pagina 4-5*.
Protezione avanzata contro malware senza file	Worry-Free Business Security ora utilizza le più recenti tecnologie di prevenzione del malware senza file per proteggere i dispositivi dagli attacchi senza file.
Supporto sistema operativo	Worry-Free Business Security ora supporta l'installazione di Security Server e Agent sui seguenti sistemi operativi: • Aggiornamento Windows 10 maggio 2019 • Windows Server 2019

Principali funzioni e vantaggi

Worry-Free Business Security comprende le seguenti funzioni e vantaggi:

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ è un'infrastruttura per la sicurezza dei contenuti client cloud di prossima generazione concepita per proteggere gli utenti contro i rischi per la sicurezza e le minacce Web. Comprende soluzioni in sede e gestite da host Trend Micro per proteggere gli utenti quando sono in rete, a casa o in viaggio. Smart Protection Network utilizza agent più leggeri che accedono alla combinazione "in-the-cloud" unica di tecnologie di reputazione file, posta elettronica e Web, nonché ai database delle minacce. La protezione dei clienti viene aggiornata e rafforzata automaticamente con il progressivo aumento di prodotti, servizi e utenti che accedono alla rete, creando in tal modo un servizio di vigilanza continua in tempo reale.

Per ulteriori informazioni su Smart Protection Network, visitare:

http://www.trendmicro.it/tecnologia-innovazione/la-nostra-tecnologia/smart-protection-network/

Servizi di reputazione file

I Servizi di reputazione file verificano la reputazione di ciascun file rispetto a un database "in-the-cloud". Poiché le informazioni sulle minacce informatiche sono memorizzate in-the-cloud, sono disponibili immediatamente a tutti gli utenti. Le reti di trasmissione dei contenuti ad elevate prestazioni e i server di cache locale garantiscono una latenza minima durante la fase di controllo. L'architettura cloud-client offre una protezione più immediata ed elimina l'obbligo dell'implementazione dei pattern, oltre a ridurre in misura significativa l'impatto complessivo del client sulle risorse.

I Security Agent devono essere in modalità Smart Scan per utilizzare i Servizi di reputazione file. In questo documento questi agent sono definiti come **agent smart scan**. Gli agent che non si trovano in modalità Smart Scan non utilizzano i servizi di reputazione file e sono denominati **agent di scansione convenzionali**. Gli amministratori Worry-Free Business Security possono configurare tutti o vari agenti in modalità Smart Scan.

Servizi di reputazione Web

Avvalendosi di uno dei database di reputazione dei domini più grandi del mondo, la tecnologia di reputazione Web di Trend Micro tiene traccia della credibilità dei domini Web assegnando un punteggio di reputazione basato su fattori quali la maturità del sito Web, i cambiamenti di percorso e le indicazioni di attività sospette rilevate mediante l'analisi del comportamento delle minacce informatiche. I siti sono continuamente sottoposti alla reputazione Web e l'accesso ai siti infetti viene bloccato. Le informazioni di reputazione Web contribuiscono a garantire che le pagine visitate dagli utenti siano sicure e prive di minacce Web quali minacce informatiche, spyware e frodi di phishing volte a indurre gli utenti a fornire informazioni personali. Per aumentare l'accuratezza e ridurre i falsi allarmi, la tecnologia

di reputazione Web di Trend Micro assegna punteggi di reputazione alle singole pagine e ai singoli collegamenti anziché classificare o bloccare siti interi. Spesso, infatti, solo alcune parti di siti legittimi sono pericolose e la reputazione può cambiare con il tempo.

Gli Agent soggetti ai criteri di Reputazione Web utilizzano i servizi Reputazione Web. Gli amministratori di Worry-Free Business Security possono sottoporre tutti o alcuni degli agent a tali criteri.

Email Reputation (solo Advanced)

La tecnologia di reputazione e-mail di Trend Micro convalida gli indirizzi IP verificandoli a fronte di un database della reputazione di fonti di spam note e utilizzando un servizio dinamico capace di valutare la reputazione del mittente e-mail in tempo reale. Le classificazioni della reputazione vengono perfezionate tramite un'analisi continua del "comportamento" degli indirizzi IP, della portata dell'attività e della cronologia precedente. I messaggi e-mail dannosi vengono bloccati in-the-cloud in base all'indirizzo IP del mittente, impedendo così a minacce come zombie o botnet di raggiungere la rete dell'utente.

La tecnologia Email Reputation identifica lo spam in base alla reputazione del Mail Transport Agent (MTA) di origine. In questo modo si riduce il carico di lavoro sul Security Server. Con la funzione Email Reputation attivata, tutto il traffico SMTP viene controllato dai database IP per verificare se l'indirizzo IP di origine è affidabile o se invece è stato classificato come vettore di spam noto.

Email Reputation offre i due livelli di servizio

- **Standard**:Il servizio standard si affida a un database in grado di identificare la reputazione di circa due miliardi di indirizzi IP. Gli indirizzi IP che vengono costantemente associati alla diffusione di messaggi di spam vengono aggiunti a un database e solo raramente rimossi.
- **Avanzato**: Il livello di servizio avanzato offre un servizio DNS basato su query come il servizio standard. La base di questo servizio è il database di reputazione standard, unitamente al database di reputazione

dinamico in tempo reale che blocca i messaggi provenienti da fonti note e sospette di spam.

Quando viene individuato un messaggio e-mail proveniente da un indirizzo IP bloccato o sospetto, Email Reputation Services (ERS) lo blocca prima che questo raggiunga l'infrastruttura. Se il servizio ERS blocca i messaggi e-mail provenienti da un indirizzo IP che l'utente ritiene sicuro, è possibile aggiungere questo indirizzo all'elenco di indirizzi IP approvati.

Smart Feedback

Trend Micro Smart Feedback rappresenta un canale di comunicazione costante tra i prodotti Trend Micro e le tecnologie e i centri per la ricerca continua delle minacce. Ogni nuova minaccia individuata tramite il controllo di reputazione di routine di ogni singolo cliente aggiorna automaticamente il database completo delle minacce di Trend Micro, consentendo in tal modo di impedire che altri clienti riscontrino la stessa minaccia.

Grazie all'elaborazione continua delle informazioni sulle minacce raccolte attraverso la vasta rete globale di clienti e partner, Trend Micro è in grado di offrire la protezione automatica in tempo reale contro le minacce più recenti e di fornire una migliore sicurezza collettiva, molto simile a un sistema di controllo di protezione reciproco della comunità. Poiché le informazioni sulle minacce raccolte si basano sulla reputazione della fonte di comunicazione, e non sul contenuto della comunicazione specifica, la privacy delle informazioni personali o professionali è sempre protetta.

Esempi di informazioni inviate a Trend Micro:

- Checksum dei file
- Siti Web visitati
- Informazioni sui file, compresi dimensioni e percorsi
- Nomi dei file eseguibili

È possibile interrompere la partecipazione al programma in qualsiasi momento dalla console Web.

Per i dettagli, consultare *Partecipazione al programma Smart Feedback a pagina 13-7*.

Suggerimento

Per proteggere gli endpoint non è necessario partecipare al programma Smart Feedback. La partecipazione è facoltativa ed è possibile sospenderla in qualsiasi momento. Trend Micro consiglia di partecipare al programma Smart Feedback per contribuire a migliorare la protezione complessiva di tutti i clienti Trend Micro.

Per ulteriori informazioni su Smart Protection Network, visitare:

http://www.trendmicro.it/tecnologia-innovazione/la-nostra-tecnologia/smart-protection-network/

Filtro URL

Il filtro URL contribuisce a controllare l'accesso ai siti Web per ridurre i tempi di inattività dei dipendenti, limitare il consumo di ampiezza di banda Internet e creare un ambiente Internet più sicuro. È possibile scegliere un livello di protezione del filtro URL oppure specificare quali tipi di siti Web tenere sotto controllo.

Vantaggi della protezione

La tabella riportata di seguito descrive come i vari componenti di Worry-Free Business Security proteggono i computer dalle minacce.

TABELLA 1-1. Vantaggi della protezione

MINACCIA	PROTEZIONE
Virus/malware. Virus, cavalli di Troia, worm, backdoor e rootkit **Spyware/Grayware**. Spyware, dialer, strumenti per hacker, applicazioni per decifratura password, adware, programmi ingannevoli e keylogger.	Scansioni basate su file (scansione manuale, scansione in tempo reale, scansione pianificata)
Minacce per la sicurezza trasmesse tramite messaggi e-mail	**Scansione posta POP3 Mail** in Security Agent
Worm/virus in rete e intrusioni	Firewall in Security Agent
Siti Web e siti di phishing presumibilmente pericolosi	Reputazione Web e Filtro URL nel Security Agent
Minacce alla sicurezza che si diffondono attraverso periferiche USB e altre periferiche esterne	Controllo dispositivi in Security Agent
Comportamento dannoso	Monitoraggio del comportamento in Security Agent
Programmi ransomware che colpiscono documenti eseguiti negli endpoint	Monitoraggio del comportamento e Intelligenza computazionale predittiva nel Security Agent

Descrizione delle minacce

Le organizzazioni che non dispongono di personale addetto alla sicurezza e con politiche di sicurezza troppo permissive sono esposte in modo crescente alle minacce, anche se sono dotate di infrastrutture di sicurezza di base. Quando vengono scoperte le minacce, è possibile che si siano già diffuse in molte risorse informatiche, richiedendo tempo e sforzi considerevoli per l'eliminazione completa. Inoltre i costi imprevisti correlati all'eliminazione delle minacce possono risultare sconcertanti.

Le informazioni sulla sicurezza di rete di Trend Micro e i server cloud che compongono Trend Micro Smart Protection Network individuano e rispondono alle minacce di nuova generazione.

Virus e minacce informatiche

Esistono decine di migliaia di virus e malware e ogni giorno ne vengono creati di nuovi. Sebbene in origine fossero diffusi soprattutto in DOS e Windows, i virus informatici odierni, grazie alla loro capacità di sfruttare le vulnerabilità possono causare notevoli danni alle reti aziendali, ai sistemi e-mail e ai siti Web.

- **Programma Joke**: Programma simile a un virus che spesso manipola l'aspetto degli oggetti sul monitor di un computer.
- **probabile virus/malware**: File sospetti con alcune caratteristiche di virus/minacce informatiche. Per dettagli, consultare l'Enciclopedia delle minacce di Trend Micro:

  http://about-threats.trendmicro.com/threatencyclopedia.aspx
- **Rootkit**: Un programma o una raccolta di programmi che installa ed esegue un codice su un sistema senza il consenso o la consapevolezza dell'utente finale. Utilizza un virus stealth per mantenere una presenza costante e non rilevabile sul computer. I rootkit non infettano i computer ma cercano piuttosto di fornire un ambiente non rilevabile per consentire l'esecuzione di un codice dannoso. I rootkit vengono installati sui sistemi tramite social engineering, con l'esecuzione di minacce informatiche o semplicemente accedendo ad un sito Web dannoso. Una volta installato, l'aggressore può virtualmente eseguire qualunque funzione sul sistema, incluso l'accesso remoto, le intercettazioni, operazioni che nascondono i processi, i file, le chiavi di registro e i canali di comunicazione.
- **Cavallo di Troia**: Questo tipo di processo utilizza spesso le porte per accedere a computer e programmi eseguibili. I cavalli di Troia non sono in grado di riprodursi, ma risiedono nei sistemi per compiere operazioni dannose, ad esempio l'apertura delle porte, per consentire l'ingresso degli hacker. Le soluzioni antivirus tradizionali sono in grado di rilevare

e rimuovere i virus ma non i cavalli di Troia, soprattutto se sono già in esecuzione nel sistema.

- **Virus**: Programma in grado di replicarsi. Per farlo, un virus deve attaccarsi ad altri file di programma che gli consentono di attivarsi quando il programma che lo ospita viene eseguito, inclusi:
  - **Codice dannoso ActiveX**: Codice presente nelle pagine Web che eseguono controlli ActiveX™.
  - **Virus del settore boot**: Virus che infetta il settore di boot di una partizione o un disco.
  - **File COM ed EXE infettante**: Programma eseguibile con estensione `.com` o `.exe`.
  - **Codice dannoso Java**: Codice virus indipendente dal sistema operativo scritto o incluso in un codice Java™.
  - **Virus da macro**: Virus codificato come una macro di applicazione e spesso incluso in un documento.
  - **Packer**: Programma eseguibile compresso e/o codificato per Windows o Linux™ (spesso è un cavallo di Troia). La compressione di programmi eseguibili ne rende più difficile il rilevamento per i prodotti antivirus.
  - **Virus di prova**: Un file inerte che agisce come un virus reale e può essere rilevato dal software di scansione antivirus. I virus di prova, come gli script di prova EICAR, possono essere utilizzati per verificare che l'antivirus installato funzioni correttamente.
  - **Virus VBScript**, **JavaScript** o **HTML**: Virus presente in una pagina Web e scaricato tramite un browser.
  - **Worm**: Programma (o gruppo di programmi) autonomo in grado di diffondere copie funzionanti di se stesso o di suoi segmenti ad altri sistemi, spesso tramite e-mail.
  - **Altro**: Virus/minacce informatiche che non rientrano nelle altre categorie.

Spyware e grayware

Ci sono altre minacce che potrebbero mettere a repentaglio i Endpoint, oltre ai virus e alle minacce informatiche. Per spyware e grayware si intendono applicazioni o file non classificati come virus o cavalli di Troia ma che possono avere un'influenza negativa sulle prestazioni dei client della rete e introdurre notevoli rischi per la sicurezza, la riservatezza e causare problemi legali alle organizzazioni. Spesso spyware e grayware attivano una varietà di azioni indesiderate e pericolose come la visualizzazione di irritanti finestre pop-up, la registrazione delle sequenze di tasti premute dall'utente o l'esposizione delle vulnerabilità del client agli attacchi.

Se si trova un'applicazione o un file che Worry-Free Business Security non può rilevare come grayware ma si pensa che sia un tipo di grayware, inviarlo a Trend Micro per un'analisi:

https://success.trendmicro.com/solution/1059565

Tipo	Descrizione
Spyware	Raccoglie dati, quali nomi utente e password e li trasmette a terzi.
Adware	Visualizza delle pubblicità e raccoglie dati, quali le preferenze di navigazione Web in modo da indirizzare pubblicità mirata attraverso un browser Web.
Dialer	Modifica le impostazioni Internet del client e può forzare il client a chiamare numeri telefonici predeterminati attraverso un modem. Si tratta in genere di numeri a pagamento o internazionali che rappresentano un notevole costo per l'organizzazione.
Programma Joke	Causa un comportamento anomalo del client come l'apertura e la chiusura dell'unità CD-ROM o la visualizzazione di diverse finestre di dialogo.
Strumento per hacker	Consente agli hacker di penetrare nel computer.
Strumento di accesso remoto	Consente agli hacker di accedere al computer in remoto e controllarlo.

Tipo	Descrizione
Applicazione di decifratura delle password	Consente agli hacker di decifrare i nomi utente e le password.
Altri	Altri tipi di programmi potenzialmente dannosi.

Spam

Il termine spam indica tutti i messaggi e-mail non richiesti (messaggi di posta indesiderati), spesso di natura commerciale, inviati indiscriminatamente a elenchi di diversi destinatari, individui o newsgroup. Esistono due tipi di spam: I messaggi e-mail commerciali non richiesti (UCE) e i messaggi e-mail indesiderati (UBE).

Intrusioni

Per intrusione si intende l'accesso a una rete o a un client compiuto con la forza o senza autorizzazione. Può indicare anche il superamento della protezione di una rete o un client.

Comportamento dannoso

Un comportamento dannoso è quello che apporta delle modifiche non autorizzate effettuate da un software al sistema operativo, alle chiavi di registro, ad altri software o a file e cartelle.

Falsi punti di accesso

Con falsi punti di accesso, detti anche Evil Twin, si intendono dei punti di accesso Wi-Fi disponibili presso diverse strutture che sembrano legittimi ma che in realtà sono stati realizzati da hacker per spiare le comunicazioni wireless.

Tentativi di phishing

I programmi phish o phishing sono metodi di frode in rapida ascesa che, presentandosi come sito Web legittimo, tentano di raggirare gli utenti Web inducendoli a divulgare informazioni riservate.

In una situazione tipo, un utente ignaro riceve un messaggio e-mail urgente (apparentemente autentico) che lo informa della presenza di un problema nell'account che deve essere immediatamente risolto, pena la chiusura dell'account stesso. Il messaggio e-mail include un URL a un sito Web apparentemente esistente; si tratta infatti di una semplice copia di un indirizzo e-mail e di un sito Web autentici, ma il backend che riceve i dati raccolti è diverso.

Il messaggio invita l'utente ad accedere al sito e confermare alcune informazioni relative all'account. In questo modo, un hacker riceve i dati forniti dall'utente, quali nome di accesso, password, numero di carta di credito o codice fiscale.

Il phishing è rapido, economico e facile da realizzare. Potenzialmente, è anche alquanto redditizio per i criminali che lo praticano. Rilevare il phishing è difficile anche per gli utenti più esperti. È difficile rintracciarlo anche per le forze dell'ordine. È quasi impossibile perseguirlo.

Si prega segnalare a Trend Micro qualsiasi sito Web che si sospetta possa essere un sito di phishing. Per ulteriori informazioni, consultare *Invio di contenuti sospetti a Trend Micro a pagina C-4*.

Attacchi tramite invii di posta in massa

I virus e le minacce informatiche per e-mail hanno la capacità di diffondersi mediante i messaggi e-mail grazie all'automatizzazione del client e-mail del computer infetto o alla diffusione di virus/minacce informatiche. Le caratteristiche legate all'invio di posta in massa descrivono una situazione in cui un'infezione si diffonde rapidamente in un ambiente Microsoft Exchange. Trend Micro ha elaborato un motore di scansione in grado di rilevare i comportamenti che in genere si verificano nel corso di un attacco di posta in massa. Questi comportamenti vengono registrati nel file di pattern antivirus che viene aggiornato utilizzando i server Trend Micro ActiveUpdate.

È possibile attivare il Messaging Security Agent (solo Advanced) in modo che esegua determinate operazioni per contrastare gli attacchi di posta in massa ogniqualvolta viene rilevato un comportamento del genere. L'operazione prevista per contrastare un attacco di posta in massa ha la priorità su qualsiasi altra operazione. L'operazione predefinita nel caso di attacchi di posta in massa è l'eliminazione del messaggio.

Ad esempio: Messaging Security Agent viene configurato per mettere in quarantena i messaggi quando rileva un'infezione da worm o cavallo di Troia. È possibile anche attivare il riconoscimento dei comportamenti di invio di posta in massa e impostare l'agent in modo che elimini tutti i messaggi che mostrano un comportamento di invio di posta in massa. L'agent riceve un messaggio contenente un worm come ad esempio una variante di MyDoom. Questo worm utilizza il proprio motore SMTP per inviarsi a indirizzi di posta elettronica raccolti dal computer infetto. Quando l'agent rileva il worm MyDoom e riconosce il comportamento di invio di posta in massa, elimina il messaggio e-mail contenente il worm, invece di metterlo in quarantena come avverrebbe per altri tipi di worm.

Minacce Web

Le minacce Web comprendono un'ampia gamma di minacce che hanno origine da Internet. I metodi di tali minacce sono sofisticati e usano una combinazione di diversi file e tecniche piuttosto che un singolo file o approccio. Ad esempio, i creatori di minacce Web modificano costantemente la versione o la variante utilizzata. Poiché la minaccia Web non si trova solo sul client infetto, ma in una determinata posizione di un sito Web, il creatore della minaccia ne modifica continuamente il codice per evitare che venga individuata.

Negli ultimi anni, persone precedentemente classificate come hacker, autori di virus, spammer e creatori di spyware sono diventati noti come cybercriminali. Le minacce Web consentono a costoro di perseguire due tipi di obiettivi. Il primo consiste nell'appropriarsi di informazioni da rivendere. Ciò determina la violazione della riservatezza delle informazioni in forma di furto di identità Il client infettato può essere utilizzato per un attacco di phishing o per altre attività volte a carpire informazioni. Tra l'altro, questo tipo di minaccia rischia di mettere a repentaglio la fiducia nei confronti del

Web commerce e quindi l'affidabilità delle transazioni su Internet. Il secondo obiettivo consiste nell'appropriarsi della capacità della CPU di un utente allo scopo di utilizzarla per condurre attività a fini di lucro. Tali attività includono l'invio di posta indesiderata (spam) e l'esecuzione di attacchi di tipo DoS (Denial of Service) o attività di tipo pay-per-click.

Capitolo 2

Informazioni preliminari

In questo capitolo viene descritto come far funzionare Worry-Free Business Security.

Rete Worry-Free Business Security

Worry-Free Business Security è composto dai seguenti componenti:

- *Security Server a pagina 2-2*
- *Agent a pagina 2-4*
- *Console Web a pagina 2-4*

Security Server

Security Server rappresenta il fulcro di Worry-Free Business Security Advanced. Security Server ospita la console Web, una console di gestione centralizzata Web per Worry-Free Business Security. Il Security Server consente di installare gli agent sui client presenti in una rete e, unitamente agli agent, forma una relazione agent-server. Con Security Server è possibile consultare le informazioni sullo stato, visualizzare gli Agent, configurare la sicurezza del sistema e scaricare i componenti da una postazione centralizzata. Security Server contiene inoltre il database in cui memorizza i registri delle minacce informatiche segnalate dagli agent.

Security Server esegue queste importanti funzioni:

- Installa, controlla e gestisce gli agent.
- Scarica i componenti necessari per gli agent. Per impostazione predefinita, il Security Server scarica i componenti dal server Trend Micro ActiveUpdate, per poi distribuirli agli agent.

Server di scansione

Il Security Server comprende un servizio chiamato Scan Server, installato automaticamente durante l'installazione del Security Server. Per questo motivo non è necessario installarlo separatamente. Lo Scan Server funziona con il nome di processo `iCRCService.exe` e compare come **Trend Micro Smart Scan Service** in Microsoft Management Console.

Quando i Security Agent utilizzano un metodo di scansione denominato **smart scan**, lo Scan Server permette a questi agent di eseguire le scansioni in maniera più efficiente. Il processo smart scan è il seguente:

- Il Security Agent esegue la scansione del client in cerca di minacce alla sicurezza utilizzando **Pattern agente Smart Scan**, versione ridotta del tradizionale Virus Pattern. Pattern agente Smart Scan contiene la maggior parte di firme di minacce disponibili nel Virus Pattern.
- Un Security Agent non in grado di determinare il rischio del file durante la scansione, verifica il rischio inviando una query di scansione allo Scan Server. Lo Scan Server verifica il rischio sfruttando il **Pattern per Smart Scan**, che contiene tutte le firme di minacce non disponibili nel Pattern agente Smart Scan.
- Il Security Agent memorizza nella cache il risultato della query di scansione fornito dal server di scansione per migliorare le prestazioni della scansione.

Conservando in hosting alcune delle definizioni delle minacce, lo Scan Server aiuta a ridurre il consumo di banda per i Security Agent durante il download dei componenti. Invece di scaricare il Virus Pattern, i Security Agent scaricano Pattern agente Smart Scan che è di dimensioni significativamente inferiori.

Se i Security Agent non sono in grado di connettersi allo Scan Server, inviano query di scansione a Trend Micro Smart Protection Network, che ha il medesimo ruolo dello Scan Server.

Non è possibile disinstallare lo Scan Server separatamente dal Security Server. Per non utilizzare lo Scan Server:

1. Sul computer del Security Server, aprire Microsoft Management Console e disattivare il servizio **Trend Micro Smart Scan Service**.
2. Nella console Web, far passare i Security Agent alla scansione convenzionale da **Amministrazione** > **Impostazioni globali** > **scheda Desktop/Server** e selezionare l'opzione **Disattiva Smart Scan Service**.

Agent

Gli agent proteggono i client dalle minacce alla sicurezza. I client includono desktop, server e server Microsoft Exchange. Gli agent Worry-Free Business Security sono:

TABELLA 2-1. Agent Worry-Free Business Security

AGENT	DESCRIZIONE
Security Agent	Protegge desktop e server dalle minacce alla sicurezza e dalle intrusioni
Messaging Security Agent (solo Advanced)	Protegge i server Microsoft Exchange da minacce alla sicurezza trasmesse tramite e-mail

Un agent invia notifiche al Security Server dal quale è stato installato. Per fornire al Security Server i dati più aggiornati riguardanti il client, l'agent invia informazioni sullo stato degli eventi in tempo reale. L'agent riporta eventi quali il rilevamento di minacce, l'avvio e lo spegnimento, l'avvio di una scansione e il completamento di un aggiornamento.

Console Web

La console Web è l'elemento centrale per il monitoraggio dei Security Agent in tutta la rete aziendale. La console è dotata di un insieme di impostazioni e valori predefiniti che è possibile configurare in base ai propri requisiti e alle proprie specifiche di sicurezza. La console Web utilizza tecnologie Internet standard quali Java, CGI, HTML e HTTP.

Utilizzare la console Web per:

- Implementare gli agent sugli endpoint.
- Organizzare gli agent in gruppi logici, per poterli configurare e gestire contemporaneamente.
- Configurare le impostazioni di prodotto e avviare Scansione manuale negli endpoint.

- Ricevere le notifiche e visualizzare i rapporti di registro per le attività correlate alle minacce.
- Ricevere le notifiche e inviare gli avvisi sulle infezioni mediante messaggi e-mail al rilevamento delle minacce negli endpoint.

Apertura della console Web

Aprire la console Web da qualsiasi endpoint sulla rete utilizzando un browser Web supportato. Per ulteriori informazioni sui requisiti del browser, fare riferimento al documento *Requisiti di sistema*.

Procedura

1. Per aprire la console Web, selezionare una delle opzioni riportate di seguito:
   - Sull'endpoint che ospita Security Server, accedere a Desktop e fare clic sul collegamento Worry-Free Business Security.
   - Sull'endpoint che ospita Security Server, fare clic sul **menu Start di Windows** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.
   - Su un qualsiasi endpoint nella rete, aprire un browser Web e digitare quanto segue nella barra degli indirizzi:

     `https://{Nome_Security_Server o Indirizzo IP}:{numero porta}/SMB`

     Ad esempio:

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://my-test-server:8059/SMB`

     `http://192.168.0.10:8059/SMB`

Suggerimento

Se NON si utilizza SSL, digitare `http` invece di `https`. La porta predefinita per le connessioni HTTP è la 8059, mentre per le connessioni HTTP è la 4343.

Se l'ambiente non è in grado di risolvere i nomi di server tramite DNS, utilizzare il nome del server al posto dell'indirizzo IP.

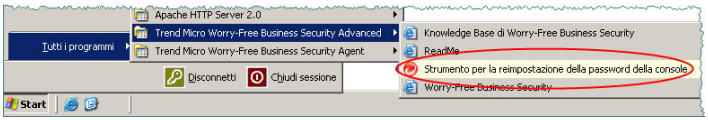
Nel browser viene visualizzata la schermata di accesso di Worry-Free Business Security.

2. Digitare la password e fare clic su **Accedi**.

   Il browser visualizza la schermata **Stato in tempo reale**.

Operazioni successive

Se non è possibile accedere alla console Web, verificare quanto segue.

ELEMENTI DA CONTROLLARE	DETTAGLI
Password	Se la password è stata dimenticata, utilizzare lo Strumento per la reimpostazione della password della console per reimpostarla. È possibile accedere a questo strumento su Security Server nella cartella Trend Micro Worry-Free Business Security del menu Start di Windows. 
Cache del browser	In caso di aggiornamento da una versione precedente di Worry-Free Business Security, il browser e i file della cache del server proxy possono impedire il corretto caricamento della console Web. Cancellare la memoria cache sul browser e su tutti i server proxy che si trovano tra Trend Micro Security Server e l'endpoint in uso per accedere alla console Web.
Certificato SSL	Controllare anche che il server Web funzioni correttamente. Se si sta utilizzando SSL, verificare che il certificato SSL sia ancora valido. Per ulteriori informazioni, consultare la documentazione del server Web.

Elementi da controllare	Dettagli

Impostazioni della directory virtuale	Le impostazioni della directory virtuale potrebbero sollevare dei problemi in caso di esecuzione della console Web su un server IIS e se viene visualizzato il seguente messaggio:
	`Impossibile visualizzare la pagina`
	`HTTP Errore 403.1 - Accesso negato: Esecuzione accesso negata.`
	`Internet Information Services (IIS)`
	È possibile che venga visualizzato questo messaggio quando viene utilizzato uno dei seguenti indirizzi per accedere alla console:
	`http://{nome server}/SMB/`
	`http://{nome server}/SMB/default.htm`
	La console si potrebbe aprire invece senza problemi quando si utilizza il seguente indirizzo:
	`http://{nome server}/SMB/console/html/cgi/cgichkmasterpwd.exe`
	Per risolvere questo problema, controllare le autorizzazioni di esecuzione della directory virtuale SMB.
	Per attivare gli script:
	1. Aprire il gestore di Internet Information Services (IIS).
	2. Nella directory virtuale SMB, selezionare **Proprietà**.
	3. Selezionare la scheda Directory virtuale e impostare le autorizzazioni di esecuzione su `Script` anziché su `nessuna`. Modificare anche le autorizzazioni di esecuzione della directory virtuale di installazione del client.

Navigazione nella console Web

La console Web è composta delle seguenti sezioni principali:

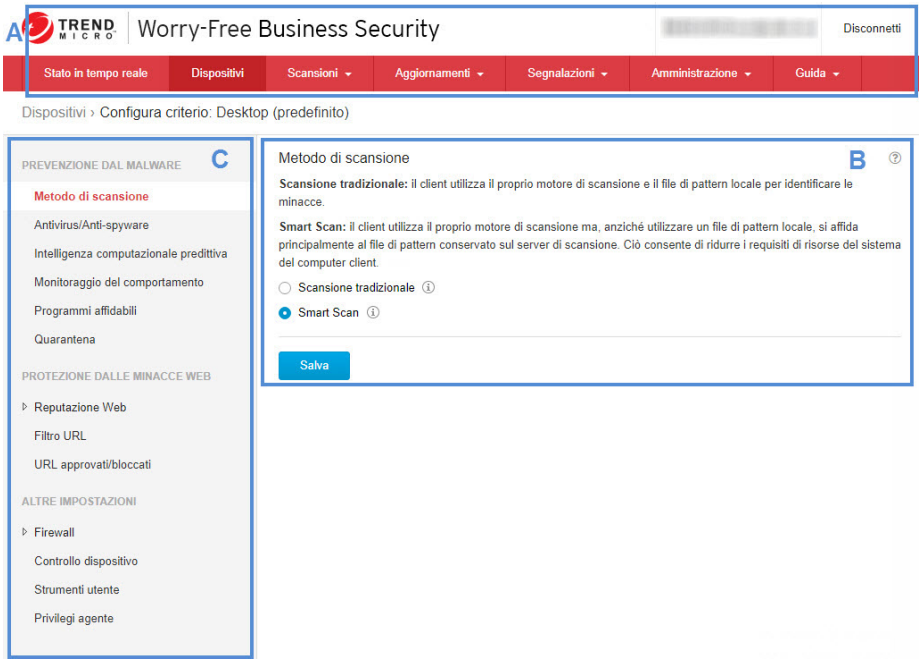


TABELLA 2-2. Sezioni principali della console Web

SEZIONE	DESCRIZIONE
A. Menu principale	Il menu principale si trova lungo il lato superiore della console Web. Viene inoltre fornito il collegamento **Disconnetti** per consentire di terminare la sessione corrente.
B. Area di configurazione	L'area di configurazione si trova sotto le voci del menu principale. Tale area consente di selezionare le opzioni e di configurare le impostazioni in base alla voce di menu selezionata.

Sezione	Descrizione
C. Barra laterale dei menu (non disponibile su tutte le schermate)	La barra laterale dei menu viene visualizzata quando si seleziona un gruppo di Security Agent nella schermata **Dispositivi** e si fa clic su **Configura criterio**. La barra laterale consente di configurare le impostazioni di sicurezza e le scansioni per i computer desktop e server che appartengono al gruppo. Se si seleziona un Messaging Security Agent nella schermata **Dispositivi** (solo Avanzate), è possibile utilizzare la barra laterale per configurare le impostazioni di sicurezza e le scansioni per i server Microsoft Exchange.

Tabella 2-3. Sezione menu principale

Elemento di menu	Description
Stato in tempo reale	Monitora lo stato di sicurezza complessivo dei Security Agent e lo stato operativo del Security Server
Dispositivi	• Personalizzare le impostazioni di sicurezza per gli agent • Replica delle impostazioni tra i gruppi
Scansioni	• Scansione degli endpoint alla ricerca di minacce • Pianificare scansioni per i client
Aggiornamenti	• Controllare i server Trend Micro ActiveUpdate (o l'origine aggiornamenti personalizzata) per individuare i componenti più aggiornati, compresi i file di pattern antivirus, il motore di scansione, i componenti di disinfezione e il programma dell'agent • Configurare l'origine degli aggiornamenti • Assegnare ai Security Agent funzioni di Update Agent
Rapporti	Generare rapporti per tenere traccia delle minaccia e di altri eventi correlati alla sicurezza

Elemento di menu	Description
Amministrazione	• Impostare le notifiche di eventi anomali legati a minacce o al sistema • Configurare le impostazioni globali per facilitare la manutenzione • Utilizzare strumenti di gestione per facilitare la gestione della rete e dei client • Visualizzare le informazioni sulla licenza del prodotto, gestire la password dell'amministratore e garantire la sicurezza dell'ambiente aziendale per quanto riguarda lo scambio di informazioni digitali aderendo al programma Smart Feedback • Automatizzare gli aggiornamenti del prodotto e notificare agli utenti quando risulta disponibile un nuovo pacchetto di aggiornamento
Guida	• Eseguire la ricerca di contenuti e argomenti specifici • Visualizzare la Guida dell'amministratore • Accedere alle informazioni più recenti della Knowledge Base (KB) • Visualizzare informazioni su sicurezza, vendite, assistenza e versione

Icone della console Web

La tabella seguente descrive le icone visualizzate nella console Web e ne illustra il significato.

Tabella 2-4. Icone della console Web

Icona	Descrizione
	Icona Guida. Apre la Guida in linea.
	Icona Aggiorna. Aggiorna la visualizzazione della schermata corrente.
	Icona Espandi/Comprimi sezione. Visualizza/Nasconde le sezioni. È possibile espandere una sola sezione alla volta.
	Icona di informazione. Visualizza le informazioni relative a un elemento specifico.

Icona	Descrizione
	Icona Personalizza notifiche. Visualizza le varie opzioni di notifica.

Capitolo 3

Installazione degli Agent

Questo capitolo descrive le fasi necessarie per installare Security Agent e Messaging Security Agent (solo Advanced). Vengono inoltre fornite informazioni su come rimuovere questi agent.

Installazione di Security Agent

Eseguire un'installazione da zero del Security Agent sui client Windows (desktop e server). Utilizzare il metodo di installazione più adatto agli specifici requisiti.

Prima di installare il Security Agent, chiudere le applicazioni in esecuzione sui client. Se si esegue l'installazione mentre sono in esecuzione altre applicazioni, il completamento dell'installazione potrebbe richiedere più tempo.

Nota

Per informazioni sull'aggiornamento dei Security Agent a questa versione, vedere la *Guida all'installazione e all'aggiornamento*.

Requisiti di installazione del Security Agent

Visitare il sito Web seguente per un elenco completo dei requisiti di installazione e dei prodotti compatibili di terze parti:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Considerazioni sull'installazione del Security Agent

Prima di installare i Security Agent, valutare le informazioni riportate di seguito:

- **Caratteristiche dell'agent:** Alcune funzioni del Security Agent non sono disponibili su determinate piattaforme Windows. Per i dettagli, consultare *Funzioni disponibili per i Security Agent a pagina 3-3*.
- **Piattaforme x64**. Per la piattaforma x64 è disponibile una versione ridotta di Security Agent. Per la piattaforma IA-64 al momento non è invece disponibile alcun supporto.

- **Supporto IPv6**: Il Security Agent può essere installato su endpoint dual-stack o IPv6 puri. Tuttavia, alcuni metodi di installazione potrebbero avere requisiti specifici.

  Per i dettagli, consultare *Installazione di Security Agent e supporto IPv6 a pagina 3-5*.

- **Elenco eccezioni**:Assicurarsi che gli elenchi di eccezioni per le funzioni seguenti siano configurati correttamente:

  - **Monitoraggio del comportamento**:Aggiungere le applicazioni importanti del client all'elenco Programmi approvati per evitare che tali applicazioni siano bloccate dal Security Agent. Per ulteriori informazioni, vedere *Configurazione del monitoraggio del comportamento a pagina 5-12*.

  - **Reputazione Web**:Aggiungere i siti Web considerati sicuri all'Elenco URL approvati per evitare che il Security Agent blocchi l'accesso ai siti Web. Per ulteriori informazioni, vedere *Configurazione della reputazione Web per Security Agent a pagina 5-23*.

- **Directory di installazione dell'agent**:Durante l'installazione del Security Server, il programma di installazione richiede di specificare la directory di installazione dell'agent, che per impostazione predefinita si trova in `$ProgramFiles\Trend Micro\Security Agent`. Per installare i Security Agent in una directory diversa, specificare la nuova directory in **Amministrazione** > **Impostazioni globali** > **Sistema** > **sezione Installazione del Security Agent**.

Funzioni disponibili per i Security Agent

Le funzioni per i Security Agent disponibili sul client dipendono dal sistema operativo del computer. Quando si installa un agent su un particolare sistema operativo, è necessario conoscere le funzioni non supportate .

TABELLA 3-1. Funzioni per i Security Agent

FUNZIONE	SISTEMA OPERATIVO WINDOWS		
	10	SBS 2011	SERVER 2012/2012 R2/2016/2019
Scansione manuale (normale e aggressiva), scansione in tempo reale e scansione pianificata	Sì	Sì	Sì
Firewall	Sì	Sì	Sì
Reputazione Web	Sì	Sì	Sì
Filtro URL	Sì	Sì	Sì
Monitoraggio del comportamento	Sì	Sì	Sì
Controllo dispositivo	Sì	Sì	Sì
Damage Cleanup Services	Sì	Sì	Sì
Mail Scan (POP3)	Sì	Sì	Sì
Aggiornamenti manuali e pianificati	Sì	Sì	Sì
Update Agent	Sì	Sì	Sì
Agent Plug-in Manager	Sì	Sì	Sì
Smart Feedback	Sì	Sì	Sì

Funzione	Sistema operativo Windows		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
Barra degli strumenti di Trend Micro Anti-Spam	Sì Client di posta elettronica supportati (32 e 64 bit): • Outlook 2010 • Outlook 2013 • Outlook 2016	No	No
HouseCall	Sì	Sì	Sì
Case Diagnostic Tool	Sì	Sì	Sì
Wi-Fi Advisor	Sì	No	No

Installazione di Security Agent e supporto IPv6

In questo argomento vengono illustrate le considerazioni relative all'installazione del Security Agent su client dual-stack o IPv6 puri.

Sistema operativo

Il Security Agent può essere installato solo sui seguenti sistemi operativi che supportano l'indirizzamento IPv6:

- Windows SBS 2011
- Windows 10 (tutte le edizioni)
- Windows Server 2012/2012 R2 (tutte le edizioni)
- Windows Server 2016 (Standard, Datacenter, Essentials)
- Windows Server 2019 (Standard, Datacenter, Essentials)

Visitare il sito Web seguente per un elenco completo dei requisiti di sistema:

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

Metodi di installazione supportati

Per installare il Security Agent su client dual-stack o IPv6 puri, è possibile usare tutti i metodi di installazione disponibili. Alcuni metodi di installazione necessitano di requisiti particolari per installare correttamente il Security Agent.

TABELLA 3-2. Metodi di installazione e supporto IPv6

METODO DI INSTALLAZIONE	REQUISITI E CONSIDERAZIONI
Pagina Web interna e Installazione notifica e-mail	Se si sta effettuando l'installazione su un client IPv6 puro, il Security Server deve essere dual-stack o IPv6 puro e il relativo nome host o indirizzo IPv6 deve essere incluso nell'URL. Per i client dual-stack, l'indirizzo IPv6 visualizzato nella schermata dello stato di installazione dipende dall'opzione selezionata nella sezione **Indirizzo IP preferito** sulla scheda **Amministrazione** > **Impostazioni globali** > **Desktop/Server**.
Vulnerability Scanner e Installazione remota	Un Security Server IPv6 puro non può installare il Security Agent su client IPv4 puri. Analogamente, un Security Server IPv4 puro non può installare l'agent su client IPv6 puri.

Indirizzi IP del Security Agent

Un Security Server installato in un ambiente che supporta l'indirizzamento IPv6 può gestire i seguenti Security Agent:

- Un Security Server installato su un client IPv6 puro può gestire i Security Agent IPv6 puri.
- Un Security Server installato su un client dual-stack con indirizzi IPv4 e IPv6 assegnati può gestire Security Agent IPv6 puri, dual-stack e IPv4 puri.

Quando vengono installati o aggiornati, i Security Agent effettuano la registrazione al Security Server usando un indirizzo IP.

- I Security Agent IPv6 puri effettuano la registrazione usando il proprio indirizzo IPv6.

- I Security Agent IPv4 puri effettuano la registrazione usando il proprio indirizzo IPv4.
- I Security Agent dual-stack effettuano la registrazione usando il proprio indirizzo IPv4 o IPv6. È possibile scegliere l'indirizzo IP che questi agent utilizzeranno dalla sezione **Indirizzo IP preferito** sulla scheda **Amministrazione** > **Impostazioni globali** > **Desktop/Server**.

Metodi di installazione del Security Agent

Questa sezione fornisce un riepilogo dei diversi metodi di installazione disponibili per l'installazione da zero del Security Agent. Tutti i metodi di installazione richiedono diritti di amministratore locale sugli endpoint di destinazione.

Se si stanno installando i Security Agent e si desidera attivare il supporto IPv6, consultare le linee guida in *Installazione di Security Agent e supporto IPv6 a pagina 3-5*.

TABELLA 3-3. Metodi di installazione

METODO DI INSTALLAZIONE/ SUPPORTO SISTEMA OPERATIVO	CONSIDERAZIONI SULL'IMPLEMENTAZIONE					
	IMPLEMENTAZIONE WAN	GESTIONE CENTRALIZZATA	RICHIEDE INTERVENTO UTENTE	RICHIEDE RISORSA IT	IMPLEMENTAZIONE DI MASSA	AMPIEZZA DI BANDA UTILIZZATA
Pagina Web interna Supporto per tutti i sistemi operativi	Sì	Sì	Sì	No	No	Basso, se pianificato
Notifica e-mail Supporto per tutti i sistemi operativi	Sì	Sì	Sì	No	No	Alto, se le installazioni vengono avviate nello stesso momento

Metodo di installazione/ Supporto sistema operativo	Considerazioni sull'implementazione					
	Implementazione WAN	Gestione centralizzata	Richiede intervento utente	Richiede risorsa IT	Implementazione di massa	Ampiezza di banda utilizzata
Installazione remota Supporto per tutti i sistemi operativi	No	Sì	No	Sì	Sì	Basso, se pianificato
Impostazione script di accesso Supporto per tutti i sistemi operativi	No	Sì	No	Sì	Sì	Alto, se le installazioni vengono avviate nello stesso momento
Client Packager Supporto per tutti i sistemi operativi	Sì	No	Sì	Sì	No	Basso, se pianificato
Trend Micro Vulnerability Scanner (TMVS) Supportato su tutti i sistemi operativi eccetto Windows 10	No	Sì	No	Sì	Sì	Basso, se pianificato

Per implementazioni su un singolo sito e in aziende in cui le policy IT vengono applicate rigorosamente, gli amministratori dell'IT possono scegliere di implementare mediante **Installazione remota** o **Impostazione script di accesso**.

Nelle aziende in cui le policy IT vengono applicate con minor rigore, Trend Micro consiglia di installare i Security Agent utilizzando la **pagina Web interna**. Con questo metodo, tuttavia, gli utenti che desiderano installare Security Agent devono disporre dei privilegi di amministratore.

L'installazione remota è utile per le reti con Active Directory. Se sulla rete non è presente Active Directory, utilizzare la pagina Web interna.

Installazione dalla pagina Web interna

Informazioni preliminari

Per installare la pagina Web interna, è richiesto quanto segue:

Elementi da controllare	Requisito
Security Server	Il Security Server deve essere installato su: • Windows 7, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 o SBS 2008, 2011 • con Internet Information Server (IIS) 7.0, 7.5, 8.0, 8.5, 10 o Apache 2.4
Endpoint di destinazione	• Il dispositivo di destinazione deve essere installato su Windows 10, Server 2012, 2012 R2, 2016, 2019 o SBS 2011. • L'endpoint di destinazione deve disporre di Internet Explorer 9.0 o versioni successive. • Gli utenti devono utilizzare un account amministratore per accedere all'endpoint. **Nota** Se il dispositivo di destinazione utilizza un sistema operativo desktop, attivare prima l'account amministratore integrato. Per ulteriori informazioni, consultare il sito di assistenza Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Elementi da controllare	Requisito
Impostazioni di sicurezza di Internet Explorer	Gli utenti devono attenersi alla seguente procedura: 1. Avviare Internet Explorer e aggiungere l'URL del Security Server (ad esempio `https://<nome Security Server>:4343/SMB/console/html/client`) all'elenco dei siti affidabili. Accedere all'elenco da **Strumenti** > **Opzioni Internet** > **scheda Sicurezza**, quindi selezionare l'icona **Siti attendibili** e fare clic su **Siti**. 2. Modificare le impostazioni di sicurezza di Internet Explorer e attivare **Richiesta di conferma automatica per controlli ActiveX**. Accedere a **Strumenti** > **Opzioni Internet** > **scheda Sicurezza** e fare clic su **Livello personalizzato**.
IPv6	In caso di ambiente misto composto da endpoint IPv4 puri, IPv6 puri e dual-stack, il Security Server deve disporre di indirizzi IPv4 e IPv6, in modo che tutti gli endpoint possano connettersi alla pagina Web interna del Security Server.

Per installare il Security Agent dalla pagina Web interna, inviare agli utenti le seguenti istruzioni. Per inviare la notifica di installazione per e-mail, vedere *Installazione con notifica e-mail a pagina 3-32*.

Procedura

1. Accedere all'endpoint utilizzando un account amministratore.
2. Aprire Internet Explorer e digitare uno degli indirizzi riportati di seguito:
   - Security Server con SSL:

     `https://<nome Security Server o indirizzo IP>:4343/SMB/console/html/client`
   - Security Server senza SSL:

     `http://<nome Security Server o indirizzo IP>:8059/SMB/console/html/client`
3. Per avviare l'installazione del Security Agent, fare clic su **Installa ora**.

L'installazione viene avviata. Quando viene richiesto, consentire l'installazione del controllo ActiveX. Sulla barra delle applicazioni di Windows viene visualizzata l'icona di Security Agent.

Nota

Per ottenere un elenco delle icone visualizzate nella barra delle applicazioni di Windows, vedere *Controllo dello stato dei Security Agent a pagina A-2*.

Operazioni successive

Se gli utenti riscontrano che non è possibile eseguire l'installazione dalla pagina Web interna, provare i metodi riportati di seguito.

- Verificare la presenza della comunicazione endpoint-server mediante ping e telnet.
- Controllare se TCP/IP sull'endpoint è attivato e configurato correttamente.
- Se si utilizza un server proxy per la comunicazione endpoint-server, controllare che le impostazioni proxy siano state configurate correttamente.
- Nel browser Web, eliminare la cronologia dei componenti aggiuntivi e delle esplorazioni di Trend Micro.

Installazione con Impostazione script di accesso

Impostazione script di accesso automatizza l'installazione di Security Agent per i client non protetti quando accedono alla rete. L'Impostazione script di accesso aggiunge allo script di accesso del server un programma denominato `AutoPcc.exe`.

`AutoPcc.exe` installa il Security Agent nei client non protetti e aggiorna file e componenti di programma. Per poter utilizzare AutoPcc tramite lo script di accesso, i client devono appartenere al dominio.

Se si dispone già di uno script di accesso, Impostazione script di accesso aggiunge un comando per l'esecuzione di `AutoPcc.exe`. Altrimenti, crea un file batch denominato `ofcscan.bat` contenente il comando per eseguire `AutoPcc.exe`.

Impostazione script di accesso aggiunge alla fine dello script gli elementi riportati di seguito:

```
\\<Nome_server>\ofcscan\autopcc
```

Dove:

- `<Nome_server>` è il nome o l'indirizzo IP del computer Security Server.
- "`ofcscan`" è il nome della cartella condivisa sul Security Server.
- "`autopcc`" è il collegamento al file eseguibile autopcc che installa il Security Agent.

Percorso dello script di accesso su tutte le versioni di Windows Server (tramite una directory ad accesso condiviso di rete):

```
\\Windows server\unità di sistema\windir\sysvol\domain\scripts
\ofcscan.bat
```

Procedura

1. Nel computer utilizzato per eseguire l'installazione del server, aprire `<Cartella di installazione Security Server>\PCCSRV\Admin`.
2. Fare doppio clic su `SetupUsr.exe`.

   Viene caricata l'utilità **Impostazione script di accesso**. La console visualizza una struttura ad albero con tutti i domini della rete.
3. Individuare il server di cui si desidera modificare lo script di accesso, selezionarlo e fare clic su **Seleziona**. Accertarsi che il server sia il controller di dominio primario e di disporre dei privilegi di amministratore del server.

   Per Impostazione script di accesso, vengono richiesti il nome utente e la password.

4. Immettere il nome utente e la password. Fare clic su **OK** per continuare.

   Viene visualizzata la schermata **Selezione utente**. L'elenco **Utenti** contiene i profili degli utenti che si collegano al server. L'elenco **Utenti selezionati** contiene invece i profili degli utenti di cui si desidera modificare lo script di accesso.

5. Per modificare lo script di accesso di un profilo utente, selezionarlo dall'elenco Utenti e fare clic su **Aggiungi**.

6. Per modificare lo script di accesso di tutti gli utenti, fare clic su **Aggiungi tutti**.

7. Per escludere il profilo di un utente precedentemente selezionato, fare clic sul suo nome nell'elenco **Utenti selezionati** e quindi su **Elimina**.

8. Per ripristinare le opzioni predefinite, fare clic su **Rimuovi tutto**.

9. Quando tutti i profili utenti di destinazione si trovano nell'elenco **Utenti selezionati**, fare clic su **Applica**.

   Viene visualizzato un messaggio in cui viene confermata la corretta modifica degli script di accesso al server.

10. Fare clic su **OK**.

    Si ritorna alla schermata iniziale dell'Impostazione script di accesso.

11. Per chiudere il programma Impostazione script di accesso, fare clic su **Esci**.

Installazione con Client Packager

Client Packager crea un pacchetto di installazione che può essere inviato agli utenti con supporti convenzionali come i CD-ROM. Gli utenti eseguono il pacchetto sui propri client per installare o aggiornare il Security Agent e aggiornare i componenti.

Client Packager è particolarmente utile:

- Durante l'implementazione del Security Agent o dei componenti sui client in uffici remoti a larghezza di banda ridotta.
- Se l'ambiente prevede limitazioni per la connessione a Internet, in presenza di una LAN chiusa o in assenza di una connessione.

I Security Agent installati mediante Client Packager inviano notifiche al server in cui è stato creato il pacchetto.

Procedura

1. Nel computer Security Server, passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\ClientPackager`.
2. Fare doppio clic su `ClnPack.exe`.

   Viene aperta la console di Client Packager.
3. Selezionare il sistema operativo per cui si desidera creare il pacchetto. Implementare il pacchetto solo sui client che eseguono questo tipo di sistema operativo. Creare un altro pacchetto da implementare su un altro tipo di sistema operativo.
4. Selezionare il metodo di scansione del pacchetto.

   Per ulteriori informazioni sui metodi di scansione, vedere *Metodi di scansione a pagina 5-3*.

   I componenti inclusi nel pacchetto dipendono dal metodo di scansione selezionato. Per le smart scan, tutti i componenti, salvo il Pattern dei virus, saranno inclusi. Per le scansioni convenzionali, tutti i componenti, salvo Pattern agente Smart Scan, saranno inclusi.
5. Selezionare il tipo di pacchetto che si desidera creare.

TABELLA 3-4. Tipi di pacchetti client

TIPO PACCHETTO	DESCRIZIONE
Installazione	Selezionare **Configurazione** per creare il pacchetto come file MSI, conforme al formato di pacchetto di Windows Installer. Il pacchetto installa il Security Agent con i componenti attualmente disponibili nel Security Server. Se il client destinazione possiede una versione del Security Agent precedente installata ed è necessario aggiornarla, creare il file MSI dal Security Agent che gestisce l'agent. Altrimenti, l'agent non viene aggiornato.
Aggiornamento	Selezionare **Aggiorna** per creare un pacchetto contenente i componenti attualmente disponibili nel Security Server. Il pacchetto viene creato come file eseguibile. Utilizzare questo pacchetto in caso di problemi durante l'aggiornamento dei componenti sul client in cui è installato il Security Agent.

6. Fare clic su **Modalità invisibile** per creare un pacchetto che viene installato in background, in modo impercettibile per l'utente del client e senza visualizzare la finestra sullo stato dell'installazione. Attivare questa opzione se si intende implementare il pacchetto da remoto sul client.

7. Fare clic su **Disattiva prescansione (solo nuova install.)** per non eseguire la scansione del client in cerca di minacce prima di installare il Security Agent. Disattivare l'opzione qualora sia certo che il client sia privo di minacce.

   Se la pre-scansione è attivata, il programma di installazione esegue la scansione per rilevare virus e malware nelle aree del computer più vulnerabili, comprese quelle riportate di seguito:

   - Area boot e la directory boot (per i virus del settore boot)
   - Cartella Windows
   - Cartella Programmi

8. Assicurarsi che la posizione del file `ofcscan.ini` all'interno del campo **File di origine** sia corretta. Per modificare il percorso, fare clic su (...)

per cercare il file `ofcscan.ini`. Per impostazione predefinita, questo file si trova in `<Cartella di installazione del server>\PCCSRV`.

9. In File di destinazione, fare clic su (...), specificare il percorso in cui si desidera creare il pacchetto e digitare il nome del file del pacchetto (ad esempio `ClientSetup.exe`).

10. Fare clic su **Crea**.

    Quando Client Packager ha completato la creazione del pacchetto, viene visualizzato il messaggio "Creazione pacchetto completata". Individuare il package nella directory specificata nel passaggio precedente.

Operazioni successive

Implementare l'impostazione sui client.

Requisiti per il client:

- Spazio su disco
  - Scansione convenzionale: minimo 1,5 GB (2 GB consigliati)
  - Smart Scan: 500 MB

  1 GB di spazio libero su disco, se il metodo di scansione per il pacchetto è scansione convenzionale, 500 MB per smart scan
- Windows Installer 4.5 o versioni successive (per l'esecuzione di un pacchetto MSI)

Linee guida per l'implementazione del pacchetto:

- Inviare il pacchetto agli utenti e chiedergli di eseguirlo con un doppio clic sul file (`.msi` o `.exe`).

  Nota

  Inviare il pacchetto solo agli utenti con Security Agent che riporta al server la posizione nella quale è stato creato.

- Indicare agli utenti di fare clic con il pulsante destro del mouse sul file del pacchetto e di selezionare **Esegui come amministratore**.

- È possibile usufruire delle funzioni di Active Directory per eseguire automaticamente l'implementazione del Security Agent su tutti i client contemporaneamente con il file `.msi`, piuttosto che richiedere a ciascun utente di installare il Security Agent autonomamente. Utilizzare **Configurazione computer** invece di **Configurazione utente**, in modo che il Security Agent venga installato indipendentemente da quale utente accede al client.
- Se il Security Agent appena installato non è in grado di collegarsi al Security Server, il Security Agent mantiene le impostazioni predefinite. Quando il Security Agent si connette al Security Server, ottiene le impostazioni per il proprio gruppo nella console Web.
- Se si verificano problemi con l'aggiornamento del Security Agent tramite Client Packager, Trend Micro consiglia di disinstallare prima la versione precedente del Security Agent, per poi installare la nuova versione. Per istruzioni sulla disinstallazione, vedere *Rimozione di agent a pagina 3-39*.

Installazione con Installazione remota

Informazioni preliminari

È possibile installare in remoto Security Agent su uno o più endpoint connessi alla rete.

Per installare con Installazione remota, sono previsti i seguenti requisiti:

Elementi da controllare	Requisito
Endpoint di destinazione	• Utilizzare un account amministratore per accedere a ciascun endpoint di destinazione.

Elementi da controllare	Requisito
	Nota • Se il dispositivo di destinazione utilizza un sistema operativo desktop, attivare prima l'account amministratore integrato. Per ulteriori informazioni, consultare il sito di assistenza Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account). • Quando si esegue un'installazione remota su Windows 10, non è possibile utilizzare l'account Microsoft per accedere al client di destinazione • Sull'endpoint di destinazione non deve essere installato Security Server. L'Installazione remota non installa Security Agent su un endpoint sul quale è già in esecuzione Security Server.
Condivisione file e stampanti	Attivare temporaneamente Condivisione file e stampanti sull'endpoint. **Nota** Se i criteri di protezione aziendali prevedono la disattivazione di Windows Firewall, andare alla sezione Registro remoto. 1. Aprire Windows Firewall nel Pannello di controllo. 2. Fare clic su **Consenti programma con Windows Firewall**. Se viene richiesta una password di amministrazione o una conferma, eseguire l'operazione richiesta. Viene visualizzata la finestra di dialogo delle impostazioni di Windows Firewall. 3. Nell'**elenco Programma o porta** della scheda **Eccezioni**, verificare che la casella di controllo **Condivisione file e stampanti** sia selezionata. 4. Fare clic su **OK**. 5. Dopo avere installato i Security Agent, è possibile ripristinare le impostazioni originali, se necessario.

Elementi da controllare	Requisito
Controllo account utente	Disattivare il controllo dell'account utente. **Nota** modificare la seguente chiave di registro per disattivare il controllo dell'account utente: `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] “EnableLUA”=dword:00000000`. Dopo avere installato i Security Agent, è possibile ripristinare le impostazioni originali, se necessario.
Registro remoto	Avviare temporaneamente il servizio Registro remoto. 1. **Nota** Nella finestra Esegui immettere `services.msc` per aprire Microsoft Management Console. 2. Fare clic con il tasto destro del mouse su **Registro remoto** e scegliere **Avvia**. 3. Dopo avere installato i Security Agent, è possibile ripristinare le impostazioni originali, se necessario.
IPv6	Un Security Server dual-stack può installare Security Agent su qualsiasi endpoint. Un Security Server IPv6 puro può installare Security Agent soltanto su endpoint IPv6 puri o dual-stack.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic su **Aggiungi dispositivi**.
3. Selezionare **Desktop o Server**, dalla sezione **Tipo di computer**.
4. Selezionare **Installazione remota** dalla sezione **Metodo**.
5. Fare clic su **Avanti**.

Viene visualizzata una nuova schermata.

6. Selezionare un client dall'elenco di client nella casella **Gruppi e computer**, quindi fare clic su **Aggiungi**. Viene richiesto un nome utente e una password per il client.

7. Immettere nome utente e password, quindi fare clic su **Accedi**. Il client compare nella casella di riepilogo **Computer selezionati**.

8. Ripetere questi passaggi fino a quando nell'elenco non vengono visualizzati tutti i computer Windows presenti nella casella di riepilogo **Computer selezionati**.

9. Fare clic su **Installa**.

   Viene visualizzata una finestra di dialogo di conferma.

10. Fare clic su **Sì** per confermare l'installazione dell'agent sui client.

    Mentre viene eseguita la copia dei file del Security Agent su ogni client, compare una schermata di avanzamento.

    Al termine dell'installazione su un client, nel campo **Stato** dell'elenco dei **Computer selezionati**, viene visualizzato lo stato dell'installazione e accanto al nome del computer un segno di spunta verde.

Operazioni successive

Se l'installazione remota non termina correttamente, attenersi alla seguente procedura:

- Verificare la presenza della comunicazione client/server mediante ping e telnet.
- Controllare se TCP/IP sul client è stato attivato e configurato correttamente.
- Se si utilizza un server proxy per la comunicazione client/server, controllare che le impostazioni proxy siano state configurate correttamente.

- Nel browser Web, eliminare la cronologia dei componenti aggiuntivi e delle esplorazioni di Trend Micro.

Installazione con Vulnerability Scanner

Informazioni preliminari

Esegue scansioni di vulnerabilità per rilevare le soluzioni antivirus installate, cercare i client non protetti presenti nella rete e installare i Security Agent sui client.

Per installare con Vulnerability Scanner, sono previsti i seguenti requisiti:

Elementi da controllare	Requisito
Dove avviare il Vulnerability Scanner	È possibile eseguire Vulnerability Scanner sul Security Server o su qualsiasi client nella rete. Il client non deve avere in esecuzione il Terminal Server.
Client di destinazione	• Il client destinazione non deve avere il Security Server installato. Vulnerability Scanner non installa il Security Agent su un client in cui è già in esecuzione il Security Server. • Gli utenti devono utilizzare un account amministratore per accedere al client. **Nota** Se il client di destinazione utilizza un sistema operativo desktop, attivare prima l'account amministratore integrato. Per ulteriori informazioni, consultare il sito di assistenza Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Sono disponibili diversi metodi per l'esecuzione delle scansioni di vulnerabilità.

- *Esecuzione di una scansione di vulnerabilità manuale a pagina 3-22*
- *Esecuzione di una scansione DHCP a pagina 3-23*

- *Configurazione di una scansione di vulnerabilità pianificata a pagina 3-26*

Esecuzione di una scansione di vulnerabilità manuale

Esegue scansioni di vulnerabilità su richiesta.

Procedura

1. Avviare Vulnerability Scanner.

PER AVVIARE VULNERABILITY SCANNER SU:	PASSAGGI
Security Server	a. Passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS`. b. Fare doppio clic su `TMVS.exe`.
Un client in rete	a. In Security Server passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility`. b. Copiare la cartella `TMVS`nell'altro client. c. Sull'altro client, aprire la cartella `TMVS`, quindi fare doppio clic su `TMVS.exe`.

2. Andare alla sezione **Scansione manuale**.
3. Immettere l'intervallo di indirizzi IP dei client da controllare.
   a. Immettere un intervallo di indirizzi IPv4.

      Nota

      Vulnerability Scanner può eseguire query per un intervallo di indirizzi IPv4 solo se eseguito su un client IPv4 puro o dual-stack. Vulnerability Scanner supporta soltanto gli intervalli di indirizzi IP di classe B, ad esempio, da 168.212.1.1 a 168.212.254.254.

   b. Per un intervallo di indirizzi IPv6, immettere una lunghezza o un prefisso IPv6.

Nota

Vulnerability Scanner può eseguire query per un intervallo di indirizzi IPv6 solo se eseguito su un client IPv6 puro o dual-stack.

4. Fare clic su **Impostazioni**.

   Viene visualizzata la schermata **Impostazioni**.

5. Configurare le impostazioni della scansione di vulnerabilità. Per i dettagli, consultare *Impostazioni di Scansione vulnerabilità a pagina 3-28*.

6. Fare clic su **OK**.

   La schermata Impostazioni si chiude.

7. Fare clic su **Avvia**.

   I risultati della scansione di vulnerabilità vengono visualizzati nella tabella **Risultati** all'interno della scheda **Scansione manuale**.

   Nota

   Se nel computer è in esecuzione Windows Server 2008, le informazioni sull'indirizzo MAC non vengono visualizzate nella tabella **Risultati**.

8. Per salvare i risultati in un file CSV (comma-separated value), fare clic su **Esporta**, individuare la cartella in cui salvare il file, digitare il nome del file e fare clic su **Salva**.

Esecuzione di una scansione DHCP

Esegue le scansioni della vulnerabilità sui client che richiedono indirizzi IP da un server DHCP.

Vulnerability Scanner esegue l'ascolto sulla porta 67 (la porta di ascolto del server DHCP per le richieste DHCP). Se rileva una richiesta DHCP proveniente da un client, la scansione di vulnerabilità viene eseguita sul client.

Nota

Vulnerability Scanner non rileva le richieste DHCP se partono da Windows Server 2008 o Windows 7.

Procedura

1. Configurare le impostazioni DHCP nel file `TMVS.ini` situato nella cartella riportata di seguito: `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS`.

   TABELLA 3-5. Impostazioni DHCP nel file `TMVS.ini`

IMPOSTAZIONE	DESCRIZIONE
DhcpThreadNum=x	Specificare il numero di thread per la modalità DHCP. Il valore minimo è 3 e il valore massimo è 100. Il valore predefinito è 3.
DhcpDelayScan=x	La durata del ritardo in secondi prima che venga eseguito il controllo del software antivirus nel computer che effettua la richiesta. Il valore minimo è 0 (senza attesa) e il valore massimo è 600. Il valore predefinito è 60.
LogReport=x	Il valore 0 disattiva la registrazione, il valore 1 la attiva. Vulnerability Scanner invia i risultati della scansione al server Worry-Free Business Security. I registri vengono visualizzati nella schermata **Registri eventi di sistema** della console Web.
OsceServer=x	L'indirizzo IP o il nome DNS del server Worry-Free Business Security.
OsceServerPort=x	La porta del server Web nel server Worry-Free Business Security.

2. Avviare Vulnerability Scanner.

PER AVVIARE VULNERABILITY SCANNER SU:	PASSAGGI
Security Server	a. Passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS`. b. Fare doppio clic su `TMVS.exe`.
Un client in rete	a. In Security Server passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility`. b. Copiare la cartella `TMVS`nell'altro client. c. Sull'altro client, aprire la cartella `TMVS`, quindi fare doppio clic su `TMVS.exe`.

3. A fianco della sezione **Scansione manuale**, fare clic su **Impostazioni**.

   Viene visualizzata la schermata **Impostazioni**.

4. Configurare le impostazioni della scansione di vulnerabilità. Per i dettagli, consultare *Impostazioni di Scansione vulnerabilità a pagina 3-28*.

5. Fare clic su **OK**.

   La schermata Impostazioni si chiude.

6. Nella tabella **Risultati** fare clic sulla scheda **Scansione DHCP**.

   Nota

   La scheda **Scansione DHCP** non è disponibile nei computer con Windows Server 2008 e Windows 7.

7. Fare clic su **Avvio DHCP**.

   Vulnerability Scanner avvia l'ascolto delle richieste DHCP e l'esecuzione di controlli di vulnerabilità sui client mano a mano che essi si connettono alla rete.

8. Per salvare i risultati in un file CSV (comma-separated value), fare clic su **Esporta**, individuare la cartella in cui salvare il file, digitare il nome del file e fare clic su **Salva**.

Configurazione di una scansione di vulnerabilità pianificata

Le scansioni della vulnerabilità vengono eseguite automaticamente in base a una pianificazione.

Procedura

1. Avviare Vulnerability Scanner.

PER AVVIARE VULNERABILITY SCANNER SU:	PASSAGGI
Security Server	a. Passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS`. b. Fare doppio clic su `TMVS.exe`.
Un client in rete	a. In Security Server passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility`. b. Copiare la cartella `TMVS`nell'altro client. c. Sull'altro client, aprire la cartella `TMVS`, quindi fare doppio clic su `TMVS.exe`.

2. Andare alla sezione **Scansione pianificata**.
3. Fare clic su **Aggiungi/Modifica**.

   Viene visualizzata la schermata **Scansione pianificata**.
4. Digitare un nome per la scansione di vulnerabilità pianificata.
5. Immettere l'intervallo di indirizzi IP dei computer da controllare.
   a. Immettere un intervallo di indirizzi IPv4.

Nota

Vulnerability Scanner può eseguire query per un intervallo di indirizzi IPv4 solo se è eseguito su una macchina host IPv4 pura o dual-stack con un indirizzo IPv4 disponibile. Vulnerability Scanner supporta soltanto gli intervalli di indirizzi IP di classe B, ad esempio, da 168.212.1.1 a 168.212.254.254.

b. Per un intervallo di indirizzi IPv6, immettere una lunghezza o un prefisso IPv6.

Nota

Vulnerability Scanner può eseguire query per un intervallo di indirizzi IPv6 solo se è eseguito su una macchina host IPv6 pura o dual-stack con un indirizzo IPv6 disponibile.

6. Specificare un'ora di inizio con il formato 24 ore, quindi selezionare con quale frequenza si desidera eseguire la scansione. Selezionare una frequenza giornaliera, settimanale o mensile.

7. Se sono state configurate le impostazioni di scansione vulnerabilità manuale e si desidera usarle, selezionare **Usa impostazioni correnti**. Per ulteriori informazioni sulle impostazioni di scansione di vulnerabilità manuale, vedere *Esecuzione di una scansione di vulnerabilità manuale a pagina 3-22*.

   Se non sono state specificate le impostazioni di scansione vulnerabilità manuale o si desidera usare altre impostazioni, selezionare **Modifica impostazioni**, quindi fare clic su **Impostazioni**. Viene visualizzata la schermata **Impostazioni**. Configurare le impostazioni di scansione, quindi fare clic su **OK**. Per i dettagli, consultare *Impostazioni di Scansione vulnerabilità a pagina 3-28*.

8. Fare clic su **OK**.

   La schermata **Scansione pianificata** viene chiusa. La scansione di vulnerabilità pianificata creata viene visualizzata nella sezione **Scansione pianificata**. Se sono state attivate le notifiche, Vulnerability Scanner invia i risultati della scansione di vulnerabilità pianificata.

9. Per eseguire immediatamente la scansione di vulnerabilità pianificata, fare clic su **Esegui ora**.

   I risultati della scansione di vulnerabilità vengono visualizzati nella tabella **Risultati** all'interno della scheda **Scansione pianificata**.

   Nota

   Se nel computer è in esecuzione Windows Server 2008, le informazioni sull'indirizzo MAC non vengono visualizzate nella tabella **Risultati**.

10. Per salvare i risultati in un file CSV (comma-separated value), fare clic su **Esporta**, individuare la cartella in cui salvare il file, digitare il nome del file e fare clic su **Salva**.

11. Per interrompere le scansioni della vulnerabilità pianificate, accedere alla sezione **Scansioni pianificate**, selezionare la scansione pianificata, quindi fare clic su **Elimina**.

Impostazioni di Scansione vulnerabilità

Durante le scansioni di vulnerabilità, configurare le seguenti impostazioni. Per i dettagli sui diversi tipi di scansioni vulnerabilità, vedere *Installazione con Vulnerability Scanner a pagina 3-21*.

Impostazioni	Descrizione e istruzioni
Query prodotto	Vulnerability Scanner è in grado di verificare la presenza di software di sicurezza nei client destinazione. 1. Selezionare il software di sicurezza da controllare. 2. Vulnerability Scanner utilizza le porte predefinite mostrate sullo schermo per controllare la presenza di software. Se l'amministratore del software modifica le porte predefinite, apportare le modifiche necessarie, altrimenti Vulnerability Scanner non rileva il software. 3. Per Norton Antivirus Corporate Edition, è possibile cambiare le impostazioni di timeout in **Impostazioni**.
	Altre impostazioni query del prodotto Consente di impostare il numero di client che verranno contemporaneamente controllati da Vulnerability Scanner per verificare la presenza di software di sicurezza: 1. Passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS` e aprire `TMVS.ini` utilizzando un editor di testo, ad esempio Blocco note. 2. Per definire il numero di client controllati: • Per le scansioni di vulnerabilità manuali, modificare il valore per `ThreadNumManual`. Specificare un valore compreso tra 8 e 64. Ad esempio, digitare `ThreadNumManual=60` se si desidera che Vulnerability Scanner controlli 60 client contemporaneamente. • Per le scansioni di vulnerabilità pianificate, modificare il valore per `ThreadNumSchedule`. Specificare un valore compreso tra 8 e 64. Ad esempio, digitare `ThreadNumSchedule=50` se si desidera che Vulnerability Scanner controlli 50 client contemporaneamente. 3. Salvare il file `TMVS.ini`.

Impostazioni	Descrizione e istruzioni
Impostazioni di recupero descrizione	Quando Vulnerability Scanner è in grado si eseguire il "ping" dei client, può reperire ulteriori informazioni sui client. Sono disponibili due metodi di recupero delle informazioni: • **Recupero normale**: recupera le informazioni del dominio e del computer • **Recupero rapido**: recupera solo il nome del computer
Impostazioni avvisi	Per inviare automaticamente i risultati della scansione di vulnerabilità a se stessi o ad altri amministratori nell'organizzazione: 1. Selezionare **Risultati e-mail all'amministratore di sistema**. 2. Fare clic su **Configura** per specificare le impostazioni e-mail. 3. Nel campo **A** immettere l'indirizzo e-mail del destinatario. 4. Nel campo **Da**, immettere l'indirizzo e-mail del mittente. 5. Nel campo **Server SMTP** digitare l'indirizzo del server SMTP. Ad esempio, digitare `smtp.azienda.com`. Le informazioni sul server SMTP sono obbligatorie. 6. Nel campo **Oggetto** immettere un nuovo oggetto per il messaggio, oppure accettare quello predefinito. 7. Fare clic su **OK**. Per comunicare agli utenti che sui computer non è installato il software di sicurezza: 1. Selezionare **Visualizza una notifica sui computer non protetti**. 2. Fare clic su **Personalizza** per configurare il messaggio di notifica. 3. Nella schermata **Messaggio di notifica**, digitare un nuovo messaggio o accettare il messaggio predefinito. 4. Fare clic su **OK**.
Salvare come file CSV	Salvare i risultati della scansione vulnerabilità in un file CSV (comma-separated value). Il file viene salvato sul client in cui è stato avviato Vulnerability Scanner. Accettare il percorso del file predefinito o modificarlo in base alle preferenze.

Impostazioni	Descrizione e istruzioni
Impostazioni ping	Utilizzare le impostazioni "ping" per convalidare l'esistenza di un client e verificare il sistema operativo usato. Se queste impostazioni sono disattivate, Vulnerability Scanner esegue la scansione di tutti gli indirizzi IP nell'intervallo specificato, anche di quelli che non sono utilizzati su nessun client, quindi il tentativo di eseguire la scansione impiegherà più tempo di quanto previsto. 1. Accettare le impostazioni predefinite o immettere nuovi valori nei campi **Dimensioni pacchetto** e **Timeout**. 2. Selezionare **Rilevare il tipo di sistema operativo usando l'impronta del sistema operativo ICMP**. Se si seleziona questa opzione, Vulnerability Scanner determina se un client gira su Windows o su un altro sistema operativo. Per i client con Windows, Vulnerability Scanner è in grado di identificare la versione di Windows.
	Altre impostazioni ping Per impostare il numero di client che verranno sottoposti contemporaneamente a ping da parte di Vulnerability Scanner: 1. Passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\TMVS` e aprire `TMVS.ini` utilizzando un editor di testo, ad esempio Blocco note. 2. Modificare il valore per `EchoNum`. Specificare un valore compreso tra 1 e 64. Ad esempio, digitare `EchoNum=60` se si desidera che Vulnerability Scanner effettui il ping di 60 client contemporaneamente. 3. Salvare il file `TMVS.ini`.

Impostazioni	Descrizione e istruzioni
Impostazioni di Security Server	1. Selezionare **Installazione automatica di Security Agent su computer non protetti** per installare il Security Agent sui client analizzati dal Vulnerability Scanner. 2. Specificare il nome host o l'indirizzo IPv4/IPv6 e il numero di porta del Security Server. I Security Agent installati dal Vulnerability Scanner invieranno notifiche a questo server. 3. Configurare le credenziali amministrative da utilizzare durante l'accesso ai client selezionando **Installa Account**. Nella schermata **Informazioni account**, digitare un nome utente e una password, quindi fare clic su **OK**.

Installazione con notifica e-mail

Utilizzare questo metodo di installazione per inviare un messaggio e-mail con un collegamento al programma di installazione.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic su **Aggiungi dispositivi**.
3. Selezionare **Desktop o Server**, dalla sezione **Tipo di computer**.
4. Selezionare **Installazione notifica e-mail** dalla sezione **Metodo**.
5. Fare clic su **Avanti**.

   Viene visualizzata una nuova schermata.
6. Inserire l'oggetto del messaggio e-mail e i destinatari.
7. Fare clic su **Applica**. Viene aperto il client e-mail predefinito con destinatari, oggetto e il collegamento al programma di installazione.

Migrazione a un Security Agent

Quando si installa il Security Agent, il programma di installazione controlla la presenza di software di protezione endpoint Trend Micro o terze parti installati sul client.

Il programma di installazione è in grado di svolgere le seguenti operazioni:

- Rimuovere altri software di protezione endpoint attualmente installati sul client e sostituirli con il Security Agent
- Rilevare altri software di protezione endpoint, ma non rimuoverli

Visitare il sito Web seguente per un elenco completo dei software di protezione endpoint:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Se il software sul client non può essere rimosso automaticamente o è solo rilevabile, ma non rimuovibile, disinstallarlo prima manualmente. In base al tipo di processo di disinstallazione, potrebbe essere necessario riavviare il client.

Problematiche di migrazione e possibili soluzioni

La disinstallazione automatica di software di protezione endpoint terze parti potrebbe non terminare correttamente per i seguenti motivi:

- Il numero di versione del software di terzi o la chiave del prodotto è incompatibile.
- Il programma di disinstallazione del software di terzi non funziona.
- Alcuni file del software di terzi sono mancanti o danneggiati.
- La chiave di registro del software di terzi non può essere disinfettata.
- Il software di terzi non ha un programma di disinstallazione.

Possibili soluzioni a questi problemi:

- Rimuovere manualmente il software di terzi.

- Interrompere il servizio del software di terzi.
- Rimuovere il servizio o il processo del software di terzi.

Esecuzione di operazioni post-installazione sui Security Agent

Procedura

1. Verificare quanto segue:
   - I collegamenti al Security Agent vengono visualizzati nel menu Start di Windows dell'endpoint.
   - **Trend Micro Worry-Free Business Security Agent** è incluso nell'elenco Installazione applicazioni del pannello di controllo dell'endpoint.
   - Il Security Agent compare nella schermata **Dispositivi** della console Web e si trova nel gruppo **Server (predefiniti)** o **Desktop (predefiniti)**, a seconda del tipo di sistema operativo dell'endpoint.

     Nota

     Se il Security Agent non compare, eseguire un'operazione di verifica della connessione da **Amministrazione** > **Impostazioni globali** > **Sistema (scheda)** > **Verifica connessione agente**.

   - I seguenti servizi del Security Agent sono visualizzati in **Microsoft Management Console**:
     - Trend Micro Security Agent Listener (`tmlisten.exe`)
     - Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`)
     - Firewall di Trend Micro Security Agent (`TmPfw.exe`), se il firewall è stato attivato durante l'installazione
     - Servizio di Prevenzione modifiche non autorizzate Trend Micro (`TMBMSRV.exe`), se Monitoraggio del comportamento o Controllo dispositivo è stato attivato durante l'installazione

- Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. Se il Security Agent non compare nella console Web, potrebbe non essere in grado di inviare il proprio stato al server. Effettuare una delle seguenti operazioni:

   - Aprire un browser Web sul client, digitare `https://{Trend Micro Security Server_Nome}:{numero porta}/SMB/cgi/cgionstart.exe` nella casella di testo dell'indirizzo e premere INVIO.

     Se nella schermata successiva viene visualizzato -2, significa che l'agent è in grado di comunicare con il server. In questo caso, il problema potrebbe dipendere dal fatto che nel database del server non è presente un record relativo all'agent.

   - Verificare la presenza della comunicazione client/server mediante ping e telnet.

   - Se si dispone di un'ampiezza di banda limitata, verificare se essa sia la causa del timeout tra il server e il client.

   - Verificare che la cartella `\PCCSRV` del server disponga di privilegi condivisi e che a tutti gli utenti siano stati assegnati privilegi di controllo completi

   - Verificare che le impostazioni proxy di Trend Micro Security Server siano corrette.

3. Provare il Security Agent utilizzando lo script di prova EICAR.

   L'istituto EICAR (European Institute for Computer Antivirus Research) ha sviluppato un virus di prova che consente di collaudare la propria installazione e configurazione. Il file consiste in un file di testo inerte il cui pattern binario è compreso nel file di pattern antivirus della maggioranza dei produttori di antivirus. Il file non è un virus e non contiene codice di programmazione.

   È possibile scaricare il virus di prova EICAR dai seguenti indirizzi URL:

   http://www.eicar.org/anti_virus_test_file.htm

In alternativa, è possibile creare un virus di prova EICAR digitando quanto segue in un file di testo da denominare eicar.com:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Nota

Prima di effettuare la prova, svuotare la cache del server cache e del browser locale.

Installazione di Messaging Security Agent

I Messaging Security Agent sono installabili solo se l'utente è in possesso della versione Advanced di Worry-Free Business Security.

Eseguire un'installazione da zero del Messaging Security Agent sui server Microsoft Exchange.

Nota

Per informazioni sull'aggiornamento dei Messaging Security Agent a questa versione, vedere la Guida all'installazione e all'aggiornamento.

Requisiti di installazione di Messaging Security Agent

Visitare il sito Web seguente per un elenco completo dei requisiti di installazione:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security.aspx

Installazione del Messaging Security Agent (solo Advanced)

Informazioni preliminari

Note e promemoria di installazione:

- Non è necessario interrompere o avviare i servizi Microsoft Exchange prima o dopo l'installazione.
- Se sull'endpoint sono presenti informazioni derivanti da una precedente installazione di Messaging Security Agent, non è possibile installare correttamente Messaging Security Agent. Utilizzare il Pannello di controllo di Windows per eliminare eventuali residui di un'installazione precedente.

  Per ulteriori informazioni, consultare *Disinstallazione del Messaging Security Agent da Microsoft Exchange Server (solo Advanced) a pagina 3-42*.
- Se si sta installando Messaging Security Agent su un server che esegue strumenti di blocco, rimuovere lo strumento di blocco in modo da non disabilitare il servizio IIS e impedire il buon esito dell'installazione.
- Inoltre, è possibile installare il Messaging Security Agent durante l'installazione del Security Server. Per ulteriori informazioni, fare riferimento alla Guida all'installazione e all'aggiornamento.
- Messaging Security Agent non supporta alcune funzioni di Microsoft Exchange Server Enterprise come il gruppo di disponibilità dei dati (DAG).

Procedura

1. Andare su **Dispositivi**.
2. Fare clic su **Aggiungi dispositivi**.
3. Selezionare **Server Exchange**.
4. In **Informazioni sul server Exchange**, immettere le informazioni seguenti:
   - **Nome server**: il nome del server Microsoft Exchange su cui installare l'agent.
   - **Account**: il nome utente dell'amministratore del dominio predefinito.

- **Password**: la password dell'amministratore del dominio predefinito.

5. Fare clic su **Avanti**.

   La procedura guidata di installazione visualizza una schermata diversa a seconda del tipo di installazione necessario.

   - **Installazione da zero**: l'agent non esiste sul server Microsoft Exchange, quindi verrà installato.
   - **Aggiorna**: sul server Microsoft Exchange esiste una versione dell'agent e verrà aggiornata alla versione corrente.
   - **Nessuna installazione richiesta**: la versione corrente dell'agent è già presente sul server Microsoft Exchange. Se l'agent attualmente non è presente nella Struttura dei gruppi di protezione, verrà aggiunto automaticamente.
   - **Non valida**: problema di installazione dell'agent.

   Nota

   Per **Tipo di gestione spam**, verrà usato **End User Quarantine**.

6. In **Directory**, modificare o accettare la destinazione predefinita e le directory condivise per l'installazione del Messaging Security Agent. Le directory di destinazione e condivise predefinite sono `C:\Programmi\Trend Micro\Messaging Security Agent` e `C$`, rispettivamente.

7. Fare clic su **Avanti**.

   Viene visualizzata una nuova schermata.

8. Verificare che le impostazioni del server Microsoft Exchange specificate nelle schermate precedenti siano corrette e fare clic su **Avanti** per avviare l'installazione.

9. Per visualizzare lo stato dell'installazione, fare clic sulla scheda **Stato in tempo reale**.

Rimozione di agent

Il comando **Disinstalla agent** offre le seguenti modalità per rimuovere Security Agent e Messaging Security Agent (solo Avanzate):

- *Rimozione di agent dalla console Web a pagina 3-40*

  Utilizzare questa opzione per gli agent inattivi. Un agent inattivo compare costantemente come disconnesso sulla console Web, poiché il client sul quale l'agent è installato potrebbe essere rimasto spento per un periodo prolungato o riformattato prima che l'agent potesse essere disinstallato.

  Quando si rimuovono agent dalla console Web:

  - L'agent, se esiste ancora sul client, non viene disinstallato.
  - Il server interrompe la gestione dell'agent.
  - Quando l'agent ricomincia a comunicare con il server (ad esempio, dopo aver acceso il client), l'agent viene aggiunto di nuovo alla console Web. Il Security Agent applica le impostazioni del suo gruppo originale. Se il gruppo non esiste più, l'agent viene raggruppato in **Server (predefiniti)** o **Desktop (predefiniti)**, a seconda del sistema operativo del client e applica le impostazioni di quel gruppo.

  Suggerimento

  WFBS mette a disposizione un'altra funzione che verifica la presenza di e rimuove gli agent inattivi dalla console Web. Utilizzare questa funzione per automatizzare l'operazione di rimozione agent. Per utilizzare questa funzione, andare su **Amministrazione** > **Impostazioni globali** > **scheda Sistema** e accedere alla sezione Rimozione di Security Agent inattivi.

- *Disinstallazione di agent dalla console Web a pagina 3-40*

  È possibile disinstallare l'agent (e di conseguenza rimuoverlo dalla console Web), qualora si riscontrino problemi con il programma

dell'agent. Trend Micro consiglia di reinstallare immediatamente l'agent per mantenere il client protetto dalle minacce.

Rimozione di agent dalla console Web

Procedura

1. Andare su **Dispositivi**.
2. Per rimuovere Security Agent, selezionare un gruppo, quindi scegliere gli agent. Per rimuovere un Messaging Security Agent, selezionarlo.

   Suggerimento

   Per selezionare più Security Agent adiacenti, fare clic sul primo agent dell'intervallo, tenere premuto il tasto MAIUSC e quindi fare clic sull'ultimo agent dell'intervallo. Per selezionare più agent non contigui, fare clic sul primo agent dell'intervallo, tenere premuto il tasto CTRL e quindi fare clic sugli agent da selezionare .

3. Fare clic su **Altro** > **Disinstalla agent**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Rimuovere gli agent selezionati**.
5. Fare clic su **Applica**.

Disinstallazione di agent dalla console Web

Durante la disinstallazione del Messaging Security Agent, il servizio di amministrazione di IIS o il server Apache e tutti i servizi correlati vengono interrotti e riavviati automaticamente.

Procedura

1. Andare su **Dispositivi**.

2. Per disinstallare Security Agent, selezionare un gruppo, quindi scegliere gli agent. Per disinstallare un Messaging Security Agent, selezionarlo.

   Suggerimento

   Per selezionare più Security Agent adiacenti, fare clic sul primo agent dell'intervallo, tenere premuto il tasto MAIUSC e quindi fare clic sull'ultimo agent dell'intervallo. Per selezionare più agent non contigui, fare clic sul primo agent dell'intervallo, tenere premuto il tasto CTRL e quindi fare clic sugli agent da selezionare .

3. Fare clic su **Altro** > **Disinstalla agent**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Disinstallare gli agent selezionati**.

5. Fare clic su **Applica**.

   Viene visualizzata una finestra di popup con il numero di notifiche di disinstallazione inviate dal server e il numero di agent che hanno ricevuto la notifica.

   Nota

   Per un Messaging Security Agent, immettere il nome utente e la password del server Microsoft Exchange quando richiesto.

6. Fare clic su **OK**.

7. Per verificare che l'agent sia stato disinstallato, aggiornare la schermata Impostazioni di sicurezza. L'agent non dovrebbe più essere visualizzato nella Struttura dei gruppi di protezione.

Disinstallazione di Security Agent dall'endpoint

In base alla configurazione, la disinstallazione può richiedere o meno una password. Se è richiesta una password, assicurarsi di condividere la password solo con gli utenti che devono eseguire il programma di

disinstallazione e cambiarla immediatamente se viene divulgata ad altri utenti.

La password può essere impostata o disattivata in **Amministrazione** > **Impostazioni globali** > **scheda Desktop/Server** > **Password disinstallazione di Security Agent**.

Procedura

1. Fare clic su **Pannello di controllo** > **Installazione applicazioni**.
2. Trovare il **Trend Micro Worry-Free Business Security Agent** e fare clic su **Modifica** o **Disinstalla**, a seconda dell'opzione disponibile.
3. Seguire le istruzioni visualizzate.
4. Se richiesto, digitare la password per la disinstallazione.

   Il Security Server informa l'utente sul progresso e il completamento della disinstallazione. Per completare la disinstallazione, non è necessario riavviare il client.

Disinstallazione del Messaging Security Agent da Microsoft Exchange Server (solo Advanced)

Durante la disinstallazione del Messaging Security Agent, il servizio di amministrazione di IIS o il server Apache e tutti i servizi correlati vengono interrotti e riavviati automaticamente.

Procedura

1. Accedere al server Microsoft Exchange con privilegi di amministratore.
2. Fare clic su **Pannello di controllo** > **Disinstalla un programma**.
3. Selezionare **Trend Micro Messaging Security Agent** e fare clic su **Modifica**.

4. Seguire le istruzioni visualizzate.

Capitolo 4

Gestione dei dispositivi

Worry-Free Business Security divide la schermata **Dispositivi** in due sezioni principali.

- Struttura dei dispositivi

  La struttura dei dispositivi rappresenta un elenco espandibile di gruppi logici. È possibile gestire i gruppi in base al tipo di endpoint oppure impostare manualmente i gruppi e ordinare i Security Agent in base alle proprie esigenze.

  Per ulteriori informazioni, consultare *Utilizzo della struttura dei dispositivi a pagina 4-2*.

- Tabella di informazioni sul gruppo

  Quando si seleziona un gruppo dalla struttura dei dispositivi, a destra nel gruppo viene visualizzato un elenco di Security Agent.

  Per ulteriori informazioni, consultare *Utilizzo dei comandi dei dispositivi a pagina 4-5*.

Utilizzo della struttura dei dispositivi

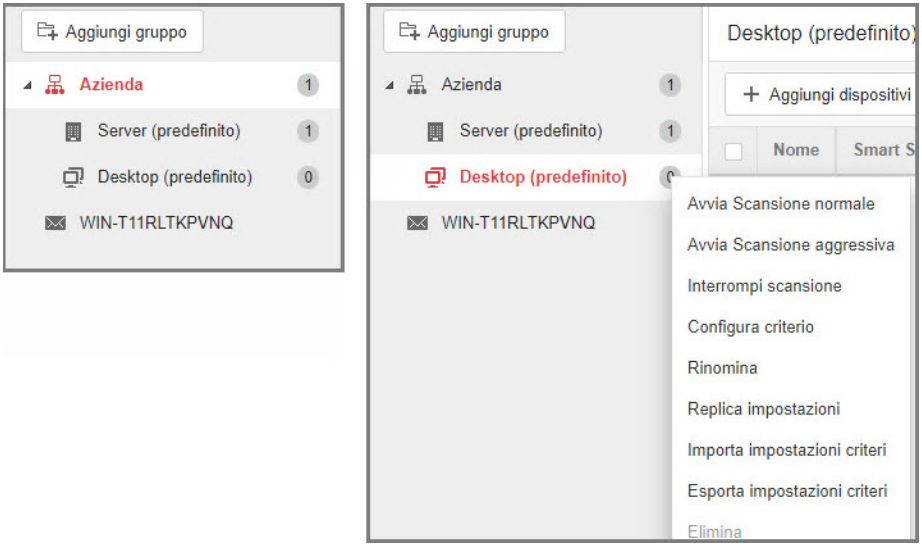


FIGURA 4-1. Utilizzo del menu di comando della struttura dei dispositivi

Per aprire il menu della struttura dei dispositivi, procedere nel modo seguente:

- Selezionare un gruppo nella struttura dei dispositivi e fare clic sull'icona ingranaggio accanto al nome del gruppo
- Selezionare un Messaging Security Agent e fare clic sull'icona ingranaggio accanto al nome dell'agent

A seconda del tipo di gruppo selezionato, è possibile che alcuni comandi siano disponibili solo in tipi di gruppi specifici o che vengano disattivati.

TABELLA 4-1. Comandi della struttura dei dispositivi

COMANDO	DESCRIZIONE
Aggiungi gruppo	Aggiunge un nuovo gruppo nella struttura dei dispositivi Per ulteriori informazioni, consultare *Aggiunta di gruppi a pagina 4-8*.
Avvia scansione normale	• Avvia la scansione di tutti gli endpoint nel gruppo selezionato • Avvia la scansione del server Exchange
Avvia scansione aggressiva	Avvia una scansione avanzata su tutti i dispositivi nel gruppo selezionato per analizzare ed eliminare le minacce che Scansione normale non è in grado di rimuovere. **Nota** L'esecuzione della scansione aggressiva può influire sulle prestazioni del dispositivo e può produrre un numero maggiore di falsi positivi.
Interrompi scansione	• Termina la scansione di tutti gli endpoint nel gruppo selezionato • Termina la scansione del server Exchange
Configura impostazioni globali	Consente di configurare le impostazioni complessive di Security Agent per le scansioni di sicurezza, gli elenchi approvati/bloccati, il controllo Security Agent e la gestione dispositivi Per ulteriori informazioni, consultare *Impostazioni globali a pagina 11-2*.

Comando	Descrizione
Configura criterio	• Consente di configurare le impostazioni di sicurezza per tutti i Security Agent appartenenti al gruppo selezionato Per ulteriori informazioni, consultare *Riepilogo delle Impostazioni di sicurezza base per i Security Agent a pagina 5-2*. • Configura le impostazioni di sicurezza per il Messaging Security Agent selezionato Per ulteriori informazioni, consultare *Gestione delle Impostazioni di sicurezza di base per i Messaging Security Agent (solo Advanced) a pagina 6-1*.
Rinomina	Modifica il nome del gruppo selezionato
Replica impostazioni	Copia le impostazioni da un gruppo a un altro. I Security Agent nel gruppo di destinazione adottano quindi le stesse impostazioni del gruppo di origine Per ulteriori informazioni, consultare *Replica delle impostazioni a pagina 4-16*.
Importa impostazioni criteri	Importa le impostazioni ottenute da un altro gruppo Per ulteriori informazioni, consultare *Importazione ed esportazione delle impostazioni dei gruppi del Security Agent a pagina 4-18*.
Esporta impostazioni criteri	Esporta le impostazioni del gruppo selezionato Per ulteriori informazioni, consultare *Importazione ed esportazione delle impostazioni dei gruppi del Security Agent a pagina 4-18*.
Elimina	Elimina un gruppo dalla struttura dei dispositivi

Utilizzo dei comandi dei dispositivi

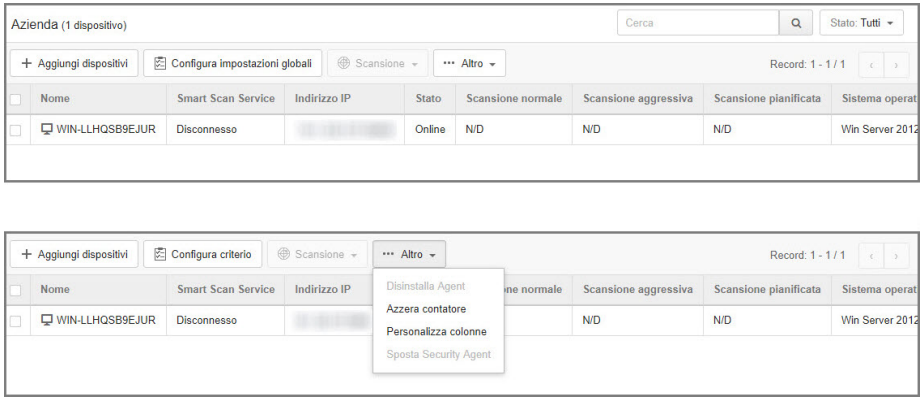


FIGURA 4-2. Utilizzo del menu di comando del dispositivo

Quando si seleziona un gruppo dalla struttura dei dispositivi, a destra nel gruppo viene visualizzato un elenco di Security Agent in una tabella. La barra dei menu nella parte superiore della tabella contiene i comandi che è possibile utilizzare per gestire i Security Agent. A seconda del tipo di gruppo selezionato, è possibile che alcuni comandi siano disponibili solo in tipi di gruppi specifici o che vengano disattivati.

Utilizzare la barra di ricerca nella parte superiore della schermata **Dispositivi** per cercare gli endpoint utilizzando nomi, etichette o indirizzi IP.

Suggerimento

Per cercare endpoint all'interno di una rete, è possibile digitare parti di indirizzi IP. Ad esempio, effettuando la ricerca di "192" verranno restituiti tutti gli indirizzi IP contenenti "192", mentre con "192." verrebbero restituiti tutti gli indirizzi IP che iniziano con "192". Tuttavia, non è possibile utilizzare caratteri jolly e simboli speciali (*, +, (,), -, &) per cercare nomi di endpoint.

TABELLA 4-2. Comandi di dispositivo

COMANDO	DESCRIZIONE
Aggiungi dispositivi	Installare uno dei seguenti componenti: • **Security Agent** su un endpoint (desktop o server) • **Messaging Security Agent** su un Microsoft Exchange Server (solo Advanced) Per ulteriori informazioni, consultare *Aggiunta degli agent ai gruppi a pagina 4-7*.
Configura criterio	Consente di configurare le impostazioni di sicurezza per tutti i Security Agent appartenenti al gruppo selezionato Per ulteriori informazioni, consultare *Riepilogo delle Impostazioni di sicurezza base per i Security Agent a pagina 5-2*.
Avvia scansione normale	Avvia la scansione degli endpoint selezionati
Avvia scansione aggressiva	Avvia una scansione avanzata su tutti i dispositivi nel gruppo selezionato per analizzare ed eliminare le minacce che Scansione normale non è in grado di rimuovere. **Nota** L'esecuzione della scansione aggressiva può influire sulle prestazioni del dispositivo e può produrre un numero maggiore di falsi positivi.
Interrompi scansione	Termina la scansione degli endpoint selezionati
Disinstalla agent	Consente di rimuovere Security Agent dagli endpoint selezionati Per ulteriori informazioni, consultare *Rimozione di agent a pagina 3-39*.
Azzera contatore	Reimposta i contatori di rilevamento del rischio per la sicurezza per tutti i Security Agent nella rete. Le informazioni di registro correlate sono ancora disponibili attraverso Query del registro
Personalizza colonne	Consente di scegliere le colonne da visualizzare nella tabella Per ulteriori informazioni, consultare *Personalizzazione delle colonne dell'elenco dispositivi a pagina 4-9*.

Comando	Descrizione
Sposta Security Agent	Consente di spostare i Security Agent selezionati in un altro gruppo o su un altro Security Server. Per ulteriori informazioni, consultare *Spostamento di agent a pagina 4-11*.

Aggiunta degli agent ai gruppi

In seguito all'installazione di un agent e all'invio dallo stesso di notifiche al Security Server, il server lo aggiunge al gruppo.

- I Security Agent installati sulle piattaforme server vengono aggiunti al gruppo **Server (predefiniti)**.
- I Security Agent installati sulle piattaforme desktop vengono aggiunti al gruppo **Desktop (predefiniti)**.

Nota

Spostandoli, è possibile assegnare Security Agent ad altri gruppi. Per i dettagli, consultare *Spostamento di agent a pagina 4-11*.

- Ogni Messaging Security Agent (solo Advanced) rappresenta il proprio gruppo. Non è possibile organizzare più Messaging Security Agent in un gruppo.

Se il numero di agent nella Struttura dei gruppi di sicurezza non è corretto, è possibile che gli agent siano stati rimossi senza inviare notifiche al server (ad esempio, se la comunicazione client-server si è interrotta durante la rimozione dell'agent). Questo comporta la conservazione delle informazioni sull'agent da parte del server nel proprio database, mostrando l'agent non in linea nella console Web. Quando si reinstalla l'agent, il server crea un nuovo record nel database e considera l'agent come nuovo, con conseguenti agent duplicati nella struttura dei gruppi di sicurezza. Per controllare i record di agenti duplicati, utilizzare la funzione Verifica connessione agente in **Amministrazione** > **Impostazioni globali** > **Sistema**.

Installazione di Security Agent

Consultare i seguenti argomenti:

- *Requisiti di installazione del Security Agent a pagina 3-2*
- *Considerazioni sull'installazione del Security Agent a pagina 3-2*
- *Metodi di installazione del Security Agent a pagina 3-7*
  - *Installazione dalla pagina Web interna a pagina 3-9*
  - *Installazione con Impostazione script di accesso a pagina 3-11*
  - *Installazione con Client Packager a pagina 3-13*
  - *Installazione con Installazione remota a pagina 3-17*
  - *Installazione con Vulnerability Scanner a pagina 3-21*
  - *Installazione con notifica e-mail a pagina 3-32*
- *Esecuzione di operazioni post-installazione sui Security Agent a pagina 3-34*

Installazione del Messaging Security Agent (solo Advanced)

Consultare i seguenti argomenti:

- *Requisiti di installazione di Messaging Security Agent a pagina 3-36*
- *Installazione del Messaging Security Agent (solo Advanced) a pagina 3-36*

Aggiunta di gruppi

Consente di aggiungere un gruppo di server o desktop, che può contenere uno o più Security Agent.

Non è possibile aggiungere un gruppo contenente Messaging Security Agent. Dopo che un Messaging Security Agent viene installato e invia notifiche al Security Server, costituisce automaticamente il proprio gruppo nella **Struttura dei gruppi di sicurezza**.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic su **Aggiungi gruppo**.

   Viene visualizzata una nuova schermata.
3. Selezionare un tipo di gruppo.
   - **Desktop**
   - **Server**
4. Inserire un nome per il gruppo.
5. Per applicare le impostazioni di un gruppo esistente al gruppo che sta per essere aggiunto, fare clic su **Importa le impostazioni dal gruppo**, quindi selezionare il gruppo. Vengono visualizzati solo i gruppi relativi al tipo di gruppo selezionato.
6. Fare clic su **Salva**.

Personalizzazione delle colonne dell'elenco dispositivi

È possibile scegliere le colonne da visualizzare facendo clic su **Altro** > **Personalizza colonne** nella parte superiore dell'elenco dispositivi.

Colonna	Informazioni visualizzate
Per i Security Agent	
Client	
Indirizzo IP	Indirizzo IP del client in cui è installato l'agent
Stato	• **Online**: l'agent è connesso al Security Server • **Offline**: l'agent è disconnesso dal Security Server

COLONNA	INFORMAZIONI VISUALIZZATE
Versione Agent	Versione dell'agent
Sistema operativo	Sistema operativo del client in cui è installato l'agent
Architettura	• **x64**: Sistema operativo a 64 bit • **x86**: Sistema operativo a 32 bit
Versione di Exchange	Versione del server Microsoft Exchange
Scansione	
Smart Scan Service **Nota** Questa colonna viene visualizzata solo se il metodo di scansione è smart.	• **Collegato**: l'agent è connesso a Smart Scan Service • **Disconnesso**: l'agent è disconnesso da Smart Scan Service **Nota** Smart Scan Service è ospitato sul Security Server. Se un agent è disconnesso, significa che non è in grado di connettersi al Security Server o che Smart Scan Service non funziona (ad esempio, se il servizio è stato interrotto). • **Disattivato**: l'agent usa la scansione convenzionale
Pattern per Smart Scan Agent / Pattern antivirus	Versione del Pattern per Smart Scan Agent o Pattern antivirus
Scansione pianificata	Data e ora dell'ultima scansione pianificata
Scansione aggressiva	Data e ora dell'ultima scansione aggressiva
Scansione POP3	• **Attivata** • **Disattivata**
Metodo di scansione	• **Smart**: Scansioni locali e nel cloud • **Tradizionale**: Solo scansioni locali Per i dettagli, consultare *Metodi di scansione a pagina 5-3*.
Scansione normale	Data e ora dell'ultima scansione normale

Colonna	Informazioni visualizzate
Minaccia	
Virus rilevati	Numero di virus/minacce informatiche rilevati
Spyware rilevati	Numero di spyware/grayware rilevati
Spam rilevato	Numero dei messaggi di e-mail spam rilevati
URL violati	Numero di accessi ad URL proibiti
Motore di scansione dei virus	Versione motore di scansione virus
Per i Messaging Security Agent (solo Avanzate)	
Name	Nome host del client in cui è installato l'agent
Indirizzo IP	Indirizzo IP del client in cui è installato l'agent
Online/Offline	• **Online**: l'agent è connesso al Security Server • **Offline**: l'agent è disconnesso dal Security Server
Piattaforma	Sistema operativo del client in cui è installato l'agent
Architettura	• **x64**: Sistema operativo a 64 bit • **x86**: Sistema operativo a 32 bit
Versione di Exchange	Versione del server Microsoft Exchange
Pattern antivirus	Versione del pattern antivirus
Motore antivirus	Versione motore di scansione virus
Versione Agent	Versione dell'agent

Spostamento di agent

Esistono diversi modi per spostare gli agent.

Agent da spostare	Dettagli	Modalità di spostamento agent
Security Agent	Spostamento di Security Agent tra gruppi. Dopo lo spostamento, gli agent ereditano le impostazioni del loro nuovo gruppo.	Utilizzare la console Web per spostare uno o più agent. Vedere *Spostamento di Security Agent tra gruppi a pagina 4-12*.
	Nel caso di almeno due Security Server, spostare i Security Agent tra server. Dopo lo spostamento, un agent viene raggruppato nel gruppo **Desktop (predefiniti)** o **Server (predefiniti)** sull'altro Security Server, a seconda del sistema operativo del client. L'agente acquisisce le impostazioni del nuovo gruppo.	• Utilizzare la console Web per spostare uno o più agent. Vedere *Spostamento di agent tra Security Server utilizzando la console Web a pagina 4-13*. • Utilizzare lo strumento Client Mover su un client per spostare l'agent installato su quel client. Vedere *Spostamento di un Security Agent tra Security Server con Client Mover a pagina 4-14*.
Messaging Security Agent (solo Advanced)	Nel caso di almeno due Security Server, spostare i Messaging Security Agent tra server. Dopo lo spostamento, l'agent costituirà il proprio gruppo sull'altro Security Server e conserverà le proprie impostazioni.	Utilizzare la console Web per spostare più agent contemporaneamente. Vedere *Spostamento di agent tra Security Server utilizzando la console Web a pagina 4-13*.

Spostamento di Security Agent tra gruppi

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.

3. Selezionare gli agent da spostare.

Suggerimento

Per selezionare più Security Agent adiacenti, fare clic sul primo agent dell'intervallo, tenere premuto il tasto MAIUSC e quindi fare clic sull'ultimo agent dell'intervallo. Per selezionare più agent non contigui, fare clic sul primo agent dell'intervallo, tenere premuto il tasto CTRL e quindi fare clic sugli agent da selezionare .

4. Trascinare gli agent nei loro nuovi gruppi.

Spostamento di agent tra Security Server utilizzando la console Web

Informazioni preliminari

Durante lo spostamento di un agent tra Security Server:

- Se un agent con una versione precedente passa su un Security Server con la versione corrente, l'agent viene aggiornato automaticamente.
- Non spostare un agent con una versione corrente su un Security Server dotato di versione precedente, in quanto l'agent diventerebbe non gestito (la registrazione dell'agent viene eliminata dal server precedente e la registrazione al nuovo server fallisce, non comparendo pertanto nella console Web). L'agent mantiene la versione corrente e non effettuerà il downgrade a quella precedente.
- I Security Server devono avere la stessa versione di lingua.
- Registrare nome host e porta di ascolto del Security Server sul quale l'agent verrà spostato. Il nome host e la porta di ascolto si trovano sulla schermata Impostazioni di sicurezza del Security Server, sopra il pannello delle attività.

Procedura

1. Nella console Web del Security Server che attualmente gestisce gli agent, andare su **Dispositivi**.
2. Per spostare i Security Agent, selezionare un gruppo e quindi selezionare gli agent. Per spostare un Messaging Security Agent, selezionarlo.
3. Fare clic su **Altro** > **Sposta Security Agent**.

   Viene visualizzata una nuova schermata.
4. Immettere nome host e porta in ascolto del Security Server sul quale gli agent verranno spostati.
5. Fare clic su **Sposta**.
6. Per controllare che gli agent ora comunichino con l'altro Security Server, aprire la console Web di quel server e trovare gli agent nella Struttura dei gruppi di protezione.

Nota

Se Security Agent non è incluso nella struttura dei gruppi di protezione, riavviare Trend Micro Security Server Master Service.

Spostamento di un Security Agent tra Security Server con Client Mover

Informazioni preliminari

Durante lo spostamento di un agent tra Security Server:

- Se un agent con una versione precedente passa su un Security Server con la versione corrente, l'agent viene aggiornato automaticamente.
- Non spostare un agent con una versione corrente su un Security Server dotato di versione precedente, in quanto l'agent diventerebbe non gestito (la registrazione dell'agent viene eliminata dal server precedente

e la registrazione al nuovo server fallisce, non comparendo pertanto nella console Web). L'agent mantiene la versione corrente e non effettuerà il downgrade a quella precedente.

- I Security Server devono avere la stessa versione di lingua.
- Registrare nome host e porta di ascolto del Security Server sul quale l'agent verrà spostato. Il nome host e la porta di ascolto si trovano sulla schermata Impostazioni di sicurezza del Security Server, sopra il pannello delle attività.
- Accedere al client utilizzando un account amministratore.

Procedura

1. Sul client, aprire una finestra del prompt dei comandi.

   Nota

   È necessario aprire il prompt dei comandi come amministratore.

2. Digitare `cd` e il percorso della cartella di installazione di Security Agent. Ad esempio: `cd C:\Programmi\Trend Micro\Security Agent`

3. Eseguire Client Mover utilizzando la sintassi riportata di seguito:

   ```
   <nome file eseguibile> -s <nome server> -p <porta di
   ascolto server> -c <porta di ascolto client> -pwd <Password
   privilegio di 'Rimozione e sblocco' dell'agent>
   ```

   TABELLA 4-3. Parametri Client Mover

PARAMETRO	SPIEGAZIONE
`<nome file eseguibile>`	`IpXfer.exe` (32 bit) `IpXfer_x64.exe` (64 bit)
`<nome server>`	Il nome del server Worry-Free Business Security di destinazione (il server al quale viene trasferito l'agent)

Parametro	Spiegazione
`<porta di ascolto server>`	La porta di ascolto (o porta attendibile) del Security Server di destinazione.
`<porta di ascolto client>`	Il numero della porta usato dal Security Agent per comunicare con il server
`<Password privilegio di 'Rimozione e sblocco' dell'agent>`	La password utilizzata per rimuovere e sbloccare il Security Agent

Esempio:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -pwd Password
```

4. Per controllare che il Security Agent ora comunichi con l'altro Security Server, aprire la console Web di quel server e trovare l'agent nella Struttura dei gruppi di protezione.

Nota

Se Security Agent non è incluso nella struttura dei gruppi di protezione, riavviare Trend Micro Security Server Master Service.

Replica delle impostazioni

Replica impostazioni tra i gruppo del Security Agent o tra Messaging Security Agent (solo Advanced).

Replica delle impostazioni del gruppo del Security Agent

Utilizzare questa funzione per applicare le impostazioni di uno specifico gruppo desktop o server a un altro gruppo dello stesso tipo. Non è possibile replicare le impostazioni di un gruppo server in un gruppo desktop e viceversa.

Se esiste un solo gruppo per un particolare tipo di gruppo, questa funzione è disabilitata.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic sull'icona ingranaggi accanto al nome del gruppo.
4. Fare clic su **Replica impostazioni**.

   Viene visualizzata una nuova schermata.
5. Selezionare i gruppi destinazione che ereditano le impostazioni.
6. Fare clic su **Applica**.

Replica delle impostazioni di Messaging Security Agent (solo Avanzate)

È possibile replicare le impostazioni soltanto tra Messaging Security Agent appartenenti allo stesso dominio.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic sull'icona ingranaggi accanto a Messaging Security Agent.
4. Fare clic su **Replica impostazioni**.

   Viene visualizzata una nuova schermata.
5. Selezionare il Messaging Security Agent che eredita le impostazioni.
6. Fare clic su **Applica**.

7. Se la replica non viene completata correttamente:
   a. Avviare l'Editor del Registro di sistema (regedit).
   b. Accedere a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
   c. Fare clic con il pulsante destro su **winreg** > **Autorizzazioni**.
   d. Aggiungere **Smex Admin Group** del dominio di destinazione e abilitare **Consenti lettura**.

Importazione ed esportazione delle impostazioni dei gruppi del Security Agent

Esportare le impostazioni di un gruppo desktop o server in un file `.dat` per eseguire il backup delle impostazioni. Inoltre, è possibile utilizzare il file `.dat` per importare le impostazioni in un altro gruppo.

Nota

È possibile importare ed esportare le impostazioni tra gruppi di server e desktop. Le impostazioni non dipendono dal tipo di gruppo. È anche possibile utilizzare la funzione **Replica impostazioni**, sebbene dipenda dal tipo di gruppo. Per ulteriori dettagli sulla funzione **Replica impostazioni**, vedere *Replica delle impostazioni a pagina 4-16*.

Tabella 4-4. Impostazioni importabili ed esportabili

Selezione	Schermata che contiene le informazioni	Impostazioni esportabili/ importabili
Gruppo desktop ( ) o gruppo server ( )	Dispositivi (**Dispositivi** > **Configura criterio**)	• Antivirus/anti-spyware (Scansione in tempo reale) • Intelligenza computazionale predittiva • Monitoraggio del comportamento • Programmi affidabili • Quarantena • Reputazione Web • Filtro URL • Firewall • Controllo dispositivo • Strumenti utente (disponibili solo nei gruppi desktop) • Privilegi degli agenti
	Scansione manuale (**Scansioni** > **Scansione manuale**)	Tutte le impostazioni
	Scansione pianificata (**Scansioni** > **Scansione pianificata**)	Tutte le impostazioni

Esportazione delle impostazioni

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop/server.
3. Fare clic sull'icona ingranaggi accanto al nome del gruppo.

4. Fare clic su **Esporta impostazioni criteri**.

   Viene visualizzata una nuova schermata.

5. Fare clic su **Esporta**.

   Viene visualizzata una finestra di dialogo.

6. Fare clic su **Salva**, scegliere un percorso, quindi fare clic su **Salva**.

Importazione delle impostazioni

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop/server.
3. Fare clic su **Importa impostazioni criteri**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Sfoglia**, trovare il file, quindi fare clic su **Importa**.

Capitolo 5

Gestione delle impostazioni di sicurezza di base per i Security Agent

In questo capitolo viene descritto come configurare le impostazioni di sicurezza di base per i Security Agent.

Riepilogo delle Impostazioni di sicurezza base per i Security Agent

TABELLA 5-1. Riepilogo delle Impostazioni di sicurezza base per i Security Agent

OPZIONE	DESCRIZIONE	PREDEFINITO
Metodo di scansione	Stabilisce se Smart Scan è attivato o meno.	L'attivazione o la disattivazione viene selezionata durante l'installazione.
Antivirus/Anti-spyware	Consente di configurare le opzioni di scansione in tempo reale, antivirus e anti-spyware.	Attivato (Scansione in tempo reale)
Intelligenza computazionale predittiva	Consente di configurare le opzioni di Intelligenza computazionale predittiva	Disattivata
Monitoraggio del comportamento	Consente di configurare le opzioni di monitoraggio del comportamento.	Attivata per gruppi di desktop Disattivata per gruppi di server
Programmi affidabili	Consente di specificare i programmi che non devono essere sottoposti a monitoraggio per comportamento sospetto.	N/D
Quarantena	Consente di specificare la directory di quarantena.	http://<Nome server o indirizzo IP di Security Server>
Reputazione Web	Consente di configurare le opzioni In ufficio e Fuori ufficio di Reputazione Web.	In ufficio: Attivata, Basso Fuori ufficio: Attivo, Medio
Filtro URL	Blocca i siti Web che violano i criteri configurati.	Attivata, Basso

Opzione	Descrizione	Predefinito
URL approvati/bloccati	Configurare gli elenchi approvati/bloccati globali.	Disattivata
Firewall	Consente di configurare le opzioni del firewall.	Disattivata
Controllo dispositivo	Consente di configurare l'esecuzione automatica, nonché l'accesso a dispositivi USB e alla rete.	Disattivata
Strumenti utente	Configurare Wi-Fi Advisor e Barra degli strumenti Trend Micro Anti-Spam	Disattivata: Wi-Fi Advisor Disattivata: barra degli strumenti Anti-spam nei client di posta supportati
Privilegi degli agenti	Consente di configurare l'accesso alle impostazioni dalla console dell'agent Disattiva aggiornamento Security Agent e implementazione hotfix	N/D

Metodi di scansione

Quando eseguono una scansione per rilevare eventuali minacce per la sicurezza, i Security Agent possono utilizzare uno dei due metodi di scansione seguenti.

- **Smart scan**: I Security Agent che utilizzano Smart Scan vengono definiti **agent Smart Scan** in questo documento. Gli agent Smart Scan utilizzano le scansioni locali e le query in-the-cloud fornite da Servizi di reputazione file.
- **Scansione convenzionale**: I Security Agent che non utilizzano Smart Scan vengono definiti **agent di scansione convenzionale**. Un agent di scansione convenzionale memorizza tutti i componenti nel client ed esegue la scansione di tutti i file in locale.

La tabella seguente consente di confrontare i due metodi di scansione:

TABELLA 5-2. Confronto tra Scansione convenzionale e Smart Scan

CRITERI DI CONFRONTO	SCANSIONE CONVENZIONALE	SMART SCAN
Comportamento della scansione	Il Security Agent di scansione convenzionale esegue la scansione nel client.	• L'agent Smart Scan esegue la scansione nel client. • Se il Security Agent non è in grado di determinare il rischio del file durante la scansione, il Security Agent verifica il rischio inviando una query di scansione al server di scansione (per i Security Agent connessi a Smart Scan Server) oppure a Trend Micro Smart Protection Network (per i Security Agent non connessi a Smart Scan Server). **Nota** Scan Server è un servizio eseguito in Smart Scan Server. • Il Security Agent memorizza nella cache il risultato della query di scansione per migliorare le prestazioni della scansione.
Componenti in uso e aggiornati	Tutti i componenti del Security Agent disponibili nella fonte aggiornamenti, ad eccezione di Pattern agente Smart Scan	Tutti i componenti disponibili nella fonte aggiornamenti, ad eccezione del Pattern dei virus
Fonte aggiornamenti tipica	Server ActiveUpdate	Server ActiveUpdate

Configurazione dei metodi di scansione

Informazioni preliminari

Durante l'installazione del Security Server, viene fornita l'opzione per l'attivazione di smart scan. Se si attiva l'opzione, il metodo di scansione predefinito è smart scan, ovvero tutti i Security Agent utilizzeranno smart scan. Altrimenti, il metodo predefinito è scansione convenzionale. È possibile cambiare i metodi di scansione per i vari agent in base a singoli requisiti specifici. Ad esempio:

- Se gli agent attualmente utilizzano la scansione convenzionale e il completamento della scansione è un'operazione notevolmente lunga, è possibile passare al metodo smart scan, ideato per ottenere maggiore velocità ed efficienza. Un altro caso in cui potrebbe essere richiesto il passaggio al metodo smart scan è quando lo spazio su disco di un agent si sta esaurendo, poiché gli agent smart scan scaricano pattern di dimensioni ridotte e pertanto richiedono meno spazio su disco.

  Prima di passare al metodo smart scan, andare su **Amministrazione** > **Impostazioni globali**, fare clic sulla scheda **Desktop/Server** e passare alla sezione **Impostazioni generali di scansione**. Verificare che l'opzione **Disattiva Smart Scan Service** sia stata disattivata.

- Far passare gli agenti alla scansione convenzionale se si nota un peggioramento delle prestazioni del Security Server, con conseguente incapacità da parte degli agent di gestire con tempestività tutte le query di scansione.

La seguente tabella elenca alcune considerazioni da ricordare quando di cambiano i metodi di scansione:

TABELLA 5-3. Considerazioni per il cambio dei metodi di scansione

CONSIDERAZIONE	DETTAGLI
Connessione del Security Server	Verificare che i Security Agent possano connettersi al Security Server. Solo gli agent online ricevono la notifica del passaggio a un metodo di scansione diverso. Gli agent offline ricevono la notifica non appena si connettono. Inoltre, verificare che il Security Server disponga degli ultimi componenti, visto che gli agent devono scaricare i nuovi componenti dal Security Server, vale a dire Pattern agente Smart Scan per gli agent che passano al metodo smart scan e Virus Pattern per gli agent che passano alla scansione convenzionale.
Numero dei Security Agent che effettuano il cambio	Se il numero di agenti che cambia metodo è relativamente esiguo, l'operazione consente di utilizzare in maniera efficiente le risorse del Security Server. Il Security Server è in grado di eseguire altre operazioni importanti mentre gli agent cambiano i metodi di scansione.
Tempistica	Se i Security Agent cambiano metodo per la prima volta, gli agent devono scaricare i la **versione completa** di Pattern agente Smart Scan (per gli agent che passano al metodo smart scan) o Virus Pattern (per gli agent che passano alla scansione convenzionale). Per fare in modo che il processo di download termini in tempi brevi, è opportuno effettuare il passaggio durante l'orario a traffico ridotto. Disattivare temporaneamente anche "Aggiorna ora" negli agent, per impedire agli utenti di avviare aggiornamenti e riattivare la funzione una volta terminato il passaggio a un metodo di scansione. **Nota** Successivamente, gli agent scaricano versioni **incrementali ridotte** di Pattern agente Smart Scan o Virus Pattern, a patto che si aggiornino frequentemente.
Supporto IPv6	Un agente smart scan IPv6 puro offline non può inviare query direttamente a Trend Micro Smart Protection Network. Per consentire all'agent smart scan di inviare query, è necessario un server proxy dual-stack in grado di convertire gli indirizzi IP, come ad esempio DeleGate.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Andare su **Metodo di scansione**.
5. Selezionare il metodo di scansione preferito.
6. Fare clic su **Salva**.

Scansione in tempo reale per i Security Agent

La scansione in tempo reale è una scansione continua e costante. Ogniqualvolta un file viene aperto, scaricato, copiato o modificato, la scansione in tempo reale del **Security Agent** analizza il file per rilevare eventuali minacce.

Configurazione della scansione in tempo reale per i Security Agent

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Antivirus/Anti-spyware**.

   Viene visualizzata una nuova schermata.

5. Fare clic su **Attiva antivirus/anti-spyware in tempo reale**.
6. Configurazione delle impostazioni di scansione. Per i dettagli, consultare *Destinazioni di scansione e azioni per i Security Agent a pagina 7-10*:

   Nota

   Se gli utenti hanno i privilegi per configurare impostazioni di scansione personalizzate, durante la scansione vengono utilizzate le impostazioni di scansione impostate dall'utente.

7. Fare clic su **Salva**.

Intelligenza computazionale predittiva

Intelligenza computazionale predittiva di Trend Micro utilizza una tecnologia di machine learning avanzata per correlare le informazioni sulle minacce ed eseguire analisi dei file in modo approfondito per rilevare emergenti rischi per la sicurezza sconosciuti attraverso il fingerprinting DNA digitale, la mappatura API e altre caratteristiche del file. Intelligenza computazionale predittiva esegue anche un'analisi comportamentale su processi sconosciuti o di bassa prevalenza per determinare se una minaccia emergente o sconosciuta sta tentando di infettare la rete.

Intelligenza computazionale predittiva è uno strumento potente che contribuisca a proteggere l'ambiente da minacce non identificate e dagli attacchi zero-day.

Tipo di rilevamento	Descrizione
File	Dopo il rilevamento di un file sconosciuto o di bassa prevalenza, l'Security Agent sottopone il file alla scansione con il Motore avanzato scansione minacce per estrarne le caratteristiche, quindi invia il resoconto al motore di Intelligenza computazionale predittiva, gestito da Trend Micro Smart Protection Network. Tramite l'utilizzo della modellazione di malware, Intelligenza computazionale predittiva confronta l'esempio con un modello di malware, assegna un punteggio di probabilità e determina il probabile tipo di malware contenuto nel file. A seconda della configurazione della Intelligenza computazionale predittiva, l'Security Agent può inoltre tentare di mettere in “quarantena” il file interessato, per evitare che la minaccia si propaghi nella rete.
Processo	Dopo aver rilevato un processo sconosciuto o di bassa prevalenza, l'Security Agent monitora il processo con il Motore di intelligenza contestuale, quindi invia il resoconto del comportamento rilevato al motore di Intelligenza computazionale predittiva. Tramite l'utilizzo della modellazione di malware comportamentale, Intelligenza computazionale predittiva confronta il comportamento del processo con il modello, assegna un punteggio di probabilità e determina il probabile tipo di malware eseguito dal processo. A seconda della configurazione dell'Intelligenza computazionale predittiva, l'Security Agent può inoltre tentare di “terminare” il processo o script interessato e di disinfettare il file che lo ha eseguito.

Configurazione di Intelligenza computazionale predittiva

Nota

Intelligenza computazionale predittiva richiede quanto segue:

- Attivare il monitoraggio del comportamento in **Configura criterio** > **Monitoraggio del comportamento**
- Una connessione Internet funzionale per la connessione alla Smart Protection Network

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Intelligenza computazionale predittiva**.
5. Selezionare **Attiva Intelligenza computazionale predittiva**.
6. Selezionare il tipo di rilevamenti e azioni correlate effettuati da Intelligenza computazionale predittiva.

TIPO DI RILEVAMENTO	AZIONI
File	• **Quarantena**: selezionare questa azione per mettere automaticamente in quarantena i file che presentano caratteristiche di minacce informatiche in base all'analisi eseguita da Intelligenza computazionale predittiva • **Solo registrazione**: selezionare questa azione per eseguire la scansione dei file sconosciuti e registrare l'analisi della Intelligenza computazionale predittiva da utilizzare per ulteriori indagini interne

Tipo di rilevamento	Azioni
Processo	• **Termina**: selezionare questa azione per terminare automaticamente i processi o gli script che presentano comportamenti tipici delle minacce informatiche in base all'analisi della Intelligenza computazionale predittiva **Importante** Intelligenza computazionale predittiva tenta di disinfettare i file che hanno eseguito processi o script dannosi. Se l'operazione di disinfezione non è riuscita, Intelligenza computazionale predittiva mette in quarantena i file colpiti. • **Solo registrazione**: selezionare questa azione per eseguire la scansione dei processi o degli script sconosciuti e registrare l'analisi della Intelligenza computazionale predittiva da utilizzare per ulteriori indagini interne

7. Fare clic su **Salva**.

Monitoraggio del comportamento

I Security Agent controllano costantemente i client alla ricerca di modifiche insolite al sistema operativo o al software installato. Gli amministratori (o gli utenti) possono creare degli elenchi di eccezioni per consentire a determinati programmi di funzionare pur effettuando una modifica monitorata o per bloccare completamente determinati programmi. Inoltre, è sempre consentito l'avvio dei programmi con una firma digitale valida.

Un'altra funzione di Monitoraggio del comportamento consiste nel proteggere i file EXE e DLL da eventuale eliminazione o modifica. Quando Monitoraggio del comportamento è abilitato, gli utenti possono creare eccezioni per approvare o bloccare programmi specifici. Inoltre, gli utenti

possono decidere di proteggere in modo unitario tutti i programmi Intuit QuickBooks.

Configurazione del monitoraggio del comportamento

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Monitoraggio del comportamento**.
5. Aggiornare le seguenti impostazioni come richiesto:
   - **Attiva monitoraggio del comportamento**

     Nota

     Per consentire agli utenti di personalizzare le impostazioni di Monitoraggio del comportamento, andare su **Dispositivi** > **{gruppo}** > **Configura criterio** > **Privilegi agente** > **Monitoraggio del comportamento** e selezionare **Consenti agli utenti di modificare le impostazioni di Monitoraggio del comportamento**.
   - **Attiva il blocco comportamento malware per minacce note e potenziali**: il blocco del comportamento delle minacce informatiche si basa sull'applicazione di una serie di regole interne definite in **file di pattern**. Queste regole identificano i comportamenti noti e sospetti più diffusi tra le minacce informatiche. Esempi di comportamento sospetto sono l'esecuzione improvvisa e inaspettata di nuovi servizi, modifiche al firewall o modifiche dei file di sistema.

     Il Monitoraggio del comportamento malware fornisce le seguenti opzioni di scansione dei livelli delle minacce:

- **Minacce note**: blocca i comportamenti associati alle minacce note
- **Minacce note e potenziali**: blocca i comportamenti associati alle minacce note e interviene in caso di comportamenti potenzialmente dannosi

- **Chiedi agli utenti prima di eseguire programmi nuovi, scaricati tramite HTTP o applicazioni di posta elettronica (a eccezione delle piattaforme server)**: il monitoraggio del comportamento opera in abbinamento con Reputazione Web, per verificare la prevalenza dei file scaricati tramite canali HTTP o le applicazioni e-mail. Dopo aver rilevato un file "nuovo" mai incontrato prima, gli amministratori possono scegliere se chiedere conferma agli utenti prima di eseguirlo. Trend Micro classifica un programma come nuovo in base al numero di rilevamenti del file o all'età storica del file determinata da Smart Protection Network.

  Nota

  Per i canali HTTP, vengono analizzati i file eseguibili (.exe). Per le applicazioni e-mail (solo Outlook e Windows Live Mail), vengono analizzati i file eseguibili (.exe) contenuti nei file di archivio (zip/rar) non protetti da password.

- **Attiva protezione Intuit QuickBooks**: protegge tutti i file e le cartelle Intuit QuickBooks da modifiche non autorizzate effettuate da altri programmi. L'attivazione di questa caratteristica non influisce sulle modifiche effettuate dall'interno dei programmi Intuit QuickBooks, ma impedisce solamente le modifiche effettuate da altre applicazioni non autorizzate.

  Sono supportati i seguenti prodotti:

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

Nota

Tutti i file eseguibili Intuit dispongono di una firma digitale e gli aggiornamenti a questi file non vengono bloccati. Se sono presenti altri programmi che tentano di modificare il file binario Intuit, l'agent visualizza un messaggio con il nome del programma che sta tentando di aggiornare i file binari. È possibile consentire ad altri programmi di aggiornare i file Intuit. A tal fine, aggiungere il programma desiderato all'Elenco eccezioni Monitoraggio del comportamento dell'agent. Rimuovere il programma dall'elenco eccezioni una volta completato l'aggiornamento.

- **Protezione ransomware**: impedisce le modifiche non autorizzate o la crittografia dei file sui computer da parte di minacce "ransomware". Un ransomware è un tipo di malware che impedisce l'accesso ai file e richiede un pagamento per il ripristino dei file interessati.
  - **Attiva la protezione del documento da crittografia o modifiche non autorizzate**: Protegge i documenti da modifiche non autorizzate.
    - **Esegue il backup automatico dei file modificati dai programmi sospetti**: Se è attivata la protezione del documento, effettua automaticamente il backup di file modificati da programmi sospetti.
  - **Attiva il blocco dei processi comunemente associati a ransomware**: Protegge i dispositivi dagli attacchi ransomware bloccando i processi comunemente associati a tentativi di manomissione.
  - (Solo gruppi di desktop) **Attiva la scansione del programma per rilevare e bloccare i file eseguibili compromessi**: aumenta il rilevamento monitorando i processi alla ricerca di comportamenti ransomware.
  - **I programmi che mostrano un comportamento anomalo associato ad attacchi hacker vengono terminati**: la prevenzione anti-minaccia opera assieme all'ispezione del programma per monitorare il comportamento di programmi e

rilevare i comportamenti anomali che potrebbero indicare lo sfruttamento della vulnerabilità di un programma da parte di un aggressore. Una volta rilevati, Monitoraggio del comportamento termina i processi del programma.

Nota

Protezione da minacce richiede la selezione dell'opzione **Attiva l'ispezione del programma per rilevare e bloccare i file eseguibili compromessi**.

Nota

Per ridurre le possibilità che Worry-Free Business Security rilevi un processo sicuro come dannoso, assicurarsi che il computer sia connesso a Internet in modo da poter utilizzare i server Trend Micro per eseguire ulteriori verifiche.

- **Eccezioni**: Le eccezioni includono l'Elenco Programmi approvati e l'Elenco Programmi bloccati. I programmi nell'Elenco Programmi approvati possono essere avviati anche se tale operazione viola una modifica monitorata, mentre i programmi nell'Elenco Programmi bloccati non possono mai essere avviati.
  - **Inserire il percorso completo del programma**: Digitare il percorso completo UNC o Windows del programma. Separare più voci con punto e virgola (;). Fare clic su **Aggiungi all'elenco Approvati** o **Aggiungi all'elenco Approvati**. Se necessario, utilizzare le variabili ambientali per specificare i percorsi.
  - **Elenco Programmi approvati**: i programmi in questo elenco possono essere avviati. Fare clic sull'icona corrispondente per eliminare una voce.

    L'Elenco Programmi approvati supporta i caratteri jolly e le variabili ambientali.

    Per un elenco delle variabili ambientali supportate, vedere *Variabili ambientali supportate a pagina 5-16*.

- **Elenco Programmi bloccati**: i programmi in questo elenco non possono essere avviati. Fare clic sull'icona corrispondente per eliminare una voce.

  L'Elenco Programmi bloccati supporta solo i caratteri jolly.

6. Fare clic su **Salva**.

Variabili ambientali supportate

Nella tabella seguente vengono elencate le variabili ambientali che è possibile utilizzare quando si aggiunge un percorso di file o cartella all'elenco.

Variabile ambientale	Esempio	Percorso equivalente
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

Programmi affidabili

I programmi inclusi nell'elenco Programmi affidabili non vengono sottoposti a monitoraggio per attività di accesso ai file sospette.

Configurazione di un programmi affidabili

Nota

L'elenco Programmi affidabili non supporta i caratteri jolly e le variabili ambientali.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Programmi affidabili**.

   Viene visualizzata una nuova schermata.
5. Per escludere un programma dal monitoraggio di attività di accesso ai file sospette, digitare il percorso di file completo e fare clic su **Aggiungi all'elenco Programmi affidabili**.

   `<nome_unità>:/<percorso>/<nome_file>`

   Esempio 1: `C:\Windows\system32\regedit.exe`

   Esempio 2: `D:\backup\tool.exe`

   Questa impostazione impedisce agli hacker di utilizzare nomi di programmi riportati nell'elenco delle esclusioni, ma rilasciati in un percorso di file differente per l'esecuzione.

6. Fare clic su **Salva**.

Directory di quarantena

Se l'azione per un file infetto è "Quarantena", il Security Agent codifica il file e lo sposta **temporaneamente** in una cartella di quarantena:

- `<Cartella di installazione Security Agent>\quarantine` per agent aggiornati dalla versione 6.x o precedente
- `<Cartella di installazione Security Agent>\SUSPECT\Backup` per gli agent appena installati e per quelli aggiornati dalla versione 7.x o successiva

Security Agent invia il file infetto a una directory centralizzata di quarantena, configurabile dalla console Web in **Dispositivi** > **{Gruppo}** > **Configura criterio** > **Quarantena**.

Directory di quarantena centralizzata predefinita

La directory di quarantena centralizzata predefinita si trova sul Security Server. La directory è in formato URL e contiene il nome host del server o l'indirizzo IP del Security Server, in formato `http://server`. Il percorso assoluto equivalente è `<Cartella di installazione Security Server>\PCCSRV\Virus`.

- Se il server gestisce agent IPv4 e IPv6, usare il nome host in modo che tutti i client possano inviare file in quarantena al server.
- Se il server dispone solo di un indirizzo IPv4 (o è identificato con tale indirizzo), solo gli agent IPv4 puri e dual-stack possono inviare file in quarantena al server.
- Se il server dispone solo di un indirizzo IPv6 (o è identificato con tale indirizzo), solo gli agent IPv6 puri e dual-stack possono inviare file in quarantena al server.

Directory di quarantena centralizzata alternativa

È possibile specificare una directory di quarantena centralizzata alternativa immettendo il percorso in formato URL o UNC o un percorso assoluto. I

Security Agent devono essere in grado di connettersi a questa directory. Ad esempio, la directory deve avere un indirizzo IPv6 se riceverà file in quarantena da client dual-stack e IPv6 puri. Trend Micro consiglia di designare una directory dual-stack, identificando la directory con il corrispondente nome host e specificando la directory con un percorso UNC.

Linee guida per specificare la directory di quarantena centralizzata

Utilizzare la tabella riportata di seguito come riferimento su quando utilizzare URL, percorso UNC o percorso di file assoluto:

TABELLA 5-4. Directory di quarantena

DIRECTORY DI QUARANTENA	FORMATO ACCETTATO	ESEMPIO	NOTE
Directory predefinita sul Security Server	URL	`http:// <nome host del server o IP>`	Se si mantiene la directory predefinita, configurare le impostazioni di manutenzione per la directory, ad esempio la dimensione della cartella di quarantena, in **Amministrazione** > **Impostazioni globali** > **scheda Sistema** > **sezione Manutenzione della quarantena**.
	Percorso UNC	`\\<nome host del server o IP>\ ofcscan\Virus`	
Un'altra directory sul Security Server	Percorso UNC	`\\<nome host del server o IP>\ D$ \Quarantined Files`	Per non utilizzare la directory predefinita (ad esempio in caso di spazio su disco insufficiente), immettere il percorso UNC verso un'altra directory. In tal caso, inserire il percorso assoluto equivalente in **Amministrazione** > **Impostazioni globali** > **scheda Sistema** > **sezione Manutenzione della quarantena** per consentire l'applicazione delle impostazioni di manutenzione.

Directory di quarantena	Formato accettato	Esempio	Note
Una directory su un altro Security Server (se sono presenti altri Security Server nella rete)	URL	`http:// <nome host del server2 o IP>`	Accertarsi che gli agent siano in grado di connettersi a questa directory. Se si specifica una directory non valida, l'agent conserva i file di quarantena fino a quando non viene specificata una directory di quarantena valida. Nei registri di virus e malware sul server, il risultato della scansione è "Impossibile inviare il file da mettere in quarantena alla cartella in quarantena specificata". Se si utilizza il percorso UNC, assicurarsi che la directory di quarantena sia condivisa per il gruppo "Tutti" e che tutti i membri del gruppo abbiano i permessi di lettura e scrittura.
	Percorso UNC	`\\<nome host del server2 o IP>\ofcscan\Virus`	
Un altro computer della rete	Percorso UNC	`\\<nome_computer>\temp`	
Una directory sul client diversa	Percorso assoluto	`C:\temp`	Specificare un percorso assoluto se: • I file in quarantena devono trovarsi solo sul client. • Gli agent non devono archiviare i file nella directory predefinita nel client. Se il percorso non esiste, il Security Agent lo crea automaticamente.

Configurazione della directory di quarantena

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.

3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.

4. Fare clic su **Quarantena**.

   Viene visualizzata una nuova schermata.

5. Configurare la directory di quarantena. Per i dettagli, consultare *Directory di quarantena a pagina 5-18*.

6. Fare clic su **Salva**.

Reputazione Web

Reputazione Web contribuisce a impedire l'accesso a URL sul Web o incorporati in messaggi e-mail che comportano rischi di sicurezza. Reputazione Web controlla la reputazione dell'URL rispetto ai server di reputazione Web Trend Micro e quindi correla la reputazione con gli specifici criteri di reputazione Web attuati sul client. In base ai criteri in uso:

- Il Security Agent blocca o consente l'accesso al sito Web.
- Il Messaging Security Agent (solo Advanced) mette in quarantena, elimina o contrassegna il messaggio e-mail che contiene l'URL dannoso oppure ne consente l'invio se gli URL sono sicuri.

Reputazione Web invia una notifica e-mail all'amministratore e una notifica online all'utente riguardante i rilevamenti.

Configurare un livello di sicurezza diverso per i Security Agent in base alla posizione del client (In ufficio/Fuori ufficio).

Se la reputazione Web blocca un URL che invece è ritenuto sicuro, è possibile aggiungere l'URL all'elenco degli URL approvati.

Suggerimento

Per risparmiare ampiezza di banda della rete, Trend Micro consiglia di aggiungere i siti Web aziendali interni all'elenco degli URL approvati da reputazione Web.

Punteggio di reputazione

Il punteggio di reputazione di un URL indica se è presente una minaccia Web o meno. Trend Micro calcola il punteggio utilizzando delle tecniche di misurazione esclusive.

Trend Micro considera un URL una minaccia Web se il suo punteggio rientra in una soglia definita e sicuro se il punteggio supera tale soglia.

Nei Security Agent esistono tre livelli di protezione che determinano se l'accesso a un URL va consentito o bloccato.

- **Alto**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce
  - **Altamente sospetto**: Si sospetta la natura fraudolenta della pagina o si tratta di una possibile origine di minacce
  - **Sospetto**: Associate a spam o probabilmente compromesse
  - **Non testato**: Anche se Trend Micro verifica attivamente le pagine Web per garantire la sicurezza, gli utenti possono trovare pagine non verificate quando visitano pagine Web nuove o poco conosciute. Bloccando le pagine non verificate si migliora la sicurezza, ma si impedisce anche l'accesso alle pagine sicure.
- **Medio**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce
  - **Altamente sospetto**: Si sospetta la natura fraudolenta della pagina o si tratta di una possibile origine di minacce

- **Basso**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce

Configurazione della reputazione Web per Security Agent

Nel momento in cui viene inviata una richiesta HTTP/HTTPS, il servizio Reputazione Web valuta i potenziali rischi di tutti gli URL in questione, eseguendo una ricerca nel database di sicurezza di Trend Micro.

Nota

(Solo standard) Configurare le impostazioni di Reputazione Web per In ufficio/Fuori ufficio. Se l'opzione Location Awareness è disattivata, verranno utilizzate le impostazioni In ufficio per le connessioni Fuori ufficio. Per ulteriori informazioni su Location Awareness, vedere *Configurazioni delle impostazioni di desktop/server a pagina 11-5*.

Se Reputazione Web e Prevenzione degli attacchi al browser sono entrambi abilitati, gli URL non bloccati da Reputazione Web vengono sottoposti a scansione da Prevenzione degli attacchi al browser. Prevenzione degli attacchi al browser analizza gli oggetti incorporati (ad esempio: jar, class, pdf, swf, html, js) nelle pagine Web degli URL.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Reputazione Web** > **In ufficio** o **Reputazione Web** > **Fuori ufficio**.

   Viene visualizzata una nuova schermata.

5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Attiva Reputazione Web**
   - Livello sicurezza: **Alto**, **Medio** o **Basso**
   - Prevenzione minacce del browser: **blocca le pagine che contengono script dannosi**
6. Fare clic su **Salva**.

Filtro URL

Il filtro URL contribuisce a controllare l'accesso ai siti Web per ridurre i tempi di inattività dei dipendenti, limitare il consumo di ampiezza di banda Internet e creare un ambiente Internet più sicuro. È possibile scegliere un livello di protezione del filtro URL oppure specificare quali tipi di siti Web tenere sotto controllo.

Nota

Per proteggere i clienti, Trend Micro blocca automaticamente tutti gli URL che includono contenuto considerato illegale in molte parti del mondo.

Configurazione del filtro URL

È possibile selezionare tipi specifici di siti Web da bloccare nelle diverse ore del giorno selezionando **Personalizzata**.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.

4. Fare clic su **Filtro URL**.

   Viene visualizzata una nuova schermata.

5. Aggiornare le informazioni riportate di seguito, in base alle necessità:

   - **Attiva Filtro URL**
   - **Efficacia del filtro**
     - **Alto**: Blocca le minacce alla sicurezza conosciute o potenziali, il contenuto inappropriato o potenzialmente offensivo, il contenuto che incide su produttività o ampiezza di banda e le pagine senza classificazione.
     - **Medio**: Blocca le minacce alla sicurezza note e il contenuto inappropriato
     - **Basso**: Blocca le minacce alla sicurezza note
     - **Personalizzato**: Consente di selezionare categorie a piacimento e di decidere se bloccare tali categorie durante l'orario di lavoro o il tempo libero.
   - **Regole del filtro**: Selezionare le categorie o sottocategorie da bloccare.
   - **Ore di lavoro**: I giorni e le ore non specificate come Ore di lavoro sono considerate Ore tempo libero.

6. Fare clic su **Salva**.

URL approvati/bloccati

L'approvazione e il blocco automatici degli URL permettono di controllare l'accesso ai siti Web e di creare un ambiente Internet più sicuro. Gli URL approvati o bloccati sono identificabili nelle Impostazioni globali.

È anche possibile creare elenchi personalizzati di approvazione o blocco degli URL per gruppi specifici. Quando si seleziona l'opzione **Personalizza**

gli URL approvati o bloccati per questo gruppo, Security Agent utilizza l'elenco personalizzato di URL approvati o bloccati del gruppo per controllare l'accesso ai siti Web.

Configurazione degli URL approvati/bloccati

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **URL approvati/bloccati**.

   Viene visualizzata una nuova schermata.
5. Aggiornare le informazioni seguenti, in base alle necessità.
   - **Personalizza gli URL approvati o bloccati per questo gruppo**: Gli URL specificati in questo elenco hanno la precedenza su tutte le altre impostazioni.
   - Nella casella di testo **URL da approvare**, digitare gli URL dei siti Web da escludere dalle verifiche di Reputazione Web e Filtro URL. Separare più URL con un punto e virgola (;). Fare clic su **Aggiungi**.

     Suggerimento

     Fare clic su **Importa dalle impostazioni globali** per inserire tutte le voci. È quindi possibile personalizzare gli URL per questo gruppo.
   - Nella casella di testo **URL da bloccare**, digitare gli URL dei siti Web da bloccare nel Filtro URL. Separare più URL con un punto e virgola (;). Fare clic su **Aggiungi**.

Suggerimento

Fare clic su **Importa dalle impostazioni globali** per inserire tutte le voci. È quindi possibile personalizzare gli URL per questo gruppo.

6. Fare clic su **Salva**.

Firewall

Il firewall può bloccare o consentire l'accesso a un determinato tipo di traffico di rete creando una barriera tra il client e la rete. Inoltre, il firewall identifica dei pattern nei pacchetti di rete che rivelare un possibile attacco ai client.

In Worry-Free Business Security sono disponibili due opzioni per la configurazione del firewall: modalità semplice e modalità avanzata. La modalità semplice attiva il firewall con le impostazioni predefinite consigliate da Trend Micro. La modalità avanzata consente invece di personalizzare le impostazioni del firewall.

Suggerimento

Trend Micro consiglia di disinstallare altri firewall basati su software prima dell'implementazione e dell'attivazione del firewall di Trend Micro.

Impostazioni predefinite del firewall in modalità semplice

Il firewall è dotato di impostazioni predefinite che costituiscono una base di partenza per la propria strategia di protezione tramite firewall del client. Le impostazioni predefinite sono intese a includere condizioni comuni che si verificano sui client come, ad esempio, la necessità di accedere a Internet e scaricare o caricare file via FTP.

Nota

Per impostazione predefinita, Worry-Free Business Security disabilita il firewall su tutti i nuovi gruppi e Security Agent.

TABELLA 5-5. Impostazioni predefinite del firewall

IMPOSTAZIONI	STATO
Livello sicurezza	Basso Traffico in entrata e in uscita consentito, bloccati solo i virus di rete.
Sistema di rilevamento anti-intrusione	Disattivata
Messaggio di avviso (invio)	Disattivata

TABELLA 5-6. Eccezioni firewall predefinite

NOME ECCEZIONE	AZIONE	DIREZIONE	PROTOCOLLO	PORTA
DNS	Consenti	In entrata e in uscita	TCP/UDP	53
NetBIOS	Consenti	In entrata e in uscita	TCP/UDP	137, 138, 139, 445
HTTPS	Consenti	In entrata e in uscita	TCP	443
HTTP	Consenti	In entrata e in uscita	TCP	80
Telnet	Consenti	In entrata e in uscita	TCP	23
SMTP	Consenti	In entrata e in uscita	TCP	25
FTP	Consenti	In entrata e in uscita	TCP	21
POP3	Consenti	In entrata e in uscita	TCP	110
MSA	Consenti	In entrata e in uscita	TCP	16372, 16373

Nome eccezione	Azione	Direzione	Protocollo	Porta
LDAP	Consenti	In entrata e in uscita	TCP/UDP	389

Tabella 5-7. Impostazioni firewall predefinite in base al percorso

Percorso	Impostazioni firewall
In ufficio	Disattivo
Fuori ufficio	Disattivo

Filtraggio del traffico

Il firewall filtra tutto il traffico in entrata e in uscita e offre la possibilità di bloccare alcuni tipi di traffico in base ai seguenti criteri:

- Direzione (in entrata/in uscita)
- Protocollo (TCP/UDP/ICMP/ICMPv6)
- Porte di destinazione
- Computer di destinazione

Scansione dei virus di rete

Il firewall esamina inoltre tutti i pacchetti alla ricerca di virus di rete.

Stateful Inspection

Il firewall è di tipo "stateful inspection", monitora cioè tutte le connessioni al computer client e archivia tutti gli stati di connessione. È in grado di identificare condizioni specifiche in ogni connessione, prevedere quali azioni seguiranno e individuare le interruzioni in una connessione normale. L'uso efficace del firewall, quindi, non sono implica la creazione di profili e criteri, ma anche l'analisi delle connessioni e il filtro dei pacchetti che passano attraverso il firewall.

Driver comune firewall

Il driver comune per firewall, in combinazione con le impostazioni definite dall'utente del firewall, blocca le porte durante un'infezione. Il driver

comune per firewall utilizza il file dei pattern dei virus di rete per ricercare i virus di rete.

Configurazione del firewall

Configurare il firewall per In ufficio/Fuori ufficio. Se l'opzione Location Awareness è disattivata, verranno utilizzate le impostazioni In ufficio per le connessioni Fuori ufficio.

Per ulteriori informazioni su Location Awareness, vedere *Configurazioni delle impostazioni di desktop/server a pagina 11-5*.

Trend Micro disabilita il firewall per impostazione predefinita.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Firewall** > **In ufficio** o **Fuori ufficio**.
5. Selezionare **Attiva firewall**.
6. Selezionare quanto segue:
   - **Modalità semplice**: Attiva il firewall con le impostazioni predefinite.

     Per i dettagli, consultare *Firewall a pagina 5-27*.
   - **Modalità avanzata**: Abilita il firewall con le impostazioni personalizzate.
7. Se viene selezionata la **Modalità avanzata**, aggiornare le seguenti opzioni a seconda delle esigenze:

- **Livello sicurezza**: Il livello di sicurezza controlla le regole del traffico da implementare per le porte che non sono incluse nell'elenco delle eccezioni.
  - **Alto**: blocca tutto il traffico in entrata e in uscita, ad eccezione di quello consentito dall'elenco delle eccezioni.
  - **Medio**: blocca tutto il traffico in entrata e consente tutto il traffico in uscita, ad eccezione di quello consentito e bloccato nell'elenco delle eccezioni.
  - **Basso**: consente tutto il traffico in entrata e in uscita, ad eccezione di quello bloccato dall'elenco delle eccezioni. Questa è l'impostazione predefinita per la modalità minima.
- **Impostazioni**
  - **Attiva sistema di rilevamento anti-intrusione**: Il sistema di rilevamento anti-intrusione consente di identificare i pattern nei pacchetti di rete che possono indicare un attacco sul computer.

    Per i dettagli, consultare *Sistema di rilevamento anti-intrusione a pagina D-3*.
  - **Attiva messaggio avviso**: Quando Worry-Free Business Security rileva una violazione, invia una notifica al client.
- **Eccezioni**: Le porte nell'elenco delle eccezioni non vengono bloccate.

  Per i dettagli, vedere *Utilizzo delle eccezioni Firewall a pagina 5-31*.

8. Fare clic su **Salva**.

Utilizzo delle eccezioni Firewall

L'elenco delle eccezioni del firewall contiene voci che possono essere configurate per consentire il blocco di vari tipi di traffico di rete in base ai numeri di porta dei client e agli indirizzi IP. Durante un'infezione, il Security

Server applica le eccezioni ai criteri di Trend Micro che vengono automaticamente implementati per proteggere la rete.

Ad esempio, durante un'infezione è possibile scegliere di bloccare tutto il traffico dei client, inclusa la porta HTTP (porta 80). Se tuttavia si desidera comunque concedere l'accesso a Internet ai client bloccati, è possibile aggiungere il server proxy Web all'elenco delle eccezioni.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Firewall** > **In ufficio** o **Firewall** > **Fuori ufficio**.

   Viene visualizzata una nuova schermata.
5. Selezionare **Attiva firewall**.
6. Selezionare **Modalità avanzata**.
7. Per aggiungere un'eccezione:
   a. Fare clic su **Aggiungi**.

      Viene visualizzata una nuova schermata.
   b. Digitare un nome per l'eccezione.
   c. Accanto a **Operazione**, fare clic su una delle seguenti opzioni:
      - **Consenti tutto il traffico di rete**
      - **Blocca tutto il traffico di rete**
   d. Accanto a **Direzione**, fare clic su **In entrata** o **In uscita** per selezionare il tipo di traffico a cui applicare le impostazioni dell'eccezione.

e. Selezionare il tipo di protocollo di rete dall'elenco Protocollo.

- **Tutti**
- **TCP/UDP** (impostazione predefinita)
- **TCP**
- **UDP**
- **ICMP**
- **ICMPv6**

f. Fare clic su una delle seguenti opzioni per specificare le porte del client:

- **Tutte le porte** (impostazione predefinita)
- **Intervallo**: immettere un intervallo di porte.
- **Porte specificate**:specificare le singole porte. Per separare i numeri di porta, utilizzare la virgola ",".

g. Nella sezione **Computer**, selezionare gli indirizzi IP dei client da includere nell'eccezione. Ad esempio, se si seleziona **Blocca tutto il traffico di rete (In entrata e In uscita)** e si immette l'indirizzo IP di un singolo computer della rete, qualsiasi client con questa eccezione tra i criteri non potrà inviare o ricevere dati da quell'indirizzo IP. Fare clic su una delle opzioni riportate di seguito.

- **Tutti gli indirizzi IP** (impostazione predefinita)
- **IP unico**: immettere un nome host o un indirizzo IPv4 o IPv6. Per risolvere il nome host del client in un indirizzo IP, fare clic su **Risolvi**.
- **Intervallo IP (Per IPv4 o IPv6)**: digitare due indirizzi IPv4 o due indirizzi IPv6 nei campi **Da** e **A**. Non è possibile immettere un indirizzo IPv6 in un campo e un indirizzo IPv4 nell'altro.
- **Intervallo IP (per IPv6)**: immettere una lunghezza e un prefisso di indirizzo IPv6.

h. Fare clic su **Salva**.

8. Per modificare un'eccezione, fare clic su **Modifica**, quindi modificare le impostazioni nella schermata visualizzata.
9. Per spostare un'eccezione in alto o in basso nell'elenco, selezionare l'eccezione, quindi fare clic su **Sposta su** o **Sposta giù** finché non raggiunge la posizione desiderata.
10. Per rimuovere un'eccezione, selezionare l'eccezione e fare clic su **Rimuovi**.

Disattivazione del firewall su un gruppo di agent

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Firewall** > **In ufficio** o **Firewall** > **Fuori ufficio**.

   Viene visualizzata una nuova schermata.
5. Selezionare **Disattiva firewall**.
6. Fare clic su **Salva**.

Disattivazione del firewall su tutti gli agent

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.

2. Fare clic su **Desktop/Server**.
3. In **Impostazioni firewall**, selezionare **Disabilita firewall e disinstalla driver**.
4. Fare clic su **Salva**.

Controllo dispositivo

Controllo dispositivo regola l'accesso ai dispositivi di archiviazione esterni connessi agli endpoint. In particolare, Controllo dispositivo limita l'accesso a tutti i tipi di dispositivi di archiviazione che si connettono tramite un'interfaccia USB, ad eccezione dei dispositivi mobili e delle fotocamere digitali.

Configurazione del controllo dispositivo

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Controllo dispositivo**.
5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Attiva controllo dispositivo**
   - **Attiva Prevenzione esecuzione automatica USB**
   - **Autorizzazioni**:impostare per i dispositivi USB e le risorse di rete.

TABELLA 5-8. Autorizzazioni controllo dispositivo

AUTORIZZAZIONI	FILE NEL DISPOSITIVO	FILE IN ENTRATA
Accesso completo	Operazioni consentite: Copia, Sposta, Apri, Salva, Elimina, Esegui	Operazioni consentite: salvataggio, spostamento, copia Ciò significa che un file può essere salvato, spostato e copiato nel dispositivo.
Nessun accesso	Operazioni non consentite: tutte le operazioni Il dispositivo e i file che contiene sono visibili all'utente (ad esempio, da Esplora risorse di Windows).	Operazioni non consentite: salvataggio, spostamento, copia
Lettura	Operazioni consentite: Copia, Apri Operazioni non consentite: Salva, Sposta, Elimina, Esegui	Operazioni non consentite: salvataggio, spostamento, copia
Modifica	Operazioni consentite: Copia, Sposta, Apri, Salva, Elimina Operazioni non consentite: Esegui	Operazioni consentite: salvataggio, spostamento, copia
Lettura ed esecuzione	Operazioni consentite: Copia, Apri, Esegui Operazioni non consentite: Salva, Sposta, Elimina	Operazioni non consentite: salvataggio, spostamento, copia

- **Eccezioni**:Se un utente non ha l'autorizzazione per leggere un determinato dispositivo, potrà comunque eseguire o aprire qualsiasi file o programma dell'Elenco Approvati.

  Tuttavia, se l'opzione Prevenzione esecuzione automatica è attivata, anche se un file è incluso nell'Elenco Approvati, non sarà comunque possibile eseguirlo.

Per aggiungere un'eccezione all'Elenco Approvati, immettere il nome del file e il percorso o la firma digitale e fare clic su **Aggiungi all'elenco Approvati**.

6. Fare clic su **Salva**.

Strumenti utente

- **Barra degli strumenti Anti-Spam**: Filtra i messaggi di spam in Microsoft Outlook, fornisce statistiche e permette di modificare determinate impostazioni.
- **HouseCall**: Determina la sicurezza di una connessione wireless verificando l'autenticità dei punti di accesso in base alla validità dei rispettivi SSID, a metodi di autenticazione e requisiti di crittografia. Un avviso a comparsa mostrerà se la connessione non è sicura.
- **Case Diagnostic Tool**: Quando si verifica un problema, Trend Micro Case Diagnostic Tool (CDT) raccoglie le informazioni di debugging necessarie dal prodotto del cliente. Attiva e disattiva automaticamente lo stato di debug del prodotto e raccoglie i file necessari a seconda della categoria del problema. Queste informazioni vengono utilizzate da Trend Micro per risolvere i problemi legati al prodotto.

  Tale strumento è disponibile solo sulla console del Security Agent.
- **Client Mover**: questo strumento permette di trasferire i client da un server all'altro. I server devono avere la stessa versione di lingua e devono essere dello stesso tipo.
- **Strumento di comunicazione client/server**: utilizzare questo strumento per risolvere i problemi di comunicazione tra client e server.

Configurazione degli strumenti dell'utente

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Strumenti utente**.

   Viene visualizzata una nuova schermata.
5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Wi-Fi Advisor**: controlla la protezione delle reti wireless sulla base della validità dei rispettivi SSID, dei metodi di autenticazione e dei requisiti di crittografia.
   - **Barra degli strumenti di Anti-Spam**: filtra i messaggi di spam in Microsoft Outlook.
6. Fare clic su **Salva**.

Privilegi degli agenti

Assegnare i privilegi degli agenti per consentire agli utenti di modificare le impostazioni di Security Agent nel client.

Suggerimento

Per implementare un criterio di protezione regolamentato in tutta l'organizzazione, Trend Micro consiglia di assegnare agli utenti dei privilegi limitati. Questo consente di impedire agli utenti di modificare le impostazioni di scansione o scaricare il Security Agent.

Configurazione dei privilegi agente

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un gruppo desktop o server.
3. Fare clic su **Configura criterio**.

   Viene visualizzata la schermata **Configura criterio: <nome gruppo>**.
4. Fare clic su **Privilegi agent**.
5. Aggiornare le seguenti impostazioni come richiesto:

Sezione	Privilegi
Antivirus/Anti-spyware	• Impostazioni scansione in tempo reale • Impostazioni scansione manuale • Impostazioni scansione pianificata • Salta scansione pianificata
Firewall	Impostazioni firewall
Reputazione Web - Continua la navigazione	Visualizza un collegamento che consente agli utenti di continuare a sfogliare un URL dannoso fino al riavvio del computer. Gli avvisi continueranno a essere visualizzati in altri URL dannosi.
Filtri URL - Continua a sfogliare	Visualizza un collegamento che consente agli utenti di continuare a sfogliare un URL vietato fino al riavvio del computer. Gli avvisi continueranno a essere visualizzati in altri URL vietati.
Monitoraggio del comportamento	Consente agli utenti di modificare le impostazioni di monitoraggio del comportamento.
Programmi affidabili	Consente agli utenti di modificare l'elenco di programmi attendibili.

Sezione	Privilegi
Impostazioni Proxy	Consente agli utenti di configurare le impostazioni proxy. **Nota** La disattivazione di questa funzione ripristina impostazioni proxy predefinite.
Privilegi di aggiornamento	• Consente agli utenti di eseguire aggiornamenti manuali • Utilizzare Trend Micro ActiveUpdate come origine di aggiornamento secondaria • Disattiva la distribuzione di hotfix **Nota** La distribuzione di hotfix, patch, patch di sicurezza/critiche e service pack a un gran numero di agenti contemporaneamente può aumentare in modo significativo il traffico di rete. Considerare la possibilità di attivare questa opzione su più gruppi, in modo da poter scaglionare la distribuzione. Attivando questa opzione è possibile disattivare l'**aggiornamento della build** automatico sugli agenti (ad esempio, dalla build Beta alla build di rilascio della versione del prodotto corrente) ma NON gli **aggiornamenti delle versioni** automatici (ad esempio, dalla versione 7.x alla versione corrente). Per disattivare gli aggiornamenti automatici delle versioni, eseguire il pacchetto di installazione del Security Server e scegliere l'opzione per ritardare gli aggiornamenti.
Protezione client	Impedisci agli utenti o ad altri processi di modificare file di programma, registri e processi Trend Micro.

6. Fare clic su **Salva**.

Capitolo 6

Gestione delle Impostazioni di sicurezza di base per i Messaging Security Agent (solo Advanced)

In questo capitolo viene illustrato il Messaging Security Agent e viene descritto come impostare le opzioni di scansione in tempo reale, configurare le impostazioni anti-spam, il filtro dei contenuti, il blocco degli allegati e le opzioni di gestione della quarantena per l'agent.

Messaging Security Agent

I Messaging Security Agent proteggono i server Microsoft Exchange. L'agent consente di evitare l'attacco delle minacce trasmesse tramite e-mail grazie alla scansione dei messaggi in entrata e in uscita dall'Archivio cassette postali di Microsoft Exchange e dei messaggi che transitano tra il server Microsoft Exchange e le destinazioni esterne. Inoltre, Messaging Security Agent è in grado di:

- Ridurre lo spam
- Bloccare i messaggi e-mail in base al contenuto
- Bloccare o limitare i messaggi e-mail con allegati
- Rilevare URL dannosi nei messaggi e-mail
- Impedire la perdita di dati confidenziali

Informazioni importanti sui Messaging Security Agent

- I moduli Messaging Security Agent possono essere installi solo sui server Microsoft Exchange.
- Messaging Security Agent non supporta alcune funzioni di Microsoft Exchange Server Enterprise come il gruppo di disponibilità dei dati (DAG).
- La Struttura dei gruppi di protezione nella console Web visualizza tutti i Messaging Security Agent. Non è possibile combinare più Messaging Security Agent in un gruppo. Ogni Messaging Security Agent deve essere amministrato e gestito individualmente.
- Worry-Free Business Security utilizza il Messaging Security Agent per raccogliere informazioni dai server Microsoft Exchange. Ad esempio, il Messaging Security Agent segnala i rilevamenti dello spam o il completamento degli aggiornamenti dei componenti al Security Server. Queste informazioni vengono visualizzate nella console Web. Il Security Server utilizza anche queste informazioni per generare i registri e i rapporti circa lo stato della sicurezza nei server Microsoft Exchange.

Ogni minaccia rilevata genera una voce di registro/notifica. Di conseguenza, se Messaging Security Agent rileva varie minacce in un unico messaggio e-mail, vengono generate più voci di registro e notifiche. Può accadere che una stessa minaccia venga rilevata varie volte, specialmente se si utilizza la modalità cache di Outlook 2003. Quando la modalità cache è attivata, la stessa minaccia può essere rilevata sia nella cartella di coda del trasferimento che nella cartella della posta inviata o della posta in uscita.

- Nei computer sui quali è in esecuzione Microsoft Exchange Server 2007, il Messaging Security Agent utilizza un database SQL Server. Per evitare eventuali problemi, i servizi di Messaging Security Agent sono progettati per dipendere dall'istanza del servizio di SQL Server `MSSQL$SCANMAIL`. Ogni volta che questa istanza viene arrestata o riavviata, anche i seguenti servizi del Messaging Security Agent vengono arrestati:

  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  Se `MSSQL$SCANMAIL` viene arrestato o riavviato, riavviare manualmente questi servizi. Esistono diversi eventi, tra cui l'aggiornamento di SQL Server, che possono causare l'arresto o il riavvio di `MSSQL$SCANMAIL`.

Scansione dei messaggi e-mail da parte di Messaging Security Agent

Il Messaging Security Agent si avvale della sequenza riportata di seguito per sottoporre a scansione i messaggi e-mail:

1. Esamina la presenza di spam (anti-spam)
   a. Confronta il messaggio e-mail con l'elenco di mittenti approvati/bloccati definito dall'amministratore
   b. Verifica la presenza di eventi di phishing
   c. Confronta il messaggio e-mail con l'elenco delle eccezioni fornito da Trend Micro

d. Confronta il messaggio e-mail con il database di definizioni di spam

e. Applica le regole della scansione euristica

2. Verifica la presenza di violazioni alle regole di filtro dei contenuti
3. Sottopone a scansione gli allegati che superano i parametri definiti dall'utente
4. Verifica la presenza di virus/minacce informatiche (antivirus)
5. Scansione di URL dannosi

Impostazioni predefinite di Messaging Security Agent

Valutare le opzioni elencate nella tabella come supporto per ottimizzare le configurazioni di Messaging Security Agent.

TABELLA 6-1. Le azioni predefinite di Trend Micro per Messaging Security Agent

OPZIONI DI SCANSIONE	SCANSIONE IN TEMPO REALE	SCANSIONE MANUALE E PIANIFICATA
Anti-spam		
Spam	Mettere in quarantena i messaggi nella cartella di spam dell'utente (questa è l'impostazione predefinita, se Outlook Junk Email o End User Quarantine sono installati)	Non pertinente
Phishing	Elimina intero messaggio	Non pertinente
Filtro dei contenuti		
Filtra messaggi che soddisfano qualsiasi condizione definita	Metti in quarantena intero messaggio	Sostituisci

Opzioni di scansione	Scansione in tempo reale	Scansione manuale e pianificata
Filtra messaggi che soddisfano tutte le condizioni definite	Metti in quarantena intero messaggio	Non pertinente
Monitora il contenuto dei messaggi di particolari account e-mail.	Metti in quarantena intero messaggio	Sostituisci
Crea un'eccezione per particolari account e-mail	Ignora	Ignora
Blocco allegati		
Azione	Sostituisci allegato con testo/file	Sostituisci allegato con testo/file
Altro		
File crittografati e protetti da password	Ignora (quando si imposta l'azione su Ignora, i file crittografati e i file protetti da password vengono ignorati e l'evento non viene registrato)	Ignora (quando si imposta l'azione su Ignora, i file crittografati e i file protetti da password vengono ignorati e l'evento non viene registrato)
File esclusi (file oltre le limitazioni di scansione specificate)	Ignora (quando si imposta l'azione su Ignora, i file o il testo dei messaggi per cui valgono le restrizioni di scansione specificate vengono ignorati e l'evento non viene registrato)	Ignora (quando si imposta l'azione su Ignora, i file o il testo dei messaggi per cui valgono le restrizioni di scansione specificate vengono ignorati e l'evento non viene registrato)

Configurazione della scansione in tempo reale per i Messaging Security Agent

La scansione in tempo reale è una scansione continua e costante. La scansione in tempo reale nel **Messaging Security Agent** (solo Advanced) protegge tutti i possibili punti di ingresso di virus effettuando la scansione in

tempo reale di tutti i messaggi in entrata, messaggi SMTP, documenti pubblicati su cartelle pubbliche e file replicati da altri server Microsoft Exchange.

Configurazione della scansione in tempo reale per Messaging Security Agent

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Antivirus**.

   Viene visualizzata una nuova schermata.
5. Selezionare **Attiva Antivirus in tempo reale**.
6. Configurazione delle impostazioni di scansione. Per i dettagli, consultare *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*.
7. Fare clic su **Salva**.

   Configurare chi riceve le notifiche quando si verifica un evento. Vedere *Configurazione degli eventi per le notifiche a pagina 10-4*.

Anti-Spam

Worry-Free Business Security offre due sistemi per contrastare lo spam: **Email Reputation** e **Scansione dei contenuti**.

Messaging Security Agent utilizza i seguenti componenti per filtrare i messaggi e-mail ed evitare problemi legati a spam e phishing.

- Motore anti-spam Trend Micro (TMASE - Trend Micro Anti-Spam Engine)
- File di pattern anti-spam Trend Micro

Trend Micro aggiorna con frequenza il motore e il file di pattern e li rende disponibili per lo scaricamento. Security Server può scaricare questi componenti con un aggiornamento manuale o pianificato.

Il motore anti-spam utilizza file di definizione anti-spam e regole euristiche per filtrare i messaggi e-mail. Esegue la scansione dei messaggi e assegna a ognuno un punteggio di spamming in base all'aderenza alle regole e ai pattern del file di pattern. Messaging Security Agent mette a confronto il punteggio di spamming con il livello di rilevamento dello spam definito dall'utente. Quando il punteggio di spamming supera il livello di rilevamento, l'agent interviene contro lo spam.

Ad esempio: gli spammer utilizzano nei loro messaggi e-mail una gran quantità di punti esclamativi o più punti esclamativi uno di seguito all'altro (!!!!). Quando Messaging Security Agent rileva un messaggio che contiene punti esclamativi utilizzati in questi termini, aumenta il punteggio di spamming del messaggio e-mail.

Suggerimento

Oltre a utilizzare Anti-spam per eliminare lo spam, è possibile configurare il filtro del contenuto in modo che controlli l'intestazione, l'oggetto, il corpo e gli allegati ed escluda lo spam e altri contenuti indesiderati.

Gli utenti non possono modificare il metodo utilizzato dal motore anti-spam per l'assegnazione dei punteggi, ma possono regolare i livelli di rilevamento utilizzati da Messaging Security Agent per separare la posta dallo spam.

Nota

Microsoft Outlook può filtrare automaticamente e inviare i messaggi che il Messaging Security Agent considera spam alla cartella della posta indesiderata.

Servizi Email Reputation

La tecnologia Email Reputation identifica lo spam in base alla reputazione del Mail Transport Agent (MTA) di origine. In questo modo si riduce il carico di lavoro sul Security Server. Con la funzione Email Reputation attivata, tutto il traffico SMTP viene controllato dai database IP per verificare se l'indirizzo IP di origine è affidabile, se è stato inserito in una blacklist o se è un vettore di spam noto.

Email Reputation offre i due livelli di servizio, ovvero:

- **Standard**: Il servizio standard si affida a un database in grado di identificare la reputazione di circa due miliardi di indirizzi IP. Gli indirizzi IP che vengono costantemente associati alla diffusione di messaggi di spam vengono aggiunti a un database e solo raramente rimossi.
- **Avanzato**: Il livello di servizio avanzato offre un servizio DNS basato su query come il servizio standard. La base di questo servizio è il database di reputazione standard, unitamente al database di reputazione dinamico in tempo reale che blocca i messaggi provenienti da fonti note e sospette di spam.

Quando viene individuato un messaggio e-mail proveniente da un indirizzo IP bloccato o sospetto, Email Reputation blocca il messaggio prima che questo raggiunga il gateway.

Configurazione di Email Reputation

Configurare l'opzione Email Reputation per bloccare i messaggi da origini di spam note o sospette. Creare inoltre esclusioni per consentire o bloccare i messaggi provenienti da altri mittenti.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Anti-spam** > **Email Reputation**.

   Viene visualizzata una nuova schermata.
5. Dalla scheda **Destinazione**, aggiornare i seguenti campi secondo le esigenze:
   - **Attiva anti-spam in tempo reale (Reputazione e-mail)**
   - **Livello del servizio**:
     - **Standard**
     - **Avanzato**
   - **Indirizzi IP approvati**: i messaggi e-mail provenienti da questi indirizzi IP non vengono mai bloccati. Immettere l'indirizzo IP da approvare e fare clic su **Aggiungi**. Se necessario, è possibile importare un elenco di indirizzi IP da un file di testo. Per rimuovere un indirizzo IP, selezionare l'indirizzo e fare clic su **Rimuovi**.
   - **Indirizzi IP bloccati**: i messaggi e-mail provenienti da questi indirizzi IP vengono sempre bloccati. Immettere l'indirizzo IP da bloccare e fare clic su **Aggiungi**. Se necessario, è possibile importare un elenco di indirizzi IP da un file di testo. Per rimuovere un indirizzo IP, selezionare l'indirizzo e fare clic su **Rimuovi**.
6. Fare clic su **Salva**.
7. Visitare: http://ers.trendmicro.com/ per visualizzare le segnalazioni.

Nota

Email Reputation è un servizio basato sul Web. Gli amministratori possono configurare il livello del servizio unicamente dalla console Web.

Scansione dei contenuti

La scansione dei contenuti identifica lo spam in base al contenuto del messaggio piuttosto che dall'IP di origine. Messaging Security Agent utilizza il motore anti-spam e il file dei pattern anti-spam di Trend Micro per escludere lo spam da ogni messaggio e-mail prima che venga inviato all'archivio di informazioni. Il server Microsoft Exchange non elabora la posta rifiutata indesiderata, evitando che i messaggi raggiungano le caselle postali dell'utente.

Nota

Attenzione a non confondere Scansione dei contenuti (anti-spam basato su firme e regole euristiche) Filtro dei contenuti (scansione e blocco di messaggi e-mail sulla base di categorie di parole chiave). Vedere *Filtro dei contenuti a pagina 6-16*.

Configurazione della scansione dei contenuti

Il Messaging Security Agent individua i messaggi di spam in **tempo reale** ed esegue le azioni necessarie per proteggere i server Microsoft Exchange.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Anti-spam** > **Scansione dei contenuti**.

   Viene visualizzata una nuova schermata.

5. Selezionare **Attiva Anti-spam in tempo reale**.

6. Selezionare la scheda **Destinazione** per specificare il metodo e la frequenza di rilevamento spam che il Messaging Security Agent deve utilizzare per l'eliminazione dello spam:

   a. Selezionare il livello di rilevamento **basso**, **medio** o **alto**, dall'elenco dei livelli di rilevamento spam. Messaging Security Agent utilizza questo livello per esaminare tutti i messaggi.

      - **Alto**: è il più rigoroso livello di rilevamento dello spam. Messaging Security Agent monitora tutti i messaggi e-mail alla ricerca di file o testo sospetti, ma vi è un'alta probabilità che si verifichino falsi allarmi. I falsi allarmi riguardano i messaggi e-mail che Messaging Security Agent filtra come spam, mentre sono in realtà messaggi del tutto legittimi.

      - **Medio**: questa è l'impostazione predefinita e consigliata. Messaging Security Agent monitora i messaggi adottando un livello alto di rilevamento dello spam; presenta una moderata possibilità di falsi allarmi.

      - **Basso**: è il livello meno rigoroso di rilevamento dello spam. Messaging Security Agent filtra solo i messaggi indesiderati più ovvi e diffusi, ma vi è una scarsissima probabilità di falsi allarmi. Filtro in base al punteggio di spamming.

   b. Per fare in modo che il Messaging Security Agent elimini i tentativi di phishing, fare clic su **Rileva phishing**. Per i dettagli, consultare *Tentativi di phishing a pagina 1-13*.

   c. Aggiungere gli indirizzi all'elenco Mittenti approvati e Mittenti bloccati. Per i dettagli, consultare *Elenchi di mittenti approvati e bloccati a pagina 6-13*.

      - **Mittenti approvati**: i messaggi e-mail provenienti da questi indirizzi o nomi di dominio non vengono mai bloccati. Immettere gli indirizzi e-mail o i nomi di dominio da approvare

e fare clic su **Aggiungi**. Se necessario, è possibile importare un elenco di indirizzi o di nomi di dominio da un file di testo. Per rimuovere indirizzi o nomi di dominio, selezionare l'indirizzo e fare clic su **Rimuovi**.

- **Mittenti bloccati**: i messaggi e-mail provenienti da questi indirizzi o nomi di dominio vengono sempre bloccati. Immettere gli indirizzi e-mail o i nomi di dominio da bloccare e fare clic su **Aggiungi**. Se necessario, è possibile importare un elenco di indirizzi o di nomi di dominio da un file di testo. Per rimuovere indirizzi o nomi di dominio, selezionare l'indirizzo e fare clic su **Rimuovi**.

Nota

L'amministratore Microsoft Exchange conserva un elenco Mittenti approvati/bloccati separato per il server Microsoft Exchange. Se un utente finale crea un mittente approvato, ma il mittente è inserito nell'elenco dei mittenti bloccati dell'amministratore, Messaging Security Agent rileva i messaggi provenienti dal mittente in questione ed esegue operazioni per bloccare questi messaggi.

7. Fare clic sulla scheda **Operazione** per impostare le operazioni che il Messaging Security Agent deve eseguire quando rileva un messaggio di spam o un tentativo di phishing.

Nota

Per ulteriori informazioni sulle operazioni, vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*.

Messaging Security Agent esegue una delle operazioni riportate di seguito in base alle singole configurazioni.

- **Inserisci messaggio nella cartella di quarantena spam lato server**
- **Inserisci in quarantena il messaggio nella cartella di spam utente**

Nota

Se si sceglie questa operazione, configurare la End User Quarantine. Per i dettagli, consultare *Configurazione di Manutenzione spam a pagina 6-74*.

- **Elimina intero messaggio**
- **Contrassegna e recapita**

8. Fare clic su **Salva**.

Elenchi di mittenti approvati e bloccati

Un elenco di mittenti approvati è un elenco di indirizzi e-mail affidabili. Il Messaging Security Agent non filtra i messaggi provenienti da questi indirizzi alla ricerca di spam, salvo nel caso in cui sia attivata l'opzione **Rileva tentativi di phishing**. Se l'opzione **Rileva tentativi di phishing** è stata abilitata e l'agent rileva un problema legato al phishing in un messaggio e-mail, il messaggio non viene consegnato anche se appartiene a un elenco dei mittenti approvati. Un elenco di mittenti bloccati è un elenco di indirizzi e-mail sospetti. L'agent classifica sempre i messaggi e-mail provenienti dai destinatari bloccati come spam e interviene di conseguenza.

Esistono due elenchi di mittenti approvati: uno relativo all'amministratore Microsoft Exchange e uno agli utenti finali.

- L'elenco dei mittenti approvati e bloccati dell'amministratore di Microsoft Exchange (schermata **Anti-spam**) consente di controllare la modalità con cui Messaging Security Agent tratta i messaggi e-mail destinati al server Microsoft Exchange.
- L'utente finale gestisce la Cartella di spam appositamente creata durante l'installazione. Gli elenchi degli utenti finali influenzano soltanto i messaggi destinati all'archivio della casella di posta lato server di ogni singolo utente finale.

Linee guida generali

- Gli elenchi dei mittenti approvati e bloccati su un server Microsoft Exchange prevalgono sugli elenchi di mittenti approvati e bloccati su un

client. Ad esempio, il mittente utente@esempio.com è incluso nell'elenco dei mittenti bloccati dell'amministratore, ma l'utente finale ha aggiunto l'indirizzo al suo elenco dei mittenti approvati. I messaggi inviati da questo mittente arrivano nell'archivio del server Microsoft Exchange e Messaging Security Agent li contrassegna come spam ed esegue operazioni per bloccarli. Se l'agent esegue l'azione Mettere in quarantena i messaggi nella cartella di spam utente, cercherà di consegnare il messaggio nella cartella dello spam dell'utente finale, ma il messaggio verrà invece reindirizzato alla casella della posta in arrivo dell'utente finale poiché l'utente ha approvato il mittente.

- Se si utilizza Outlook, esiste un limite in termini di dimensione per quanto riguarda la quantità e la dimensione degli indirizzi dell'elenco. Per evitare errori di sistema, Messaging Security Agent limita la quantità di indirizzi che un utente finale può includere nell'elenco dei mittenti approvati (questo limite viene calcolato in base alla lunghezza e al numero di indirizzi e-mail).

Corrispondenza con caratteri jolly

Per quanto riguarda gli elenchi di mittenti approvati e mittenti bloccati, Messaging Security Agent supporta la corrispondenza con caratteri jolly. Il carattere utilizzato è l'asterisco (*).

Messaging Security Agent non supporta la corrispondenza con caratteri jolly nella parte del nome utente. Tuttavia, se si digita un pattern come "*@trend.com", l'agent lo considera sempre come "@trend.com".

È possibile utilizzare un carattere jolly solo se è:

- Accanto a un solo punto e al primo o ultimo carattere di una stringa
- A sinistra di un simbolo @ e come primo carattere della stringa
- Qualsiasi sezione mancante all'inizio o alla fine di una stringa, che ha la stessa funzione di un carattere jolly

TABELLA 6-2. Indirizzi e-mail corrispondenti ai caratteri jolly

PATTERN	ESEMPI CORRISPONDENTI	ESEMPI NON CORRISPONDENTI
giovanni@esempio.com	giovanni@esempio.com	Qualsiasi indirizzo diverso dal modello
@esempio.com *@esempio.com	giovanni@esempio.com maria@esempio.com	giovanni@ms1.esempio.com giovanni@esempio.com.it maria@esempio.com.it
esempio.com	giovanni@esempio.com giovanni@ms1.esempio.com maria@ms1.rd.esempio.com maria@esempio.com	giovanni@esempio.com.it maria@mioesempio.com.it giorgio@esempio.comon
*.esempio.com	giovanni@ms1.esempio.com maria@ms1.rd.esempio.com giorgio@ms1.esempio.com	giovanni@esempio.com giovanni@mioesempio.com.it maria@ms1.esempio.comon
esempio.com.*	giovanni@esempio.com.it giovanni@ms1.esempio.com.it giovanni@ms1.rd.esempio.com.it maria@esempio.com.it	giovanni@esempio.com maria@ms1.esempio.com giovanni@mioesempio.com.it
.esempio.com.	giovanni@ms1.esempio.com.it giovanni@ms1.rd.esempio.com.it maria@ms1.esempio.com.it	giovanni@esempio.com giovanni@ms1.esempio.com giovanni@trend.esempio.it
..*.esempio.com *****.esempio.com	Corrisponde a "*.esempio.com"	

Pattern	Esempi corrispondenti	Esempi non corrispondenti
esempio.com esempio.com esempio.*.com @*.esempio.com	Modelli non validi	

Filtro dei contenuti

Il filtro dei contenuti esamina i messaggi e-mail in entrata e in uscita sulla base delle regole definite dall'utente. Ogni regola contiene un elenco di parole chiave e di frasi. Il filtro del contenuto prende in considerazione l'intestazione e/o il contenuto dei messaggi confrontando il messaggio con l'elenco di parole chiave. Quando il filtro del contenuto individua una parola che corrisponde a una parola chiave, può eseguire operazioni affinché il contenuto indesiderato non venga consegnato ai client Microsoft Exchange. Messaging Security Agent invia notifiche ogniqualvolta prende provvedimenti contro contenuti indesiderati.

Nota

Attenzione a non confondere Scansione dei contenuti (anti-spam basato su firme e regole euristiche) Filtro dei contenuti (scansione e blocco di messaggi e-mail sulla base di categorie di parole chiave). Vedere *Scansione dei contenuti a pagina 6-10*.

Il filtro dei contenuti consente all'amministratore di valutare e controllare la consegna dei messaggi e-mail sulla base del testo del messaggio stesso. Può essere utilizzato per monitorare i messaggi in entrata e in uscita e per controllare la presenza di contenuto molesto, offensivo o in qualche modo riprovevole. Il filtro dei contenuti fornisce inoltre una funzione di verifica dei sinonimi che consente di estendere la portata dei criteri adottati. Ad esempio, è possibile creare regole per il controllo degli aspetti riportati di seguito.

- Linguaggio contenente delle molestie di natura sessuale
- Linguaggio con contenuti razzisti
- Spam incorporato nel corpo di un messaggio e-mail

Nota

Per impostazione predefinita, il filtro del contenuto non è attivato.

Gestione delle regole del filtro dei contenuti

Le regole dei filtri dei contenuti del Messaging Security Agent sono visualizzate nella schermata **Filtro dei contenuti**. Accedere a questa schermata da:

- Per Scansione in tempo reale:

  Dispositivi > **{Messaging Security Agent}** > **Configura criterio** > **Filtro dei contenuti**

- Per la Scansione manuale:

  Scansioni > **Manuale** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

- Per la Scansione pianificata:

  Scansioni > **Pianificata** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

Procedura

1. In questa schermata sono visualizzate informazioni riassuntive riguardanti le regole, fra cui:

   - **Regola**: Worry-Free Business Security dispone di regole predefinite che filtrano i contenuti in base alle seguenti categorie: **volgarità**, **discriminazione razziale**, **discriminazione sessuale**, **truffe** e **catene di Sant'Antonio**. Le regole sono disattivate per impostazione

predefinita. È possibile modificare queste regole secondo specifici requisiti oppure eliminarle. Se nessuna di queste regole soddisfa i requisiti, l'utente può aggiungere le proprie.

- **Azione**: Messaging Security Agent esegue questa operazione quando rileva contenuti indesiderati.
- **Priorità**: Messaging Security Agent applica ogni filtro in sequenza in base all'ordine visualizzato in questa schermata.
- **Attivato**: un'icona verde indica una regola attiva, mentre un'icona rossa indica una regola disattivata.

2. Effettuare le operazioni riportate di seguito:

Operazione	Passaggi
Attivare/Disattivare le regole di filtro dei contenuti	Selezionare o annullare la selezione di **Attiva filtro dei contenuti in tempo reale** nella parte superiore della schermata.
Aggiungere una regola	Fare clic su **Aggiungi**. Si apre una nuova schermata dove è possibile scegliere il tipo di regola da aggiungere. Per dettagli, consultare *Tipi di regole di filtro dei contenuti a pagina 6-21*.

OPERAZIONE	PASSAGGI
Modificare una regola	a. Fare clic sul nome della regola. Viene visualizzata una nuova schermata. b. Le opzioni disponibili nella schermata dipendono dal tipo di regola. Per determinare il tipo di regola, controllare il percorso di navigazione nella parte superiore della schermata e osservare il secondo elemento nel percorso di navigazione. Ad esempio: Filtro dei contenuti > **Regola Soddisfa una qualsiasi condizione** > Modifica regola Per i dettagli sulle impostazioni di una regola modificabili, vedere uno dei seguenti argomenti: • *Aggiunta di una regola di filtro dei contenuti per le condizioni di associazione a pagina 6-25* • *Aggiunta di regole di filtro dei contenuti per tutte le condizioni di associazione a pagina 6-22* **Nota** Questo tipo di regola non è disponibile per le scansioni di filtraggio contenuti manuali e pianificate. • *Aggiunta di una regola di monitoraggio del filtro dei contenuti a pagina 6-28* • *Creazione di eccezioni alle regole per il filtro dei contenuti a pagina 6-31*

OPERAZIONE	PASSAGGI
Riordinare le regole	Il Messaging Security Agent applica le regole di filtro dei contenuti per i messaggi e-mail seguendo l'ordine della schermata **Filtro dei contenuti**. L'ordine con cui le regole vengono applicate viene configurato dall'utente. L'agent filtra tutti i messaggi e-mail in base alle regole finché una violazione non attiva un'operazione che interrompe la scansione (ad esempio Elimina o Metti in quarantena). È possibile modificare l'ordine delle regole per ottimizzare il filtro dei contenuti. a. Selezionare una casella di controllo che corrisponde alla regola di cui si vuole cambiare l'ordine. b. Fare clic su **Riordina**. Viene visualizzata una casella intorno al numero d'ordine della regola. c. Nella casella della colonna **Priorità**, eliminare il numero di ordine esistente e immetterne uno nuovo. **Nota** Accertarsi di immettere un numero non superiore al numero totale di regole nell'elenco. Se si immette un numero superiore rispetto al numero totale di regole, Worry-Free Business Security ignora l'immissione e non modifica l'ordine della regola. d. Fare clic su **Salva riordino**. La regola sposta il livello di priorità immesso e tutti gli altri numeri di ordine delle regole cambiano di conseguenza. Se si seleziona la regola numero 5 e la si cambia in regola numero 3, i numeri 1 e 2 rimangono invariati, mentre il numero 3 e i successivi aumentano di un'unità.
Attivare/Disattivare il monitoraggio	Fare clic sull'icona sotto alla colonna Attivato.

Operazione	Passaggi
Rimuovere regole	Quando si elimina una regola, Messaging Security Agent aggiorna l'ordine delle regole restanti per adattarsi alla modifica. **Nota** l'eliminazione di una regola è un processo irreversibile; spesso è preferibile semplicemente disattivarla. a. Selezionare una regola. b. Fare clic su **Rimuovi**.

3. Fare clic su **Salva**.

Tipi di regole di filtro dei contenuti

È possibile creare regole che filtrano i messaggi e-mail in base alle condizioni specificate o agli indirizzi e-mail del mittente o del destinatario. In una regola si possono specificare le seguenti condizioni: quali campi dell'intestazione analizzare, se esaminare o meno il corpo del messaggio e-mail e quali parole chiave cercare.

È possibile creare regole per eseguire le seguenti funzioni:

- **Filtra messaggi che soddisfano qualsiasi condizione definita**: Questo tipo di regola è in grado di filtrare il contenuto di qualsiasi messaggio durante una scansione. Per i dettagli, consultare *Aggiunta di una regola di filtro dei contenuti per le condizioni di associazione a pagina 6-25*.
- **Filtrare i messaggi che soddisfano tutte le condizioni definite**: Questo tipo di regola è in grado di filtrare il contenuto di qualsiasi messaggio durante una scansione. Per i dettagli, consultare *Aggiunta di regole di filtro dei contenuti per tutte le condizioni di associazione a pagina 6-22*.

Nota

Questo tipo di regola non è disponibile per le scansioni di filtraggio contenuti manuali e pianificate.

- **Monitora il contenuto dei messaggi di particolari account e-mail**: Questo tipo di regola monitora il contenuto dei messaggi di particolari account e-mail. Le regole di monitoraggio sono simili a una regola generale di filtro dei contenuti, solo che filtrano il contenuto proveniente soltanto da determinati account e-mail. Per i dettagli, consultare *Aggiunta di una regola di monitoraggio del filtro dei contenuti a pagina 6-28*.
- **Crea eccezioni per particolari account e-mail**: Questo tipo di regola crea un'eccezione per determinati account e-mail. Se viene creata un'eccezione per un account, l'account non viene sottoposto al filtraggio per l'individuazione di violazioni delle regole dei contenuti. Per i dettagli, consultare *Creazione di eccezioni alle regole per il filtro dei contenuti a pagina 6-31*.

Dopo avere creato la regola, Messaging Security Agent inizia a filtrare tutti i messaggi in entrata e in uscita in base alla regola. Quando si verifica una violazione dei contenuti, Messaging Security Agent prende provvedimenti contro tale violazione. L'Azione eseguita da Security Server dipende anche dalle impostazioni della regola.

Aggiunta di regole di filtro dei contenuti per tutte le condizioni di associazione

Questo tipo di regola non è disponibile per le scansioni di filtraggio contenuti manuali e pianificate.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Filtro dei contenuti**.

   Viene visualizzata una nuova schermata.

5. Fare clic su **Aggiungi**.

   Viene visualizzata una nuova schermata.

6. Selezionare **Filtra messaggi che soddisfano tutte le condizioni definite**.

7. Fare clic su **Avanti**.

8. Immettere il nome della regola nel campo **Nome regola**.

9. Selezionare la parte del messaggio che si desidera analizzare per individuare i contenuti indesiderati. Messaging Security Agent è in grado di filtrare i messaggi e-mail per:

   - Intestazione (Da, A e CC)
   - Oggetto
   - Dimensione del corpo o dell'allegato del messaggio
   - Nome file allegato

   Nota

   Durante la scansione in tempo reale, Messaging Security Agent supporta solo il filtro dei contenuti dell'intestazione e dell'oggetto.

10. Fare clic su **Avanti**.

11. Selezionare un'operazione da eseguire quando Messaging Security Agent rileva contenuti indesiderati. Il Messaging Security Agent è in grado di eseguire le operazioni descritte di seguito (per le descrizioni vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*):

    - Sostituisci con testo/file

      Nota

      Non è possibile sostituire il testo nei campi Da, A, Cc o Oggetto.

    - Metti in quarantena intero messaggio

- Parte del messaggio in quarantena
- Elimina intero messaggio
- Archivia
- Ignora intero messaggio

12. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che comunichi ai destinatari dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

13. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che comunichi ai mittenti dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

14. Nella sezione **Opzioni avanzate**, fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazione archivio**.

    a. Nel campo **Directory di quarantena**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail in quarantena oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\quarantine`

    b. Nel campo **Directory di archiviazione**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail archiviate oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\backup per filtro dei contenuti`

15. Fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazioni di sostituzione**.

a. Nel campo **Nome del file sostitutivo**, immettere il nome del file con il quale Filtro dei contenuti sostituirà un messaggio e-mail quando viene attivata una regola che utilizza l'operazione "Sostituisci con testo/file" oppure accettare il valore predefinito.

b. Nel campo **Testo sostitutivo**, digitare o incollare il contenuto del testo sostitutivo che Filtro dei contenuti dovrà utilizzare quando un messaggio e-mail attiva una regola la cui operazione sia "Sostituisci con testo/file" oppure accettare il testo predefinito.

16. Fare clic sul pulsante **Fine**.

    La procedura guidata viene chiusa e viene visualizzata la schermata Filtro dei contenuti.

Aggiunta di una regola di filtro dei contenuti per le condizioni di associazione

- Per Scansione in tempo reale:

  Dispositivi > **{Messaging Security Agent}** > **Configura criterio** > **Filtro dei contenuti**

- Per la Scansione manuale:

  Scansioni > **Manuale** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

- Per la Scansione pianificata:

  Scansioni > **Pianificata** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

Procedura

1. Fare clic su **Aggiungi**.

   Viene visualizzata una nuova schermata.

2. Selezionare **Filtrare messaggi che soddisfano qualsiasi condizione definita**.
3. Fare clic su **Avanti**.
4. Immettere il nome della regola nel campo **Nome regola**.
5. Selezionare la parte del messaggio che si desidera analizzare per individuare i contenuti indesiderati. Messaging Security Agent è in grado di filtrare i messaggi e-mail per:
   - Intestazione (Da, A e CC)
   - Oggetto
   - Corpo
   - Allegato

   Nota

   Durante la scansione in tempo reale, Messaging Security Agent supporta solo il filtro dei contenuti dell'intestazione e dell'oggetto.
6. Fare clic su **Avanti**.
7. Aggiungere le parole chiave per la parte di destinazione da filtrare per individuare contenuti indesiderati. Per informazioni dettagliate sull'uso delle parole chiave, fare riferimento a *Parole chiave a pagina D-5*.
   a. Se necessario, selezionare se attivare o meno la distinzione tra maiuscole e minuscole per i contenuti.
   b. Importare i nuovi file di parole chiave da un file `.txt` a seconda delle esigenze.
   c. Definire un elenco dei sinonimi.
8. Fare clic su **Avanti**.
9. Selezionare un'operazione da eseguire quando Messaging Security Agent rileva contenuti indesiderati. Il Messaging Security Agent è in grado di eseguire le operazioni descritte di seguito (per le descrizioni vedere

Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18):

- Sostituisci con testo/file

  Nota

  Non è possibile sostituire il testo nei campi Da, A, Cc o Oggetto.

- Metti in quarantena intero messaggio
- Parte del messaggio in quarantena
- Elimina intero messaggio
- Archivia

10. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che comunichi ai destinatari dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

11. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che comunichi ai mittenti dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

12. Nella sezione **Opzioni avanzate**, fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazione archivio**.

    a. Nel campo **Directory di quarantena**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail in quarantena oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\quarantine`

b. Nel campo **Directory di archiviazione**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail archiviate oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\backup per filtro dei contenuti`

13. Fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazioni di sostituzione**.

    a. Nel campo **Nome del file sostitutivo**, immettere il nome del file con il quale Filtro dei contenuti sostituirà un messaggio e-mail quando viene attivata una regola che utilizza l'operazione "Sostituisci con testo/file" oppure accettare il valore predefinito.

    b. Nel campo **Testo sostitutivo**, digitare o incollare il contenuto del testo sostitutivo che Filtro dei contenuti dovrà utilizzare quando un messaggio e-mail attiva una regola la cui operazione sia "Sostituisci con testo/file" oppure accettare il testo predefinito.

14. Fare clic sul pulsante **Fine**.

    La procedura guidata viene chiusa e viene visualizzata la schermata Filtro dei contenuti.

Aggiunta di una regola di monitoraggio del filtro dei contenuti

- Per Scansione in tempo reale:

  Dispositivi > **{Messaging Security Agent}** > **Configura criterio** > **Filtro dei contenuti**

- Per la Scansione manuale:

  Scansioni > **Manuale** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

- Per la Scansione pianificata:

  Scansioni > **Pianificata** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

Procedura

1. Fare clic su **Aggiungi**.

   Viene visualizzata una nuova schermata.

2. Selezionare **Monitora il contenuto dei messaggi di particolari account e-mail**.

3. Fare clic su **Avanti**.

4. Immettere il nome della regola nel campo **Nome regola**.

5. Impostare gli account e-mail da monitorare.

6. Fare clic su **Avanti**.

7. Selezionare la parte del messaggio che si desidera analizzare per individuare i contenuti indesiderati. Messaging Security Agent è in grado di filtrare i messaggi e-mail per:

   - Oggetto
   - Corpo
   - Allegato

   Nota

   Durante la scansione in tempo reale, Messaging Security Agent supporta solo il filtro di queste parti del messaggio e-mail. Durante le scansioni manuali e pianificate, non supporta il filtro del contenuto dell'intestazione e dell'oggetto.

8. Aggiungere le parole chiave per la parte di destinazione da filtrare per individuare contenuti indesiderati. Per informazioni dettagliate sull'uso delle parole chiave, fare riferimento a *Parole chiave a pagina D-5*.

   a. Se necessario, selezionare se attivare o meno la distinzione tra maiuscole e minuscole per i contenuti.

   b. Importare i nuovi file di parole chiave da un file `.txt` a seconda delle esigenze.

c. Definire un elenco dei sinonimi.

9. Fare clic su **Avanti**.

10. Selezionare un'operazione da eseguire quando Messaging Security Agent rileva contenuti indesiderati. Il Messaging Security Agent è in grado di eseguire le operazioni descritte di seguito (per le descrizioni vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*):

    - Sostituisci con testo/file

      Nota

      Non è possibile sostituire il testo nei campi Da, A, Cc o Oggetto.

    - Metti in quarantena intero messaggio
    - Parte del messaggio in quarantena
    - Elimina intero messaggio
    - Archivia

11. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che comunichi ai destinatari dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

12. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che comunichi ai mittenti dei messaggi e-mail che i contenuti sono stati filtrati.

    Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

13. Nella sezione **Opzioni avanzate**, fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazione archivio**.

a. Nel campo **Directory di quarantena**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail in quarantena oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\quarantine`

b. Nel campo **Directory di archiviazione**, immettere il percorso della cartella Filtro dei contenuti in cui inserire le e-mail archiviate oppure accettare il valore predefinito: `<Cartella di installazione di Messaging Security Agent>\storage\backup per filtro dei contenuti`

14. Fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazioni di sostituzione**.

a. Nel campo **Nome del file sostitutivo**, immettere il nome del file con il quale Filtro dei contenuti sostituirà un messaggio e-mail quando viene attivata una regola che utilizza l'operazione "Sostituisci con testo/file" oppure accettare il valore predefinito.

b. Nel campo **Testo sostitutivo**, digitare o incollare il contenuto del testo sostitutivo che Filtro dei contenuti dovrà utilizzare quando un messaggio e-mail attiva una regola la cui operazione sia "Sostituisci con testo/file" oppure accettare il testo predefinito.

15. Fare clic sul pulsante **Fine**.

La procedura guidata viene chiusa e viene visualizzata la schermata Filtro dei contenuti.

Creazione di eccezioni alle regole per il filtro dei contenuti

- Per Scansione in tempo reale:

  Dispositivi > **{Messaging Security Agent}** > **Configura criterio** > **Filtro dei contenuti**

- Per la Scansione manuale:

Scansioni > **Manuale** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

- Per la Scansione pianificata:

  Scansioni > **Pianificata** > **{Espandere Messaging Security Agent}** > **Filtro dei contenuti**

Procedura

1. Fare clic su **Aggiungi**.

   Viene visualizzata una nuova schermata.

2. Selezionare **Creare eccezioni per particolari account e-mail**.

3. Fare clic su **Avanti**.

4. Immettere il nome della regola.

5. Immettere nell'apposito spazio gli account e-mail da escludere dal filtro dei contenuti e fare clic su **Aggiungi**.

   L'account e-mail viene aggiunto all'elenco degli account e-mail esenti. Messaging Security Agent non applica agli account e-mail di questo elenco le regole dei contenuti con una priorità inferiore a quella di questa regola.

6. Una volta soddisfatti dell'elenco degli account e-mail, fare clic su **Fine**.

   La procedura guidata viene chiusa e compare la schermata **Filtro dei contenuti**.

Prevenzione della perdita di dati

Utilizzare Prevenzione della perdita di dati per evitare la perdita di dati dalla posta in uscita. Questa funzione è in grado di proteggere dati quali il codice fiscale, i numeri di telefono, i numeri di conto corrente bancario e altre informazioni aziendali riservate che corrispondono a un determinato pattern.

In questa versione sono supportate le seguenti versioni di Microsoft Exchange:

TABELLA 6-3. Versioni di Microsoft Exchange supportate

SUPPORTATA	NON SUPPORTATA
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

Lavoro di preparazione

Prima di effettuare il monitoraggio dei dati sensibili per evitare potenziali perdite, determinare quanto segue:

- I dati che necessitano di protezione da utenti non autorizzati
- Ubicazione dei dati
- Dove e come i dati vengono trasmessi
- Gli utenti autorizzati ad accedere o a trasmettere queste informazioni

Questo importante controllo richiede immissioni da parte di molteplici reparti e personale in grado di utilizzare correttamente le informazioni sensibili nell'organizzazione. Nelle procedure seguenti si suppone che siano state identificate le informazioni sensibili e che siano stati impostati criteri di sicurezza relativi alla gestione delle informazioni aziendali riservate.

La funzione Prevenzione della perdita di dati comprende tre parti base:

- **Regole** (pattern da ricercare)
- **Domini da escludere** dai filtri
- **Mittenti approvati** (account e-mail da escludere dal filtro)

Per i dettagli, consultare *Gestione delle regole per Prevenzione della perdita di dati a pagina 6-34*.

Gestione delle regole per Prevenzione della perdita di dati

Messaging Security Agent visualizza tutte le regole di Prevenzione della perdita di dati nella schermata **Prevenzione della perdita di dati** (**Dispositivi** > **{Messaging Security Agent}** > **Configura criterio** > **Prevenzione della perdita di dati**).

Procedura

1. In questa schermata sono visualizzate informazioni riassuntive riguardanti le regole, fra cui:

   - **Regola**: Worry-Free Business Security dispone di regole predefinite (vedere *Regole per la Prevenzione della perdita di dati predefinite a pagina 6-41*). Le regole sono disattivate per impostazione predefinita. È possibile modificare queste regole secondo specifici requisiti oppure eliminarle. Se nessuna di queste regole soddisfa i requisiti, l'utente può aggiungere le proprie.

     Suggerimento

     Per visualizzare la regola, passare con il mouse sopra il nome corrispondente. Le regole che utilizzano un'espressione regolare sono contrassegnate con una lente di ingrandimento (

).

   - **Azione**: Messaging Security Agent esegue questa operazione quando viene attivata una regola.
   - **Priorità**: Messaging Security Agent applica ogni regola in sequenza in base all'ordine visualizzato in questa schermata.
   - **Attivato**: un'icona verde indica una regola attiva, mentre un'icona rossa indica una regola disattivata.

2. Effettuare le operazioni riportate di seguito:

OPERAZIONE	PASSAGGI
Attiva/Disattiva la Prevenzione per la perdita di dati	Selezionare o annullare la selezione di **Attiva la prevenzione per la perdita di dati in tempo reale** nella parte superiore della schermata.
Aggiungere una regola	Fare clic su **Aggiungi**. Si apre una nuova schermata dove è possibile scegliere il tipo di regola da aggiungere. Per dettagli, consultare *Aggiunta delle regole per Prevenzione della perdita di dati a pagina 6-42*.
Modificare una regola	Fare clic sul nome della regola. Viene visualizzata una nuova schermata. Per i dettagli sulle impostazioni di una regola modificabili, vedere *Aggiunta delle regole per Prevenzione della perdita di dati a pagina 6-42*.

Importazione ed esportazione delle regole	Importare una o più regole da (o esportarle in) un file di testo normale, come descritto di seguito. Se si preferisce, è possibile modificare le regole direttamente utilizzando questo file.
	
	`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`
	
	`RuleName=Bubbly`
	
	`UserExample=`
	
	`Value=Bubbly`
	
	`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`
	
	`RuleName=Master Card No.`
	
	`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b`

OPERAZIONE	PASSAGGI
	Per esportare regole in un file di testo normale, selezionare una o più regole nell'elenco, quindi fare clic su **Esporta**. **Suggerimento** È possibile selezionare le regole che appaiono solo su una schermata. Per selezionare le regole attualmente visualizzate in schermate diverse, aumentare il valore Righe per pagina sulla parte superiore della tabella dell'elenco Regola, per visualizzare un numero di righe sufficiente per comprendere tutte le regole da esportare.
	Per importare le regole: a. Creare un file di testo normale nel formato mostrato sopra. Inoltre, è possibile fare clic su **Scarica più regole predefinite** sotto alla tabella, quindi salvare le regole. b. Fare clic su **Importa**. Compare una nuova finestra. c. Fare clic su **Sfoglia** per individuare il file da importare, quindi scegliere **Importa**. Prevenzione della perdita di dati importa le regole e le accoda alla fine dell'elenco di regole corrente. **Suggerimento** Se vi sono più di 10 regole, le regole importate non saranno visibili nella prima pagina. Utilizzare le icone di navigazione nella pagina sulla parte superiore e inferiore dell'elenco di regole per visualizzare l'ultima pagina dell'elenco. Le nuove regole importate appaiono in questo punto.

OPERAZIONE	PASSAGGI
Riordinare le regole	Il Messaging Security Agent applica le regole di Prevenzione della perdita di dati ai i messaggi e-mail seguendo l'ordine della schermata **Prevenzione della perdita di dati**. L'ordine con cui le regole vengono applicate viene configurato dall'utente. L'agent filtra tutti i messaggi e-mail in base alle regole finché una violazione non attiva un'operazione che interrompe la scansione (ad esempio Elimina o Metti in quarantena). Modificare l'ordine di queste regole per ottimizzare la Prevenzione della perdita di dati. a. Selezionare una casella di controllo che corrisponde alla regola di cui si vuole cambiare l'ordine. b. Fare clic su **Riordina**. Viene visualizzata una casella intorno al numero d'ordine della regola. c. Nella casella della colonna **Priorità**, eliminare il numero di ordine esistente e immetterne uno nuovo. **Nota** Accertarsi di immettere un numero non superiore al numero totale di regole nell'elenco. Se si immette un numero superiore rispetto al numero totale di regole, Worry-Free Business Security ignora l'immissione e non modifica l'ordine della regola. d. Fare clic su **Salva riordino**. La regola sposta il livello di priorità immesso e tutti gli altri numeri di ordine delle regole cambiano di conseguenza. Se si seleziona la regola numero 5 e la si cambia in regola numero 3, i numeri 1 e 2 rimangono invariati, mentre il numero 3 e i successivi aumentano di un'unità.
Attivare/Disattivare il monitoraggio	Fare clic sull'icona sotto alla colonna Attivato.

OPERAZIONE	PASSAGGI
Rimuovere regole	Quando si elimina una regola, Messaging Security Agent aggiorna l'ordine delle regole restanti per adattarsi alla modifica. **Nota** l'eliminazione di una regola è un processo irreversibile; spesso è preferibile semplicemente disattivarla. a. Selezionare una regola. b. Fare clic su **Rimuovi**.

OPERAZIONE	PASSAGGI
Esclusione di account di dominio specifici	All'interno di un'azienda, lo scambio di informazioni riservate è una necessità quotidiana. Inoltre, il carico di elaborazione sui Security Server sarebbe estremo se Prevenzione della perdita di dati dovesse filtrare tutti i messaggi interni. Per questi motivi, è necessario impostare uno o più domini predefiniti, rappresentanti il traffico di posta interno dell'azienda, in modo che Prevenzione della perdita di dati non filtri i messaggi inviati da un account e-mail all'altro all'interno del dominio dell'azienda. Questo elenco consente a tutti i messaggi e-mail interni (nell'ambito del dominio di un'azienda) di bypassare le regole per la prevenzione della perdita di dati. È necessario almeno uno di questi domini. Se si utilizzano più domini, aggiungerli a questo elenco. Ad esempio: `*@esempio.com` a. Fare clic sull'icona più (+) per espandere la sezione **Specificare account di domini specifici esclusi dalla Prevenzione della perdita di dati**. b. Posizionare il cursore nel campo **Aggiungi** e immettere il dominio, utilizzando il seguente pattern: `*@esempio.com` c. Fare clic su **Aggiungi**. Il dominio appare nell'elenco mostrato al di sotto del campo **Aggiungi**. d. Fare clic su **Salva** per completare il processo. **AVVERTENZA!** Prevenzione della perdita di dati non effettua l'aggiunta del dominio fino a quando non si seleziona **Salva**. Selezionando **Aggiungi**, ma non **Salva**, il dominio non viene aggiunto.

OPERAZIONE	PASSAGGI
Aggiunta di account e-mail all'elenco Mittenti approvati	La posta proveniente dai mittenti approvati viaggia al di fuori della rete, senza alcuni filtro di Prevenzione della perdita di dati. Prevenzione della perdita di dati ignora il contenuto delle e-mail inviare da account e-mail nell'elenco approvati. a. Fare clic sull'icona del segno (+) per espandere la sezione **Mittenti approvati**. b. Posizionare il cursore nel campo **Aggiungi** e immettere l'indirizzo e-mail completo, utilizzando il seguente pattern: `esempio@esempio.com` c. Fare clic su **Aggiungi**. L'indirizzo appare nell'elenco mostrato al di sotto del campo **Aggiungi**. d. Fare clic su **Salva** per completare il processo. **Nota** Prevenzione della perdita di dati non effettua l'aggiunta dell'indirizzo fino a quando non si seleziona **Salva**. Selezionando **Aggiungi**, ma non **Salva**, l'indirizzo non viene aggiunto.

Operazione	Passaggi

Importazione di account e-mail nell'elenco Mittenti approvati	È possibile importare un elenco di indirizzi e-mail da un file di testo normale formattato con un account e-mail per riga, ad esempio:
	`admin@esempio.com`
	`ceo@esempio.com`
	`president@esempio.com`
	a. Fare clic sull'icona del segno (+) per espandere la sezione **Mittenti approvati**.
	b. Fare clic su **Importa**.
	Compare una nuova finestra.
	c. Fare clic su **Sfoglia** per individuare il file di testo normale da importare, quindi scegliere **Importa**.
	Prevenzione della perdita di dati importa le regole e le accoda alla fine dell'elenco corrente.

3. Fare clic su **Salva**.

Regole per la Prevenzione della perdita di dati predefinite

In Prevenzione della perdita di dati sono incluse alcune regole predefinite, come illustrato nella seguente tabella.

Tabella 6-4. Regole per la Prevenzione della perdita di dati predefinite

Nome regola	Esempio	Espressione regolare
Numero di account Visa	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
Numero di account MasterCard	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b

Nome regola	Esempio	Espressione regolare
Numero di account American Express	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Numero di account Diners Club/Carte Blanche	3111-111111-1111	.REG. [^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w](([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
Data ISO	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

Nota

Dalla console Web, è possibile scaricare un file zip contenente più regole DLP. Portarsi in **Impostazioni di sicurezza** > **{Messaging Security Agent}** > **Configura impostazioni** > **Prevenzione della perdita di dati** e fare clic **Scarica più regole predefinite**.

Aggiunta delle regole per Prevenzione della perdita di dati

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Prevenzione della perdita di dati**.

   Viene visualizzata una nuova schermata.

5. Fare clic su **Aggiungi**.

   Viene visualizzata una nuova schermata.

6. Selezionare la parte di messaggio da valutare. Messaging Security Agent è in grado di filtrare i messaggi e-mail per:

   - Intestazione (Da, A e CC)
   - Oggetto
   - Corpo
   - Allegato

7. Aggiungere una regola.

   Per aggiungere una regola in base a una parola chiave:

   a. Selezionare **Parola chiave**.

   b. Digitare la parola chiave nel campo visualizzato. La parola chiave deve essere composta da 1 a 64 caratteri alfanumerici.

   c. Fare clic su **Avanti**.

   Per aggiungere una regola in base a espressioni generate automaticamente:

   a. Per istruzioni su come definire le espressioni regolari, vedere *Espressioni regolari a pagina D-10*.

   b. Selezionare **Espressione regolare (generata automaticamente)**.

   c. Nel campo visualizzato, immettere un **Nome regola**. Il campo è obbligatorio.

   d. Nel campo **Esempio**, digitare o incollare un esempio del tipo di stringa (fino a 40 caratteri) a cui deve corrispondere l'espressione regolare. I caratteri alfanumerici sono visualizzati tutti in maiuscolo

nell'area in ombra con le righe delle caselle al di sotto del campo **Esempio**.

e. Se sono contenute delle costanti in un'espressione, selezionarle facendo clic sulle caselle in cui sono visualizzati i caratteri.

   Quando si fa clic su ciascuna casella, i rispettivi bordi diventano rossi per indicare che si tratta di una costante e lo strumento di generazione automatica modifica l'espressione regolare mostrata al di sotto dell'area in ombra.

   Nota

   I caratteri non alfanumerici (ad esempio, spazi, punti e virgola e altri segni di punteggiatura) sono automaticamente considerati costanti e non possono essere trasformati in variabili.

f. Per verificare che l'espressione regolare generata corrisponda al pattern desiderato, selezionare **Specificare un altro esempio per verificare la regola (facoltativo)**.

   Viene visualizzato un campo di prova al di sotto di questa opzione.

g. Digitare un altro esempio del pattern appena immesso.

   Ad esempio, se questa espressione corrisponde a una serie di numeri di account del pattern “01-EX????? 20??”, digitare un altro esempio che corrisponda, come "01-Extreme 2010" e fare clic su **Test**.

   Lo strumento convalida il nuovo esempio rispetto all'espressione regolare esistente e inserisce un segno di spunta verde accanto al campo, nel caso in cui il nuovo esempio corrisponda. Se l'espressione regolare non corrisponde al nuovo esempio, accanto al campo viene visualizzata un'icona di X rossa.

AVVERTENZA!

Le espressioni regolari generate da questo strumento sono indipendenti dall'uso di maiuscole e minuscole. Queste espressioni possono corrispondere solo ai pattern con lo stesso numero di caratteri dell'esempio. Non sono in grado di valutare un pattern di uno o più caratteri determinati.

h. Fare clic su **Avanti**.

Per aggiungere una regola in base a espressioni definite dall'utente:

AVVERTENZA!

Le espressioni regolari sono un potente strumento di ricerca delle stringhe. Accertarsi di conoscere l'utilizzo della sintassi delle espressioni regolari, prima di utilizzare queste espressioni. La scrittura non corretta delle espressioni regolari può avere un impatto significativo sulle prestazioni. Trend Micro consiglia di cominciare con l'utilizzo delle espressioni regolari semplici. Quando si creano nuove regole, utilizzare l'operazione di archiviazione e osservare il modo in cui Prevenzione della perdita di dati gestisce i messaggi utilizzando la regola. Quando si è certi che la regola non ha conseguenze impreviste, è il momento di modificare l'azione.

a. Per istruzioni su come definire le espressioni regolari, vedere *Espressioni regolari a pagina D-10*.

b. Selezionare **Espressione regolare (definita dall'utente)**.

   Vengono visualizzati i campi **Nome regola** ed **Espressione regolare**.

c. Nel campo visualizzato, immettere un **Nome regola**. Il campo è obbligatorio.

d. Nel campo **Espressione regolare**, immettere un'espressione regolare che inizia con il prefisso `.REG.`, costituita da un massimo di 255 caratteri, incluso il prefisso.

AVVERTENZA!

Prestare estrema attenzione quando si incolla in questo campo. Se negli appunti vengono inclusi caratteri estranei, come uno specifico avanzamento di riga del sistema operativo o un tag HTML, l'espressione incollata risulterà inaccurata. Per questo motivo, Trend Micro consiglia di digitare manualmente le espressioni.

e. Per verificare che l'espressione regolare corrisponda al pattern desiderato, selezionare **Specificare un altro esempio per verificare la regola (facoltativo)**.

Viene visualizzato un campo di prova al di sotto di questa opzione.

f. Digitare un altro esempio del pattern appena immesso (massimo 40 caratteri).

Ad esempio, se l'espressione deve corrispondere a una serie di numeri di account del pattern "ACC-????? 20??" digitare un altro esempio che corrisponda, del tipo "Acc-65432 2012" e fare clic su **Test**.

Lo strumento convalida il nuovo esempio rispetto all'espressione regolare esistente e inserisce un segno di spunta verde accanto al campo, nel caso in cui il nuovo esempio corrisponda. Se l'espressione regolare non corrisponde al nuovo esempio, accanto al campo viene visualizzata un'icona di X rossa.

g. Fare clic su **Avanti**.

8. Selezionare un'azione che il Messaging Security Agent deve compiere quando viene attivata una regola (per le descrizioni, vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*):

- Sostituisci con testo/file

Nota

Non è possibile sostituire il testo nei campi Da, A, Cc o Oggetto.

- Metti in quarantena intero messaggio

- Parte del messaggio in quarantena
- Elimina intero messaggio
- Archivia
- Ignora intero messaggio

9. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che avvisi i destinatari interessati in caso di Prevenzione della perdita di dati a fronte di uno specifico messaggio di e-mail.

   Per diversi motivi, è possibile evitare di notificare ai destinatari di e-mail il blocco di un messaggio contenente informazioni sensibili. Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

10. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che avvisi i mittenti interessati in caso di Prevenzione della perdita di dati a fronte di uno specifico messaggio di e-mail.

    Per diversi motivi, è possibile evitare di notificare ai mittenti di e-mail il blocco di un messaggio contenente informazioni sensibili. Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

11. Nella sezione **Opzioni avanzate**, fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazione archivio**.

    a. Nel campo **Directory di quarantena**, immettere il percorso della cartella Prevenzione della perdita di dati in cui inserire i messaggi e-mail in quarantena oppure accettare il valore predefinito:
    `<Cartella di installazione di Messaging Security Agent>\storage\quarantine`

    b. Nel campo **Directory di archiviazione**, immettere il percorso della cartella Prevenzione della perdita di dati in cui inserire i messaggi e-mail in quarantena oppure accettare il valore predefinito:
    `<Cartella di installazione di Messaging Security Agent>\storage\backup per filtro dei contenuti`

12. Fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazioni di sostituzione**.

    a. Nel campo **Nome del file sostitutivo**, immettere il nome del file con il quale Prevenzione della perdita di dati sostituirà un messaggio e-mail quando viene attivata una regola che utilizza l'operazione "Sostituisci con testo/file" oppure accettare il valore predefinito.

    b. Nel campo **Testo sostitutivo**, digitare o incollare il contenuto del testo sostitutivo che Prevenzione della perdita di dati dovrà utilizzare quando un messaggio e-mail attiva una regola la cui operazione sia Sostituisci con testo/file oppure accettare il testo predefinito.

13. Fare clic sul pulsante **Fine**.

    La procedura guidata viene chiusa e viene visualizzata nuovamente la schermata Prevenzione della perdita di dati.

Blocco allegati

Il Blocco allegati impedisce che gli allegati presenti nei messaggi e-mail vengano consegnati all'archivio di informazioni di Microsoft Exchange. Configurare Messaging Security Agent in modo da bloccare gli allegati a seconda del tipo di allegato o del nome di allegato e quindi sostituire, mettere in quarantena o eliminare tutti i messaggi contenenti allegati corrispondenti ai criteri.

Il blocco può verificarsi durante una scansione in tempo reale, manuale e pianificata, ma le operazioni di eliminazione e messa in quarantena non sono disponibili durante le scansioni manuali e pianificate.

L'estensione di un allegato identifica il tipo di file, ad esempio `.txt`, `.exe` o `.dll`. Tuttavia, Messaging Security Agent esamina l'intestazione del file piuttosto che il nome per accertarsi del tipo di file effettivo. Spesso virus/minacce informatiche sono associati a determinati tipi di file. Configurando Messaging Security Agent affinché blocchi i file in base al tipo, è possibile

ridurre il rischio per la sicurezza dei server Microsoft Exchange. In maniera analoga, attacchi specifici sono spesso associati a un determinato nome file.

Suggerimento

Il blocco è un metodo efficace per controllare il diffondersi delle infezioni virali. È possibile mettere temporaneamente in quarantena tutti i tipi di file ad alto rischio o quelli il cui nome è associato a virus/minacce informatiche noti. In seguito, quando si è disponibili, esaminare con calma la cartella di quarantena e intervenire contro i file infetti.

Configurazione del blocco degli allegati

La configurazione delle opzioni di blocco degli allegati per i server Microsoft Exchange prevede l'impostazione delle regole per bloccare i messaggi che contengono determinati allegati.

- Per Scansione in tempo reale:

  Dispositivi > **{Messaging Security Agent}** > **Configura criterio** > **Blocco allegati**

- Per la Scansione manuale:

  Scansioni > **Manuale** > **{Espandere Messaging Security Agent}** > **Blocco allegati**

- Per la Scansione pianificata:

  Scansioni > **Pianificata** > **{Espandere Messaging Security Agent}** > **Blocco allegati**

Procedura

1. Dalla scheda **Destinazione**, aggiornare i seguenti campi secondo le esigenze:

   - **Tutti gli allegati**: L'agente consente di bloccare tutti i messaggi e-mail che contengono allegati. Tuttavia, questo tipo di scansione

richiede una notevole elaborazione. Perfezionare questo tipo di scansione selezionando i tipi di allegati o i nomi da escludere.

- **Tipi di allegati da escludere**
- **Nomi di allegati da escludere**

- **Allegati specificati**: quando si seleziona questo tipo di scansione, l'agente esegue soltanto la scansione dei messaggi e-mail contenenti gli allegati identificati. Questo tipo di scansione può essere molto esclusiva ed è l'ideale per rilevare messaggi e-mail contenenti allegati sospetti che potrebbero contenere minacce. L'esecuzione di questa scansione è molto rapida quando si specifica una quantità relativamente ridotta di nomi o tipi di allegati.
  - **Tipi di allegati**: l'agente esamina l'intestazione del file anziché il nome per determinare con certezza il tipo di file effettivo.
  - **Nomi degli allegati**: per impostazione predefinita, l'agente esamina l'intestazione del file anziché il nome per determinare con certezza il tipo di file effettivo. Quando si imposta Blocco allegati per sottoporre a scansione nomi specifici, l'agent rileva i tipi di allegato in base al loro nome.
- **Blocca tipi o nomi di allegati all'interno di file .ZIP**

2. Fare clic sulla scheda **Operazione** per impostare le operazioni che il Messaging Security Agent deve eseguire quando rileva allegati. Il Messaging Security Agent è in grado di eseguire le operazioni descritte di seguito (per le descrizioni vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*):
   - Sostituisci con testo/file
   - Metti in quarantena intero messaggio
   - Parte del messaggio in quarantena
   - Elimina intero messaggio
3. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che comunichi con i destinatari dei messaggi e-mail con allegati.

Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

4. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che comunichi con i mittenti dei messaggi e-mail con allegati.

   Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

5. Fare clic sull'icona del segno (+) per espandere la sottosezione **Impostazioni di sostituzione**.

   a. Nel campo **Nome del file sostitutivo**, immettere il nome del file con il quale Blocco allegati sostituirà un messaggio e-mail quando viene attivata una regola che utilizza l'operazione "Sostituisci con testo/file" oppure accettare il valore predefinito.

   b. Nel campo **Testo sostitutivo**, digitare o incollare il contenuto del testo sostitutivo che Blocco allegati dovrà utilizzare quando un messaggio e-mail attiva una regola la cui operazione sia "Sostituisci con testo/file" oppure accettare il testo predefinito.

6. Fare clic su **Salva**.

Reputazione Web

Reputazione Web contribuisce a impedire l'accesso a URL sul Web o incorporati in messaggi e-mail che comportano rischi di sicurezza. Reputazione Web controlla la reputazione dell'URL rispetto ai server di reputazione Web Trend Micro e quindi correla la reputazione con gli specifici criteri di reputazione Web attuati sul client. In base ai criteri in uso:

- Il Security Agent blocca o consente l'accesso al sito Web.

- Il Messaging Security Agent (solo Advanced) mette in quarantena, elimina o contrassegna il messaggio e-mail che contiene l'URL dannoso oppure ne consente l'invio se gli URL sono sicuri.

Reputazione Web invia una notifica e-mail all'amministratore e una notifica online all'utente riguardante i rilevamenti.

Configurare un livello di sicurezza diverso per i Security Agent in base alla posizione del client (In ufficio/Fuori ufficio).

Se la reputazione Web blocca un URL che invece è ritenuto sicuro, è possibile aggiungere l'URL all'elenco degli URL approvati.

Suggerimento

Per risparmiare ampiezza di banda della rete, Trend Micro consiglia di aggiungere i siti Web aziendali interni all'elenco degli URL approvati da reputazione Web.

Punteggio di reputazione

Il punteggio di reputazione di un URL indica se è presente una minaccia Web o meno. Trend Micro calcola il punteggio utilizzando delle tecniche di misurazione esclusive.

Trend Micro considera un URL una minaccia Web se il suo punteggio rientra in una soglia definita e sicuro se il punteggio supera tale soglia.

Nei Security Agent esistono tre livelli di protezione che determinano se l'accesso a un URL va consentito o bloccato.

- **Alto**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce
  - **Altamente sospetto**: Si sospetta la natura fraudolenta della pagina o si tratta di una possibile origine di minacce
  - **Sospetto**: Associate a spam o probabilmente compromesse

- **Non testato**: Anche se Trend Micro verifica attivamente le pagine Web per garantire la sicurezza, gli utenti possono trovare pagine non verificate quando visitano pagine Web nuove o poco conosciute. Bloccando le pagine non verificate si migliora la sicurezza, ma si impedisce anche l'accesso alle pagine sicure.

- **Medio**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce
  - **Altamente sospetto**: Si sospetta la natura fraudolenta della pagina o si tratta di una possibile origine di minacce
- **Basso**: Blocca pagine con indicazione:
  - **Pericoloso**: È stata verificata la natura fraudolenta della pagina o si tratta di un'origine nota di minacce

Configurazione della Reputazione Web per Messaging Security Agent

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Reputazione Web**.

   Viene visualizzata una nuova schermata.
5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Attiva Reputazione Web**
   - Livello sicurezza: **Alto**, **Medio** o **Basso**

- URL approvati
  - **URL da approvare**: separare più URL con un punto e virgola (;). Fare clic su **Aggiungi**.

    Nota

    L'approvazione di un URL comporta l'approvazione di tutti i sottodomini corrispondenti.

    Utilizzare i caratteri jolly con cautela in quanto possono approvare interi gruppi di URL.

  - **Elenco URL approvati**: gli URL contenuti in questo elenco non vengono bloccati.

6. Fare clic sulla scheda **Operazione** e selezionare un'operazione per il Messaging Security Agent quando viene attivato il criterio della reputazione Web (per le descrizioni, vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*):
   - Sostituisci con testo/file

     Nota

     Non è possibile sostituire il testo nei campi Da, A, Cc o Oggetto.

   - Mettere in quarantena i messaggi nella cartella di spam utente
   - Elimina intero messaggio
   - Contrassegna e recapita
7. Selezionare **Esegui operazioni sugli URL non valutati da Trend Micro** per trattare come sospetti gli URL non classificati. La stessa operazione specificata al punto precedente verrà eseguita sui messaggi e-mail contenenti URL non classificati.
8. Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che avvisi i destinatari interessati in caso di azione della Reputazione Web a fronte di uno specifico messaggio e-mail.

Per diversi motivi, è possibile evitare di notificare ai destinatari di messaggi e-mail il blocco di un messaggio contenente un URL pericoloso. Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

9. Selezionare **Notifica ai mittenti** per impostare il Messaging Security Agent in modo che avvisi i mittenti interessati in caso di Reputazione Web a fronte di uno specifico messaggio di e-mail.

   Per diversi motivi, è possibile evitare di notificare ai mittenti di e-mail il blocco di un messaggio contenente un URL pericoloso. Selezionare **Non notificare ai mittenti esterni** per inviare le notifiche solo ai mittenti di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

10. Fare clic su **Salva**.

Mobile Security

Le impostazioni di Mobile Security impediscono a dispositivi non autorizzati l'accesso e il download di informazioni dal server Microsoft Exchange. Gli amministratori identificano i dispositivi a cui consentire l'accesso al server Microsoft Exchange e stabiliscono se i loro utenti possono eseguire download o aggiornare posta elettronica, calendario, contatti e attività.

Possono inoltre applicare criteri di sicurezza ai dispositivi. Questi criteri permettono di controllare la lunghezza e la complessità delle password, se i dispositivi debbano essere bloccati dopo un periodo di inattività, se debbano utilizzare la crittografia e se i loro dati debbano essere cancellati dopo una serie di tentativi di accesso non riusciti.

Supporto di Mobile Security

TABELLA 6-5. Supporto dei dispositivi mobili

SISTEMA OPERATIVO	VERSIONE IIS	CRITERI DI PROTEZIONE DATI DEL DISPOSITIVO		CONTROLLO DI ACCESSO		
		EXCHANGE 2007 (O VERSIONE SUCCESSIVA) A 64-BIT	EXCHANGE 2003 A 32 BIT	EXCHANGE 2010 (E VERSIONE SUCCESSIVA) A 64 BIT	EXCHANGE 2007 A 64 BIT	EXCHANGE 2003 A 32 BIT
• Windows 2008 (64 bit) • SBS 2008 (64 bit)	7 +	Sì	Incompatibile	Sì	No	Incompatibile
Windows 2003 (64 bit)	6.0	Sì	Incompatibile	No	No	Incompatibile
• Windows 2003 (32 bit) • SBS 2003 (32 bit)	6.0	Incompatibile	No	Incompatibile	Incompatibile	No

TABELLA 6-6. Supporto sistema operativo dei dispositivi mobili

SO MOBILE	VERSIONE SISTEMA OPERATIVO
iOS	3.0 - 6.1 (4.3 - 7.0)

SO MOBILE	VERSIONE SISTEMA OPERATIVO
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

Configurazione del controllo accesso dispositivo

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Mobile Security** > **Controllo accesso dispositivo**.

   Viene visualizzata una nuova schermata.
5. Selezionare **Attivazione controllo accesso al dispositivo**.
6. Fare clic su **Aggiungi**.
7. Digitare il nome del criterio e una descrizione significativa.
8. Selezionare per quali dispositivi consentire o bloccare l'accesso al server Microsoft Exchange identificando i relativi proprietari:
   - **Chiunque**
   - **Specifica i proprietari dei dispositivi**
9. Se si seleziona **Specifica i proprietari dei dispositivi**:
   a. Digitare il nome del proprietario di un dispositivo e fare clic su **Cerca** per trovarlo nell'elenco di indirizzi globale del server Microsoft Exchange.

b. Selezionare il proprietario del dispositivo e fare clic su **Aggiungi**.

10. Se è conosciuto, selezionare il sistema operativo del dispositivo dall'elenco a discesa **Tipo**.

11. Se è conosciuto, selezionare **Specifica intervallo dei numeri di versione** e identificare quali versioni di tale sistema operativo sono ammesse.

12. Indicare se Messaging Security Agent deve consentire o bloccare l'accesso a posta, calendario, contatti o attività del proprietario del dispositivo.

13. Fare clic su **Salva**.

Annullamento della cancellazione dei dati di un dispositivo in attesa

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Mobile Security** > **Cancellazione dati dispositivo**.

   Viene visualizzata una nuova schermata.

5. Identificare il dispositivo nella tabella di cancellazione dei dispositivi e fare clic su **Annulla cancellazione dati**.
6. Fare clic su **OK**.

Cancellazione manuale dei dati dai dispositivi

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Mobile Security** > **Cancellazione dati dispositivo**.

   Viene visualizzata una nuova schermata.
5. Fare clic su **Seleziona dispositivi**.

   Viene visualizzata una nuova schermata.
6. Digitare il nome del proprietario del dispositivo e fare clic su **Cerca** per trovare il dispositivo.
7. Se il dispositivo è disponibile per la cancellazione, selezionarlo e fare clic su **Cancellazione dati**.

   Nota

   Non è possibile selezionare un dispositivo se il suo stato dopo una ricerca è **Cancellazione dati completata** o **In attesa di cancellazione dati**.

Configurazione dei criteri di sicurezza

Worry-Free Business Security utilizza il criterio predefinito di Microsoft Exchange come criterio predefinito. Il criterio predefinito viene incluso nell'elenco dei criteri di protezione.

Worry-Free Business Security non aggiorna i criteri non predefiniti aggiunti tramite la console di gestione di Microsoft Exchange o the il Cmdlet di Exchange.

Trend Micro raccomanda agli amministratori di gestire i criteri di protezione dalla console di gestione Worry-Free Business Security o da Microsoft Exchange.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Mobile Security** > **Criteri di sicurezza**.

   Viene visualizzata una nuova schermata.
5. Fare clic su **Aggiungi**.
6. Digitare il nome del criterio e una descrizione significativa.
7. Digitare il nome del proprietario di un dispositivo e fare clic su **Cerca** per trovarlo nell'elenco di indirizzi globale del server Microsoft Exchange.
8. Selezionare il proprietario del dispositivo e fare clic su **Aggiungi**.
9. Selezionare il criterio di sicurezza da applicare al dispositivo:
   - **Lunghezza minima della password**: per indicazioni sulle password dei dispositivi mobili, vedere *Requisiti di complessità delle password a pagina 6-61*.
   - **Numero minimo di set di caratteri necessari**: per indicazioni sulle password dei dispositivi mobili, vedere *Requisiti di complessità delle password a pagina 6-61*.
   - **Blocca dispositivo dopo inattività**
   - **Richiedi codifica sul dispositivo**: il dispositivo mobile deve supportare la codifica.

- **Cancella dati dal dispositivo dopo l'accesso non riuscito**

10. Fare clic su **Salva**.

Requisiti di complessità delle password

I requisiti per la complessità delle password variano a seconda dei tipi di dispositivo e dei sistemi operativi.

Le tabelle che seguono indicano il comportamento di ogni "Opzione" di complessità per i dispositivi testati al momento del rilascio di Worry-Free Business Security 9.0 SP3.

Nota

La funzionalità della complessità delle password dipende dal tipo di dispositivo e dalla versione del sistema operativo. Se la password specificata non rispetta i requisiti di complessità, la maggior parte dei dispositivi visualizza un messaggio per l'utente in cui si indicano quali sono i requisiti specifici da applicare.

TABELLA 6-7. Dispositivi Android

LIVELLO DI COMPLESSITÀ	REQUISITI DI COMPLESSITÀ	
	ANDROID 4	ANDROID 2
Opzione 1	Una combinazione dei seguenti tipi di caratteri: • Almeno un carattere maiuscolo (A-Z) o minuscolo (a-z) • Almeno un numero (0-9) o un carattere speciale (!@#$ %^&*()_-=+~ ` []{}|;:'"?/<>,.)	Alfanumerico

Livello di complessità	Requisiti di complessità	
	Android 4	Android 2
Opzione 2	Una combinazione dei seguenti tipi di caratteri: • Almeno un carattere maiuscolo (A-Z) o minuscolo (a-z) • Almeno due numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno due numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 3	Una combinazione dei seguenti tipi di caratteri: • Almeno un carattere maiuscolo (A-Z) o minuscolo (a-z) • Almeno tre numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno tre numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 4	Una combinazione dei seguenti tipi di caratteri: • Almeno un carattere maiuscolo (A-Z) o minuscolo (a-z) • Almeno quattro numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno quattro numeri (0-9) o caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tabella 6-8. Dispositivi iOS

Livello di complessità	Requisiti di complessità
Opzione 1	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno un carattere speciale (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Livello di complessità	Requisiti di complessità
Opzione 2	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno due caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 3	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno tre caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 4	Una combinazione dei seguenti tipi di caratteri: • Alfanumerico • Almeno quattro caratteri speciali (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tabella 6-9. Dispositivi Windows Phone

Livello di complessità	Requisiti di complessità	
	Windows Phone 8	Windows Phone 7
Opzione 1	Almeno uno dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione di almeno due dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Livello di complessità	Requisiti di complessità	
	Windows Phone 8	Windows Phone 7
Opzione 2	Una combinazione di almeno due dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione di almeno due dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 3	Una combinazione di almeno tre dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione di almeno tre dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 4	Una combinazione di tutti i seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Una combinazione di tutti i seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Tabella 6-10. Dispositivi BlackBerry

Livello di complessità	Requisiti di complessità
Opzione 1	Almeno un carattere maiuscolo (A-Z) o minuscolo (a-z)

Livello di complessità	Requisiti di complessità
Opzione 2	Una combinazione di almeno due dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 3	Una combinazione di almeno tre dei seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Opzione 4	Una combinazione di tutti i seguenti tipi di caratteri: • caratteri maiuscoli (A-Z) • caratteri minuscoli (a-z) • caratteri numerici (0-9) • Caratteri speciali (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Quarantena per i Messaging Security Agent

Quando il Messaging Security Agent rileva una minaccia, spam, allegati con limitazioni e/o contenuti con limitazioni in messaggi e-mail, l'agent è in grado di spostare il messaggio in una cartella di quarantena. Questo processo rappresenta un'alternativa all'eliminazione del messaggio o dell'allegato e impedisce agli utenti di aprire il messaggio infetto e di diffondere la minaccia.

La cartella di quarantena predefinita nel Message Security Agent è:

```
<Cartella di installazione Messaging Security Agent>\storage
\quarantine
```

Per aumentare la sicurezza, i file in quarantena vengono crittografati. Per aprire un file crittografato, utilizzare lo strumento Restore Encrypted Virus and Spyware (strumento `VSEncode.exe`). Vedere *Ripristino dei file crittografati a pagina 14-19*.

Gli amministratori hanno la possibilità di consultare il database di quarantena per raccogliere informazioni sui messaggi messi in quarantena.

Utilizzare la cartella di Quarantena per:

- Ovviare alla probabilità di eliminazione permanente di messaggi importanti, qualora venissero erroneamente individuati da filtri aggressivi
- Rivedere i messaggi che avviano i filtri di contenuto per determinare la gravità dell'infrazione dei criteri
- Conservare le prove del possibile abuso da parte di un dipendente del sistema di messaggistica aziendale

Nota

Non confondere la cartella di quarantena con la cartella di spam utente finale. La cartella di quarantena è una cartella basata su file. Tutte le volte che un Messaging Security Agent mette in quarantena un messaggio e-mail, lo invia alla cartella di quarantena. La cartella di spam utente finale si trova nell'archivio informazioni della casella di posta di ciascun utente. La cartella di spam utente finale riceve soltanto i messaggi e-mail risultanti da un'operazione di quarantena anti-spam a una cartella di spam dell'utente e non quelli provenienti da operazioni di quarantena conseguenti a filtro dei contenuti, criteri antivirus/anti-spyware o criteri di blocco degli allegati.

Consultazione delle directory di quarantena

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.

3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.

4. Fare clic su **Quarantena** > **Query**.

   Viene visualizzata una nuova schermata.

5. Aggiornare le informazioni riportate di seguito, in base alle necessità:

   - Intervallo data/ora
   - Motivi della quarantena
     - **Tutti i motivi**
     - **Tipi specificati**: selezionare Scansione antivirus, Anti-spam, Filtro dei contenuti, Blocco allegati e/o Parti non analizzabili dei messaggi.
   - Stato del reinvio
     - **Mai reinviato**
     - **Reinviato almeno una volta**
     - **Entrambe le precedenti**
   - Criteri avanzati
     - **Mittente**: messaggi provenienti da mittenti specifici. Se necessario, utilizzare i caratteri jolly.
     - **Destinatario**: messaggi da destinatari specifici. Se necessario, utilizzare i caratteri jolly.
     - **Oggetto**: messaggi con oggetti specifici. Se necessario, utilizzare i caratteri jolly.
     - **Ordina per**: configurare la condizione di ordinamento della pagina dei risultati.
     - **Schermo**: numero di risultati per pagina.

6. Fare clic su **Cerca**. Vedere *Visualizzazione dei risultati della query e azioni correttive a pagina 6-68*.

Visualizzazione dei risultati della query e azioni correttive

La schermata dei risultati **Query quarantena** visualizza le seguenti informazioni sui messaggi:

- **Ora della scansione**
- **Mittente**
- **Destinatario**
- **Oggetto**
- **Motivo**: Il motivo per cui il messaggio e-mail è stato messo in quarantena.
- **Nome file**: Il nome del file allegato al messaggio e-mail che è stato bloccato.
- **Percorso di quarantena**: Il percorso della cartella di quarantena del messaggio e-mail. Gli amministratori sono in grado di decodificare il file con VSEncoder.exe (vedere *Ripristino dei file crittografati a pagina 14-19*) e di rinominarlo con l'estensione `.eml` per poterlo visualizzare.

  AVVERTENZA!
  Visualizzare file infetti può diffondere l'infezione.

- **Stato del reinvio**

Procedura

1. Se si ritiene che il messaggio non sia sicuro, eliminare il messaggio.

AVVERTENZA!

La cartella di quarantena contiene i messaggi e-mail che presentano un rischio elevato di infezione. È importante prestare molta attenzione quando si maneggiano i messaggi e-mail della cartella di quarantena, per evitare di infettare accidentalmente il client.

2. Se si ritiene che un messaggio sia sicuro, selezionarlo e fare clic sull'icona di reinvio ( ).

Nota

Se un messaggio messo in quarantena inviato originariamente utilizzando Microsoft Outlook viene nuovamente inviato, il destinatario potrebbe ricevere diverse copie dello stesso messaggio. Questo accade perché il motore di scansione antivirus suddivide ogni messaggio analizzato in varie sezioni.

3. Qualora non sia possibile reinviare il messaggio, è possibile che l'account dell'amministratore di sistema sul server Microsoft Exchange non esista.

   a. Utilizzando l'editor del Registro di sistema di Windows, aprire la seguente voce di registro sul server:

      `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

   b. Modificare la voce come segue:

AVVERTENZA!

Modificare in modo errato il registro può danneggiare gravemente il sistema. Prima di apportare modifiche al registro, eseguire il backup dei dati di maggiore importanza presenti sul computer.

- `ResendMailbox {casella postale dell'amministratore}`

  Esempio: `admin@esempio.com`

- `ResendMailboxDomain` `{dominio dell'amministratore}`

  Esempio: `esempio.com`

- `ResendMailSender` `{account e-mail dell'amministratore}`

  Esempio: `admin`

c. Chiudere l'editor del Registro di sistema.

Gestione delle directory di quarantena

Utilizzare questa funzione per eliminare manualmente o automaticamente i messaggi messi in quarantena. Questa funzione consente di eliminare tutti i messaggi, i messaggi che sono stati reinviati e i messaggi che non sono stati reinviati.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Quarantena** > **Manutenzione**.

   Viene visualizzata una nuova schermata.
5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Attiva manutenzione automatica**: disponibile solo per la manutenzione automatica.
   - File da eliminare
     - **Tutti i file in quarantena**
     - **I file in quarantena che non sono mai stati reinviati**

- **I file in quarantena che sono stati reinviati almeno una volta**

- **Azione**: il numero di giorni per cui si desidera memorizzare i messaggi. Ad esempio, se la data è 21 novembre e nel campo **Elimina i file selezionati più vecchi di** è stato immesso il valore `10`, quando esegue l'eliminazione automatica Messaging Security Agent elimina tutti i file con data precedente all'11 novembre.

6. Fare clic su **Salva**.

Configurazione delle directory di quarantena

Consente di configurare le directory di quarantena nel server Microsoft Exchange. La directory di quarantena verrà esclusa dalla scansione.

Nota

Le directory di quarantena sono basate su file e non risiedono nell'Archivio informazioni.

Messaging Security Agent mette in quarantena i messaggi e-mail in base alle operazioni configurate. Le seguenti directory sono le directory di quarantena:

- **Antivirus**: mette in quarantena i messaggi e-mail che contengono virus/minacce informatiche, spyware/grayware, worm, cavalli di Troia e altre minacce dannose.
- **Anti-spam**: mette in quarantena messaggi e-mail di spam e di phishing.
- **Blocco allegati**: mette in quarantena i messaggi e-mail contenenti allegati con limitazioni.
- **Filtro dei contenuti**: mette in quarantena i messaggi e-mail che contengono contenuti con limitazioni.

Per impostazione predefinita, tutte le directory hanno gli stessi percorsi (`<Cartella di installazione Messaging Security Agent>\storage`

`\quarantine`). È possibile modificare i percorsi per ogni singola directory o per tutte.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Quarantena** > **Directory**.

   Viene visualizzata una nuova schermata.
5. Definire il percorso per le seguenti directory di quarantena:
   - **Antivirus**
   - **Anti-Spam**
   - **Filtro dei contenuti**
   - **Blocco allegati**
6. Fare clic su **Salva**.

Impostazioni di notifica per i Messaging Security Agent

Worry-Free Business Security invia notifiche sotto forma di messaggi e-mail per diversi avvisi.

È possibile configurare le notifiche in modo che siano applicabili solo ai messaggi e-mail interni utilizzando le definizioni posta interna personalizzata. Queste definizioni risultano utili se l'azienda dispone di almeno due domini e si desidera che i messaggi e-mail provenienti dai due

domini siano considerati come posta interna. Ad esempio: esempio.com e esempio.net.

I destinatari riportati nell'elenco Definizioni posta interna riceveranno i messaggi di notifica quando si seleziona la casella di controllo **Non notificare a destinatari esterni** in Impostazioni di notifica per **Antivirus**, **Filtro dei contenuti** e **Blocco allegati**. Attenzione a non confondere l'elenco Definizione posta interna con l'elenco Mittenti approvati.

Per evitare che tutti i messaggi e-mail provenienti da indirizzi con domini esterni siano etichettati come spam, aggiungere gli indirizzi e-mail esterni agli elenchi **Mittenti approvati** per Anti-spam.

Informazioni sulle definizioni della posta interna personalizzate

Messaging Security Agent suddivide il traffico e-mail in due grandi categorie: interno ed esterno. L'agent interroga il server Microsoft Exchange per ottenere informazioni sulla definizione degli indirizzi interni ed esterni. Tutti gli indirizzi interni condividono un dominio comune e tutti quelli esterni non appartengono a questo dominio.

Ad esempio, se l'indirizzo interno del dominio è "@trend_1.com", il Messaging Security Agent classifica indirizzi come "abc@trend_1.com" e "xyz@trend_1.com" come indirizzi interni. L'agent classifica tutti gli altri indirizzi (ad esempio "abc@trend_2.com" e "jondoe@123.com") come indirizzi esterni.

È possibile definire un solo dominio come indirizzo interno per Messaging Security Agent. Se si utilizza Microsoft Exchange System Manager per modificare l'indirizzo primario su un server, Messaging Security Agent non riconosce il nuovo indirizzo come indirizzo interno perché Messaging Security Agent non può rilevare il cambiamento del criterio del destinatario.

Esempio: l'utente dispone di due indirizzi di dominio per la propria azienda, @esempio_1.com e @esempio_2.com. @esempio_1.com viene impostato come indirizzo primario. Messaging Security Agent considera interni i messaggi e-mail con l'indirizzo primario (ossia, abc@esempio_1.com o xyz@esempio_1.com sono interni). In seguito, si utilizza Microsoft Exchange System Manager per modificare l'indirizzo primario in @esempio_2.com. Questo significa che Microsoft Exchange a questo punto riconosce come

indirizzi interni gli indirizzi quali abc@esempio_2.com e xyz@esempio_2.com.

Configurazione delle impostazioni di notifica per i Messaging Security Agent

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Operazioni** > **Impostazioni di notifica**.

   Viene visualizzata una nuova schermata.
5. Aggiornare le informazioni riportate di seguito, in base alle necessità:
   - **Indirizzo e-mail**: l'indirizzo per conto del quale Worry-Free Business Security invia i messaggi di notifica.
   - **Definizione posta interna**
     - **Predefinito**: Worry-Free Business Security considera i messaggi e-mail provenienti dallo stesso dominio come posta interna.
     - **Personalizzato**: specificare singoli indirizzi e-mail o domini da trattare come messaggi interni.
6. Fare clic su **Salva**.

Configurazione di Manutenzione spam

La schermata **Manutenzione spam** consente di configurare le impostazioni di End User Quarantine (EUQ) o quarantena lato server.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Operazioni** > **Manutenzione spam**.

   Viene visualizzata una nuova schermata.
5. Fare clic su **Attiva strumento End User Quarantine**.

   Quando si attiva lo strumento EUQ, viene creata una cartella di quarantena sul lato server per ogni casella di posta del client e la cartella `Posta indesiderata` viene aggiunta alla struttura ad albero delle cartelle Outlook. Dopo l'attivazione dello strumento EUQ e la creazione delle cartelle Posta indesiderata, EUQ filtra i messaggi di spam inserendoli automaticamente nella cartella Posta indesiderata dell'utente. Per i dettagli, consultare *Gestione della End User Quarantine a pagina 6-76*.

   Suggerimento

   Se si seleziona questa opzione, Trend Micro consiglia di disattivare la Barra degli strumenti di Trend Micro Anti-Spam degli agent per migliorare le prestazioni dei client.

   Deselezionare l'opzione **Attiva strumento End User Quarantine** per disattivare lo strumento di quarantena dell'utente finale per tutte le caselle di posta del server Microsoft Exchange. Quando si disattiva lo strumento EUQ, le cartelle Posta indesiderata non vengono rimosse, ma i messaggi individuati come spam non vengono spostati automaticamente in queste cartelle.
6. Fare clic su **Crea cartella di spam ed elimina i messaggi di spam** per generare (immediatamente) cartelle di Posta indesiderata per i client di posta appena creati e per quelli che hanno eliminato la propria cartella

Posta indesiderata. Per gli altri client di posta esistenti, verranno eliminati i messaggi di spam precedenti al numero di giorni specificato nel campo Impostazioni della cartella spam del client.

7. In **Elimina i messaggi di spamming più vecchi di {numero} giorni**, modificare il numero di giorni per cui Messaging Security Agent conserva i messaggi di spam. Il valore predefinito è 14 giorni e il limite massimo 30 giorni.

8. Per disattivare lo strumento End User Quarantine per gli utenti selezionati:

   a. In **Elenco eccezioni dello strumento End User Quarantine** immettere l'indirizzo e-mail dell'utente finale per il quale si intende disattivare la quarantena.

   b. Fare clic su **Aggiungi**.

      L'indirizzo e-mail dell'utente finale verrà aggiunto all'elenco degli indirizzi per cui lo strumento EUQ è disattivato.

      Per rimuovere un utente finale dall'elenco e ripristinare il servizio EUQ, selezionare l'indirizzo e-mail dell'utente finale dall'elenco e fare clic su **Elimina**.

9. Fare clic su **Salva**.

Gestione della End User Quarantine

Durante l'installazione, il Messaging Security Agent aggiunge una cartella, `Posta indesiderata`, alla casella di posta lato server di ciascun utente finale. Quando riceve messaggi indesiderati, il sistema li mette in quarantena nella cartella in base alle regole del filtro anti-spam definite da Messaging Security Agent. Gli utenti finali hanno la possibilità di visualizzare questa cartella per aprire, leggere o eliminare i messaggi e-mail sospetti. Vedere *Configurazione di Manutenzione spam a pagina 6-74*.

In alternativa, gli amministratori possono creare la cartella "Posta indesiderata" su Microsoft Exchange. Quando l'amministratore crea un

account di casella di posta, l'entità della casella di posta non viene creata immediatamente nel server Microsoft Exchange, ma verrà creata nei seguenti casi:

- Un utente finale accede alla casella di posta per la prima volta
- Il primo messaggio e-mail arriva nella casella di posta

Prima che la Quarantena utente finale possa creare una cartella Posta indesiderata, è necessario che l'amministratore crei l'entità della casella di posta.

Cartella posta indesiderata lato client

Gli utenti finali possono aprire i messaggi e-mail messi in quarantena nella cartella dello spam. Quando si apre uno di questi messaggi, nel messaggio e-mail vengono visualizzati due pulsanti: **Mittente approvato** e **Visualizza elenco mittenti approvati**.

- Quando un utente finale apre un messaggio e-mail contenuto nella cartella Posta indesiderata e fa clic su **Mittente approvato**, l'indirizzo del mittente del messaggio in questione viene aggiunto all'elenco dei **Mittenti approvati** dell'utente finale.
- Selezionando **Visualizza elenco mittenti approvati**, si apre un'altra schermata che consente agli utenti finali di visualizzare e modificare il proprio elenco di mittenti approvati per parametri quali indirizzo e-mail o dominio.

Mittenti approvati

Quando l'utente finale riceve un messaggio e-mail nella cartella Posta indesiderata e fa clic su **Approva mittente**, il Messaging Security Agent sposta il messaggio nella casella locale Posta in arrivo dell'utente finale e aggiunge l'indirizzo del mittente all'elenco personale Mittenti approvati dell'utente finale. Messaging Security Agent inserisce l'evento nel registro.

Quando il server Microsoft Exchange riceve messaggi dagli indirizzi inseriti nell'elenco Mittenti approvati dell'utente finale, li smista nella casella della posta in arrivo dell'utente finale, a prescindere dall'intestazione o dal contenuto del messaggio.

Nota

Messaging Security Agent fornisce inoltre agli amministratori un elenco dei mittenti approvati e bloccati. Prima di prendere in considerazione l'elenco degli utenti finali, Messaging Security Agent applica quello dell'amministratore.

Funzione di manutenzione di End User Quarantine

La funzione di manutenzione di Messaging Security Agent esegue le seguenti operazioni programmate ogni 24 ore all'orario predefinito (2:30):

- Eliminazione automatica dei messaggi di spam scaduti
- Creazione di una nuova cartella di spam dopo l'eliminazione
- Creazione delle cartelle di spam per account e-mail appena creati
- Gestione delle regole dei messaggi e-mail

La funzione di manutenzione è parte integrante di Messaging Security Agent e non richiede alcuna configurazione.

Assistenza Trend Micro/Programma di debug

Il programma di assistenza/debug può risultare utile per eseguire il debug o per fornire informazioni sullo stato dei processi di Messaging Security Agent. Se si riscontrano difficoltà impreviste, è possibile utilizzare il programma di debug per creare dei report da inviare all'assistenza tecnica di Trend Micro per ulteriori analisi.

Ciascun Messaging Security Agent inserisce messaggi nel programma, quindi registra l'azione nei file di registro al momento dell'esecuzione. È possibile inoltrare i registri allo staff tecnico di Trend Micro per facilitare le operazioni di debug del flusso effettivo del programma nell'ambiente in uso.

È inoltre possibile utilizzare il programma di debug per generare registri nei seguenti moduli:

- Servizio principale Messaging Security Agent

- Server di configurazione remota di Messaging Security Agent
- System Watcher di Messaging Security Agent
- API di Virus Scan (VSAPI)
- SMTP (Simple Mail Transport Protocol)
- CGI (Common Gateway Interface)

Per impostazione predefinita, MSA conserva i registri nella seguente directory predefinita:

```
<Cartella di installazione Messaging Security Agent>\Debug
```

Visualizzare il risultato con un qualsiasi editor di testo.

Generazione di rapporti del programma di debug di sistema

Generare rapporti del programma di debug per aiutare l'assistenza Trend Micro a risolvere i problemi.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare un Messaging Security Agent.
3. Fare clic su **Configura criterio**.

   Viene visualizzata una nuova schermata.
4. Fare clic su **Operazioni** > **Assistenza tecnica/Programma di debug**.

   Viene visualizzata una nuova schermata.
5. Selezionare i moduli da monitorare:
   - Servizio principale di **Messaging Security Agent**
   - Server di configurazione remota di **Messaging Security Agent**

- System Watcher di **Messaging Security Agent**
- **API di Virus Scan (VSAPI)** su server Exchange 2003, 2007 o 2010.
- **Scansione a livello di archivio** su server Exchange 2013.
- **SMTP (Simple Mail Transfer Protocol)** su server Exchange 2003.
- **Servizio di trasporto** su server Exchange 2007, 2010 o 2013.
- **CGI (Common Gateway Interface)**

6. Fare clic su **Applica**.

   Il programma di debug inizia a raccogliere i dati circa i moduli selezionati.

Monitoraggio in tempo reale

Monitoraggio in tempo reale visualizza informazioni in tempo reale sul server Microsoft Exchange selezionato e sul relativo Messaging Security Agent. Vengono visualizzate informazioni sui messaggi analizzati e sulle statistiche di protezione, compreso il numero di virus e di messaggi spam rilevati, di allegati bloccati e di violazioni dei contenuti. Verifica anche se l'agent sta funzionando correttamente.

Uso del Monitoraggio in tempo reale

Procedura

1. Per accedere al Monitoraggio in tempo reale dalla console Web:
   a. Andare su **Dispositivi**.
   b. Selezionare un Messaging Security Agent.
   c. Fare clic su **Configura criterio**.

      Viene visualizzata una nuova schermata.

d. Fare clic sul collegamento **Monitoraggio in tempo reale** nella parte superiore destra dello schermo.

2. Per accedere al Monitoraggio in tempo reale dal menu Start di Windows, fare clic su **Programmi** > **Trend Micro Messaging Security Agent** > **Monitoraggio in tempo reale**.

3. Fare clic su **Reimposta** per azzerare le statistiche della protezione.

4. Fare clic su **Cancella contenuto** per cancellare le informazioni obsolete sui messaggi sottoposti a scansione.

Aggiunta di una declinazione di responsabilità ai messaggi e-mail in uscita

È possibile aggiungere un messaggio di declinazione di responsabilità solo ai messaggi e-mail in uscita.

Procedura

1. Creare un file di testo e aggiungere il testo della declinazione di responsabilità a questo file.

2. Modificare le seguenti chiavi nel registro:

   - Prima chiave:

     Percorso: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Chiave: `EnableDisclaimer`

     Tipo: `REG_DWORD`

     Valore dati: `0 - disattiva, 1 - attiva`

   - Seconda chiave:

Percorso: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

Chiave: `DisclaimerSource`

Tipo: `REG_SZ`

Valore: Il percorso completo del file contenente la declinazione di responsabilità.

Ad esempio, `C:\Data\Disclaimer.txt`.

Nota

Per impostazione predefinita, Worry-Free Business Security rileva se un messaggio di posta in uscita viene inviato a un dominio interno o esterno e aggiunge una declinazione di responsabilità a ogni messaggio inviato a domini esterni. L'utente può sostituire l'impostazione predefinita e aggiungere una declinazione di responsabilità a ogni messaggio in uscita, fatta eccezione per i domini inclusi nelle seguenti chiavi di registro:

- Terza chiave:

  Percorso: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

  Chiave: `InternalDomains`

  Tipo: `REG_SZ`

  Valore: Digitare i nomi dei domini da escludere. Separare le voci con un punto e virgola (;).

  Ad esempio: `dominio1.org;dominio2.org`

  Nota

  I nomi dei domini inseriti qui sono i nomi DNS dei server Exchange.

Capitolo 7

Gestione delle scansioni

In questo capitolo viene descritto come eseguire scansioni sui Security Agent e sui Messaging Security Agent (solo Advanced) per proteggere rete e client dalle minacce.

Informazioni sulle scansioni

Nel corso di una scansione, il motore di scansione di Trend Micro funziona in modo integrato con il file di pattern per completare il primo livello di rilevamento utilizzando un processo detto "pattern matching". Poiché ogni minaccia contiene una firma univoca o una stringa di caratteri riconoscibili che lo distinguono da qualsiasi altro codice, porzioni rivelatrici inerti di questo codice vengono rilevate nel file di pattern. Il motore confronta alcune parti di ogni file analizzato con pattern del file di pattern, alla ricerca di qualche corrispondenza.

Quando il motore di scansione individua un file contenente una minaccia, esegue operazioni quali la disinfezione, la quarantena, l'eliminazione o la sostituzione con testo/file (solo Advanced). È possibile personalizzare tali operazioni al momento dell'impostazione delle operazioni di scansione.

Worry-Free Business Security offre **tre tipi di scansione**. Ciascuna scansione si prefigge uno scopo e un utilizzo diverso, ma tutte sono configurate approssimativamente allo stesso modo.

- Scansione in tempo reale. Per maggiori dettagli, consultare *Scansione in tempo reale a pagina 7-3*.
- Scansione manuale. Per maggiori dettagli, consultare *Scansione manuale a pagina 7-3*.
- Scansione pianificata. Per maggiori dettagli, consultare *Scansione pianificata a pagina 7-7*.

I Security Agent utilizzano uno dei due metodi di scansione per le scansioni:

- Smart Scan
- Scansione convenzionale

Per maggiori dettagli, consultare *Metodi di scansione a pagina 5-3*.

Scansione in tempo reale

La scansione in tempo reale è una scansione continua e costante.

Ogniqualvolta un file viene aperto, scaricato, copiato o modificato, la scansione in tempo reale del **Security Agent** analizza il file per rilevare eventuali minacce. Per ulteriori dettagli sulla configurazione della Scansione in tempo reale, vedere *Configurazione della scansione in tempo reale per i Security Agent a pagina 5-7*.

In caso di messaggi e-mail, la scansione in tempo reale nel **Messaging Security Agent** (solo Advanced) protegge tutti i possibili punti di ingresso di virus, effettuando la scansione in tempo reale di tutti i messaggi in entrata, messaggi SMTP, documenti pubblicati su cartelle pubbliche e file replicati da altri server Microsoft Exchange. Per ulteriori dettagli sulla configurazione della Scansione in tempo reale, vedere *Configurazione della scansione in tempo reale per Messaging Security Agent a pagina 6-6*.

Scansione manuale

La scansione manuale è una scansione su richiesta.

La Scansione manuale sui **Security Agent** elimina le minacce dai file e sradica le infezioni obsolete, se presenti, per ridurre al minimo ulteriori infezione.

La Scansione manuale sui **Messaging Security Agents** (solo Advanced) esegue la scansione di tutti i file nell'archivio informazioni del server Microsoft Exchange.

Il tempo impiegato per la scansione dipende dalle risorse hardware del client e dal numero di file sui quali eseguire la scansione. Una Scansione manuale in corso è interrompibile dall'amministratore del Security Server se la scansione è stata eseguita da remoto da una console Web, o in alternativa dall'utente se la scansione è stata eseguita direttamente sul client.

Suggerimento

Trend Micro consiglia di eseguire le scansioni manuali tutte le volte che si verifica un'infezione virale.

Esecuzione di scansioni manuali

Questa procedura descrive in che modo gli amministratori del Security Server eseguono scansioni manuali su **Security Agent** e **Messaging Security Agent** (solo Advanced) dalla console Web.

Nota

Selezionando con il pulsante destro del mouse l'icona del Security Agent nella barra delle applicazioni di Windows e poi scegliendo **Eseguire la scansione**, la scansione manuale è eseguibile anche direttamente dai client. La scansione manuale direttamente dai server Microsoft Exchange è impossibile.

Procedura

1. Raggiungere **Scansioni** > **Scansione manuale**.
2. (Opzionale) Personalizzare le impostazioni di scansione prima di eseguire la Scansione manuale.

Istruzioni e note	Impostazioni di scansione consigliate
Per personalizzare le impostazioni di scansione del **Security Agent**, fare clic su un gruppo desktop o server. Vedere *Destinazioni di scansione e azioni per i Security Agent a pagina 7-10*. **Nota** Le impostazioni di scansione per i Security Agent sono utilizzate anche quando gli utenti eseguono la Scansione manuale direttamente dai client. Tuttavia, se gli utenti detengono i privilegi per configurare le proprie impostazioni di scansione, durante la scansione vengono utilizzate le impostazioni di scansione impostate dall'utente.	Destinazione • Tutti i file analizzabili: Include tutti i file analizzabili. I file non analizzabili sono i file protetti da password, i file codificati o i file che eccedono le limitazioni di scansione definite dall'utente. • Esegui scansione dei file compressi fino al livello 1: Sottopone a scansione i file compressi che contengono 1 livello di compressione. L'impostazione predefinita è "disattivato" per il gruppo di server predefinito e "attivato" per il gruppo di desktop predefinito. Esclusioni • Non effettua la scansione delle directory in cui sono installati i prodotti Trend Micro. Impostazioni avanzate • Modifica elenco Approvati spyware/ grayware (solo per anti-spyware)

Istruzioni e note	Impostazioni di scansione consigliate
Per personalizzare le impostazioni di scansione del **Messaging Security Agent**, espandere un agent e fare clic su: • **Antivirus**. Selezionare affinché l'agent esegua una scansione che individui virus e altri malware. Vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*. • **Filtro dei contenuti**: Selezionare affinché l'agent esegua la scansione dei messaggi e-mail alla ricerca di contenuti non autorizzati. Vedere *Gestione delle regole del filtro dei contenuti a pagina 6-17*. • **Blocco allegati**: Selezionare affinché l'agent esegua la scansione dei messaggi e-mail alla ricerca di violazioni delle regole relative agli allegati. Vedere *Configurazione del blocco degli allegati a pagina 6-49*.	• L'agent esegue la scansione di tutti i file analizzabili. Nella scansione vengono inclusi anche i corpi dei messaggi e-mail. • Quando l'agent rileva un file contenente un virus o malware, lo disinfetta. Se la disinfezione non è possibile, il file viene sostituito con del testo o un altro file. • Quando l'agent rileva un file con un Trojan o worm, sostituisce la minaccia informatica con testo o un altro file. • Quando rileva un file con un Packer, l'agent sostituisce il Packer con testo o un altro file. • L'agent non disinfetta i file infetti compressi. In questo modo, la durata della scansione in tempo reale viene ridotta.

3. Selezionare i gruppi o i Messaging Security Agent sui quali eseguire la scansione.

4. Fare clic su **Eseguire la scansione**.

   Il Security Server invia una notifica agli agent per l'esecuzione della Scansione manuale. La schermata Risultati di notifica scansione che compare mostra il numero di agent che hanno ricevuto la notifica e quelli che non l'hanno ricevuta.

5. Per interrompere le scansioni in corso, fare clic su **Interrompi scansione**.

   Il Security Server invia un'altra notifica agli agent per l'interruzione della Scansione manuale. La schermata Risultati di notifica interruzione scansione che compare mostra il numero di agent che hanno ricevuto la

notifica e quelli che non l'hanno ricevuta. I Security Agent potrebbero non ricevere la notifica se si disconnettono durante la scansione o in caso di interruzioni della connessione di rete.

Scansione pianificata

Una scansione pianificata è simile a una scansione manuale, ma effettua le scansioni di tutti i file e dei messaggi e-mail (solo Advanced) in momenti prestabiliti e con frequenze predeterminate. Utilizzare le scansioni pianificate per automatizzare le scansioni di routine dei client e per migliorare l'efficienza della gestione delle minacce.

Suggerimento

Eseguire le scansioni pianificate lontano dagli orari lavorativi, per minimizzare potenziali interruzioni per utenti e rete.

Configurazione delle scansioni pianificate

Trend Micro consiglia di non pianificare una scansione contemporaneamente a un aggiornamento pianificato. In situazioni del genere, la scansione pianificata può subire interruzioni premature. Analogamente, se si avvia una scansione manuale quando è in esecuzione una scansione pianificata, la scansione pianificata viene interrotta, anche se continuerà a rispettare la pianificazione per le volte successive.

Procedura

1. Raggiungere **Scansioni** > **Scansione pianificata**.
2. Fare clic sulla scheda **Pianificazione**.
   a. Configurare la frequenza di scansione (giornaliera, settimanale o mensile) e l'ora di inizio. Ogni gruppo o Messaging Security Agent può avere la propria pianificazione.

Nota

Per le scansioni pianificate mensili, se si selezionano 31, 30 o 29 giorni e un mese ha meno di questo numero di giorni, la scansione non viene eseguita per quel mese.

b. (Opzionale) Selezionare **Dopo la scansione pianificata, spegnere il client**.

c. Fare clic su **Salva**.

3. Fare clic sulla scheda **Impostazioni** e configurare eventuali impostazioni di Scansione pianificata richieste.

ISTRUZIONI E NOTE	IMPOSTAZIONI DI SCANSIONE CONSIGLIATE
Per personalizzare le impostazioni di scansione del **Security Agent**, fare clic su un gruppo desktop o server. Vedere *Destinazioni di scansione e azioni per i Security Agent a pagina 7-10*. **Nota** Se gli utenti hanno i privilegi per configurare impostazioni di scansione personalizzate, durante la scansione vengono utilizzate le impostazioni di scansione impostate dall'utente.	Destinazione • Tutti i file analizzabili:Include tutti i file analizzabili. I file non analizzabili sono i file protetti da password, i file codificati o i file che eccedono le limitazioni di scansione definite dall'utente. • Esegui scansione dei file compressi fino al livello 2: Sottopone a scansione i file compressi che contengono 2 livello di compressione.
	Esclusioni • Non effettua la scansione delle directory in cui sono installati i prodotti Trend Micro.
	Impostazioni avanzate • Modifica elenco Approvati spyware/ grayware (solo per anti-spyware)

ISTRUZIONI E NOTE	IMPOSTAZIONI DI SCANSIONE CONSIGLIATE
Per personalizzare le impostazioni di scansione del **Messaging Security Agent**, espandere un agent e fare clic su: • **Antivirus**. Selezionare affinché l'agent esegua una scansione che individui virus e altri malware. Vedere *Destinazioni di scansione e azioni per i Messaging Security Agent a pagina 7-18*. • **Filtro dei contenuti**:Selezionare affinché l'agent esegua la scansione dei messaggi e-mail alla ricerca di contenuti non autorizzati. Vedere *Gestione delle regole del filtro dei contenuti a pagina 6-17*. • **Blocco allegati**:Selezionare affinché l'agent esegua la scansione dei messaggi e-mail alla ricerca di violazioni delle regole relative agli allegati. Vedere *Configurazione del blocco degli allegati a pagina 6-49*.	• L'agent esegue una scansione tutte le domeniche alle 5:00. • È possibile personalizzare la pianificazione da eseguire sui client durante le ore non di punta. L'agent esegue la scansione di tutti i file analizzabili. Nella scansione vengono inclusi anche i corpi dei messaggi e-mail. • Quando l'agent rileva un file contenente un virus o malware, lo disinfetta. Se la disinfezione non è possibile, il file viene sostituito con del testo o un altro file. • Quando l'agent rileva un file con un Trojan o worm, sostituisce la minaccia informatica con testo o un altro file. • Quando l'agent rileva un file con un Packer, lo sostituisce con testo o un altro file. • L'agent non disinfetta i file infetti compressi.

4. Selezionare i gruppi o il Messaging Security Agent che applicherà le impostazioni della Scansione pianificata.

Nota

Per disattivare la Scansione pianificata, deselezionare la casella di controllo per il gruppo o il Messaging Security Agent.

5. Fare clic su **Salva**.

Destinazioni di scansione e azioni per i Security Agent

Configurare le seguenti impostazioni per ogni tipo di scansione (scansione manuale, scansione pianificata e scansione in tempo reale):

Scheda Destinazione

Selezionare un metodo:

- **Tutti i file analizzabili**: include tutti i file analizzabili. I file non analizzabili sono i file protetti da password, i file codificati o i file che eccedono le limitazioni di scansione definite dall'utente.

  Nota

  Questa opzione garantisce la massima protezione possibile. Tuttavia, la scansione di tutti i file richiede molto tempo e numerose risorse e in determinate situazioni può risultare eccessiva. Per questo motivo, può essere opportuno limitare la quantità di file che l'agent deve includere nella scansione.

- **IntelliScan utilizza l'identificazione del "tipo di file effettivo"**: sottopone a scansione i file in base al tipo di file effettivo. Vedere *IntelliScan a pagina D-2*.

- **Esegui la scansione dei file con le seguenti estensioni**: consente di specificare manualmente i file da sottoporre a scansione in base alle loro estensioni. Separare più voci con la virgola (,).

Selezionare attivatore della scansione:

- **Lettura**: analizza i file di cui si legge il contenuto; i file vengono letti all'apertura, esecuzione, copia o spostamento.

- **Scrittura**: analizza i file su cui si effettuano operazioni di scrittura; la scrittura comprende le operazioni di modifica, salvataggio, download o copia da un'altra posizione.

- **Lettura o scrittura**

Esclusioni scansione

È possibile configurare le impostazioni riportate di seguito:

- Attivare o disattivare le esclusioni
- Escludere le directory del prodotto Trend Micro dalle scansioni
- Escludere altre directory dalle scansioni

  Vengono escluse anche tutte le sottodirectory contenute nel percorso di directory specificato.
- Escludere i nomi di file o i nomi di file con percorso completo dalle scansioni
- Escludere le estensioni dei file

  I caratteri jolly come "*" non possono essere utilizzati nelle estensioni.

Nota

(solo Advanced) Se sui client è in esecuzione il server Microsoft Exchange, Trend Micro consiglia di escludere dalla scansione tutte le cartelle del server. Per escludere dalla scansione le cartelle del server Microsoft Exchange su base globale, accedere a **Amministrazione** > **Impostazioni globali** > **Desktop/Server {scheda}** > **Impostazioni generali di scansione**, quindi selezionare **Escludi cartelle server Microsoft Exchange in caso di installazione su server Microsoft Exchange**.

Impostazioni avanzate

Tipo di scansione	Opzione
Scansione in tempo reale	**Esegui scansione dei messaggi POP3**: per impostazione predefinita, Scansione e-mail può analizzare solo i nuovi messaggi inviati mediante la porta 110 nella cartella della posta in arrivo e della posta indesiderata. Questa funzione non supporta il POP3 protetto (SSL-POP3). • Microsoft Outlook 2007, 2010 o 2013 • Mozilla Thunderbird 1.5 o versione successiva Scansione e-mail non è in grado di individuare i rischi alla sicurezza nei messaggi IMAP. Per rilevare i rischi alla sicurezza e lo spam nei messaggi IMAP, utilizzare il Messaging Security Agent (solo Advanced).
Scansione in tempo reale, scansione manuale	**Scansione unità collegate e cartelle condivise nella rete**: selezionare questa opzione per analizzare le directory posizionate fisicamente su altri computer, ma mappate sul computer locale.
Scansione in tempo reale	**Scansione disco floppy a fine sessione**:
Scansione in tempo reale	**Attiva IntelliTrap**: IntelliTrap rileva il codice dannoso, come ad esempio i bot contenuti nei file compressi. Vedere *IntelliTrap a pagina D-3*.
Scansione in tempo reale	**Varianti di malware in quarantena rilevate in memoria**: se la scansione in tempo reale e il monitoraggio del comportamento sono abilitati e si seleziona questa opzione, la memoria del processo in esecuzione viene analizzata per rilevare malware compresso. Qualsiasi malware compresso rilevato dal monitoraggio del comportamento viene messo in quarantena.
Scansione in tempo reale, scansione manuale e scansione pianificata	**Esegui scansione dei file compressi fino al livello:**: Un file compresso dispone di un livello per ciascuna compressione. Se un file infetto è stato compresso su più livelli, è necessario analizzarlo in ciascuno dei livelli per rilevare l'infezione. La scansione di più livelli, tuttavia, richiede più tempo e risorse.

Tipo di scansione	Opzione
Scansione in tempo reale, scansione manuale e scansione pianificata	**Modifica elenco Approvati spyware/grayware**: non è possibile configurare questa impostazione dalla console dell'agent.
Scansione manuale, Scansione pianificata	**Utilizzo CPU/Velocità di scansione**: il Security Agent è in grado di sospendere l'attività al termine della scansione di un file prima di passare al successivo. Selezionare le opzioni desiderate tra le seguenti: • **Alto**: nessuna sospensione tra le scansioni • **Medio**: effettua una pausa tra una scansione file e quella successiva se il consumo di risorse della CPU è superiore al 50%; in caso contrario non effettua la pausa • **Basso**: effettua una pausa tra una scansione file e quella successiva se il consumo di risorse della CPU è superiore al 20%; in caso contrario non effettua la pausa
Scansione manuale, Scansione pianificata	**Esegui disinfezione avanzata**: il Security Agent interrompe le attività di software di protezione fasulli, detti anche FakeAV. L'agent utilizza anche regole di disinfezione avanzate per rilevare e interrompere in modo proattivo le applicazioni che manifestano un comportamento da falso antivirus. **Nota** Pur fornendo una protezione proattiva, la disinfezione avanzata determina anche un altro numero di falsi allarmi.

Elenco Approvati spyware/grayware

Alcune applicazioni vengono classificate da Trend Micro come spyware/grayware non perché possono essere dannose per il sistema nel quale vengono installate, ma perché potrebbero esporre il client o la rete ad attacchi da parte di minacce informatiche o hacker.

Worry-Free Business Security comprende un elenco di applicazioni potenzialmente rischiose e, per impostazione predefinita, impedisce a queste applicazioni di venire eseguite sui client.

Se i client devono eseguire delle applicazioni che Trend Micro ha classificato come spyware/grayware, sarà necessario aggiungere il nome delle applicazioni nell'elenco approvati spyware/grayware.

Scheda Azione

Di seguito sono riportate le operazioni dei Security Agent contro virus/minacce informatiche:

TABELLA 7-1. Azioni di scansione di virus/minacce informatiche

OPERAZIONE	DESCRIZIONE
Elimina	Elimina il file infetto.
Metti in quarantena	Rinomina e sposta il file infetto in una directory di quarantena temporanea sul client. I Security Agent che inviano i file in quarantena alla directory di quarantena designata, che si trova per impostazione predefinita sul Security Server. Il Security Agent codifica i file in quarantena inviati a questa directory. Se occorre ripristinare i file in quarantena, utilizzare lo strumento VSEncrypt.
Disinfetta	Prima di consentire l'accesso completo al file, disinfetta il file infetto. Se non è possibile disinfettare il file, il Security Agent esegue una seconda operazione tra le seguenti: Metti in quarantena, Elimina, Rinomina, e Ignora. Questa operazione può essere eseguita su tutti i tipi di minacce informatiche ad eccezione di virus/minacce informatiche probabili. **Nota** Alcuni file non sono disinfettabili. Per i dettagli, consultare *File non disinfettabili a pagina D-26*.
Rinomina	Modifica l'estensione dei file infetti in "`vir`". Gli utenti non possono aprire il file rinominato immediatamente ma solo se lo associano a una determinata applicazione. All'apertura del file infetto rinominato, il virus o malware in esso contenuto potrebbe entrare in azione.

Operazione	Descrizione
Ignora	Eseguita solo durante la scansione manuale o la scansione pianificata. Il Security Agent non può utilizzare questa azione di scansione durante la Scansione in tempo reale perché la mancata esecuzione di un'operazione quando si rileva un tentativo di aprire o eseguire un file infetto consente l'esecuzione di virus//minacce informatiche. Tutte le altre azioni di scansione possono essere utilizzate.
Impedisci l'accesso	Eseguita solo durante la Scansione in tempo reale. Quando il Security Agent rileva un tentativo di aprire o eseguire un file infetto, blocca immediatamente l'operazione. Gli utenti possono eliminare manualmente il file infetto.

L'azione di scansione eseguita dal Security Agent dipende dal tipo di scansione che ha rilevato lo spyware/grayware. Sebbene sia possibile configurare azioni specifiche per ciascun tipo di virus/minacce informatiche, è possibile configurare solo un'azione valida per tutti i tipi di spyware/grayware. Ad esempio, quando il Security Agent rileva qualsiasi tipo di spyware/grayware durante una scansione manuale (tipo di scansione), esegue la disinfezione (operazione) delle relative risorse di sistema.

Di seguito sono riportate le operazioni del Security Agent contro spyware/grayware:

Tabella 7-2. Azioni di scansione spyware/grayware

Operazione	Descrizione
Disinfetta	Interrompe i processi o elimina registri, file, cookie e collegamenti.
Ignora	Non esegue alcuna operazione sui componenti spyware/grayware rilevati, ma registra il rilevamento di spyware/grayware. Questa azione può essere eseguita solo durante una Scansione manuale e Scansione pianificata. Durante Scansione in tempo reale, l'azione è "Impedisci l'accesso". Il Security Agent non esegue azioni se lo spyware/grayware rilevato non è incluso nell'elenco approvati.

Operazione	Descrizione
Impedisci l'accesso	Nega all'utente l'accesso (per copia e apertura) ai componenti grayware e spyware rilevati. Questa azione può essere eseguita solo durante Scansione in tempo reale. Durante Scansione manuale e Scansione pianificata, l'azione è "Ignora".

ActiveAction

Virus/minacce informatiche di tipo diverso richiedono azioni di scansione diverse. La personalizzazione delle azioni di scansione richiede una conoscenza dei virus/malware e può essere un compito alquanto noioso. L'Security Agent utilizza ActiveAction per contrastare questi problemi.

ActiveAction è un insieme di azioni di scansione preconfigurate per virus/minacce informatiche. Se non si ha una conoscenza approfondita delle operazioni di scansione o se non si è sicuri di quali operazioni di scansione siano adatte a determinati tipi di virus/minacce informatiche, Trend Micro consiglia di affidarsi ad ActiveAction.

L'utilizzo di ActiveAction offre i vantaggi illustrati di seguito.

- ActiveAction adotta le operazioni di scansione consigliate da Trend Micro. Non è necessario dedicare tempo alla configurazione delle operazioni.
- Gli sviluppatori di virus/minacce informatiche modificano costantemente il modo in cui i virus attaccano i dispositivi. Le impostazioni di ActiveAction vengono aggiornate per fornire protezione dalle minacce più recenti e dalle modalità di attacco di virus/minacce informatiche più recenti.

La seguente tabella illustra in che modo ActiveAction gestisce i diversi tipi di virus e malware:

TABELLA 7-3. Operazioni di scansione consigliate da Trend Micro contro virus e minacce informatiche

TIPO DI VIRUS/ MALWARE	SCANSIONE IN TEMPO REALE		SCANSIONE MANUALE/ SCANSIONE PIANIFICATA	
	PRIMA OPERAZIONE	SECONDA OPERAZIONE	PRIMA OPERAZIONE	SECONDA OPERAZIONE
Programma Joke	Metti in quarantena	Elimina	Metti in quarantena	Elimina
Programma cavallo di Troia/Worm	Metti in quarantena	Elimina	Metti in quarantena	Elimina
Packer	Metti in quarantena	N.D.	Metti in quarantena	N.D.
probabile virus/ malware	Ignora	N.D.	Ignora o azione configurata dall'utente	N.D.
Virus	Disinfetta	Metti in quarantena	Disinfetta	Metti in quarantena
virus di prova	Impedisci l'accesso	N.D.	N.D.	N.D.
Altra minaccia informatica	Disinfetta	Metti in quarantena	Disinfetta	Metti in quarantena

Nota

- Alcuni file non sono disinfettabili. Per i dettagli, consultare *File non disinfettabili a pagina D-26*.
- ActiveAction non è disponibile per la scansione spyware/grayware.
- I valori predefiniti di queste impostazioni possono cambiare quando vengono resi disponibili i nuovi file di pattern.

Impostazioni avanzate

Tipo di scansione	Opzione
Scansione in tempo reale, Scansione pianificata	**Visualizza un messaggio di avviso sul desktop o server quando viene rilevato un virus/spyware**
Scansione in tempo reale, Scansione pianificata	**Visualizza un messaggio di avviso sul desktop o server quando viene rilevato un potenziale virus/spyware**
Scansione manuale, scansione in tempo reale, scansione pianificata	**Esegui disinfezione quando viene rilevato un potenziale virus/malware**: disponibile solo se si sceglie ActiveAction e se è stata personalizzata l'azione per potenziali virus/malware.

Destinazioni di scansione e azioni per i Messaging Security Agent

Configurare le seguenti impostazioni per ogni tipo di scansione (scansione manuale, scansione pianificata e scansione in tempo reale):

Scheda **Destinazione**

- Obiettivi scansione
- Impostazioni Scansione minacce ulteriori
- Esclusioni scansione

Scheda **Azione**

- Azioni scansione/ActiveAction
- Notifiche
- Impostazioni avanzate

Obiettivi scansione

Selezionare gli obiettivi di scansione:

- **Tutti i file allegati**: Vengono esclusi solo i file codificati o protetti da password.

Nota

Questa opzione garantisce la massima protezione possibile. Tuttavia, la scansione di tutti i file richiede molto tempo e numerose risorse e in determinate situazioni può risultare eccessiva. Per questo motivo, può essere opportuno limitare la quantità di file che l'agent deve includere nella scansione.

- **IntelliScan**: Sottopone a scansione i file in base al tipo di file effettivo. Vedere *IntelliScan a pagina D-2*.
- **Specifici tipi di file**: Worry-Free Business Security sottopone a scansione i tipi di file selezionati e con le estensioni specificate. In caso di più voci, separarle con un punto e virgola (;).

Selezionare le altre opzioni:

- **Attiva IntelliTrap**: IntelliTrap rileva il codice dannoso, come ad esempio i bot contenuti nei file compressi. Vedere *IntelliTrap a pagina D-3*.
- **Scansione corpo del messaggio**: Effettua la scansione del corpo di un messaggio e-mail che potrebbe contenere delle minacce incorporate.

Impostazioni Scansione minacce ulteriori

Selezionare altre minacce che l'agent dovrebbe analizzare. Per ulteriori informazioni su queste minacce, vedere *Descrizione delle minacce a pagina 1-8*.

Selezionare opzioni aggiuntive:

- **Esegui il backup del file infetto prima di disinfettare**: Worry-Free Business Security esegue il backup della minaccia prima di disinfettare. Il file copiato mediante backup viene codificato e memorizzato nella seguente directory sul client:

  ```
  <Cartella di installazione Messaging Security Agent>
  \storage\backup
  ```

  È possibile modificare la directory nella sezione **Opzioni avanzate**, sottosezione **Impostazione di backup**.

Per decodificare il file, consultare *Ripristino dei file crittografati a pagina 14-19*.

- **Non disinfettare i file compressi infetti al fine di ottimizzare le prestazioni.**

Esclusioni scansione

Nella scheda **Destinazione**, raggiungere la sezione **Esclusioni** e selezionare tra i seguenti criteri quelli che l'agent utilizzerà per l'esclusione dei messaggi e-mail durante le scansioni:

- **Le dimensioni del corpo del messaggio superano**: Messaging Security Agent esegue la scansione dei messaggi e-mail solo se la dimensione del corpo del messaggio è inferiore o equivalente al valore specificato.
- **Le dimensioni dell'allegato superano**: Messaging Security Agent esegue la scansione dei messaggi e-mail solo se la dimensione del file allegato è inferiore o equivalente al valore specificato.

Suggerimento

Trend Micro consiglia di impostare un limite di 30 MB.

- **Il conteggio di file decompressi supera**: Se la quantità di file decompressi contenuti in un file compresso supera questo valore, Messaging Security Agent esegue la scansione dei file solo fino al limite impostato da questa opzione.
- **Le dimensioni del file decompresso superano**: Messaging Security Agent esegue la scansione solo dei file compressi con una dimensione inferiore o corrispondente a quella indicata dopo la decompressione.
- **Il numero di livelli di compressione supera**: Il Messaging Security Agent esegue la scansione solo dei file compressi con un numero di livelli specificati inferiore o corrispondente a quello indicato. Ad esempio, se si imposta il limite su 5 livelli di compressione, Messaging Security Agent esegue la scansione dei primi 5 livelli dei file compressi, ma non dei file compressi con 6 o più livelli.
- **Le dimensioni del file decompresso sono "n" volte quelle del file compresso**: Messaging Security Agent esegue la scansione dei file

compressi solo se il rapporto tra la dimensione dei file decompressi e quella dei file compressi è inferiore al valore specificato. Questa funzione impedisce a Messaging Security Agent di analizzare un file compresso che potrebbe causare un attacco DoS (Denial of Service). Questo tipo di attacco si verifica quando le risorse di un server di posta sono sovraccariche a causa di operazioni inutili. Se si impedisce a Messaging Security Agent di analizzare i file che decompressi assumono dimensioni notevoli, questo problema non dovrebbe verificarsi.

Esempio: nella tabella sottostante, il valore inserito come valore "n" è 100.

DIMENSIONE FILE (NON COMPRESSO)	DIMENSIONE FILE (NON COMPRESSO)	RISULTATO
500 KB	10 KB (rapporto 50:1)	Scansione eseguita
1.000 KB	10 KB (rapporto 100:1)	Scansione eseguita
1.001 KB	10 KB (il rapporto supera 100:1)	Scansione non eseguita *
2.000 KB	10 KB (rapporto 200:1)	Scansione non eseguita *

* Messaging Security Agent esegue sui file esclusi l'operazione indicata dall'utente.

Operazioni di scansione

Gli amministratori possono configurare Messaging Security Agent in modo che esegua le operazioni in base al tipo di minaccia rappresentata da virus/minacce informatiche, cavalli di Troia e worm. Se si utilizzano le operazioni personalizzate, impostare un'azione per ciascun tipo di minaccia.

TABELLA 7-4. Azioni personalizzate di Messaging Security Agent

AZIONE	DESCRIZIONE
Disinfetta	Rimuove il codice dannoso dal corpo e dagli allegati dei messaggi. Il rimanente testo del messaggio e-mail e qualsiasi altro file non infetto e i file disinfettati vengono consegnati ai relativi destinatari. Trend Micro consiglia di utilizzare l'azione di scansione predefinita Disinfetta per virus/minacce informatiche. In alcune circostanze, Messaging Security Agent non è in grado di disinfettare un file. Durante una scansione manuale o pianificata, il Messaging Security Agent aggiorna l'archivio informazioni e sostituisce il file con quello disinfettato.
Sostituisci con testo/file	Elimina il contenuto infetto/filtrato e lo sostituisce con testo o file. Il messaggio e-mail viene consegnato al destinatario, ma il testo sostitutivo comunica che il contenuto originale era infetto ed è stato sostituito. Per il Filtro dei contenuti e la Prevenzione della perdita di dati, è possibile sostituire esclusivamente il testo nei campi del corpo o allegati (e non in Da, A, Cc o Oggetto).
Metti in quarantena intero messaggio	(Solo Scansione in tempo reale) Sposta nella cartella della quarantena solo il contenuto infetto e il destinatario riceve il messaggio privo di tale contenuto. Per Filtro dei contenuti, Prevenzione della perdita di dati e Blocco allegati, sposta l'intero messaggio nella directory di quarantena.
Parte del messaggio in quarantena	(Solo Scansione in tempo reale) Sposta nella cartella di quarantena solo il contenuto infetto o filtrato e il destinatario riceve il messaggio privo di tale contenuto.
Elimina intero messaggio	(Solo Scansione in tempo reale) Elimina l'intero messaggio e-mail. Il destinatario originale non riceverà il messaggio.
Ignora	Registra l'infezione da virus o i file dannosi nei registri dei virus ma non esegue alcuna azione. I file esclusi, codificati o protetti da password vengono consegnati al destinatario senza che sia effettuato l'aggiornamento dei registri. Per il Filtro dei contenuti, consegna il messaggio così com'è.

Azione	Descrizione
Archivia	Sposta il messaggio nella directory di archiviazione e consegna il messaggio al destinatario originale.
Inserisci messaggio nella cartella di quarantena spam lato server	Invia il messaggio al Security Server per la quarantena.
Inserisci in quarantena il messaggio nella cartella di spam utente	Invia il messaggio alla cartella di spam dell'utente per la quarantena. La cartella si trova lato server nell'Archivio informazioni.
Contrassegna e recapita	Aggiunge un contrassegno alle informazioni dell'intestazione del messaggio e-mail che lo identifica come spam, quindi lo spedisce al destinatario originale.

Oltre a queste operazioni, è anche possibile configurare:

- **Attiva operazione per comportamento di invio di posta di massa**: Selezionare Disinfetta, Sostituisci con testo/file, Elimina intero messaggio, Ignora o Parte del messaggio in quarantena per le minacce con comportamento di invio di posta di massa.
- **In caso di disinfezione non riuscita, esegui la seguente operazione**: Impostare l'operazione secondaria per i tentativi di disinfezione non riusciti. Selezionare Sostituisci con testo/file, Elimina intero messaggio, Ignora o Metti in quarantena la parte infetta del messaggio.

ActiveAction

La seguente tabella illustra in che modo ActiveAction gestisce i diversi tipi di virus e malware:

TABELLA 7-5. Operazioni di scansione consigliate da Trend Micro contro virus e minacce informatiche

TIPO DI VIRUS/ MALWARE	SCANSIONE IN TEMPO REALE		SCANSIONE MANUALE/ SCANSIONE PIANIFICATA	
	PRIMA OPERAZIONE	SECONDA OPERAZIONE	PRIMA OPERAZIONE	SECONDA OPERAZIONE
Virus	Disinfetta	Elimina intero messaggio	Disinfetta	Sostituisci con testo/file
Programma cavallo di Troia/Worm	Sostituisci con testo/file	N.D.	Sostituisci con testo/file	N.D.
Packer	Parte del messaggio in quarantena	N.D.	Parte del messaggio in quarantena	N.D.
Altro codice dannoso	Disinfetta	Elimina intero messaggio	Disinfetta	Sostituisci con testo/file
Ulteriori minacce	Parte del messaggio in quarantena	N.D.	Sostituisci con testo/file	N.D.
Comportamento di invio di posta di massa	Elimina intero messaggio	N.D.	Sostituisci con testo/file	N.D.

Notifiche operazioni di scansione

Selezionare **Notifica ai destinatari** per impostare il Messaging Security Agent in modo che avvisi i destinatari interessati e che intervengano in caso di specifici messaggi di e-mail. Per diversi motivi, è possibile evitare di notificare ai destinatari di e-mail il blocco di un messaggio contenente informazioni sensibili. Selezionare **Non notificare a destinatari esterni** per inviare le notifiche solo ai destinatari di messaggi interni. Definire indirizzi interni da **Operazioni** > **Impostazioni di notifica** > **Definizione posta interna**.

Inoltre, è possibile anche disattivare l'invio di notifiche ai destinatari esterni dei mittenti di spoofing.

Impostazioni avanzate (operazioni di scansione)

Impostazioni	Dettagli

Macro	I virus da macro sono specifici per applicazione e infettano le utilità macro che accompagnano le applicazioni. La Scansione avanzata delle macro utilizza tecniche di scansione euristica per l'individuazione di virus delle macro, oppure elimina tutti i codici macro rilevati. La scansione euristica è un metodo valutativo di rilevamento dei virus che utilizza il riconoscimento dei pattern e tecnologie basate sulle regole per ricercare codice delle macro dannoso. Questo metodo risulta particolarmente efficace per il rilevamento di virus e minacce ancora non scoperti per i quali non esistono impronte virali note.
	
	Il Messaging Security Agent interviene contro codici macro dannosi a seconda dell'operazione configurata.
	
	• **Livello euristico**
	  • Il livello 1 utilizza i criteri più specifici, ma rileva un numero inferiore di codici macro.
	  • Il livello 4 permette di rilevare il numero più elevato possibile di codici macro, ma utilizza i criteri meno specifici e potrebbe pertanto identificare erroneamente del codice macro dannoso all'interno di codice macro sicuro.
	
	Suggerimento
	Trend Micro consiglia il livello di scansione euristico 2. Questo livello offre infatti un tasso di rilevamento elevato per l'individuazione dei virus da macro sconosciuti, rapidità nella scansione e utilizza soltanto le regole necessarie per controllare le stringhe di virus da macro. Il livello 2 è inoltre caratterizzato da un tasso ridotto di rilevamenti di codice dannoso all'interno di codice macro sicuro.
	
	• **Elimina tutte le macro rilevate dalla scansione avanzata delle macro**. Elimina tutti i codici di macro rilevati nei file analizzati

Parti non analizzabili dei messaggi	Impostare l'azione e la condizione di notifica per i file codificati e/o protetti da password. Per l'azione, selezionare Sostituisci con testo/file, Metti in quarantena intero messaggio, Elimina intero messaggio, Ignora o Parte del messaggio in quarantena.

Impostazioni	Dettagli
Parti escluse dei messaggi	Impostare l'azione e la condizione di notifica per le parti dei messaggi che sono state escluse. Per l'azione, selezionare Sostituisci con testo/file, Metti in quarantena intero messaggio, Elimina intero messaggio, Ignora o Parte del messaggio in quarantena.
Impostazione di backup	Percorso dove salvare il backup dei file infetti prima che l'agent li disinfetti.
Impostazioni di sostituzione	Configurare il testo e il file del testo sostitutivo. Se l'azione consiste nel **sostituire con testo/file**, Worry-Free Business Security sostituisce la minaccia con questa stringa di testo e questo file.

Capitolo 8

Gestione degli aggiornamenti

In questo capitolo vengono descritti i componenti di Worry-Free Business Security e le procedure di aggiornamento.

Panoramica sugli aggiornamenti

Tutti gli aggiornamenti ai componenti hanno origine dal server Trend Micro ActiveUpdate. Quando sono disponibili aggiornamenti, il Security Server scarica i componenti aggiornati e li distribuisce ai Security Agenti e ai Messaging Security Agent (solo Advanced).

Se un Security Server gestisce un numero elevato di Security Agent, l'aggiornamento potrebbe utilizzare una grande quantità risorse del computer server e influire quindi sulla stabilità e sulle prestazioni del server. Per ovviare a questo problema, Worry-Free Business Security dispone della funzione **Update Agent** che consente ad alcuni Security Agent di condividere l'attività di distribuzione degli aggiornamenti agli altri Security Agent.

La tabella seguente contiene la descrizione delle diverse opzioni di aggiornamento del Security Server e degli agent e i consigli su quando utilizzarle:

TABELLA 8-1. Opzioni di aggiornamento

SEQUENZA DI AGGIORNAMENTO	DESCRIZIONE	RACCOMANDAZIONE
1. Server ActiveUpdate o origine aggiornamenti personalizzata 2. Security Server 3. Agent	Trend Micro Security Server riceve i componenti aggiornati dal server ActiveUpdate (o da un'origine di aggiornamento personalizzata) e li implementa direttamente sugli agent (Security Agent e Messaging Security Agent).	Utilizzare questo metodo se non ci sono sezioni ad ampiezza di banda ridotta tra il Security Server e gli agent.

Sequenza di aggiornamento	Descrizione	Raccomandazione
1. Server ActiveUpdate o origine aggiornamenti personalizzata 2. Security Server 3. Update Agent, Messaging Security Agent, Security Agent senza Update Agent 4. Tutti gli altri Security Agent	Trend Micro Security Server riceve i componenti aggiornati dal server ActiveUpdate (o da un'origine di aggiornamenti personalizzata) e li distribuisce direttamente su: • Update Agent • Messaging Security Agent • Security Agent senza Update Agent Gli Update Agent quindi implementano i componenti sui rispettivi Security Agent. Se tali Security Agent non sono in grado di eseguire l'aggiornamento, vengono aggiornati direttamente dal Security Server.	Se ci sono sezioni ad ampiezza di banda ridotta tra il Security Server e i Security Agent, utilizzare questo metodo per bilanciare il carico del traffico nella rete.
1. Server ActiveUpdate 2. Security Agent	I Security Agent non in grado di eseguire l'aggiornamento da nessuna origine si aggiornano direttamente dal server ActiveUpdate. **Nota** I Messaging Security Agents non vengono mai aggiornati direttamente dal server ActiveUpdate. Se nessuna origine è disponibile, il Messaging Security Agent esce dal processo di aggiornamento.	Questo meccanismo viene fornito solo come ultima risorsa e richiede quanto segue: Attivare **Usa Trend Micro ActiveUpdate come origine aggiornamenti secondaria** in Privilegi di aggiornamento

Componenti da aggiornare

Worry-Free Business Security utilizza i componenti per proteggere gli agenti dalle minacce più recenti. Mantenere tali componenti aggiornati eseguendo aggiornamenti manuali o pianificati.

È possibile visualizzare l'elenco dei componenti attraverso le operazioni seguenti:

- Accedere a **Aggiornamenti** > **Manuale**.
- Accedere a **Stato in tempo reale** e fare clic su **Verifica stato componente** nel widget Stato agent.

Nella seguente tabella sono riportati i componenti che il Security Server scarica dal server ActiveUpdate:

TABELLA 8-2. Componenti di messaggistica (solo Advanced)

COMPONENTE	DISTRIBUITO A	DESCRIZIONE
Pattern anti-spam di Messaging Security Agent	Messaging Security Agent	Il pattern anti-spam individua lo spam più recente nei messaggi e-mail e negli allegati.
Motore di scansione anti-spam di Messaging Security Agent a 32 e a 64 bit	Messaging Security Agent	Il motore anti-spam rileva lo spam più recente nei messaggi e-mail e negli allegati.
Motore di scansione Messaging Security Agent a 32 e a 64 bit	Messaging Security Agent	Il motore di scansione rileva worm Internet, invii di posta di massa, Cavalli di Troia, siti di phishing, spyware, vulnerabilità di rete e virus nei messaggi e-mail e negli allegati.
Motore di filtraggio degli URL Messaging Security Agent a 32 e a 64 bit	Messaging Security Agent	Il motore di filtro URL consente la comunicazione tra Worry-Free Business Security e il servizio di filtro URL di Trend Micro. Il servizio di filtro URL è un sistema che valuta gli URL e trasmette a Worry-Free Business Security le informazioni sulla valutazione.

TABELLA 8-3. Antivirus e Smart Scan

COMPONENTE	DISTRIBUITO A	DESCRIZIONE
Pattern antivirus	Security Agent che utilizzano la scansione convenzionale	Il Pattern antivirus contiene informazioni che consentono agli Security Agent di identificare i virus, i malware e le minacce di tipo misto più recenti. Trend Micro crea e rilascia nuove versioni del pattern antivirus diverse volte a settimana e ogni volta che vengono scoperti virus e malware particolarmente dannosi.
Pattern IntelliTrap	Security Agent	Il pattern IntelliTrap rileva i file compressi in tempo reale impacchettati come file eseguibili. Per i dettagli, consultare *IntelliTrap a pagina D-3*.
Pattern eccezioni IntelliTrap	Security Agent	Il Pattern eccezioni IntelliTrap contiene un elenco dei file compressi "approvati".
Motore di scansione virus a 32 e a 64 bit	Security Agent	Tutti i prodotti Trend Micro si basano su un motore di scansione, sviluppato in origine in risposta ai primi virus basati su file. Il motore di scansione attuale è eccezionalmente sofisticato ed è in grado di rilevare tipi di diversi di virus e minacce informatiche. Il motore di scansione rileva inoltre virus controllati sviluppati e utilizzati a fini di ricerca. Piuttosto che eseguire la scansione di ogni singolo byte di ciascun file, il motore e il file di pattern interagiscono per identificare quanto segue: • Caratteri riconoscibili del codice del virus • Esatta posizione del virus all'interno di un file

Componente	Distribuito a	Descrizione
Pattern per Smart Scan	Non distribuito agli Security Agent. Questo pattern rimane nel Security Server e viene usato per rispondere alle query di scansione ricevute dagli Security Agent.	Nella modalità Smart Scan gli Security Agent utilizzano due pattern leggeri che vengono integrati per fornire lo stesso livello di protezione dei pattern anti-malware e anti-spyware convenzionali. **Pattern per Smart Scan** contiene la maggior parte delle definizioni dei pattern. **Pattern agente Smart Scan** contiene tutte le altre definizioni dei pattern non disponibili in Pattern per Smart Scan. L'Security Agent esegue la scansione delle minacce per la sicurezza utilizzando **Pattern agente Smart Scan**. Gli Security Agent che non sono in grado di determinare il rischio del file durante la scansione, verificano il rischio inviando una query di scansione a Scan Server, un servizio gestito dal server Security Server. Il server di scansione verifica il rischio tramite **Pattern per Smart Scan**. L'Security Agent memorizza i risultati della query di scansione forniti da Scan Server per migliorare le prestazioni della scansione.
Pattern agente Smart Scan	Security Agent che utilizzano Smart Scan	
Modello Damage Cleanup	Security Agent	Il Modello Damage Cleanup viene utilizzato dal Motore Damage Cleanup per individuare i file dei Cavalli di Troia e i relativi processi e consentire al motore di eliminarli.
Motore Damage Cleanup a 32 e a 64 bit	Security Agent	Il Motore Damage Cleanup esegue la scansione per rilevare cavalli di Troia e i relativi processi e li rimuove.

Componente	Distribuito a	Descrizione
Pattern di scansione memoria	Security Agent	Questa tecnologia permette la scansione avanzata dei virus per rilevare virus polimorfici e di mutazione e aumenta le scansioni basate sui pattern dei virus emulando l'esecuzione dei file. I risultati sono quindi analizzati in ambiente controllato per individuare indicazioni di intenzioni dannose con impatto limitato sulle prestazioni del sistema.
Motore di intelligence contestuale a 32/64 bit	Security Agent	Il motore di intelligence contestuale monitora i processi eseguiti da file a bassa prevalenza ed estrae caratteristiche di comportamento che vengono inviate per l'analisi dall'Responsabile delle query di intelligence contestuale al motore di Intelligenza computazionale predittiva.
Pattern intelligenza contestuale	Security Agent	Il pattern di intelligenza contestuale contiene un elenco di comportamenti "approvati" non rilevanti per le minacce note.
Responsabile delle query di intelligence contestuale a 32/64 bit	Security Agent	La Gestione query di intelligenza contestuale elabora i comportamenti individuati dal Motore di intelligenza contestuale e ne invia la segnalazione al motore di Intelligenza computazionale predittiva.
Motore avanzato scansione minacce a 32/64 bit	Security Agent	Il Motore avanzato scansione minacce estrae le caratteristiche dai file a bassa prevalenza e invia le relative informazioni al motore di Intelligenza computazionale predittiva.
Pattern avanzato correlazione minacce	Security Agent	Il Pattern avanzato correlazione minacce contiene un elenco di caratteristiche di file che non sono rilevanti per le minacce note.

Componente	Distribuito a	Descrizione
Driver Early Boot Cleanup a 32/64 bit	Security Agent	Il Driver Early Boot Cleanup Trend Micro viene caricato prima dei driver del sistema operativo e permette il rilevamento e il blocco dei rootkit caricati all'avvio. Dopo il caricamento dell'Security Agent, il Driver Early Boot Cleanup di Trend Micro richiama Damage Cleanup Services per disinfettare il rootkit.

Tabella 8-4. Anti-spyware

Componente	Distribuito a	Descrizione
Motore di scansione dello spyware/ grayware v.6 a 32 e a 64 bit	Security Agent	Il motore di scansione spyware/grayware esegue la scansione alla ricerca di spyware/ grayware e quindi esegue le azioni appropriate.
Pattern spyware/ grayware versione 6	Security Agent	Il pattern spyware/grayware identifica la presenza di spyware/grayware in file e programmi, moduli in memoria, registro di Windows e collegamenti degli URL.
Pattern spyware/ grayware	Security Agent	

Tabella 8-5. Virus di rete

Componente	Distribuito a	Descrizione
Pattern comune per firewall	Security Agent	Come il pattern antivirus, anche il pattern comune per firewall è utile agli agent per individuare le firme dei virus, sequenze univoche di bit e byte che segnalano la presenza di un virus di rete.

TABELLA 8-6. Monitoraggio del comportamento e Controllo dispositivo

COMPONENTE	DISTRIBUITO A	DESCRIZIONE
Pattern di rilevamento monitoraggio del comportamento a 32 e a 64 bit	Security Agent	Questo pattern contiene le regole per l'individuazione del comportamento sospetto delle minacce.
Driver principale per il monitoraggio del comportamento a 32 e a 64 bit	Security Agent	Questo driver in modalità kernel controlla gli eventi di sistema e li inoltra al Servizio principale monitoraggio del comportamento per implementare i criteri.
Servizio principale monitoraggio del comportamento a 32 e a 64 bit	Security Agent	Questo servizio in modalità utente ha le seguenti funzioni: • Rileva rootkit • Regola l'accesso ai dispositivi esterni • Protegge file, chiavi di registro e servizi
Pattern di configurazione monitoraggio del comportamento	Security Agent	Driver monitoraggio del comportamento utilizza questo pattern per individuare gli eventi di sistema normali ed escluderli dall'implementazione dei criteri.
Pattern Damage Recovery	Security Agent	Il pattern Damage Recovery contiene i criteri utilizzati per monitorare comportamenti minacciosi sospetti.
Pattern firma digitale	Security Agent	Questo pattern contiene un elenco di firme digitali valide utilizzate da Servizio principale monitoraggio del comportamento per determinare se un programma responsabile di un evento di sistema è sicuro.
Pattern implementazione dei criteri	Security Agent	Il Servizio principale monitoraggio del comportamento verifica gli eventi del sistema rispetto ai criteri in questo pattern.

Componente	Distribuito a	Descrizione
Pattern per l'attivazione della scansione memoria (32/64 bit)	Security Agent	Il servizio di attivazione della scansione di memoria esegue altri motori di scansione quando rileva che il processo in memoria è estratto.
Pattern di monitoraggio della scansione del programma	Security Agent	Il pattern di monitoraggio della scansione del programma monitora e memorizza i punti di scansione utilizzati per il monitoraggio del comportamento.
Pattern di tracciamento delle minacce a 32/64 bit	Security Agent	Il Pattern di tracciamento delle minacce identifica gli attacchi di malware senza file

Tabella 8-7. Attacchi al browser

Componente	Distribuito a	Descrizione
Pattern di prevenzione contro gli attacchi al browser	Security Agent	Questo pattern identifica gli ultimi attacchi al browser Web ed evita che possano comprometterlo.
Pattern unificato relativo allo Script Analyzer	Security Agent	Questo pattern analizza gli script delle pagine Web e identifica quelli dannosi.

Tabella 8-8. Intelligenza computazionale predittiva

Componente	Distribuito a	Descrizione
Modello di file locale di Intelligenza computazionale predittiva	Security Agent	Il Modello di file locale di Intelligenza computazionale predittiva identifica le minacce ai file eseguibili portabili quando i dispositivi si disconnettono da Internet.

Hotfix, patch e service pack

Dopo il rilascio ufficiale di un prodotto, Trend Micro spesso sviluppa gli elementi seguenti per risolvere problemi, migliorare le prestazioni del prodotto oppure aggiungere nuove funzionalità:

- *Patch critica a pagina D-2*
- *Hotfix a pagina D-2*
- *Patch a pagina D-9*
- *Service Pack a pagina D-25*

Quando questi elementi vengono resi disponibili, l'utente viene informato dal rivenditore o dal fornitore dell'assistenza. Per informazioni sulla pubblicazione di nuovi hotfix, patch e service pack, consultare il sito Web di Trend Micro:

http://downloadcenter.trendmicro.com/index.php?regs=IT

Tutte le pubblicazioni includono un file readme che contiene informazioni su installazione, implementazione e configurazione. Prima di eseguire l'installazione, leggere attentamente il file readme.

Aggiornamenti del Security Server

Aggiornamenti automatici

Il Security Server esegue automaticamente i seguenti aggiornamenti:

- Immediatamente dopo l'installazione del Security Server, si aggiorna dal server Trend Micro ActiveUpdate.
- Ad ogni avvio di Security Server vengono aggiornati i componenti.
- Per impostazione predefinita, gli aggiornamenti pianificati avvengono ogni ora (la frequenza di aggiornamento è modificabile nella console Web).

Aggiornamenti manuali

È possibile eseguire gli aggiornamenti manuali dalla console Web, se un aggiornamento è urgente.

Suggerimenti e promemoria per l'aggiornamento del server

- Dopo un aggiornamento, il Security Server distribuisce automaticamente i componenti aggiornati agli agent. Per dettagli sui componenti distribuiti agli agent, vedere *Componenti da aggiornare a pagina 8-4*.
- Un Security Server IPv6 puro non può svolgere le seguenti operazioni:
  - Ottenere aggiornamenti direttamente dal server Trend Micro ActiveUpdate o da un'origine di aggiornamento personalizzata IPv4.
  - Distribuire aggiornamenti direttamente ad agent IPv4 puri.

  Analogamente, un Security Server IPv4 puro non può ottenere aggiornamenti direttamente da un'origine di aggiornamento personalizzata IPv6 pura e distribuire aggiornamenti ad agent IPv6 puri.

  In queste situazioni, è necessario un server proxy dual-stack in grado di convertire gli indirizzi IP, come ad esempio DeleGate, per consentire al Security Server di ottenere e distribuire gli aggiornamenti.
- Se per connettersi a Internet si utilizza un server proxy, utilizzare le impostazioni del proxy corrette in **Amministrazione** > **Impostazioni globali** > **Proxy** per scaricare correttamente gli aggiornamenti.

Duplicazione dei componenti

Trend Micro rilascia i file di pattern a cadenza regolare, in modo da mantenere aggiornata la protezione del client. Poiché gli aggiornamenti dei file di pattern sono disponibili regolarmente, il Security Server utilizza un meccanismo chiamato **duplicazione dei componenti** per un download più rapido dei file di pattern.

Quando la versione più recente di un file di pattern completo è disponibile per il download dal server Trend Micro ActiveUpdate, sono disponibili anche pattern incrementali. I pattern incrementali sono versioni ridotte del file di pattern completo che colmano la differenza tra l'ultima versione del file di pattern e le versioni precedenti. Ad esempio, se la versione più recente è la 175, il pattern incrementale v_173.175 contiene firme presenti nella versione 175 e non presenti nella versione 173 (la versione 173 è la versione precedente del pattern completo in quanto i numeri di pattern aumentano a

intervalli di 2). Il pattern incrementale v_171.175 contiene i dati presenti nella versione 175 e non presenti nella versione 171.

Per ridurre il traffico di rete generato quando si scarica il pattern più recente, il Security Server esegue la duplicazione dei componenti, un metodo di aggiornamento dei componenti in cui il server scarica solo i pattern incrementali. Per sfruttare la duplicazione dei componenti, verificare che il Security Server venga aggiornato regolarmente. Diversamente, il server verrà forzato a scaricare il file di pattern completo.

La duplicazione dei componenti si applica ai seguenti componenti:

- Pattern antivirus
- Pattern per Smart Scan Agent
- Modello Damage Cleanup
- Pattern eccezioni IntelliTrap
- Pattern spyware

Configurazione dell'origine di aggiornamento del Security Server

Informazioni preliminari

Per impostazione predefinita, il Security Server preleva gli aggiornamenti dal server Trend Micro ActiveUpdate. Specificare un'origine di aggiornamento personalizzata se il Security Server non è in grado di raggiungere il server ActiveUpdate direttamente.

- Se l'origine è il **Server ActiveUpdate di Trend Micro**, accertarsi che il server disponga di connessione a Internet e, se in caso di server proxy, provare se la connessione a Internet è disponibile utilizzando le impostazioni del proxy. Per i dettagli, consultare *Configurazione delle impostazioni del proxy Internet a pagina 11-3*.
- Se l'origine è un'origine di aggiornamento personalizzata (**Percorso intranet contenente una copia del file corrente** o **Altra fonte di aggiornamento**), configurare l'ambiente e le risorse di aggiornamento

opportune per questa origine di aggiornamento. Accertarsi, inoltre, che la connessione tra il Security Server e l'origine aggiornamenti funzioni. Per ottenere supporto per la configurazione di un'origine di aggiornamento, contattare l'assistenza tecnica.

- Un Security Server IPv6 puro non può aggiornarsi direttamente dal server Trend Micro ActiveUpdate o da qualsiasi origine di aggiornamento personalizzata IPv4 pura. Analogamente, un Security Server IPv4 puro non è in grado di eseguire l'aggiornamento direttamente da origini personalizzate IPv6 pure. Per consentire a un Security Server di connettersi alle origini aggiornamenti, è necessario un server proxy dual-stack in grado di convertire gli indirizzi IP, come ad esempio DeleGate.

Procedura

1. Accedere a **Aggiornamenti** > **Origine**.
2. Nella scheda **Server**, selezionare un'origine di aggiornamento.
   - **Server ActiveUpdate di Trend Micro**
   - **Percorso intranet contenente una copia del file corrente**: Digitare il percorso dell'origine nel formato Universal Naming Convention (UNC), ad esempio `\\Web\ActiveUpdate`. Inoltre, specificare le credenziali di accesso (nome utente e password) utilizzate dal Security Server per connettersi a questa origine.
   - **Altra fonte di aggiornamenti**: Immettere l'URL per questa origine. Accertarsi che la directory virtuale HTTP destinazione (condivisione Web) sia disponibile per il Security Server.
3. Fare clic su **Salva**.

Aggiornamento manuale del Security Server

Aggiornare manualmente i componenti nel Security Server dopo aver installato o aggiornato il server e quando si verifica un'infezione.

Procedura

1. Avviare l'aggiornamento manuale in due modi:
   - Andare su **Aggiornamenti** > **Manuale**.
   - Andare su **Stato in tempo reale** e fare clic su **Verifica stato componente** nel widget Stato agent.

   Viene visualizzata la schermata **Aggiornamento manuale**.
2. Selezionare i componenti da aggiornare.

   Per ulteriori informazioni sui componenti, vedere *Componenti da aggiornare a pagina 8-4*.
3. Fare clic su **Aggiorna ora**.

   Compare una nuova schermata che mostra lo stato dell'aggiornamento. Se l'aggiornamento termina correttamente, il Security Server distribuisce automaticamente i componenti aggiornati agli agent.

Configurazione degli aggiornamenti pianificati per il Security Server

Configurare il Security Server in modo che controlli regolarmente la propria fonte aggiornamenti e scarichi automaticamente gli aggiornamenti eventualmente disponibili. L'aggiornamento pianificato rappresenta un modo semplice ed efficace per assicurare il continuo aggiornamento della protezione contro le minacce.

In presenza di virus/minacce informatiche, Trend Micro risponde velocemente alle richieste di aggiornamento dei file di pattern antivirus (la frequenza può essere superiore a quella settimanale). Vengono aggiornati regolarmente anche il motore di scansione e altri componenti. Trend Micro consiglia di aggiornare i componenti ogni giorno (o con maggiore frequenza, in caso di virus/minacce informatiche conclamati) per essere certi che l'agent si serva dei componenti più aggiornati.

Importante

Evitare di pianificare una scansione e un aggiornamento nello stesso momento. In situazioni del genere, la scansione pianificata può subire interruzioni impreviste.

Procedura

1. Accedere ad **Aggiornamenti** > **Pianificato**.
2. Selezionare i componenti da aggiornare.

   Per ulteriori informazioni sui componenti, vedere *Componenti da aggiornare a pagina 8-4*.
3. Fare clic sulla scheda **Pianificazione**, quindi specificare la pianificazione dell'aggiornamento.
   - **Gli aggiornamenti della scansione convenzionale** includono tutti i componenti, salvo Pattern per Smart Scan e Pattern agente Smart Scan. Scegliere tra aggiornamenti giornalieri, settimanali e mensili, quindi specificare un valore per **Aggiorna per un periodo di**, ovvero l'orario durante il quale il Security Server esegue l'aggiornamento. Gli aggiornamenti del Security Server potranno verificarsi in qualsiasi momento all'interno di tale intervallo temporale.

     Nota

     Per gli aggiornamenti pianificate mensili (sconsigliate), se si selezionano 31, 30 o 29 giorni e un mese ha meno di questo numero di giorni, l'aggiornamento non viene eseguito per quel mese.
   - Gli **Aggiornamenti alla Smart Scan** includono solo Pattern per Smart Scan e Pattern agente Smart Scan.
4. Fare clic su **Salva**.

Rollback dei componenti

Il termine rollback si riferisce all'azione di ripristino della versione precedente del Virus Pattern, di Pattern agente Smart Scan e del Motore di scansione virus. Se questi componenti non funzionano correttamente, ripristinare le versioni precedenti. Il Security Server conserva la versione attuale e quella precedente del Motore di scansione virus e le ultime tre versioni di Virus Pattern e Pattern agente Smart Scan.

Nota

Il rollback è consentito solo per i componenti riportati sopra.

Worry-Free Business Security utilizza diversi motori di scansione per agenti che eseguono piattaforme a 32 e a 64 bit. Questi motori di scansione devono essere ripristinati separatamente. La procedura di ripristino per tutti i tipi di motore di scansione è identica.

Procedura

1. Accedere a **Aggiornamenti** > **Rollback**.
2. Fare clic su **Sincronizza** per un componente specifico per indicare agli agenti di sincronizzare le versioni del componente alla versione presente sul server.
3. Fare clic su **Rollback** per un componente specifico per eseguire il rollback di quel componente su Security Server e sugli agenti.

Aggiornamenti di Security Agent e Messaging Security Agent

Aggiornamenti automatici

Security Agent e Messaging Security Agent (solo Advanced) eseguono automaticamente i seguenti aggiornamenti:

- Immediatamente dopo l'installazione, gli agent si aggiornano dal Security Server.
- Ogni volta che il Security Server completa un aggiornamento, effettua automaticamente il push degli aggiornamenti sugli agent.
- Ogni volta che un Update Agent completa un aggiornamento, effettua automaticamente il push degli aggiornamenti sui rispettivi Security Agent.
- Per impostazione predefinita, gli aggiornamenti pianificati vengono eseguiti:
  - Ogni 8 ore sui Security Agent in ufficio
  - Ogni 2 ore sui Security Agent fuori ufficio
- Per impostazione predefinita, il Messaging Security Agent esegue un aggiornamento pianificato ogni 24 ore alle ore 12:00.

Esecuzione di un aggiornamento manuale

Security Agent riceve automaticamente gli aggiornamenti da Security Server.

È inoltre possibile eseguire l'aggiornamento manualmente se si è temporaneamente scollegati dalla rete dell'ufficio oppure è necessario ottenere con urgenza la protezione più aggiornata contro le minacce alla sicurezza (ad esempio, dopo un'infezione).

Se si utilizza un server proxy per la connessione a Internet, verificare che siano configurate le corrette impostazioni proxy.

Procedura

1. Aprire la console principale e fare clic su **Aggiornamento**.

   Nota

   Per eseguire un aggiornamento manuale, è anche possibile fare clic con il pulsante destro del mouse sull'icona Security Agent, nella barra delle applicazioni di Windows, e poi scegliere **Aggiorna ora**.

2. Al termine dell'aggiornamento, fare clic su **Chiudi**.

Suggerimenti e promemoria per l'aggiornamento di un agent

- I Security Agent si aggiornano da Security Server, Update Agent oppure dal server Trend Micro ActiveUpdate.

  I Messaging Security Agent si aggiornano solo dal Security Server.

  Per informazioni dettagliate sul processo di aggiornamento, fare riferimento a *Panoramica sugli aggiornamenti a pagina 8-2*.

- Un agent IPv6 puro non è in grado di ottenere aggiornamenti direttamente da un Security Server/Update Agent e da un server Trend Micro ActiveUpdate IPv4 puri.

  Similmente, un agent IPv4 puro non può ottenere aggiornamenti direttamente da un Security Server/Update Agent IPv6 puro.

  In queste situazioni, è necessario un server proxy dual-stack in grado di convertire gli indirizzi IP, come ad esempio DeleGate, per consentire all'agent di ottenere gli aggiornamenti.

- Per dettagli sui componenti aggiornati dall'agent, vedere *Componenti da aggiornare a pagina 8-4*.

- Oltre ai componenti, gli agent ricevono file di configurazione aggiornati durante l'aggiornamento dal Security Server. Gli agent necessitano dei file di configurazione per applicare nuove impostazioni. Ogni volta che

si modificano le impostazioni di un agent attraverso la console Web, vengono modificati anche i file di configurazione.

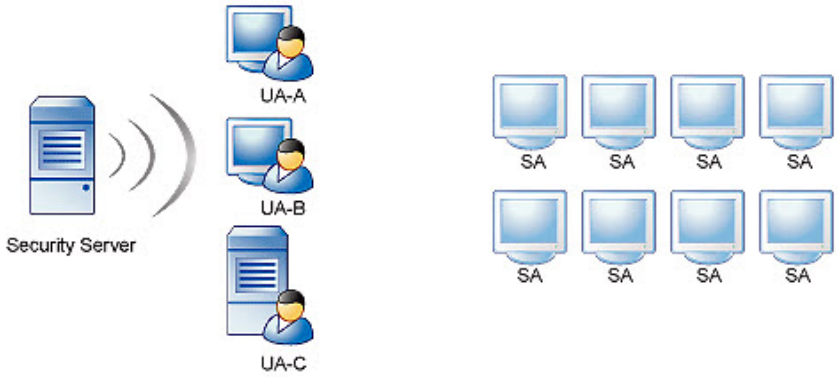
Update Agent

Gli Update Agent sono Security Agent in grado di ricevere i componenti aggiornati dal Security Server o dal server ActiveUpdate e di implementarli in altri Security Agent.

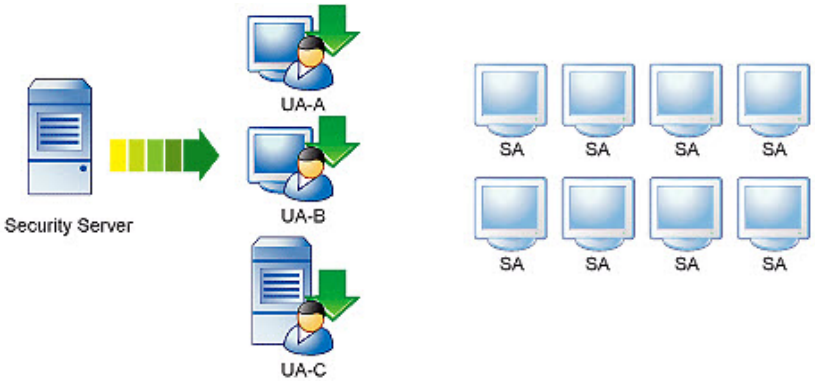
Se si individuano sezioni della rete tra i client e Trend Micro Security Server come "a bassa ampiezza di banda" o "a traffico intenso", è possibile specificare che i Security Agent fungano da Update Agent. Gli Update Agent riducono il consumo di ampiezza di banda facendo in modo che non sia più necessario per tutti i Security Agent accedere al Security Server per gli aggiornamenti dei componenti. Ad esempio, se la rete è segmentata per sede e il collegamento di rete tra i segmenti è caratterizzato da un frequente carico di traffico elevato, Trend Micro consiglia di fare in modo che almeno un Security Agent di ciascun segmento agisca da Update Agent.

Il processo di aggiornamento dell'Update Agent può essere descritto nel modo seguente:

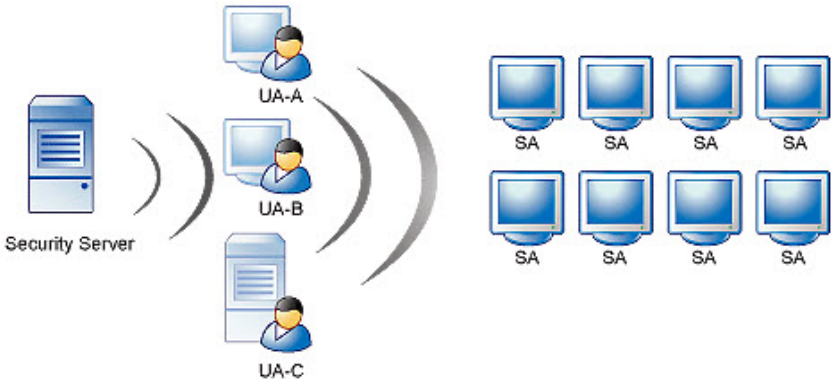
1. Il Security Server notifica agli Update Agent che sono disponibili nuovi aggiornamenti.



2. Gli Update Agent scaricano i componenti aggiornati dal Security Server.

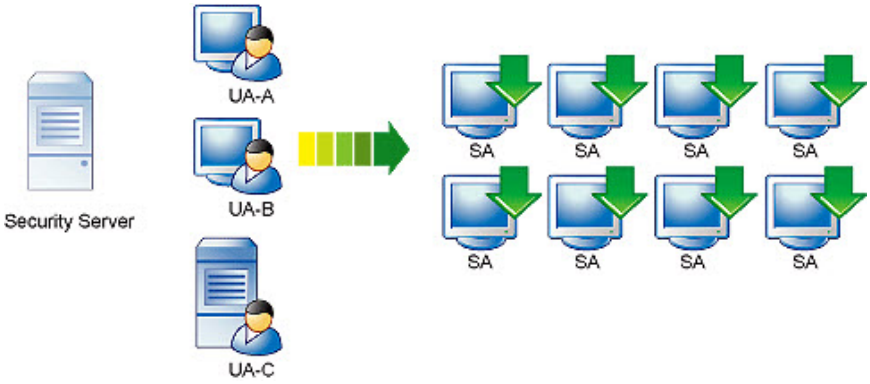


3. Il Security Server invia una notifica ai Security Agent per segnalare che i componenti aggiornati sono disponibili.



4. Ciascun Security Agent carica una copia della Update Agent Order Table per determinare l'origine dell'aggiornamento appropriata. L'ordine degli Update Agent nella Update Agent Order Table viene determinato inizialmente dall'ordine in cui sono stati aggiunti come Origini di aggiornamento alternative sulla console Web. Ciascun Security Agent esamina una voce della tabella alla volta, cominciando dalla prima, fino a quando identifica propria origine di aggiornamento.

5. I Security Agent scaricano quindi i componenti aggiornati dal rispettivo Update Agent. Se, per qualche motivo, l'Update Agent assegnato non è disponibile, il Security Agent tenta di scaricare i componenti aggiornati dal Security Server.



Configurazione degli Update Agent

Procedura

1. Accedere a **Aggiornamenti** > **Origine**.
2. Fare clic sulla scheda **Update Agent**.
3. Effettuare le operazioni riportate di seguito:

Operazione	Passaggi
Assegnazione di Security Agent come Update Agent	a. Nella sezione **Assegna Update Agent**, fare clic su **Aggiungi**. Viene visualizzata una nuova schermata. b. Dalla casella a discesa, selezionare uno o più agenti che fungano da Update Agent. c. Fare clic su **Salva**. La schermata si chiude. d. Ritornati alla sezione **Assegna Update Agent**, selezionare **Update Agent eseguono sempre l'aggiornamento solo da Security Server** se si desidera che gli Update Agent eseguano sempre il download dei componenti aggiornati dal Security Server anziché da un altro Update Agent.
Configurazione dell'aggiornamento dei Security Agent da parte degli Update Agent	a. Nella sezione **Origini di aggiornamento alternative**, selezionare **Attiva origini di aggiornamento alternative per Security Agent e Update Agent**. **Nota** La disattivazione di questa opzione comporta l'aggiornamento dei Security Agent da parte degli Update Agent, riportando l'origine di aggiornamento al Security Server. b. Fare clic su **Aggiungi**. Viene visualizzata una nuova schermata. c. Digitare gli indirizzi IP dei Security Agent che saranno aggiornati da un Update Agent. • Immettere un intervallo di indirizzi IPv4. Per specificare un singolo Security Agent, immettere l'indirizzo IP del Security Agent nei campi **da** e **a**. • Immettere una lunghezza o un prefisso IP per IPv6. d. Selezionare un Update Agent nell'elenco a discesa. Se l'elenco a discesa non è disponibile, non è stato configurato alcun Update Agent.

OPERAZIONE	PASSAGGI
	e. Fare clic su **Salva**. La schermata si chiude. f. Definire più intervalli IP, secondo le esigenze. Se sono stati definiti svariati intervalli IP, è possibile impostare la priorità dell'intervallo IP tramite l'opzione **Riordina**. Quando il Security Server notifica ai Security Agent la disponibilità di nuovi aggiornamenti, questi esaminano l'elenco degli intervalli IP per individuare l'origine di aggiornamento corretta. Il Security Agent esamina la prima voce dell'elenco e prosegue fino a quando non individua l'origine di aggiornamento appropriata. **Suggerimento** definire svariati Update Agent per lo stesso intervallo IP come misura contro il failover. Ciò significa che se i Security Agent non sono in grado di eseguire l'aggiornamento dall'Update Agent, provano con altri Update Agent. A tale scopo, creare almeno due (2) voci con lo stesso intervallo IP e assegnare a ciascuna un Update Agent diverso.
Rimozione di Update Agent	Per rimuovere gli Update Agent e annullare l'assegnazione di tutti i Security Agent assegnati, accedere alla sezione **Assegna Update Agent**, selezionare la casella di controllo corrispondente al Nome computer dell'Update Agent e fare clic su **Rimuovi**. Questa azione non comporta la rimozione dell'intervallo di indirizzi IP del Security Agent nella sezione **Origini di aggiornamento alternative** ma fa sì che i Security Agent "orfani" riportino l'origine dell'aggiornamento al Security Server. Se si dispone di un altro Update Agent, è possibile assegnarlo ai Security Agenti orfani.
Annullamento dell'assegnazione dei Security Agent agli Update Agent	Se non si desidera che i Security Agent appartenenti a un intervallo di indirizzi IP siano aggiornati da un Update Agent, accedere alla sezione **Origini di aggiornamento alternative**, selezionare la casella di controllo corrispondente all'intervallo di indirizzi IP dei Security Agent e fare clic su **Rimuovi**.

4. Fare clic su **Salva**.

Capitolo 9

Utilizzo dello stato in tempo reale

Stato in tempo reale

Worry-Free Business Security fornisce i widget che vengono utilizzati come riferimenti visivi rapidi per la gestione del Security Agent.

La schermata **Stato in tempo reale** viene visualizzata quando si apre la console Web Worry-Free Business Security o si fa clic su **Stato in tempo reale** nel menu principale.

TABELLA 9-1. Widget Stato in tempo reale

WIDGET	DESCRIZIONE
Action center	Questo widget mostra gli eventi che richiedono agli amministratori di eseguire le opportune operazioni allo scopo di risolvere i problemi.
Rilevamenti dei rischi per la sicurezza nel tempo	Questo widget fornisce una panoramica degli endpoint presenti nella rete, unitamente ai rilevamenti delle minacce e ai tipi di minacce che interessano la rete per un intervallo di tempo specifico.
Riepilogo ransomware	Questo widget fornisce una panoramica di tutti i tentativi di attacchi ransomware per un intervallo di tempo specifico.
Stato della licenza	Questo widget fornisce una panoramica dell'utilizzo delle postazioni e dello stato di scadenza della licenza.
Riepilogo server Exchange	Questo widget fornisce una panoramica dello stato di connessione dei Messaging Security Agent e una distribuzione dei rilevamenti delle minacce negli server Exchange.
Stato agente	Questo widget fornisce una panoramica della connessione e dello stato di aggiornamento dei Security Agent presenti nella rete.

La frequenza di aggiornamento delle informazioni visualizzate nella schermata **Stato in tempo reale** varia in base alla sezione. In genere, la frequenza è compresa tra 1 e 10 minuti. Per aggiornare manualmente le informazioni visualizzate nella schermata, fare clic sul pulsante **Aggiorna** del browser.

Centro azioni

Questo widget mostra gli eventi che richiedono agli amministratori di eseguire le opportune operazioni allo scopo di risolvere i problemi.

Alcuni eventi sono dotati di pulsanti d'azione consigliati. Fare clic sui pulsanti per tentare di risolvere i problemi; in alternativa, fare clic sugli eventi per visualizzare altri dettagli.

TABELLA 9-2. Eventi del Centro azioni

EVENTO	CONSIGLIO
Antivirus: minacce irrisolte	Eseguire una scansione utilizzando lo Strumento Trend Micro HouseCall.
Antivirus - Scansione in tempo reale disattivata negli endpoint	Attivare Scansione in tempo reale in tutti i dispositivi per rimanere protetti.
Antivirus - Scansione in tempo reale disattivata sui server Exchange	Attivare Scansione in tempo reale in tutti i server Exchange per rimanere protetti.
Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo	Riavviare i dispositivi per rimuovere completamente le minacce rilevate.
Eventi correlati alla licenza	Andare su **Amministrazione** > **Licenza del prodotto** per verificare lo stato della licenza.
Risorse insufficienti - Spazio su disco rimanente inferiore a %threshold%	Eseguire lo strumento Disk Cleaner per eliminare file di backup, registro e pattern inutilizzati. Per ulteriori informazioni, vedere *Risparmio di spazio su disco a pagina 14-15*.
Servizi Smart Protection - Servizio non disponibile	Controllare lo stato di Smart Scan Server nella console di Worry-Free Business Security e assicurarsi che il server funzioni in modo corretto.

Evento	Consiglio
Aggiornamento - Almeno un Messaging Security Agent non aggiornato dopo un'ora dal rilascio del pattern	Assicurarsi che gli aggiornamenti pianificati per i Messaging Security Agent siano abilitati in Security Server e che i Messaging Security Agent possano connettersi a Internet.
Aggiornamento - Velocità di implementazione inferiore al %threshold% dopo un'ora dal rilascio del pattern	Verificare la connessione Internet di Security Agent e aggiornare nuovamente Security Agent.
Aggiornamento - Componenti di Security Server non aggiornati per più di %threshold% giorni	Assicurarsi che gli aggiornamenti pianificati per i componenti siano attivati in Security Server e che questo possa connettersi a Internet.
Aggiornamento - Pattern per Smart Scan non aggiornato per più di %threshold% ore	Assicurarsi che gli aggiornamenti pianificati per il Pattern per Smart Scan siano attivati in Security Server e che questo possa connettersi a Internet.

Antivirus: minacce irrisolte

È possibile visualizzare queste informazioni facendo clic sull'evento **Antivirus - minacce irrisolte: %N%** nell'Action Center. Worry-Free Business Security genera o aggiorna queste informazioni del registro ogni volta che viene eseguita una scansione in tempo reale, manuale o pianificata.

- Fare clic su **Scarica strumento** per scaricare lo Strumento Trend Micro HouseCall e utilizzare il tool per eseguire una scansione sul dispositivo coinvolto.
- Fare clic su **Elimina da Centro azioni** per passare alla schermata **Stato in tempo reale** e rimuovere l'evento di notifica dall'Action center. I registri relativi agli eventi in questa schermata sono sempre disponibili tramite Query registro.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora dell'ultimo tentativo non riuscito di disinfettare o rimuovere il virus o il malware
Nome dispositivo	Nome del dispositivo interessato
Nome virus/malware	Nome del virus o del malware rilevato Fare clic sul collegamento per visitare l'Enciclopedia delle minacce di Trend Micro, che offre descrizioni approfondite delle minacce informatiche, comprese le istruzioni per rimuovere manualmente gli attacchi della minaccia selezionata.
Nome file	Nome del file danneggiato dal virus o dal malware
Percorso	Posizione del file infetto
Tipo di scansione	Tipo di scansione utilizzato per rilevare il virus o il malware
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento di virus o malware

Antivirus - Scansione in tempo reale disattivata negli endpoint

È possibile visualizzare queste informazioni facendo clic sull'evento **Antivirus - Scansione in tempo reale disattivata negli endpoint: %N%** nel Centro azioni.

- Fare clic su **Attiva scansione in tempo reale** per attivare la scansione in tutti i dispositivi.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Nome dispositivo	Nome del dispositivo con Scansione in tempo reale disattivata
Nome del gruppo	Nome del gruppo a cui appartiene il dispositivo

Antivirus - Scansione in tempo reale disattivata sui server Exchange

È possibile visualizzare queste informazioni facendo clic sull'evento **Antivirus - Scansione in tempo reale disattivata sui server Exchange: %N%** nel Centro azioni.

- Fare clic su **Attiva scansione in tempo reale** per attivare la scansione in tutti i server Exchange.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Nome del server Exchange	Nome del server Exchange con Scansione in tempo reale disattivata

Anti-spyware: rilevamenti che richiedono il riavvio del dispositivo

È possibile visualizzare queste informazioni facendo clic sull'evento **Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo: %N%** nell'Action center.

- Fare clic su **Elimina da Centro azioni** per passare alla schermata **Stato in tempo reale** e rimuovere l'evento di notifica dall'Action center. I registri relativi agli eventi in questa schermata sono sempre disponibili tramite Query registro.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sul rilevamento di spyware o malware in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato

Colonna	Descrizione
Nome spyware/grayware	Nome dello spyware o del grayware rilevato Fare clic sul collegamento per visitare l'Enciclopedia delle minacce di Trend Micro, che offre descrizioni approfondite delle minacce informatiche, comprese le istruzioni per rimuovere manualmente gli attacchi della minaccia selezionata.
Tipo di scansione	Tipo di scansione utilizzato per rilevare lo spyware o il grayware

Risorse insufficienti - Spazio su disco rimanente

È possibile visualizzare queste informazioni facendo clic sull'evento **Risorse insufficienti - Spazio su disco rimanente inferiore a %threshold%** nel Centro azioni.

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Nome server	Nome del server con spazio su disco insufficiente
Nome del gruppo	Nome del gruppo a cui appartiene il server

Aggiornamento: Agent non aggiornati

È possibile visualizzare queste informazioni facendo clic sull'evento **Aggiornamento - Velocità di implementazione inferiore al %threshold% dopo un'ora dal rilascio del pattern** nel Centro azioni. I Security Agent elencati in questa schermata richiedono aggiornamenti di motore o pattern.

- Fare clic su **Aggiorna ora** per indicare ai Security Agent non aggiornati di effettuare l'aggiornamento ai componenti più recenti.
- Fare clic su **Verifica stato componente** per aprire la schermata **Aggiornamento manuale**.

- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Nome dispositivo	Nome del dispositivo che richiede aggiornamenti di componente
Nome del gruppo	Nome del gruppo a cui appartiene il dispositivo
Metodo di scansione	• Smart Scan • Scansione convenzionale

Aggiornamento - Messaging Security Agent non aggiornati

È possibile visualizzare queste informazioni facendo clic sull'evento **Aggiornamento - Almeno un Messaging Security Agent non aggiornato dopo un'ora dal rilascio del pattern** nel Centro azioni.

- Fare clic su **Aggiorna ora** per indicare ai Messaging Security Agent non aggiornati di effettuare l'aggiornamento ai componenti più recenti.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Nome del server Exchange	Nome del server Exchange che richiede aggiornamenti di componenti

Rilevamenti dei rischi per la sicurezza nel tempo

Questo widget fornisce una panoramica degli endpoint presenti nella rete, unitamente ai rilevamenti delle minacce e ai tipi di minacce che interessano la rete per un intervallo di tempo specifico.

- Fare clic su o per alternare le diverse visualizzazioni.
- Fare clic sulla scheda **Minacce note**, **Minacce sconosciute** o **Violazioni dei criteri** per visualizzare le informazioni sul rilevamento per le minacce selezionate.

Visualizza	Descrizione
Grafico ( )	• Fare clic sui nomi dei tipi di minaccia alla fine del grafico per mostrare/nascondere le informazioni relative al rilevamento nel grafico. • Passare con il mouse sui nodi relativi a un determinato giorno per visualizzare il numero totale di rilevamenti per i tipi di minaccia visualizzati. Fare clic su un nodo per tornare alla schermata dei registri relativa al tipo di minaccia evidenziato in elenco.
Tabella ( )	• Fare clic sul conteggio dei rilevamenti per aprire la schermata dei registri che fornisce un elenco dei dettagli sui rilevamenti.

Rilevamenti dei rischi per la sicurezza: virus/malware

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce note** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Virus/malware** nella visualizzazione tabella
- Qualsiasi nodo di **Virus/malware** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	La data e l'ora in cui Security Agent ha segnalato le informazioni di rilevamento virus o malware a Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato

Colonna	Descrizione
Nome virus/malware	Nome del virus o del malware rilevato Fare clic sul collegamento per visitare l'Enciclopedia delle minacce di Trend Micro, che offre descrizioni approfondite delle minacce informatiche, comprese le istruzioni per rimuovere manualmente gli attacchi della minaccia selezionata.
Nome file	Nome del file danneggiato dal virus o dal malware
Percorso	Posizione del file infetto
Tipo di scansione	Tipo di scansione utilizzato per rilevare il virus o il malware
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento di virus o malware

Rilevamenti dei rischi per la sicurezza: Spyware/Grayware

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce note** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Spyware/Grayware** nella visualizzazione tabella
- Qualsiasi nodo di **Spyware/Grayware** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sul rilevamento di spyware o malware in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato Fare clic sul nome per visualizzare un elenco di spyware o grayware singoli rilevati nel dispositivo.

Colonna	Descrizione
Nome spyware/grayware	Nome dello spyware o del grayware rilevato
Tipo di scansione	Tipo di scansione utilizzato per rilevare lo spyware o il grayware
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento di spyware o grayware

Rilevamenti dei rischi per la sicurezza: Reputazione Web

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce note** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Reputazione Web** nella visualizzazione tabella
- Qualsiasi nodo di **Reputazione Web** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione degli URL in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che tenta di eseguire l'accesso a un URL vietato
URL	URL vietato
Livello di rischio	Classificazione assegnata da TrendLabs in base alla facilità di infezione e al danno potenziale.

Rilevamenti dei rischi per la sicurezza: Virus di rete

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce note** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Virus di rete** nella visualizzazione tabella
- Qualsiasi nodo di **Virus di rete** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	La data e l'ora in cui il Security Agent ha segnalato le informazioni di rilevamento di virus di rete a Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato
IP aggressore	Indirizzo IP dell'aggressore
IP vittima	Indirizzo IP della vittima
Direzione del pacchetto	Direzione del pacchetto
Nome virus di rete	Nome del virus di rete rilevato
Conteggio	Ciascun virus di rete viene conteggiato ad ogni rilevamento.

Rilevamenti dei rischi per la sicurezza: Monitoraggio del comportamento

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce sconosciute** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Monitoraggio del comportamento** nella visualizzazione tabella
- Qualsiasi nodo di **Monitoraggio del comportamento** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

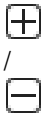
Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione del monitoraggio del comportamento in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che ha attivato la violazione di un criterio
Minaccia alla sicurezza	Tipo di minaccia alla sicurezza
Oggetto	Oggetto dell'operazione
Tipo evento	Evento di sistema correlato
Destinazione	Destinazione dell'operazione
Operazione	Azione eseguita dall'utente che ha attivato la violazione
Risultato	Azione eseguita da Worry-Free Business Security in risposta a una violazione del monitoraggio del comportamento

Rilevamenti dei rischi per la sicurezza: Intelligenza computazionale predittiva

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Minacce sconosciute** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Intelligenza computazionale predittiva** nella visualizzazione tabella
- Qualsiasi nodo di **Intelligenza computazionale predittiva** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
	Fare clic sull'icona per espandere o chiudere i dettagli del registro sotto la riga della tabella.
Data/Ora	La data e l'ora in cui Security Agent ha segnalato le informazioni di rilevamento a Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato
Nome del gruppo	Nome del gruppo a cui appartiene il dispositivo
Minaccia sconosciuta	Nome della minaccia probabile
Probabilità di minaccia	Indica il livello di aderenza del file/processo rispetto al modello di malware
Nome file	Nome dell'oggetto di file o del programma che ha eseguito il processo **Importante** Il nome di file rilevato per questo rilevamento potrebbe non essere uguale al nome di file rilevato in altri endpoint. Intelligenza computazionale predittiva associa i rilevamenti in base ai valori di hash del file, non a nomi di file specifici.
Percorso	Percorso dell'oggetto di file o del programma che ha eseguito il processo
Canale di infezione	Canale da cui ha avuto origine la minaccia
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento

Rilevamento dei rischi per la sicurezza: dettagli di Intelligenza computazionale predittiva

È possibile visualizzare queste informazioni facendo clic su qualsiasi icona
nella prima colonna nella schermata dei registri di **Rilevamento dei rischi per la sicurezza: Intelligenza computazionale predittiva**.

La sezione dei dettagli del registro è composta da due schede:

- **Minaccia sconosciuta**: fornisce i risultati dell'analisi di Intelligenza computazionale predittiva
- **Nome file**: fornisce dettagli generali correlati alle proprietà del file e informazioni di certificato per questo specifico registro di rilevamento

Suggerimento

Fare clic su **Aggiungi all'elenco delle eccezioni** per aggiungere rapidamente il valore di hash del file interessato all'Elenco eccezioni di Intelligenza computazionale predittiva. È possibile visualizzare l'intero elenco delle eccezioni nella schermata **Impostazioni globali**.

Per ulteriori informazioni, vedere *Configurazione delle impostazioni dell'Elenco eccezioni a pagina 11-14*.

Nella tabella seguente vengono discusse le informazioni fornite nella scheda **Minaccia sconosciuta**.

TABELLA 9-3. Dettagli della scheda Minaccia sconosciuta

VOCE	DESCRIZIONE
Probabilità di minaccia	Indica il livello di aderenza del file/processo rispetto al modello di malware
Tipo di minaccia probabile	Indica il tipo di minaccia più probabile contenuta nel file dopo che Intelligenza computazionale predittiva ha confrontato l'analisi con altre minacce note

Voce	Descrizione
Identificatori delle minacce	Fornisce un elenco di funzioni API utilizzate dal file/processo che potrebbero essere indicative del tipo di minaccia rilevato **Importante** L'identificazione della funzione API rappresenta un solo fattore di determinazione del tipo di minaccia. Intelligenza computazionale predittiva utilizza molte altre funzionalità e metodi di analisi dei file per calcolare la probabilità della minaccia e il tipo di minaccia probabile.
Tipo di rilevamento	Tipo di oggetto che ha attivato il rilevamento ("File" o "Processo")
Minacce note simili	Fornisce un elenco di tipi di minaccia conosciuti che presentano caratteristiche di file/processo simili per il rilevamento

Rilevamenti dei rischi per la sicurezza: Filtro URL

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Violazioni dei criteri** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Filtro URL** nella visualizzazione tabella
- Qualsiasi nodo di **Filtro URL** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione degli URL in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che tenta di eseguire l'accesso a un URL vietato

Colonna	Descrizione
URL	URL vietato

Rilevamenti dei rischi per la sicurezza: Controllo dispositivo

È possibile visualizzare queste informazioni facendo clic su uno dei seguenti collegamenti nella scheda **Violazioni dei criteri** sul widget **Rilevamenti dei rischi per la sicurezza nel tempo**:

- Il conteggio di rilevamento di **Controllo dispositivo** nella visualizzazione tabella
- Qualsiasi nodo di **Controllo dispositivo** nella visualizzazione grafico

Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	La data e l'ora in cui Security Agent ha segnalato le informazioni di violazione di Controllo dispositivo a Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che ha attivato la violazione di un criterio
Tipo	Tipo di dispositivo di archiviazione
Autorizzazione	Autorizzazione impostata per il dispositivo di archiviazione
Oggetto	Oggetto dell'operazione
Oggetto	Oggetto dell'operazione
Operazione	Operazione conclusa

Riepilogo ransomware

Questo widget fornisce una panoramica di tutti i tentativi di attacchi ransomware per un intervallo di tempo specifico.

La visualizzazione predefinita mostra un riepilogo di tutti i rilevamenti di ransomware e classifica ulteriormente i tentativi in base al canale di infezione.

- Fare clic sul conteggio del rilevamento di ransomware nella visualizzazione predefinita per aprire la schermata dei registri **Riepilogo ransomware**, che fornisce un elenco dei dettagli sui rilevamenti di ransomware.
- Utilizzare gli elenchi a discese per alternare le diverse visualizzazioni.

Fare clic su per visualizzare le informazioni sul rilevamento in un grafico.

- Passare con il mouse sui nodi relativi a un determinato giorno per visualizzare il numero totale di rilevamenti per la categoria di rilevamento visualizzata. Fare clic su un nodo per tornare alla schermata dei registri **Riepilogo ransomware**, che fornisce un elenco dei dettagli sui rilevamenti di ransomware per il giorno specifico.

Registri di Riepilogo ransomware

È possibile visualizzare queste informazioni facendo clic su un nodo nel grafico o su un conteggio di rilevamento nel widget **Riepilogo ransomware**.

- Utilizzare gli elenchi **Canale di infezione** e **Periodo** per regolare la visualizzazione.
- Fare clic su **Esporta** per salvare gli eventi del registro in un file CSV.

Colonna	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sul ransomware rilevato in Worry-Free Business Security

Colonna	Descrizione
Minaccia alla sicurezza	Tipo di ransomware • Nome virus/malware: mostra il nome di rilevamento di un file di ransomware conosciuto • Crittografia file non autorizzata: mostra quando Worry-Free Business Security ha rilevato che un programma sospetto ha crittografato un file • <URL>: mostra quando Worry-Free Business Security ha rilevato un URL collegato a ransomware
Source	Tipo di scansione che ha rilevato la minaccia
Percorso/URL	• Percorso del file di ransomware • URL infettato da ransomware
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento di ransomware
Nome dispositivo	Nome del dispositivo interessato
Canale di infezione	Canale dell'infezione ransomware
Dettagli	Fare clic su **Visualizza** per vedere i dettagli del registro.

Ransomware: dettagli registro Monitoraggio del comportamento

È possibile visualizzare queste informazioni facendo clic sul collegamento **Visualizza** nella colonna **Dettagli** nella schermata dei registri Riepilogo ransomware.

Riga	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione del monitoraggio del comportamento in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che ha attivato la violazione di un criterio

Riga	Descrizione
Minaccia alla sicurezza	Tipo di minaccia alla sicurezza
Oggetto	Oggetto dell'operazione
Tipo evento	Evento di sistema correlato
Destinazione	Destinazione dell'operazione
Operazione	Azione eseguita dall'utente che ha attivato la violazione
Risultato	Azione eseguita da Worry-Free Business Security in risposta a una violazione del monitoraggio del comportamento

Ransomware: dettagli del registro del filtro URL

È possibile visualizzare queste informazioni facendo clic sul collegamento **Visualizza** nella colonna **Dettagli** nella schermata dei registri Riepilogo ransomware.

Riga	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione degli URL in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che tenta di eseguire l'accesso a un URL vietato
URL	URL vietato
Categoria URL	Categoria dell'URL vietato
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta alla violazione degli URL

Ransomware: dettagli del registro virus

È possibile visualizzare queste informazioni facendo clic sul collegamento **Visualizza** nella colonna **Dettagli** nella schermata dei registri Riepilogo ransomware.

Riga	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sul ransomware rilevato in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo interessato
Nome virus/malware	Nome del ransomware rilevato Fare clic sul collegamento per visitare l'Enciclopedia delle minacce di Trend Micro, che offre descrizioni approfondite delle minacce informatiche, comprese le istruzioni per rimuovere manualmente gli attacchi della minaccia selezionata.
Nome file	Nome del file danneggiato dal ransomware
Percorso	Posizione del file infetto
Canale di infezione	Sistema tramite il quale il ransomware ottiene l'accesso all'endpoint
Tipo di scansione	Tipo di scansione utilizzata per rilevare il ransomware
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta al rilevamento di ransomware

Ransomware: dettagli del registro Reputazione Web

È possibile visualizzare queste informazioni facendo clic sul collegamento **Visualizza** nella colonna **Dettagli** nella schermata dei registri Riepilogo ransomware.

Riga	Descrizione
Data/Ora	Data e ora in cui Security Agent ha segnalato le informazioni sulla violazione degli URL in Worry-Free Business Security
Nome dispositivo	Nome del dispositivo che tenta di eseguire l'accesso a un URL vietato
URL	URL vietato

Riga	Descrizione
Livello di rischio	Classificazione assegnata da TrendLabs in base alla facilità di infezione e al danno potenziale.
Azione eseguita	Azione eseguita da Worry-Free Business Security in risposta alla violazione degli URL

Stato della licenza

Questo widget fornisce una panoramica dell'utilizzo delle postazioni e dello stato di scadenza della licenza.

Riepilogo server Exchange

Questo widget fornisce una panoramica dello stato di connessione dei Messaging Security Agent e una distribuzione dei rilevamenti delle minacce negli server Exchange.

Fare clic sul livello di sicurezza per configurare il livello di rilevamento dello spam per Messaging Security Agent.

Colonna	Description
Server	Nome del server Exchange
Evento	Tipo di spam e-mail
Rapporto	Uguale al numero di rilevamenti diviso il numero di messaggi della scansione

Stato agent

Questo widget fornisce una panoramica della connessione e dello stato di aggiornamento dei Security Agent presenti nella rete.

- Fare clic sul conteggio accanto allo stato per effettuare il reindirizzamento alla schermata **Dispositivi**, in cui vengono elencati i dettagli del dispositivo per lo stato particolare.

- Fare clic su **Aggiungi dispositivi** per effettuare il reindirizzamento alla schermata **Aggiungi dispositivi**, in cui è possibile installare il Security Agent su più dispositivi.

  Per ulteriori informazioni, vedere *Installazione degli Agent a pagina 3-1*.

- Fare clic su **Verifica stato componente** per effettuare il reindirizzamento alla schermata **Aggiornamento manuale**, in cui è possibile visualizzare le informazioni del componente più recenti.

  Per ulteriori informazioni, vedere *Componenti da aggiornare a pagina 8-4*.

Capitolo 10

Gestione delle notifiche

In questo capitolo viene descritto l'utilizzo delle varie opzioni di notifica.

Utilizzo delle notifiche

Per mantenere al minimo la quantità di tempo di cui gli amministratori necessitano per monitorare Worry-Free Business Security e per assicurarsi che gli amministratori ricevano avvisi preventivi via e-mail relativi a situazioni di possibili infezioni, impostare il server per l'invio di notifiche ad ogni manifestazione di eventi anomali nella rete.

Per impostazione predefinita, tutti gli eventi elencati nella schermata **Notifiche** sono selezionati e attivano l'invio da parte del server di notifiche agli amministratori.

TABELLA 10-1. Notifiche che richiedono un'azione

TIPO EVENTO	DESCRIZIONE
Eventi di minacce	
Antivirus: minacce irrisolte	Le azioni intraprese contro le minacce di virus/malware sono risultate inefficaci. Il conteggio di rilevamento non include la seguente azione di scansione: Ignorato un potenziale rischio per la sicurezza
Antivirus - Scansione in tempo reale disattivata negli endpoint	La scansione in tempo reale è disattivata negli endpoint.
Antivirus - Scansione in tempo reale disattivata sui server Exchange	Scansione in tempo reale è disattivata sui server Exchange.
Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo	È necessario che gli endpoint con rilevamenti di spyware/grayware vengano riavviati per rimuovere completamente le minacce.
Eventi di sistema	
Aggiornamento - Agent non aggiornati	I Security Agent non aggiornati richiedono un aggiornamento dei componenti.
Aggiornamento - Messaging Security Agent non aggiornati	I Messaging Security Agent non aggiornati richiedono un aggiornamento dei componenti.

Tipo evento	Descrizione
Aggiornamento - Pattern per Smart Scan non aggiornato	I Pattern per Smart Scan richiedono un aggiornamento dei pattern.
Aggiornamento - Componenti di Security Server non aggiornati	I Security Server non aggiornati richiedono un aggiornamento dei componenti.
Servizi Smart Protection - Servizio non disponibile	I Security Agent configurati per Smart Scan non possono collegarsi ai servizi Smart Protection oppure il servizio non è disponibile.
Risorse insufficienti - Spazio su disco rimanente	Lo spazio su disco rimanente in alcuni server è minore della percentuale specificata.
Eventi della licenza	
Licenza - Scaduta	La licenza è scaduta.
Licenza - Scade tra meno di 60 giorni	La licenza scade a breve.
Licenza - Uso di postazioni superiore al 110%	Uso di postazioni superiore al 110%.
Licenza - Uso di postazioni superiore al 100%	Uso di postazioni superiore al 100%.

Tabella 10-2. Notifiche di avviso

Tipo evento	Descrizione
Eventi di minacce	
Antivirus - Rilevamenti virus negli endpoint eccedenti:	Le minacce di virus/malware rilevate negli endpoint superano il numero indicato all'interno del periodo di tempo specificato.
Antivirus - Rilevamenti virus nei server Exchange eccedenti:	Le minacce di virus/malware rilevate nei server Exchange superano il numero indicato all'interno del periodo di tempo specificato.

Tipo evento	Descrizione
Antispyware - Rilevamenti spyware/grayware eccedenti:	Le minacce di spyware/grayware rilevate negli endpoint superano il numero indicato all'interno del periodo di tempo specificato.
Antispam - Rilevamenti spam nei messaggi totali ricevuti eccedenti:	I rilevamenti di spam nei messaggi totali ricevuti superano la percentuale specificata.
Reputazione Web - Violazioni URL eccedenti:	Le violazioni degli URL rilevate superano il numero indicato all'interno del periodo di tempo specificato.
Filtro URL - Violazioni URL eccedenti:	Le violazioni degli URL rilevate superano il numero indicato all'interno del periodo di tempo specificato.
Intelligenza computazionale predittiva - Rilevamenti delle minacce sconosciute eccedenti:	I rilevamenti delle minacce sconosciute superano il numero indicato all'interno del periodo di tempo specificato.
Monitoraggio del comportamento - Violazioni del monitoraggio del comportamento eccedenti:	Le violazioni del monitoraggio del comportamento rilevate superano il numero indicato all'interno del periodo di tempo specificato.
Virus di rete - Virus di rete rilevati eccedenti:	I rilevamenti dei virus di rete superano il numero indicato all'interno del periodo di tempo specificato.
Controllo dispositivo - Violazioni del controllo del dispositivo eccedenti:	Le violazioni del controllo del dispositivo rilevate superano il numero indicato all'interno del periodo di tempo specificato.

Configurazione degli eventi per le notifiche

Worry-Free Business Security offre tre metodi di consegna delle notifiche:

- Notifiche SNMP
- Registro eventi di Windows
- Notifica e-mail

Procedura

1. Andare su **Amministrazione** > **Notifiche**.
2. Per ricevere notifiche SNMP, configurare la sezione **Destinatario della notifica SNMP**.

   Simple Network Management Protocol (SNMP) è un protocollo utilizzato per la gestione della rete. Per visualizzare i dati del trap SNMP, utilizzare un browser Management Information Base.

   a. Selezionare **Attiva notifiche SNMP**.

   b. Specificare l'indirizzo IP per il trap SNMP.

   c. Specificare la stringa della community SNMP.
3. Per ricevere le notifiche dei registri degli eventi di Windows, selezionare **Scrivi nel registro eventi di Windows** in **Registrazione**.
4. Per ricevere notifiche e-mail, specificare il mittente e i destinatari.

   Suggerimento

   Separare più voci con punto e virgola (;).
5. Fare clic sulla scheda **Azione richiesta** o **Avvisi**.
6. Selezionare le caselle di controllo che corrispondono ai tipi di eventi per cui si desidera ricevere notifiche nella colonna **Notifica e-mail**.
7. Se disponibile nella colonna **Soglia avviso**, specificare il numero di rilevamenti o violazioni all'interno di ciascun periodo di tempo che attivano una notifica.
8. Per personalizzare la riga dell'oggetto e il corpo del messaggio di ciascuna notifica degli eventi, fare clic sul collegamento di notifica nella colonna **Tipo**.

   Per ulteriori informazioni sulla personalizzazione delle notifiche, vedere *Variabili token a pagina 10-6*.

9. Fare clic su **Salva**.

Variabili token

Utilizzare le variabili token per personalizzare la riga dell'oggetto e il corpo del messaggio delle notifiche degli eventi.

Per evitare che messaggi e-mail provenienti da indirizzi con domini esterni siano etichettati come spam, aggiungere gli indirizzi e-mail esterni agli elenchi Mittenti approvati per Anti-spam.

I seguenti token rappresentano gli eventi di minacce rilevati sui desktop/server e sui server Microsoft Exchange.

Token	Description	Tipo di allarme
%COUNT	Inserisce il numero di rilevamenti	Eventi di avviso: Tutti
$CSM_SERVERNAME	Inserisce il nome del Security Server	Tutti
%DATE	Inserisce il numero di giorni rimanenti nella licenza	Licenza - Scaduta Licenza - Scade tra meno di 60 giorni

Token	Description	Tipo di allarme
%DATE_TIME	Inserisce l'ora e la data dell'evento	Antivirus: minacce irrisolte Antivirus - Scansione in tempo reale disattivata negli endpoint Antivirus - Scansione in tempo reale disattivata sui server Exchange Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo Aggiornamento - Agent non aggiornati Aggiornamento - Messaging Security Agent non aggiornati Aggiornamento - Componenti di Security Server non aggiornati Servizi Smart Protection - Servizio non disponibile Risorse insufficienti - Spazio su disco rimanente

Token	Description	Tipo di allarme
%DEVICE_COUNT	Inserisce il numero di dispositivi interessati	Antivirus: minacce irrisolte Antivirus - Scansione in tempo reale disattivata negli endpoint Antivirus - Scansione in tempo reale disattivata sui server Exchange Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo Aggiornamento - Agent non aggiornati Aggiornamento - Messaging Security Agent non aggiornati Risorse insufficienti - Spazio su disco rimanente Tutti gli eventi di avviso eccetto quanto segue: Antispam - Rilevamenti spam nei messaggi totali ricevuti eccedenti:
%FROM	Inserisce l'ora e la data di inizio dell'evento	Tutti gli eventi di avviso eccetto quanto segue: Antispam - Rilevamenti spam nei messaggi totali ricevuti eccedenti:

Token	Description	Tipo di allarme
%NUMBER	Mostra il numero di eventi	Antivirus: minacce irrisolte Antivirus - Scansione in tempo reale disattivata negli endpoint Antivirus - Scansione in tempo reale disattivata sui server Exchange Anti-spyware - rilevamenti che richiedono il riavvio del dispositivo Tutti gli eventi di avviso eccetto quanto segue: Antispam - Rilevamenti spam nei messaggi totali ricevuti eccedenti:
%SEAT_IN_USE_COUNT	Inserisce il numero di postazioni desktop/server in uso	Licenza: l'utilizzo delle postazioni è superiore al 110% Licenza: l'utilizzo delle postazioni è superiore al 100%
%SEAT_PURCHASED_COUNT	Inserisce il numero di postazioni desktop/server disponibili nella propria licenza	Licenza: l'utilizzo delle postazioni è superiore al 110% Licenza: l'utilizzo delle postazioni è superiore al 100%

Token	Description	Tipo di allarme
%THRESHOLD%	Indica la soglia di un evento	Aggiornamento - Agent non aggiornati Aggiornamento - Pattern per Smart Scan non aggiornato Aggiornamento - Componenti di Security Server non aggiornati Servizi Smart Protection - Servizio non disponibile Risorse insufficienti - Spazio su disco rimanente Licenza - Uso di postazioni superiore al 110% Licenza - Uso di postazioni superiore al 100% Eventi di avviso: Tutti
%TO	Inserisce l'ora e la data di fine dell'evento	Tutti gli eventi di avviso eccetto quanto segue: Antispam - Rilevamenti spam nei messaggi totali ricevuti eccedenti:

```
Soggetto: [Security Server - <$CSM_SERVERNAME>] [Azione
richiesta] Antivirus - Minacce irrisolte: %NUMBER
Messaggio: Notifica di Trend Micro Worry-Free Business Security
* Antivirus - Minacce irrisolte: %NUMBER
* Ora segnalazione: %DATE_TIME
* Dispositivi interessati: %DEVICE_COUNT
* Suggerimento:
  eseguire una scansione utilizzando lo strumento Trend Micro HouseCall.
```

```
Soggetto: [Security Server - Server A] [Azione richiesta]
Antivirus - Minacce irrisolte: 5
Messaggio: Notifica di Trend Micro Worry-Free Business Security
* Antivirus - Minacce irrisolte: 5
```

```
* Ora segnalazione: 14 febbraio 2018
* Dispositivi interessati: 2
* Suggerimento:
  eseguire una scansione utilizzando lo strumento Trend Micro HouseCall.
```

Capitolo 11

Gestione delle impostazioni globali

In questo capitolo vengono trattate le impostazioni globali per le impostazioni di agent e sistema del Security Server.

Impostazioni globali

La console Web consente di configurare le impostazioni globali per Security Server e Security Agent.

Scheda	Description
Proxy	Se la rete utilizza un server proxy per la connessione a Internet, specificare le impostazioni del server proxy per i seguenti servizi: • Aggiornamenti dei componenti e notifiche sulla licenza • Reputazione Web, Monitoraggio del comportamento e Smart Scan Per i dettagli, consultare *Configurazione delle impostazioni del proxy Internet a pagina 11-3*.
SMTP	Le impostazioni del server SMTP si applicano a tutte le notifiche e a tutti i rapporti generati da Security Server. Per i dettagli, consultare *Configurazione delle impostazioni del server SMTP a pagina 11-4*.
Desktop/Server	Le impostazioni di sicurezza si applicano a tutti i Security Agent. Per i dettagli, consultare *Configurazioni delle impostazioni di desktop/server a pagina 11-5*.
Sistema	Le impostazioni di sistema consentono di rimuovere automaticamente gli agent inattivi, di controllare le connessioni degli agent e di gestire la cartella di quarantena. Per i dettagli, consultare *Configurazione delle impostazioni di sistema a pagina 11-10*.
Eccezioni	L'elenco delle eccezioni consente di ignorare le impostazioni dei criteri definite in Reputazione Web, Filtro URL e Intelligenza computazionale predittiva. Per i dettagli, consultare *Configurazione delle impostazioni dell'Elenco eccezioni a pagina 11-14*.

Configurazione delle impostazioni del proxy Internet

Se Security Server e agent utilizzano un server proxy per la connessione a Internet, specificare le impostazioni del server proxy per utilizzare i seguenti servizi e funzioni Trend Micro:

- **Security Server**: aggiornamenti dei componenti e manutenzione della licenza
- **Security Agent**: Reputazione Web, Filtro URL, Monitoraggio del comportamento, Smart Feedback e Smart Scan
- **Messaging Security Agent** (solo Avanzate) Reputazione Web e Anti-spam

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.
2. Dalla scheda **Proxy**, aggiornare quanto segue secondo le esigenze:
   - Proxy Security Server

     Nota

     I Messaging Security Agent utilizzano solo le impostazioni proxy del Security Server.

     - Usa un server proxy per gli aggiornamenti e le notifiche sulla licenza
     - Utilizza protocollo proxy SOCKS 4/5
     - Address: indirizzo IPv4/IPv6 o nome host
     - Porta
     - Autenticazione del server proxy
       - Nome utente

- Password
- Proxy Security Agent
  - Utilizzare le credenziali specificate per il proxy di aggiornamento

    Nota

    I Security Agent utilizzano il server proxy e la porta di Internet Explorer per connettersi a Internet. Selezionare questa opzione solo se Internet Explorer dei client e il Security Server condividono le stesse credenziali di autenticazione.
  - Nome utente
  - Password

3. Fare clic su **Salva**.

Configurazione delle impostazioni del server SMTP

Le impostazioni del server SMTP si applicano a tutte le notifiche e a tutti i rapporti generati da Worry-Free Business Security.

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.
2. Fare clic sulla scheda **SMTP** e aggiornare i seguenti campi secondo le esigenze:
   - **Server SMTP**: indirizzo IPv4/IPv6 o il nome del server SMTP.
   - **Porta**
   - **Attiva autenticazione server SMTP**
     - Nome utente

- Password

3. Per verificare che le impostazioni sono corrette, fare clic su **Invia e-mail di prova**. Se l'invio non riesce, modificare le impostazioni o controllare lo stato del server SMTP.

4. Fare clic su **Salva**.

Configurazioni delle impostazioni di desktop/server

Le opzioni Desktop/Server riguardano le impostazioni globali Worry-Free Business Security. Le impostazioni dei gruppi individuali hanno la precedenza su queste impostazioni. Se non è stata configurata un'opzione particolare per un gruppo, vengono utilizzate le opzioni desktop/server. Ad esempio, se non è stato approvato alcun URL per un gruppo particolare, potranno essere applicati al gruppo tutti gli URL approvati presenti in questa schermata.

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.

2. Fare clic sulla scheda **Desktop/Server** e aggiornare i seguenti campi secondo le esigenze:

Impostazioni	Descrizione
Location Awareness	Location Awareness consente agli amministratori di controllare le impostazioni di sicurezza in base a come il client si collega alla rete. Location Awareness controlla le impostazioni di connessione In ufficio/Fuori ufficio. Il Security Agent identifica automaticamente il percorso del client in base alle informazioni sul gateway configurate nella console

Impostazioni	Descrizione

	Web, quindi controlla i siti Web a cui hanno accesso gli utenti. Le restrizioni variano a seconda dell'ubicazione dell'utente:
	• **Attiva Location Awareness**: queste impostazioni influiscono sulle impostazioni della connessione In ufficio/Fuori ufficio di Firewall e Reputazione Web e sulla frequenza degli aggiornamenti pianificati.
	• **Informazioni sul gateway**: i client e le connessioni presenti in questo elenco utilizzano le impostazioni di Connessione interna durante la connessione in remoto alla rete (mediante VPN) e con l'opzione Location Awareness attivata.
	  • Indirizzo IP gateway
	  • Indirizzo MAC: l'aggiunta dell'indirizzo MAC migliora notevolmente la sicurezza consentendo solo al dispositivo configurato di connettersi.
	Fare clic sull'icona di eliminazione corrispondente (x) per eliminare una voce.

Avviso assistenza tecnica	L'Avviso assistenza tecnica invia una notifica al Security Agent per informare l'utente su chi contattare per ricevere assistenza. Aggiornare le informazioni riportate di seguito, in base alle necessità: • **Etichetta Servizio di assistenza** • **Indirizzo e-mail Servizio di assistenza** • **Informazioni aggiuntive**:viene visualizzato quando l'utente passa il mouse sopra l'etichetta
Impostazioni generali di scansione	• **Disattiva Smart Scan Service**: imposta tutti i Security Agent nella modalità di scansione convenzionale. Il servizio Smart Scan non sarà disponibile finché non viene nuovamente attivato da qui. Per cambiare uno o più gruppi di Security Agent, andare su **Dispositivi** > **{Gruppo}** > **Configura criterio** > **Metodo di scansione**.

Impostazioni	Descrizione
	Nota Per le linee guida sul cambio dei metodi di scansione per i Security Agent, vedere *Configurazione dei metodi di scansione a pagina 5-5*. • **Attiva la scansione differita delle operazioni sui file**: attivare questa impostazione per migliorare temporaneamente le prestazioni del sistema. **AVVERTENZA!** L'abilitazione della scansione differita può creare rischi per la sicurezza. • **Escludi sezioni Shadow Copy**: Shadow Copy o Volume Snapshot Services effettuano copie manuali o automatiche di backup o istantanee di un file o una cartella su un volume specifico. • **Escludi la cartella del database Security Server**: impedisce agli agent installati su Security Server di sottoporre a scansione il proprio database solo durante le scansioni in tempo reale. Per impostazione predefinita, WFBS non esegue la scansione del proprio database. Trend Micro consiglia di non modificare tale impostazione per evitare che il database venga danneggiato nel corso della scansione. • **Escludi le cartelle del server Microsoft Exchange in caso di installazione su Microsoft Exchange Server**: impedisce agli agent installati sul server Microsoft Exchange di sottoporre a scansione le cartelle Microsoft Exchange. • **Escludi cartelle Microsoft Domain Controller**: impedisce agli agent installati su Domain Controller di sottoporre a scansione le cartelle Domain Controller. Queste cartelle memorizzano le informazioni dell'utente, i nomi utente, le password e le informazioni importanti.
Impostazioni di scansione antivirus	• **Configura le impostazioni di scansione per file compressi di grandi dimensioni**: specificare le dimensioni massime del

Impostazioni	Descrizione
	file estratto e il numero di file nel file compresso che il modulo Agent dovrebbe sottoporre a scansione. • **Disinfetta i file compressi**: gli agent cercano di disinfettare i file infetti all'interno di un file compresso. • **Scansione fino a { } livelli OLE**: gli agent sottopongono a scansione il numero specificato di livelli Object Linking and Embedding (OLE). La funzione OLE consente agli utenti di creare oggetti mediante un'applicazione e di collegarli o incorporarli in un'altra applicazione. Ad esempio, un file .xls incorporato in un file .doc. • **Aggiungi scansione manuale al menu dei collegamenti di Windows nei client**: aggiunge un collegamento **Scansione con Security Agent** al menu contestuale. Con questa opzione, gli utenti possono fare clic su un file o una cartella (sul desktop o in Esplora risorse di Windows) ed eseguire la scansione manuale di file o cartelle.
Impostazioni di scansione spyware/ grayware	• **Esegui la scansione cookie**: Security Agent esegue la scansione per rilevare i cookie. • **Aggiungi rilevamenti cookie al registro spyware**: aggiunge ogni cookie dello spyware individuato nel registro spyware.
Impostazioni firewall	Selezionare la casella di controllo **Disabilita firewall e disinstalla driver** per disinstallare il firewall del client Worry-Free Business Security e rimuovere i driver ad esso associati. **Nota** Se si disattiva il firewall, le impostazioni correlate non saranno disponibili fino alla riattivazione del firewall.
Protezione dalle minacce Web HTTPS	Attivare questa funzionalità per verificare gli URL HTTPS rispetto alle impostazioni di Reputazione Web e Filtro URL su Chrome, Firefox e Microsoft Edge.

Impostazioni	Descrizione
	Nota Questa funzionalità non richiede un componente aggiuntivo del browser. Per impostazione predefinita, Worry-Free Business Security verifica gli URL HTTPS su Internet Explorer utilizzando componenti aggiuntivi del browser.
Impostazioni avvisi	**Mostra l'icona di avviso sulla barra delle applicazioni di Windows se il file di pattern dei virus non è aggiornato da { } giorni**:visualizza un'icona di avviso sui client quando il file di pattern non è aggiornato da un determinato numero di giorni.
Password disinstallazione di Security Agent	• **Consenti all'utente client di disinstallare Security Agent senza password**. • **Richiedi la password per consentire all'utente client di disinstallare Security Agent**.
Password di chiusura e uscita del programma Security Agent	• **Consenti agli utenti dei client di chiudere e sbloccare Security Agent nei computer in uso senza password**. • **Richiedi agli utenti client di immettere una password per chiudere e sbloccare Security Agent**. **Nota** Lo sblocco del Security Agent permette all'utente di sostituire tutte le impostazioni configurate in **Dispositivi** > **{gruppo}** > **Configura criterio** > **Privilegi agente**.
Indirizzo IP preferito	Questa opzione è disponibile solo sui Security Server dual-stack ed è applicata solo da agent dual-stack. Quando vengono installati o aggiornati, gli agent effettuano la registrazione al Security Server con un indirizzo IP. Scegliere una delle opzioni elencate di seguito. • **Prima IPv4, poi IPv6**: gli agent utilizzano prima il proprio indirizzo IPv4. Se l'agent non è in grado di effettuare la registrazione con l'indirizzo IPv4, usa l'indirizzo IPv6. Se la registrazione non riesce con entrambi gli indirizzi IP, l'agent

Impostazioni	Descrizione
	riprova con la priorità stabilita per gli indirizzi IP per questa selezione. • **Prima IPv6, poi IPv4**: gli agent utilizzano prima il proprio indirizzo IPv6. Se l'agent non è in grado di effettuare la registrazione con l'indirizzo IPv6, usa l'indirizzo IPv4. Se la registrazione non riesce con entrambi gli indirizzi IP, l'agent riprova con la priorità stabilita per gli indirizzi IP per questa selezione.

3. Fare clic su **Salva**.

Configurazione delle impostazioni di sistema

La sezione **Sistema** della schermata **Impostazioni globali** contiene opzioni che consentono di rimuovere automaticamente gli agent inattivi, di controllare le connessioni degli agent e di gestire la cartella della quarantena.

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.
2. Fare clic sulla scheda **Sistema** e aggiornare i seguenti campi secondo le esigenze:

Impostazioni	Descrizione
Rimozione di Security Agent inattivi	Quando si utilizza il programma di disinstallazione di Security Agent su un client per rimuovere gli Agent dal client, il programma invia automaticamente una notifica al Security Server. Quando il Security Server riceve questa notifica, l'icona del client viene rimossa dalla struttura dei gruppi di protezione per segnalare che il client non esiste più Se invece il Security Agent viene rimosso con altri metodi, ad esempio riformattando il disco rigido del computer oppure eliminando manualmente i file del client, il Security Server non rileva la rimozione del Security Agent, che viene quindi visualizzato come inattivo. Se un utente rimuove o disattiva l'agent per un periodo di tempo prolungato, anche in questo caso il Security Server visualizza il Security Agent come inattivo. Per visualizzare soltanto i client attivi nella struttura dei gruppi di protezione, è possibile configurare il Security Server in modo da rimuovere automaticamente i Security Agent inattivi dalla struttura dei gruppi di protezione. • **Attiva rimozione automatica dei Security Agent inattivi**: consente la rimozione automatica dei client che non si sono collegati al Security Server per un determinato numero di giorni. • **Rimuovi automaticamente un Security Agent se resta inattivo per {} giorni**: indica il numero di giorni per il quale un client può rimanere inattivo prima di essere rimosso dalla console Web.

Impostazioni	Descrizione

Verifica connessione agente	Worry-Free Business Security riporta per mezzo di icone lo stato della connessione del client nella struttura dei gruppi di protezione. Tuttavia, alcune condizioni potrebbero impedire alla struttura dei gruppi di protezione di visualizzare correttamente lo stato della connessione dell'agent. Se, ad esempio, il cavo della rete di un agent viene involontariamente scollegato, il client non sarà in grado di notificare a Trend Micro Security Server di essere momentaneamente offline. Nella struttura di gestione dei gruppi il client verrà pertanto visualizzato ancora come in linea.
	
	Dalla console Web è possibile controllare manualmente o in modo programmato la connessione tra agent e server.
	
	Nota
	La verifica della connessione non consente la selezione di gruppi o agent specifici. Essa controlla la connessione di tutti gli agent registrati con il Security Server.
	
	• **Attiva la verifica pianificata**: attiva la verifica pianificata della connessione tra agent e server.
	  • **Ogni ora**
	  • **Ogni giorno**
	  • **Ogni settimana, ogni**
	  • **Ora di inizio**: l'orario in cui dovrebbe iniziare la verifica.
	• **Verifica ora**: prova immediatamente la connettività.

Impostazioni	Descrizione
Manutenzione della quarantena	Per impostazione predefinita, i Security Agent inviano i file infetti in quarantena alla directory seguente nel Security Server: `<Cartella di installazione Security Server>\PCCSRV\Virus` Se è necessario modificare la directory (ad esempio, se lo spazio su disco non è sufficiente), digitare un percorso assoluto, ad esempio `D:\File in quarantena`, nel campo **Directory di quarantena**. In tal caso, accertarsi di applicare le stesse modifiche in **Dispositivi** > **{Gruppo}** > **Configura criterio** > **Quarantena**. In caso contrario, gli agent continueranno a inviare i file a `<Cartella di installazione Security Server>\PCCSRV\Virus`. Configurare inoltre le seguenti impostazioni di manutenzione: • **Capacità cartella di quarantena**: dimensioni della cartella di quarantena in MB. • **Dimensioni massime di un singolo file**: dimensioni massime di un solo file memorizzato nella cartella di quarantena in MB. • **Elimina tutti i file di quarantena**: elimina tutti i file presenti nella cartella della quarantena. Se la cartella è piena e viene caricato un nuovo file, questo file non viene memorizzato. Se non si desidera che gli agent inviino i file in quarantena al Security Server, configurare la nuova directory in **Dispositivi** > **{Gruppo}** > **Configura criterio** > **Quarantena** e ignorare tutte le impostazioni di manutenzione. Per istruzioni, consultare *Directory di quarantena a pagina 5-18*.

Impostazioni	Descrizione
Installazione di Security Agent	**Directory di installazione di Security Agent**: durante l'installazione, viene richiesto di digitare la directory di installazione di Security Agent, che rappresenta la posizione in cui il programma di installazione installa ciascun Security Agent. Se necessario, modificare la directory digitando un percorso assoluto. Solo gli agent futuri saranno installati in questa directory, quelli esistenti rimarranno in quella attuale. Utilizzare una delle variabili seguenti per impostare il percorso di installazione: • `$BOOTDISK`: la lettera dell'unità del disco di avvio • `$WINDIR`: la cartella di installazione di Windows • `$ProgramFiles`: la cartella dei programmi

3. Fare clic su **Salva**.

Configurazione delle impostazioni dell'Elenco eccezioni

Procedura

1. Andare su **Amministrazione** > **Impostazioni globali**.
2. Fare clic sulla scheda **Eccezioni** e configurare i seguenti campi secondo le esigenze:

Sezione	Descrizione
Reputazione Web e Filtro URL	• **Elenco URL approvati**: contiene i siti Web e relativi sottodomini esclusi dalle verifiche eseguite da Reputazione Web e dal Filtro URL. **Nota** L'elenco degli URL approvati ha la precedenza sull'elenco degli URL bloccati. Quando un URL corrisponde a una voce nell'elenco degli URL approvati, gli agent consentono sempre l'accesso all'URL, anche se è presente nell'elenco degli URL bloccati. Per gli URL personalizzati approvati/bloccati per un gruppo specifico, le impostazioni di eccezione globali saranno ignorate. • **Elenco URL bloccati**: contiene i siti Web e relativi sottodomini che vengono sempre bloccati dal filtro degli URL. • **Elenco di eccezioni processi**:Processi esclusi dalle verifiche Reputazione Web e Filtraggio degli URL. Immettere i processi critici ritenuti internamente attendibili. **Suggerimento** Quando si aggiorna l'elenco di eccezioni dei processi e il server implementa l'elenco aggiornato sugli agent, tutte le connessioni HTTP attive sul client (tramite la porta 80, 81 o 8080) saranno disconnesse per pochi secondi. Si consiglia di aggiornare l'elenco di eccezioni processi non in orari lavorativi. • **Elenco eccezioni IP**:Indirizzi IP (ad es. 192.168.0.1) esclusi dalle verifiche di Reputazione Web e Filtro URL. Digitare gli indirizzi IP critici che si ritengono sicuri. • **Inviare i registri di Reputazione Web e Filtri URL a Security Server**

Sezione	Descrizione
Elenco eccezioni di Intelligenza computazionale predittiva	Configurare le eccezioni del file di Intelligenza computazionale predittiva globale per impedire a tutti i Security Agent di rilevare un file come dannoso. Immettere il valore di hash del file SHA-1 da escludere dalla scansione. Fornire una nota facoltativa relativa al motivo dell'eccezione o per descrivere i nomi dei file associati al valore di hash.

3. Fare clic su **Salva**.

Capitolo 12

Utilizzo dei registri e dei rapporti

In questo capitolo viene descritto come utilizzare i registri e i rapporti per monitorare il sistema e analizzare la protezione.

Registri

Worry-Free Business Security mantiene aggiornati registri su incidenti, eventi e aggiornamenti relativi a virus/malware e spyware/grayware. Tali registri consentono di valutare le politiche di protezione della propria organizzazione, di identificare i client caratterizzati da un più elevato rischio di infezione e di verificare che gli aggiornamenti siano stati implementati correttamente.

Nota

Per visualizzare i file di registro in formato CSV è possibile utilizzare applicazioni per foglio di calcolo quali Microsoft Excel.

Worry-Free Business Security conserva i registri nelle seguenti categorie:

- Registri eventi della console Web
- Registri Desktop/Server
- Registri server Microsoft Exchange (solo Advanced)

TABELLA 12-1. Tipo di registro e contenuto

TIPO (ENTITÀ CHE HA GENERATO LA VOCE NEL REGISTRO)	CONTENUTO (TIPO DI REGISTRO DA CUI OTTENERE CONTENUTO)
Eventi console di gestione	• Scansione manuale (avviata dalla console Web) • Aggiornamento (aggiornamenti del Security Server) • Eventi console

Tipo (entità che ha generato la voce nel registro)	Contenuto (tipo di registro da cui ottenere contenuto)

Desktop/Server	• Registri virus
	  • Scansione manuale
	  • Scansione in tempo reale
	  • Scansione pianificata
	• Registri spyware/grayware
	  • Scansione manuale
	  • Scansione in tempo reale
	  • Scansione pianificata
	• Registri di Intelligenza computazionale predittiva:
	• Registri reputazione Web
	• Registri filtri URL
	• Registri di Monitoraggio del comportamento
	• Registri di aggiornamento
	• Registri dei virus di rete
	• Registri eventi
	• Registri di Controllo dispositivo
	• Aggiorna registri di implementazione
	• Registri ransomware
	  • Antivirus
	  • Monitoraggio del comportamento
	  • Reputazione Web
	  • Filtro URL
	  • Intelligenza computazionale predittiva

Tipo (entità che ha generato la voce nel registro)	Contenuto (tipo di registro da cui ottenere contenuto)
Server Exchange (solo Advanced)	• Registri virus • Registri blocco allegati • Registri Filtro dei contenuti / Prevenzione della perdita di dati • Registri di aggiornamento • Registri di backup • Registri di archivio • Registri eventi scansione • Registri parti non analizzabili dei messaggi • Registri reputazione Web • Registri eventi dei dispositivi mobili

Utilizzo delle query del registro

È possibile eseguire query di registro per raccogliere informazioni dal database di registro. La schermata **Query del registro** consente di impostare ed eseguire le query. È possibile esportare i risultati in un file CSV o stamparli.

Un Messaging Security Agent (solo Advanced) invia i registri al Security Server ogni cinque minuti (indipendentemente da quando è stato generato il registro).

Procedura

1. Accedere a **Rapporti** > **Query del registro**.
2. Aggiornare le seguenti opzioni, in base alle necessità:
   - **Intervallo di tempo**

- **Intervallo preconfigurato**
- **Intervallo specificato**: Per limitare la query a determinate date.

- **Tipo**: Per visualizzare il contenuto di ogni tipo di registro, consultare *Registri a pagina 12-2*.
  - **Eventi console di gestione**
  - **Desktop/Server**
  - **Server Exchange** (solo Advanced)
- **Contenuto**: Le opzioni a disposizione dipendono dal **Tipo** di registro.

3. Fare clic su **Visualizza registri**.
4. Per salvare il registro come file CSV (comma-separated value), fare clic su **Esporta**. Per visualizzare i file CSV è possibile utilizzare un'applicazione per foglio di calcolo.

Rapporti

È possibile creare manualmente segnalazioni singole o impostare il Security Server in modo che generi rapporti pianificati.

I rapporti possono essere stampati o inviati via e-mail a un amministratore o ad altre persone.

I dati disponibili in un rapporto dipendono dalla quantità di registri disponibili sul Security Server al momento della generazione del rapporto. La quantità di registri cambia quando vengono aggiunti nuovi registri e quelli esistenti vengono eliminati. In **Rapporti** > **Manutenzione**, è possibile eliminare i registri o impostare un'eliminazione pianificata dei registri.

Uso dei segnalazioni singole

Procedura

1. Accedere a **Rapporti** > **Segnalazioni singole**.
2. Effettuare le operazioni riportate di seguito:

Operazione	Passaggi
Generazione di un rapporto	a. Fare clic su **Aggiungi**. Viene visualizzata una nuova schermata. b. Configurare gli elementi riportati di seguito: • **Nome rapporto** • **Intervallo di tempo**: Limita il rapporto a determinate date. • **Contenuto**: Per selezionare tutte le minacce, selezionare la casella di controllo **Seleziona tutto**. Per selezionare le singole minacce, fare clic sulla casella di controllo corrispondente. Fare clic sull'icona del segno (+) per espandere la sezione. • **Invia rapporto a** ◦ **Destinatari**: Immettere gli indirizzi e-mail dei destinatari separandoli con punti e virgola (;). ◦ **Formato**: Scegliere PDF o un collegamento a un rapporto HTML. Se si sceglie PDF, il PDF viene allegato all'e-mail. c. Fare clic su **Aggiungi**.

OPERAZIONE	PASSAGGI
Visualizzare il rapporto	Nella colonna Nome rapporto, fare clic sui collegamenti al rapporto. Il primo collegamento apre un rapporto PDF, mentre il secondo apre un rapporto HTML. I dati disponibili in un rapporto dipendono dalla quantità di registri disponibili sul Security Server al momento della generazione del rapporto. La quantità di registri cambia quando vengono aggiunti nuovi registri e quelli esistenti vengono eliminati. In **Rapporti** > **Manutenzione**, è possibile eliminare i registri o impostare un'eliminazione pianificata dei registri. Per maggiori dettagli sui contenuti del rapporto, vedere *Interpretazione dei rapporti a pagina 12-11*.
Eliminazione di rapporti	a. Selezionare la riga contenente i collegamenti al rapporto. b. Fare clic su **Elimina**. **Nota** Per eliminare automaticamente le segnalazioni, accedere a scheda **Segnalazioni** > **Manutenzione** > **Segnalazioni** e impostare il numero massimo di singole segnalazioni che Worry-Free Business Security deve conservare. Il numero predefinito di segnalazioni singole è 10. Quando tale numero viene superato, il Security Server elimina i rapporti in eccesso a partire da quello meno recente.

Uso dei rapporti pianificati

Procedura

1. Accedere a **Rapporti** > **Rapporti pianificati**.
2. Effettuare le operazioni riportate di seguito:

OPERAZIONE	PASSAGGI
Creazione di un nuovo modello di rapporto pianificato	a. Fare clic su **Aggiungi**. Viene visualizzata una nuova schermata. b. Configurare gli elementi riportati di seguito: • **Nome modello di rapporto** • **Pianificazione**: Giornaliero, settimanale o mensile e l'ora in cui generare il rapporto Per i rapporti mensili, se si selezionano 31, 30 o 29 giorni e un mese ha meno di questo numero di giorni, WFBS non genera il rapporto per quel mese. • **Contenuto**: Per selezionare tutte le minacce, selezionare la casella di controllo **Seleziona tutto**. Per selezionare le singole minacce, fare clic sulla casella di controllo corrispondente. Fare clic sull'icona del segno (+) per espandere la sezione. • **Invia rapporto a** • **Destinatari**: Immettere gli indirizzi e-mail dei destinatari separandoli con punti e virgola (;). • **Formato**: Scegliere PDF o un collegamento a un rapporto HTML. Se si sceglie PDF, il PDF viene allegato all'e-mail. c. Fare clic su **Aggiungi**.

Operazione	Passaggi
Visualizzazione di rapporti pianificati	a. Sulla riga contenente il modello dal quale vengono generati i rapporti pianificati, fare clic su **Cronologia segnalazioni**. Viene visualizzata una nuova schermata. b. Nella colonna Visualizza, fare clic sui collegamenti a un rapporto. Il primo collegamento apre un rapporto PDF, mentre il secondo apre un rapporto HTML. I dati disponibili in un rapporto dipendono dalla quantità di registri disponibili sul Security Server al momento della generazione del rapporto. La quantità di registri cambia quando vengono aggiunti nuovi registri e quelli esistenti vengono eliminati. In **Rapporti** > **Manutenzione**, è possibile eliminare i registri o impostare un'eliminazione pianificata dei registri. Per maggiori dettagli sui contenuti del rapporto, vedere *Interpretazione dei rapporti a pagina 12-11*.
Operazioni di manutenzione del modello	
Modifica delle impostazioni del modello	Fare clic sul modello, quindi modificare le impostazioni nella nuova schermata visualizzata. I rapporti generati dopo aver salvato le modifiche utilizzeranno le nuove impostazioni.
Attivazione/ Disattivazione di un modello	Fare clic sull'icona sotto alla colonna Attivato. Per interrompere temporaneamente la generazione di rapporti pianificati, disattivare un modello e riattivarlo quando sono nuovamente richiesti.

Operazione	Passaggi
Eliminazione di un modello	Selezionare il modello e fare clic su **Elimina**. L'eliminazione di un modello non elimina i rapporti pianificati generati dal modello, ma i collegamenti ai rapporti non saranno più disponibili nella console Web. È possibile accedere ai rapporti direttamente dal computer del Security Server. I rapporti vengono eliminati solo se si eliminano manualmente dal computer o se il Security Server li elimina automaticamente secondo l'impostazione di eliminazione automatica rapporti pianificata in **Rapporti** > **Manutenzione** > **scheda Rapporti**. Per eliminare automaticamente i modelli, accedere a scheda **Segnalazioni** > **Manutenzione** > **Segnalazioni** e impostare il numero massimo di modelli che Worry-Free Business Security deve conservare. Il valore predefinito è 10 modelli. Quando tale numero viene superato, il Security Server elimina i modelli in eccesso a partire da quello meno recente.
Operazioni di manutenzione dei rapporti	
Invio di un collegamento ai rapporti pianificati	Inviare un collegamento ai rapporti pianificati (in formato PDF) via e-mail. Per accedere al file PDF, i destinatari devono semplicemente selezionare il collegamento nel messaggio e-mail. Verificare che i destinatari possano connettersi al computer del Security Server oppure il file non verrà visualizzato. **Nota** Nel messaggio e-mail viene fornito solo un collegamento al file PDF. Il file PDF effettivo non è allegato. a. Sulla riga contenente il modello dal quale vengono generati i rapporti pianificati, fare clic su **Cronologia segnalazioni**. Viene visualizzata una nuova schermata. b. Selezionare i rapporti, quindi fare clic su **Invia**. Si apre il client e-mail predefinito, con un nuovo messaggio e-mail contenente un collegamento al rapporto.

Operazione	Passaggi
Eliminazione di rapporti pianificati	a. Sulla riga contenente il modello dal quale vengono generati i rapporti pianificati, fare clic su **Cronologia segnalazioni**. Viene visualizzata una nuova schermata. b. Selezionare i rapporti e fare clic su **Elimina**. **Nota** Per eliminare automaticamente le segnalazioni, accedere a scheda **Segnalazioni** > **Manutenzione** > **Segnalazioni** e impostare il numero massimo di segnalazioni pianificate di ogni modello che Worry-Free Business Security deve conservare. Il valore predefinito per i rapporti pianificati è 10. Quando tale numero viene superato, il Security Server elimina i rapporti in eccesso a partire da quello meno recente.

Interpretazione dei rapporti

I rapporti Worry-Free Business Security contengono le seguenti informazioni. Le informazioni visualizzate possono variare in base alle opzioni selezionate.

TABELLA 12-2. Contenuti di un rapporto

VOCE RAPPORTO	DESCRIZIONE
Antivirus	**Riepilogo virus desktop/server** I rapporti sui virus mostrano informazioni dettagliate sui numeri e sui tipi di virus/minacce informatiche rilevati dal motore di scansione e sulle azioni intraprese per eliminarli. Il rapporto elenca anche i nomi dei virus e dei malware principali. Fare clic sui nomi dei virus o delle minacce informatiche per aprire una nuova pagina del browser Web e visitare l'Enciclopedia dei virus di Trend Micro, contenente ulteriori informazioni su tali virus e minacce.
	Primi 5 desktop/server con rilevamenti di virus Mostra i primi cinque computer desktop o server su cui sono stati rilevati virus e malware. Il rilevamento di incidenti relativi a virus/malware frequenti sullo stesso client potrebbe indicare che tale client rappresenta un elevato rischio per la sicurezza e che potrebbe essere necessario effettuare ulteriori indagini.
Anti-spyware	**Riepilogo spyware/grayware per PC desktop/server** Il rapporto su spyware/grayware riporta informazioni dettagliate sulle minacce spyware/grayware individuate su client, compreso il numero di rilevamenti e di azioni intraprese da WFBS per contrastarle. Il rapporto contiene anche un grafico a torta che mostra la percentuale di ogni azione anti-spyware messa in atto.
	Primi 5 desktop/server con rilevamenti di spyware/grayware Il rapporto riporta anche le prime cinque minacce spyware/grayware individuate e i cinque desktop/server con il numero più elevato di spyware/grayware. Per ulteriori informazioni sulle minacce spyware/grayware individuate, fare clic sui nomi di spyware/grayware presenti. Viene visualizzata una nuova pagina del browser Web contenente le informazioni relative allo spyware/grayware fornite dal sito Web di Trend Micro.
Riepilogo Anti-spam (solo Advanced)	**Riepilogo spam** I riepiloghi anti-spam mostrano informazioni riguardanti il numero di casi di spam e di phishing rilevati rispetto al totale dei messaggi sottoposti a scansione. Essi elencano inoltre i falsi allarmi rilevati.

Voce rapporto	Descrizione
Intelligenza computazionale predittiva	**I 5 programmi principali che violano i criteri di Intelligenza computazionale predittiva**
	I 10 computer principali che violano i criteri di Intelligenza computazionale predittiva
Reputazione Web	**Primi 10 computer che violano i criteri di Reputazione Web**
Categoria URL	**Primi 5 criteri delle categorie URL violati** Elenca le categorie di siti Web a cui si accede con maggiore frequenza che hanno violato i criteri.
	Primi 10 computer che violano i criteri delle categorie URL
Monitoraggio del comportamento	**Primi 5 programmi che violano i criteri di monitoraggio del comportamento**
	Primi 10 computer che violano i criteri di monitoraggio del comportamento
Controllo dispositivo	**Primi 10 computer che violano i criteri di controllo del dispositivo**
Riepilogo filtro dei contenuti (solo Advanced)	**Riepilogo filtro dei contenuti** I rapporti del filtro dei contenuti mostrano informazioni sul numero totale di messaggi filtrati da Messaging Security Agent.
	Prime 10 regole di filtro dei contenuti violate Elenco delle prime dieci regole violate del filtro dei contenuti. Utilizzare queste informazioni per affinare le regole dei filtri.

Voce rapporto	Descrizione
Virus di rete	**Primi 10 virus di rete rilevati** Mostra i dieci virus di rete rilevati con maggiore frequenza dal driver di firewall comune. Fare clic sui nomi dei virus per aprire una nuova pagina del browser Web e visitare l'Enciclopedia dei virus di Trend Micro, contenente ulteriori informazioni su tali virus.
	Primi 10 computer attaccati Elenca i computer della rete per i quali è stato rilevato il più elevato numero di incidenti virali.

Operazioni di manutenzione per rapporti e registri

Procedura

1. Accedere a **Rapporti** > **Manutenzione**.
2. Effettuare le operazioni riportate di seguito:

Operazione	Passaggi
Impostare il numero massimo di rapporti e modelli	È possibile limitare il numero di segnalazioni singole, rapporti pianificati (per ogni modello) e modelli disponibili sul Security Server. Quando tale numero viene superato, il Security Server elimina i rapporti/modelli in eccesso a partire da quello meno recente. a. Fare clic sulla scheda **Rapporti**. b. Immettere il numero massimo di segnalazioni singole, rapporti pianificati e modelli di rapporto da conservare.

Operazione	Passaggi
Configurare l'eliminazione automatica dei registri	a. Fare clic sulla scheda **Eliminazione automatica dei registri**. b. Selezionare i tipi di registro e specificare la durata massima dei registri. I registri con durata superiore a questo valore saranno eliminati.
Elimina manualmente i registri	a. Fare clic sulla scheda **Eliminazione manuale dei registri**. b. Per ogni tipo di registro, immettere la durata massima. I registri con durata superiore a questo valore saranno eliminati. Per eliminare tutti i registri, digitare `0`. c. Fare clic su **Elimina**.

3. Fare clic su **Salva**.

Capitolo 13

Esecuzione di operazioni di amministrazione

In questo capitolo viene descritta la modalità di esecuzione di ulteriori operazioni amministrative, come la visualizzazione della licenza del prodotto, l'uso di Plug-in Manager e la disinstallazione del Security Server.

Modifica della password della console Web

Trend Micro consiglia di utilizzare password sicure per la console Web. Una password sicura ha una lunghezza di almeno otto caratteri, una o più lettere maiuscole (A-Z), una o più lettere minuscole (a-z), uno o più numeri (0-9) e uno o più caratteri speciali o segni di punteggiatura (!@#$%^&,.:;?); Non corrisponde mai al nome utente né lo contiene al suo interno. Non fa uso del nome di battesimo o del cognome, della data di nascita o di altri elementi facilmente riconducibili all'utente.

Procedura

1. Andare su **Amministrazione** > **Password**.
2. Aggiornare le seguenti opzioni, in base alle necessità:
   - **Vecchia password**
   - **Nuova password**
   - **Conferma password**: Digitare nuovamente la nuova password per confermarla.
3. Fare clic su **Salva**.

Operazioni relative a Plug-in Manager

Plug-in Manager visualizza i programmi sia per Security Server, sia per i Security Agent, nella console Web non appena diventano disponibili. A questo punto è possibile installare e gestire i programmi dalla console Web e distribuire i programmi plug-in dei client agli agent. Scaricare e installare Plug-in Manager da **Amministrazione** > **Plug-In**. Al termine dell'installazione, è possibile verificare la presenza di programmi plug-in disponibili. Per ulteriori informazioni, consultare la documentazione per Plug-in Manager e i programmi di plug-in.

Gestione della licenza di prodotto

Dalla schermata della licenza del prodotto, è possibile rinnovare, aggiornare o visualizzare i dettagli della licenza del prodotto.

La schermata Licenza del prodotto visualizza i dettagli sulla licenza. In base alle opzioni selezionate durante l'installazione, si dispone di una versione con licenza completa o di una versione di prova. In entrambi i casi la licenza dà diritto a un Contratto di manutenzione. Alla scadenza del Contratto di manutenzione, i client della rete disporranno di una protezione molto limitata. La schermata Licenza del prodotto permette di conoscere in anticipo la data di scadenza della licenza in modo da poterla rinnovare prima di tale data.

Nota

Le licenze per i vari componenti dei prodotti Trend Micro possono variare a seconda della regione. Dopo l'installazione, verrà visualizzato un riepilogo dei componenti che la chiave di registrazione/codice di attivazione consente di utilizzare. Controllare con il proprio rivenditore o fornitore per verificare le licenze dei componenti.

Rinnovo della licenza

È possibile rinnovare o aggiornare una versione completa di Worry-Free Business Security acquistando un rinnovo della manutenzione. La versione con licenza completa richiede un codice di attivazione.

Il rinnovo della licenza avviene in due modi:

- Sulla console Web, accedere alla schermata Stato in tempo reale e seguire le istruzioni sullo schermo. Queste istruzioni compaiono 60 giorni prima e 30 giorni dopo la scadenza della licenza.
- Contattare il responsabile vendite o rivenditore aziendale di Trend Micro.

  I rivenditori possono lasciare le informazioni di contatto su un file sul Security Server. Verificare il file all'indirizzo:

```
{cartella di installazione di Security Server}\PCCSRV
\Private\contact_info.ini
```

Nota

La `{cartella di installazione di Security Server}` è tipicamente `C:\Programmi\Trend Micro\Security Server`.

Un rappresentante Trend Micro aggiornerà le informazioni di registrazione tramite Registrazione prodotto Trend Micro.

Security Server interroga il server di Registrazione prodotto e riceve direttamente la nuova data di scadenza da tale server. Quando si rinnova la licenza non è necessario immettere manualmente un nuovo codice di attivazione.

Attivazione di una nuova licenza

Il tipo di licenza determina il codice di attivazione di Worry-Free Business Security.

TABELLA 13-1. Codice di attivazione in base al tipo di licenza

TIPO DI LICENZA	CODICE DI ATTIVAZIONE
Versione con licenza Worry-Free Business Security Standard completa	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Versione con licenza di Worry-Free Business Security Advanced completa	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

Nota

In caso di dubbi sul codice di attivazione, consultare il sito Web Trend Micro al seguente indirizzo:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

La schermata Licenza del prodotto consente di cambiare il tipo di licenza specificando un nuovo codice di attivazione.

1. Andare su **Amministrazione** > **Licenza del prodotto**.
2. Fare clic su **Immetti un nuovo codice**.
3. Digitare il nuovo codice di attivazione nello spazio apposito.
4. Fare clic su **Attiva**.

Configurazione delle impostazioni di aggiornamento dei prodotti

Configurare Worry-Free Business Security per automatizzare gli aggiornamenti del prodotto.

Procedura

1. Andare su **Amministrazione** > **Aggiornamento del prodotto**.

   Viene visualizzata la scheda **Impostazioni**.

2. In **Aggiorna impostazioni**, selezionare **Attiva download aggiornamenti del prodotto**.

3. Specificare l'azione da eseguire quando risulta disponibile un nuovo pacchetto di aggiornamento.

   - **Download**: scarica automaticamente il pacchetto di aggiornamento nella cartella di download in base alla pianificazione configurata.
   - **Download e installazione**: scarica automaticamente e installa il pacchetto di aggiornamento in base alla pianificazione configurata.

4. Specificare quando eseguire l'azione.

Nota

Il completamento del processo di installazione e il riavvio di Security Server possono richiedere del tempo. Scegliere un momento con un impatto minimo per installare il pacchetto di aggiornamento.

5. Fare clic su **Salva**.

Configurazione delle notifiche di aggiornamento dei prodotti

Worry-Free Business Security può comunicare agli utenti gli aggiornamenti dei prodotti quando sono disponibili nuovi service pack, versioni o patch. È possibile impostare i seguenti tipi di notifiche di aggiornamento dei prodotti:

- Security Agent:visualizza una notifica vicino all'area di notifica sull'endpoint
- E-mail

Procedura

1. Andare su **Amministrazione** > **Aggiornamento del prodotto**.
2. Fare clic su **Notifiche**.
3. Per ricevere notifiche da Security Agent, configurare la sezione **Notifica di Security Agent**.
   a. Fare clic su **Aggiungi**.
   b. Selezionare i Security Agent dall'elenco.
   c. Fare clic su **Salva**.
4. Per ricevere le notifiche e-mail sugli aggiornamenti dei prodotti, specificare i destinatari nella sezione **Notifica e-mail**.

Nota

La ricezione di notifiche e-mail richiede la configurazione della scheda **SMTP** in **Amministrazione** > **Impostazioni globali**.

5. Fare clic su **Salva**.

Partecipazione al programma Smart Feedback

Per ulteriori informazioni su Smart Feedback, vedere *Smart Feedback a pagina 1-6*.

Procedura

1. Andare su **Amministrazione** > **Smart Protection Network**.
2. Fare clic su **Attiva Trend Micro Smart Feedback**.
3. Per inviare informazioni su potenziali minacce alla sicurezza nei file dei computer client, selezionare la casella di controllo **Attiva il feedback per i file di programma sospetti**.

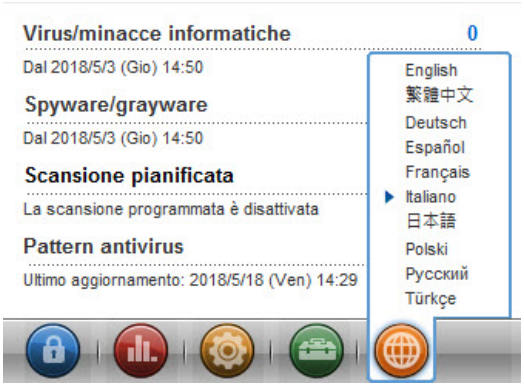
   Nota

   I file inviati a Smart Feedback non contengono dati degli utenti e vengono inviati solo per eseguire le analisi delle minacce.

4. Per consentire a Trend Micro di conoscere meglio l'organizzazione, selezionare un valore nel campo **Settore**.
5. Fare clic su **Salva**.

Modifica della lingua dell'interfaccia dell'Agent

Per impostazione predefinita, la lingua utilizzata per l'interfaccia dell'agent corrisponde alla lingua configurata sul sistema operativo del client. Gli utenti possono modificare la lingua dall'interfaccia dell'agent.



Salvataggio e ripristino delle impostazioni del programma

È possibile salvare una copia del database Security Server e dei file di configurazione importanti in modo tale da poter ripristinare il Security Server. Potrebbe risultare necessario qualora si verifichino dei problemi e si desideri reinstallare il Security Server oppure per ripristinare una configurazione precedente.

Procedura

1. Arrestare Trend Micro Security Server Master Service.
2. Copiare manualmente i seguenti file e cartelle dalla cartella in un percorso alternativo:

   AVVERTENZA!

   Non utilizzare strumenti o applicazioni di backup per questa operazione.

   ```
   <Percorso di installazione Security Server>\PCCSRV
   ```

   - `ofcscan.ini`: contiene le impostazioni globali.

- `Ous.ini`: contiene la tabella delle origini di aggiornamenti per l'implementazione di componenti antivirus.
- Cartella `Private`: contiene il firewall e le impostazioni delle origini di aggiornamento.
- `Pccnt\Common\OfcPfw.dat`: contiene le impostazioni del firewall.
- `Download\OfcPfw.dat`: contiene le impostazioni di implementazione del firewall.
- `Cartella` Log: contiene eventi di sistema e il registro di verifica della connessione.
- `Cartella` Virus: la cartella in cui WFBS mette in quarantena i file infetti.
- `Cartella` HTTDB: contiene il database WFBS.

3. Disinstallazione di Security Server. Vedere *Disinstallazione di Security Server a pagina 13-10*.
4. Eseguire una nuova installazione. Vedere la *Guida all'installazione e all'aggiornamento* di Worry-Free Business Security.
5. Una volta completata l'installazione principale, arrestare Trend Micro Security Server Master Service sul computer di destinazione.
6. Aggiornare la versione del pattern antivirus dal file di backup:
   a. Prendere la versione corrente del pattern dei virus dal nuovo server.

      ```
      <Percorso di installazione Security Server>\PCCSRV
      \Private\component.ini. [6101]

      ComponentName=Pattern antivirus

      Versione=xxxxxx 0 0
      ```

   b. Aggiornare la versione del file di pattern antivirus nel file di cui è stato eseguito il backup:

      ```
      \Private\component.ini
      ```

Nota

Se si modifica il percorso di installazione di Security Server, sarà necessario aggiornare le informazioni di percorso nei file di backup `ofcscan.ini` e `\private\ofcserver.ini`.

7. Con i backup creati, sovrascrivere il database di Worry-Free Business Security e i relativi file e cartelle nel computer di destinazione nella cartella `PCCSRV`.
8. Riavviare Trend Micro Security Server Master Service.

Disinstallazione di Security Server

La disinstallazione del Security Server comporta la rimozione anche dello Scan Server.

Worry-Free Business Security utilizza un programma di disinstallazione per rimuovere correttamente Trend Micro Security Server dal computer. Rimuovere il modulo Agent da tutti i client prima di rimuovere Security Server.

La disinstallazione di Trend Micro Security Server non comporta la disinstallazione dei moduli agent. Gli amministratori devono disinstallare o spostare tutti gli agent su un altro Security Server prima di disinstallare il Trend Micro Security Server. Vedere *Rimozione di agent a pagina 3-39*.

Procedura

1. Sul computer usato per installare il server, fare clic su **Start** > **Pannello di controllo** > **Installazione applicazioni**.
2. Fare clic su **Trend Micro Security Server**, quindi su **Modifica/Rimuovi**.

   Viene visualizzata una schermata di conferma.
3. Fare clic su **Avanti**.

Il programma di disinstallazione principale del server richiede la password dell'amministratore.

4. Digitare la password dell'amministratore nella casella di testo e fare clic su **OK**.

   Il programma di disinstallazione principale avvia la rimozione dei file dal server. Dopo la disinstallazione del Security Server viene visualizzato un messaggio di conferma.

5. Per chiudere il programma di disinstallazione, fare clic su **OK**.

Capitolo 14

Uso degli strumenti di gestione

Questo capitolo descrive l'utilizzo degli strumenti amministrativi, degli strumenti client e dei componenti aggiuntivi.

Tipi di strumenti

Worry-Free Business Security comprende un gruppo di strumenti che aiuta a eseguire varie operazioni, quali la configurazione dei server e la gestione dei client.

Nota

Non è possibile avviare gli strumenti di amministrazione e client dalla console Web. Dalla console Web è possibile scaricare i componenti aggiuntivi.

Per istruzioni sulle procedure di esecuzione degli strumenti, vedere le relative sezioni di seguito.

Gli strumenti si suddividono in tre categorie:

- **Strumenti amministrativi**
  - **Impostazione script di accesso** (`SetupUsr.exe`): Automatizza l'installazione di Security Agent. Vedere *Installazione con Impostazione script di accesso a pagina 3-11*.
  - **Vulnerability Scanner** (`TMVS.exe`): Individua i computer non protetti presenti sulla rete. Vedere *Installazione con Vulnerability Scanner a pagina 3-21*.
  - **Remote Manager Agent**: Consente ai rivenditori di gestire Worry-Free Business Security tramite una console Web centralizzata. Vedere *Installazione di Trend Micro Remote Manager Agent (utenti del portale delle licenze del cliente) a pagina 14-4*.
  - **Trend Micro Disk Cleaner**: Elimina i file di backup, i file di registro e i file di pattern Worry-Free Business Security non necessari. Vedere *Risparmio di spazio su disco a pagina 14-15*.
  - **Scan Server Database Mover**: trasferisce il database dello Scan Server in sicurezza su un'altra unità disco. Vedere *Spostamento di database Scan Server a pagina 14-18*.
- **Strumenti client**

- **Client Packager** (`ClnPack.exe`): Crea un file autoestraente contenente il Security Agent e i relativi componenti. Vedere *Installazione con Client Packager a pagina 3-13*.
- **Restore Encrypted Virus and Sypware** (`VSEncode.exe`): Apre i file infetti crittografati da Worry-Free Business Security. Vedere *Ripristino dei file crittografati a pagina 14-19*.
- **Strumento Client Mover** (`IpXfer.exe`): Trasferisce gli agent da un Security Server a un altro. Vedere *Spostamento di agent a pagina 4-11*.
- **Rigenera ID client del Security Agent** (`WFBS_WIN_All_ReGenID.exe`): l'utility ReGenID consente di rigenerare l'ID client del Security Agent, a seconda se l'agent sia su un computer clonato o su una macchina virtuale. Vedere *Utilizzo dello strumento ReGenID a pagina 14-23*.

- **Componenti aggiuntivi**: Permettono agli amministratori di visualizzare informazioni in tempo reale relative a sicurezza e sul sistema dalle console dei sistemi operativi Windows supportati. Si tratta delle stesse informazioni generali visibili nella schermata Stato in tempo reale. Vedere *Gestione dei componenti aggiuntivi di SBS e EBS a pagina 14-24*.

Nota

Alcuni strumenti disponibili nelle versioni precedenti di Worry-Free Business Security non sono disponibili in questa versione. Se tali strumenti risultano necessari, contattare l'assistenza tecnica di Trend Micro.

Trend Micro Remote Manager Agent

Trend Micro Remote Manager Agent consente ai rivenditori o ai partner di gestire Worry-Free Business Security con Trend Micro Remote Manager. È possibile installare Remote Manager Agent su Security Server una volta completata l'installazione di Security Server oppure è possibile installarlo successivamente.

Requisiti di installazione:

- GUID (Globally Unique Identifier, Identificatore univoco globale) di Remote Manager Agent
- Una connessione a Internet attiva
- 50 MB di spazio libero su disco

Seguire le procedure in uno dei collegamenti seguenti:

- *Installazione di Trend Micro Remote Manager Agent (utenti del portale delle licenze del cliente) a pagina 14-4*
- *Installazione di Trend Micro Remote Manager Agent (utenti della piattaforma di gestione delle licenze) a pagina 14-6*

Installazione di Trend Micro Remote Manager Agent (utenti del portale delle licenze del cliente)

Procedura

1. Ottenere il GUID di Remote Manager Agent.
   a. Nella console Web di Remote Manager, andare su **Clienti**.
   b. Nella colonna **Azienda**, fare clic sul cliente.
   c. Nella scheda **Prodotti**, selezionare il prodotto Worry-Free Business Security.
   d. Copiare il GUID.
2. Accedere a Security Server e spostarsi nella seguente cartella di installazione:`PCCSRV\Admin\Utility\RmAgent` e avviare l'applicazione `TMRMAgentforWFBS.exe`.

   Ad esempio:`C:\Programmi\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

Nota

Saltare questo punto se si avvia l'installazione dalla schermata di installazione del Security Server.

3. Nell'installazione guidata di Trend Micro Remote Manager Agent, leggere il contratto di licenza. Se si accettano i termini, fare clic su **Accetto i termini del contratto di licenza**, quindi su **Avanti**.

4. Fare clic su **Sì** per confermare di essere un partner certificato.

5. Selezionare **Dispongo già di un account Trend Micro Remote Manager e desidero installare l'agent**, quindi fare clic su **Avanti**.

6. Determinare il proprio scenario.

Scenario	Passaggi
Nuovo cliente	a. Selezionare **Associa con un nuovo cliente**. b. Fare clic su **Avanti**. Immettere le informazioni relative al cliente. **Nota** Se il cliente è già presente nella console TMRM e si utilizza l'opzione citata in precedenza per eseguire l'associazione con un nuovo cliente, nella struttura di rete TMRM verranno visualizzati due clienti con lo stesso nome. Per evitare questo problema, è sufficiente attenersi alla modalità descritta di seguito.
Cliente esistente	a. Selezionare **Prodotto già esistente in Remote Manager**. **Nota** È necessario che WFBS sia già stato aggiunto alla console TMRM. Per istruzioni, consultare la documentazione di TMRM. b. Immettere il GUID.

7. Fare clic su **Avanti**.

8. Selezionare l'**Area geografica** e il **Protocollo**, quindi immettere le informazioni sul proxy eventualmente richieste.

9. Fare clic su **Avanti**.

   Viene visualizzata la schermata Percorso di installazione.

10. Per utilizzare il percorso predefinito, fare clic su **Avanti**.

11. Fare clic sul pulsante **Fine**.

    Se l'installazione riesce e le impostazioni sono corrette, Remote Manager Agent viene registrato automaticamente nel server Trend Micro Remote Manager. Remote Manager Agent deve comparire come Online nella console Web di Remote Manager.

Installazione di Trend Micro Remote Manager Agent (utenti della piattaforma di gestione delle licenze)

Procedura

1. Ottenere il codice di attivazione di Worry-Free Business Security.

   a. Nella console Web di Remote Manager, andare su **Clienti**.

   b. Nella colonna **Azienda**, fare clic sul cliente.

   c. Nella scheda **Prodotti**, selezionare il prodotto Worry-Free Business Security.

   d. Copiare il codice di attivazione

2. Aggiornare le informazioni sulla licenza di Worry-Free Business Security.

   a. Sulla console Web di Worry-Free Business Security, andare su **Amministrazione** > **Licenza del prodotto**.

   b. In **Informazioni sulla licenza**, fare clic su **Immetti un nuovo codice**.

   c. Incollare il codice di attivazione nel campo **Nuovo codice di attivazione**.

d. Fare clic su **Attiva**.

e. Fare clic su **Aggiorna informazioni sulla licenza**.

3. Accedere a Security Server e spostarsi nella seguente cartella di installazione:`PCCSRV\Admin\Utility\RmAgent` e avviare l'applicazione `TMRMAgentforWFBS.exe`.

   Ad esempio:`C:\Programmi\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Nota

   Saltare questo punto se si avvia l'installazione dalla schermata di installazione del Security Server.

4. Selezionare **Dispongo già di un account Trend Micro Remote Manager e desidero installare l'agent**, quindi fare clic su **Avanti**.

5. Selezionare **Associa con la licenza della piattaforma di gestione delle licenze** e fare clic su **Avanti**.

6. Specificare le credenziali dell'account Remote Manager e fare clic su **Avanti**.

7. Se richiesto, specificare le informazioni del server proxy e fare clic su **Avanti**.

8. Se richiesto, specificare la cartella di installazione e fare clic su **Avanti**.

9. Fare clic sul pulsante **Fine**.

   Se l'installazione riesce e le impostazioni sono corrette, Remote Manager Agent viene registrato automaticamente nel server Trend Micro Remote Manager. Remote Manager Agent deve comparire come Online nella console Web di Remote Manager.

Gestione degli Agent dal server gestito

In questa sezione sono fornite informazioni su come gestire gli Agent dal server gestito.

Messaggi di stato dell'Agent

Sul server gestito, l'Agent visualizza una delle seguenti icone sulla barra delle applicazioni:

TABELLA 14-1. Icone sulla barra delle applicazioni

ICONA	DESCRIZIONE
	Un'icona verde indica che l'Agent è connesso al server delle comunicazioni Remote Manager. L'Agent funziona normalmente.
	Un'icona rossa indica che l'Agent non è connesso al server delle comunicazioni Remote Manager oppure la versione dell'Agent non corrisponde a quella del server e deve essere aggiornata.
	Un'icona con una freccia rossa indica che l'Agent si è disconnesso da Remote Manager.
	Un'icona con una X rossa indica che l'Agent è stato disconnesso.

Modifica del GUID dell'Agent sul server gestito

Se è stato immesso un GUID (Globally Unique Identifier, Identificatore univoco globale) durante l'installazione di Remote Manager Agent, eliminare l'agent e installarlo nuovamente utilizzando il GUID corretto. Se questa procedura dovesse risultare impossibile, procedere come indicato:

Procedura

1. Accedere a `C:\Program Files\Trend Micro\TMRMAgentForWFBS`.
2. Aprire il file `AgentSysConfig.xml` utilizzando un editor di testo.
3. Cercare il GUID tra i parametri `<AgentGUID>` e `</AgentGUID>`.

4. Modificare il GUID e salvare il file.
5. Nella stessa cartella, aprire il file `csmSysConfig.xml` utilizzando un editor di testo.
6. Cercare il GUID tra i parametri `<ProductGUID>` e `</ProductGUID>`.
7. Modificare il GUID e salvare il file.
8. Fare clic con il pulsante destro del mouse sull'icona di Remote Manager Agent sulla barra delle attività e fare clic su **Riavvia servizio**.

Uso dell'strumento di configurazione Agent

Lo strumento di configurazione Agent consente di effettuare modifiche alle impostazioni di configurazione di Remote Manager Agent.

Accedere a **Start** > **Programmi** > **Trend Micro Remote Manager Agent** > **strumento di configurazione Agent** oppure fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni e fare clic su **Configura**.

Per ulteriori informazioni, consultare la sezione *Configurazione dell'Agent a pagina 14-10*.

Configurazione dell'Agent

Menu di configurazione dell'Agent

Per configurare l'Agent, fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni per aprire il seguente menu:

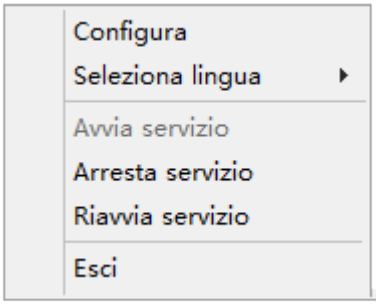


FIGURA 14-1. Menu a comparsa di strumento di configurazione Agent

Vengono visualizzate le seguenti voci:

- **Configura**: consente di aprire la schermata di configurazione dell'Agent.
- **Seleziona lingua**: oltre ad altre lingue possibili, la lingua inglese è sempre presente.
- **Servizio**: consente l'avvio, l'arresto e il riavvio.
- **Esci**: l'uscita dallo strumento non arresta il servizio Remote Manager. ma semplicemente la chiusura di strumento di configurazione Agent e la rimozione dell'icona dalla barra delle applicazioni. Lo strumento può essere riavviato in qualsiasi momento.

Finestra di dialogo principale dello strumento di configurazione

Fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni e selezionare **Configura** nel menu di configurazione dell'Agent per aprire la scheda **Generale** dello strumento di configurazione.

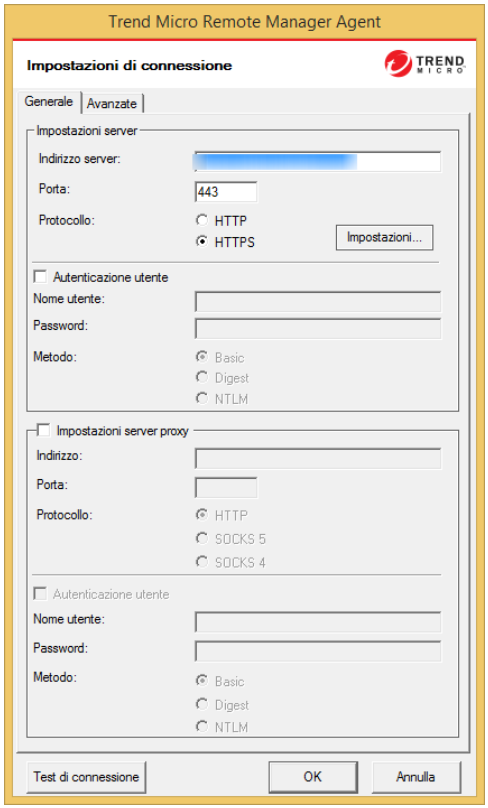


FIGURA 14-2. Scheda Generale di strumento di configurazione Agent

Le seguenti sezioni della schermata di configurazione dell'Agent sono le uniche attualmente rilevanti dello strumento.

- **Impostazioni server**: Per configurare la comunicazione del server, effettuare le seguenti impostazioni:

- **Indirizzo server**: il nome di dominio completo (FQDN) del server delle comunicazioni Remote Manager. Il nome di dominio completo varia in ciascuna regione. Contattare l'assistenza tecnica se è necessario modificare le informazioni dell'indirizzo del server.
- **Porta**: la porta che il server Remote Manager utilizza per comunicare con l'Agent. Dovrebbe essere 80 per HTTP e 443 per HTTPS.
- **Protocollo**: il protocollo utilizzato per la comunicazione tra il server e l'Agent.

Importante

Trend Micro non consiglia di modificare le informazioni relative all'**Indirizzo server** o alla **Porta** a meno che non venga richiesto dall'assistenza tecnica.

- **Impostazioni server proxy**: attivare quest'area facendo clic sulla casella di controllo **Impostazioni server proxy** nel caso in cui la rete dell'utente necessiti di un proxy per comunicare con il server Remote Manager.
  - **Indirizzo**: l'indirizzo IP del server proxy.
  - **Porta**: la porta o il server proxy
  - **Protocollo**
- **Pulsante Test di connessione**: il pulsante **Test di connessione** viene utilizzato per effettuare il test delle comunicazioni tra l'Agent e il server Remote Manager. Utilizzare questa funzione per verificare il funzionamento della connessione di base al server di comunicazione. Se non riesce (viene visualizzata una finestra di dialogo a comparsa se lo strumento non può connettersi al server), potrebbe sussistere un problema di base, legato ad esempio all'indirizzo del server di comunicazione e alla relativa porta o all'indirizzo del server proxy e alla relativa porta.

Backup e ripristino delle impostazioni dell'Agent

Per disinstallare e reinstallare l'Agent utilizzando lo stesso GUID in un intervallo di tre giorni, mantenere le impostazioni dell'Agent onde evitare la sovrapposizione di dati. A tal fine, eseguire il backup manuale dei file di configurazione, quindi sostituire i file di configurazione con la copia di backup dopo la reinstallazione dell'Agent.

Backup delle impostazioni

Procedura

1. Sul server gestito, fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Arresta servizio** per arrestare il servizio Agent.
2. Copiare tutti i file `.xml`, `.dat` e `.ini` dalla cartella di installazione: `C:\Program Files\Trend Micro\TMRMAgentForWFBS` o `C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS`.
   - File `.xml`
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - File `.dat`
     - `MSA.dat`
     - `logBuf.dat`

- `group.dat`
- `CSA.dat`
- `CriticalVA.dat`

- File `.ini`
  - `csmStatusData.ini`

3. Copiare tutti i file dalla cartella `\Cache`.
4. Riavviare il servizio Agent.

Ripristino delle impostazioni

Procedura

1. Rimuovere l'agente in locale.

   Nota

   Quando viene rimosso l'Agent localmente, questo annullerà la registrazione da Remote Manager, che eliminerà automaticamente tutti i dati associati con l'Agent. Per evitare l'annullamento della registrazione dell'Agent, modificare il valore Indirizzo server nell'interfaccia dell'Agent prima di rimuovere l'Agent.

2. Reinstallare l'Agent. Assicurarsi di utilizzare lo stesso GUID, che può essere ottenuto da `AgentSysConfig.xml`.
3. Sul server gestito, fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Arresta servizio** per arrestare il servizio Agent.
4. Sostituire i file di configurazione con i file di backup.

5. Fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Avvia servizio** per riavviare il servizio Agent.

Risparmio di spazio su disco

È possibile risparmiare spazio su disco sul Security Server e i client grazie all'esecuzione di Disk Cleaner.

Esecuzione di Disk Cleaner sul Security Server

Informazioni preliminari

Per risparmiare spazio su disco, lo strumento Disk Cleaner (`TMDiskCleaner.exe`) identifica ed elimina i file di backup, registro e pattern inutilizzati dalle seguenti directory:

- `{Security Agent}\AU_Data\AU_Temp\*`
- `{Security Agent}\Reserve`
- `{Security Server}\PCCSRV\TEMP\*` (tranne i file nascosti)
- `{Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\wss\*.log`
- `{Security Server}\PCCSRV\wss\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\Backup\*`
- `{Security Server}\PCCSRV\Virus\*` (elimina i file in quarantena precedenti a due settimane, fatta eccezione per il file NOTVIRUS)
- `{Security Server}\PCCSRV\ssaptpn.xxx` (conserva solo il pattern più recente)

- `{Security Server}\PCCSRV\lpt$vpn.xxx (conserva solo gli ultimi tre pattern)`
- `{Security Server}\PCCSRV\icrc$oth.xxx (conserva solo gli ultimi tre pattern)`
- `{Security Server}\DBBackup\* (conserva solo le due ultime sottocartelle)`
- `{Messaging Security Agent}\AU_Data\AU_Temp\*`
- `{Messaging Security Agent}\Debug\*`
- `{Messaging Security Agent}\engine\vsapi\latest\pattern\*`

Procedura

1. Nel Security Server, accedere alla seguente directory:

   `{Cartella di installazione del server}\PCCSRV\Admin\Utility\`

2. Fare doppio clic su **TMDiskCleaner.exe**.

   Viene visualizzato lo strumento Disk Cleaner di Trend Micro Worry-Free Business Security.

   Nota

   I file non possono essere ripristinati.

3. Fare clic su **Elimina file** per eseguire la scansione dei i file di backup, registro e pattern inutilizzati e quindi eliminarli.

Esecuzione di Disk Cleaner sul Security Server da interfaccia della riga di comando

Procedura

1. Sul Security Server, aprire una finestra del prompt dei comandi.
2. Al prompt dei comandi, eseguire il seguente comando:

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide`: Consente di eseguire lo strumento come processo in background.
   - `/log`: Salva un registro dell'operazione nel file DiskClean.log, che si trova nell'attuale cartella.

     Nota

     Il comando `/log` è disponibile solo quando si usa anche il comando `/hide`.

   - `/allowundo`: Consente di spostare i file nel Cestino, senza eliminarli in modo definitivo.
3. Per eseguire frequentemente lo strumento Disk Cleaner, configurare una nuova attività in Operazioni pianificate di Windows. Per ulteriori informazioni, consultare la documentazione di Windows.

Risparmio di spazio su disco sui client

Procedura

- Sui desktop/server con Security Agent:
  - Eliminare i file in quarantena
  - Eliminare i file di registro

- Eseguire l'unità di disinfezione dischi di Windows
- Su server Microsoft Exchange con Messaging Security Agent:
  - Eliminare i file in quarantena
  - Eliminare i file di registro
  - Eseguire l'unità di disinfezione dischi di Windows
  - Eliminare i registri di archivio
  - Eliminare i file di backup
  - Controllare le dimensioni dei registri transazioni o del database di Microsoft Exchange

Spostamento di database Scan Server

Se sull'unità disco su cui è installato lo Scan Server lo spazio è sufficiente, utilizzare lo strumento Scan Server Database Mover per spostare il database dello Scan Server su un'altra unità disco.

Verificare che il computer del Security Server possieda più di 1 unità disco e che la nuova unità disco possieda almeno 3 GB di spazio su disco disponibili. Le unità mappate non sono accettate. Non spostare manualmente il database o utilizzare altri strumenti.

Procedura

1. Nel computer Security Server passare a `<Cartella di installazione Security Server>\PCCSRV\Admin\Utility`.
2. Avviare `ScanServerDBMover.exe`.
3. Fare clic su **Modifica**.
4. Selezionare **Sfoglia**, quindi raggiungere la directory destinazione sull'altra unità disco.

5. Fare clic su **OK**, quindi su **Completa** una volta spostato il database.

Ripristino dei file crittografati

Per impedire l'apertura di un file infetto, Worry-Free Business Security codifica il file nei seguenti casi:

- Prima di mettere un file in quarantena
- Quando si esegue un backup di un file prima di disinfettarlo

Worry-Free Business Security fornisce uno strumento per decodificare e ripristinare i file in caso sia necessario recuperare le informazioni che contiene. Worry-Free Business Security può decodificare e ripristinare i seguenti file:

TABELLA 14-2. File soggetti a decodifica e ripristino in Worry-Free Business Security

FILE	DESCRIZIONE
File messi in quarantena nel client	Questi file si trovano nelle seguenti directory: • `<Cartella di installazione Security Agent>\SUSPECT\Backup` oppure `<Cartella di installazione Security Agent>\quarantine`, a seconda di quella disponibile. • `<Cartella di installazione Messaging Security Agent>\storage\quarantine` Questi file vengono caricati nella directory di quarantena designata, tipicamente una directory sul Security Server.
File in quarantena nella directory di quarantena designata	Per impostazione predefinita, questa directory si trova nel computer Security Server (`<Cartella di installazione Security Server>\PCCSRV\Virus`). Per modificare la directory, andare su **Amministrazione** > **Impostazioni globali** > **scheda Sistema** e accedere alla sezione Manutenzione della quarantena.

File	Descrizione
File crittografati di backup	Si tratta del backup dei file infetti che gli agent sono riusciti a disinfettare. Questi file si trovano nelle seguenti cartelle: • `<Cartella di installazione Security Agent>\Backup` • `<Cartella di installazione Messaging Security Agent>\storage\backup` Per ripristinare questi file gli utenti devono trasferirli nella directory di quarantena sul client.

AVVERTENZA!

Il ripristino di un file infetto può causare la diffusione di virus/malware ad altri file e client. Prima di ripristinare il file, isolare il client infetto e trasferire i file importanti del client in un percorso di backup.

Decrittografia e ripristino di file sul Security Agent

Procedura

1. Aprire un prompt dei comandi e passare a `<Cartella di installazione Security Agent>`.
2. Digitare quanto riportato di seguito per eseguire `VSEncode.exe`:

   ```
   VSEncode.exe /u
   ```

   Questo parametro apre una schermata contenente un elenco dei file presenti in `<Cartella di installazione Security Agent>\SUSPECT\Backup`.

   Gli amministratori possono ripristinare i file classificati come spyware/grayware nella scheda Spyware/grayware. La schermata visualizza un elenco di file che si trovano in: `<Cartella di installazione Security Agent>\BackupAS`.
3. Selezionare un file da ripristinare e fare clic su **Ripristina**.

Nota

Lo strumento è in grado di ripristinare un solo file alla volta.

4. Nella schermata visualizzata specificare la cartella nella quale deve essere ripristinato il file.

5. Fare clic su **OK**.

Nota

Se l'agent esegue di nuovo la scansione del file subito dopo che è stato ripristinato, è possibile che venga considerato infetto. Per impedire la scansione del file, aggiungerlo all'elenco di esclusione della scansione.

Vedere *Destinazioni di scansione e azioni per i Security Agent a pagina 7-10*.

Il file viene ripristinato nella cartella specificata.

6. Fare clic su **Chiudi**.

Decrittografia e ripristino di file sul Security Server, directory di quarantena personalizzata o Messaging Security Agent

Procedura

1. Se il file si trova nel computer del Security Server, aprire un prompt dei comandi e passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility\VSEncrypt`.

   Se il file si trova in un client Messaging Security Agent o in una directory di quarantena personalizzata, passare a `<Cartella di installazione del server>\PCCSRV\Admin\Utility` e copiare la cartella `VSEncrypt` nel client o nella directory di quarantena personalizzata.

2. Creare un file di testo e digitare l'intero percorso dei file da codificare o decodificare.

Ad esempio, per ripristinare i file `C:\Documenti\Reports`, digitare `C:\Documenti\Reports\*.*` nel file di testo.

I file in quarantena nel computer del Security Server si trovano in `<Cartella di installazione del server>\PCCSRV\Virus`.

3. Salvare il file di testo con estensione `INI` o `TXT`. Ad esempio salvarlo con il nome `PerCrittografia.ini` nell'unità `C:` C:.

4. Aprire un prompt dei comandi e accedere alla directory in cui si trova la cartella `VSEncrypt`.

5. Digitare quanto riportato di seguito per eseguire `VSEncode.exe`:

   ```
   VSEncode.exe /d /i <percorso del file INI o TXT>
   ```

   Dove:

   `<percorso del file INI o TXT>` è il percorso del file `INI` o `TXT` creato (ad esempio `C:\ForEncryption.ini`).

6. Utilizzare gli altri parametri per ottenere comandi diversi.

TABELLA 14-3. Parametri di ripristino

PARAMETRO	DESCRIZIONE
Nessuno (nessun parametro)	Codifica i file
`/d`	Decodifica i file
`/debug`	Crea un registro di debug e lo salva nel computer. Nel client, il registro di debug `VSEncrypt.log` viene creato in `<Cartella di installazione dell'agent>`.
`/o`	Sovrascrive il file crittografato o decrittografato già esistente
`/f <nomefile>`	Codifica o decodifica un unico file.
`/nr`	Non ripristina il nome del file originale
`/v`	Visualizza le informazioni sullo strumento

Parametro	Descrizione
`/u`	Avvia l'interfaccia utente dello strumento
`/r <Cartella di destinazione>`	Cartella contenente il file ripristinato
`/s <Nome del file originale>`	Il nome del file crittografato originale

Ad esempio, è possibile digitare `VSEncode [/d] [/debug]` per decodificare i file nella cartella `Suspect` e creare un registro di debug. Quando si decodifica o si codifica un file, Worry-Free Business Security crea il file decodificato o codificato nella stessa cartella. Prima di decodificare o codificare un file, accertarsi che il file non sia bloccato.

Ripristino dei messaggi e-mail Transport Neutral Encapsulation Format

Transport Neutral Encapsulation Format (TNEF) è un formato di incapsulamento dei messaggi utilizzato da Microsoft Exchange/Outlook. In genere, questo formato viene trasformato in un allegato e-mail chiamato `Winmail.dat` e Outlook Express lo nasconde automaticamente.

Per ulteriori informazioni, vedere https://support.microsoft.com/en-us/help/290809/.

Se il Messaging Security Agent archivia questo tipo di messaggio e-mail e l'estensione del file viene modificata in .EML, Outlook Express visualizza solo il corpo del messaggio e-mail.

Utilizzo dello strumento ReGenID

Affinché il Security Server possa identificare i singoli agent, ogni installazione del Security Agent necessita di un GUID (Globally Unique Identifier, Identificatore univoco globale). Di norma si riscontrano GUID duplicati su client o macchine virtuali clonati.

Se due o più agent riportano lo stesso GUID, avviare lo strumento ReGenID per generare un GUID unico per ogni client.

Procedura

1. Nel Security Server, accedere alla seguente directory: `<Cartella di installazione del server>\PCCSRV\Admin\Utility`.
2. Copiare `WFBS_WIN_All_ReGenID.exe` in una cartella temporanea nel client in cui è installato il Security Agent.

   Esempio: `C:\temp`
3. Fare doppio clic su `WFBS_WIN_All_ReGenID.exe` e seguire le istruzioni sullo schermo.

   Lo strumento interrompe il Security Agent e rimuove il GUID del client.
4. Riavviare il Security Agent.

   Il Security Agent genera un nuovo GUID per il client.

Gestione dei componenti aggiuntivi di SBS e EBS

Worry-Free Business Security fornisce componenti aggiuntivi che consentono agli amministratori di visualizzare informazioni in tempo reale su sicurezza e stato dell'agent dalle console dei seguenti sistemi operativi Windows:

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

Installazione dei componenti aggiuntivi di SBS e EBS manualmente

Il componente aggiuntivo di SBS o EBS viene installato automaticamente quando si installa Security Server in un endpoint in cui vengono eseguiti i sistemi operativi supportati. Per utilizzare il componente aggiuntivo su un altro endpoint in cui vengono eseguiti i sistemi operativi supportati, è necessario installarlo manualmente.

Procedura

1. Accedere alla console Web di Security Server.
2. Andare su **Amministrazione** > **Strumenti di gestione**.
3. Fare clic su **Componenti aggiuntivi**.
4. Fare clic sul collegamento **Download** per scaricare il programma di installazione.
5. Copiare e avviare il programma di installazione nell'endpoint di destinazione.

Uso dei componenti aggiuntivi di SBS e EBS

Procedura

1. Aprire la console di SBS e EBS.
2. Nella scheda **Protezione**, fare clic su **Trend Micro Worry-Free Business Security** per visualizzare le informazioni sullo stato.

Appendice A

Icone dei Security Agent

Questa appendice descrive le varie icone dei Security Agent visualizzate sui client.

Controllo dello stato dei Security Agent

La seguente immagine mostra la console del Security Agent con tutte le funzionalità aggiornate e correttamente funzionanti:

Nella seguente tabella vengono elencate le icone e il rispettivo significato sull'interfaccia utente principale della console del Security Agent:

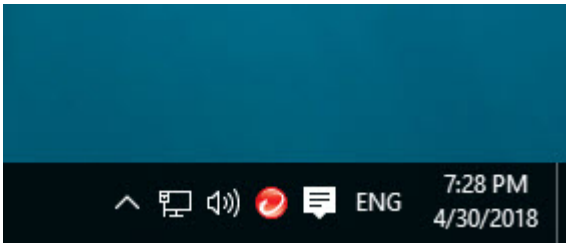
TABELLA A-1. Icone dell'interfaccia utente principale della console del Security Agent

ICONA	STATO	SPIEGAZIONE E AZIONE
	Protezione attiva: la protezione è attiva e il software è aggiornato	Il software è aggiornato e correttamente funzionante. Nessuna operazione richiesta.
	Riavvia il computer: riavviare il computer per completare la rimozione delle minacce alla sicurezza	Security Agent ha rilevato minacce che non possono essere risolte immediatamente. Riavviare il computer per completare la rimozione delle minacce.
	Protezione a rischio: Contattare l'amministratore	La scansione in tempo reale è stata disattivata o la protezione è a rischio per un'altra ragione. Attivare la scansione in tempo reale e se il problema non si risolve, contattare l'assistenza.
	Aggiorna ora: Non si riceve una aggiornamento da (numero) giorni.	Il pattern antivirus è precedente a 3 giorni. Aggiornare il Security Agent immediatamente.

Icona	Stato	Spiegazione e azione
	Smart Scan non disponibile: Verificare la connessione Internet	Security Agent non ha eseguito l'accesso al server di scansione da oltre 15 minuti. Verificare di essere collegati alla rete per eseguire la scansione con gli ultimi pattern.
	Riavvia il computer: Riavviare il computer per completare l'installazione dell'aggiornamento	Riavviare il computer per completare l'aggiornamento.
	Aggiornamento del programma: Il software di sicurezza si sta aggiornando	È in corso un aggiornamento. Non disconnettersi dalla rete fino al termine.

Visualizzazione delle icone di Security Agent nella barra delle applicazioni di Windows

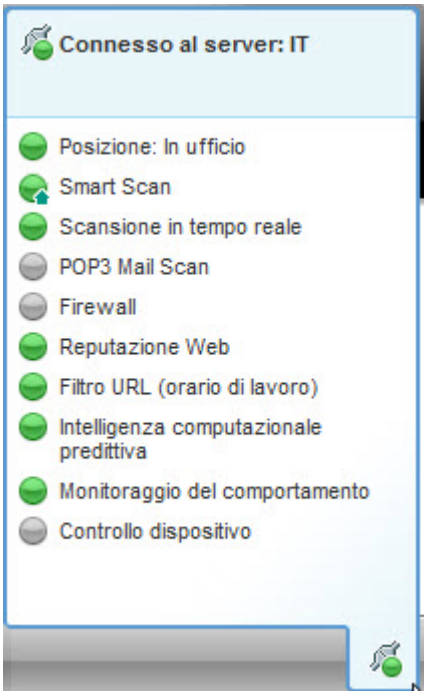
Nella barra delle applicazioni di Windows verranno visualizzate le seguenti icone di Security Agent:



Icona	Significato
	Lo stato è normale
	(Animato) Scansione manuale o Scansione pianificata in corso. Security Agent utilizza una scansione convenzionale o Smart Scan.
	Security Agent sta eseguendo un aggiornamento.
	È necessario effettuare un'operazione: • La scansione in tempo reale è disattivata • Per rimuovere completamente il malware è necessario eseguire un riavvio • È necessario eseguire un riavvio a causa di un aggiornamento del motore • È necessario eseguire un riavvio per ripristinare i file crittografati dal ransomware • È necessario effettuare l'aggiornamento **Nota** Aprire la console principale di Security Agent per verificare quale operazione è necessario eseguire.

Accesso al flyover della console

Il flyover della console Security Agent si aprirà passando il puntatore del mouse sull'icona piccola in basso a destra della console Security Agent.



Nella seguente tabella vengono elencate le icone del flyover della console e ne viene descritto significato:

TABELLA A-2. Icone del flyover della console

FUNZIONE	ICONA	SIGNIFICATO
Connessione		Collegato a Security Server
		Non collegato a Security Server, ma la scansione in tempo reale è ancora in esecuzione. Il file di pattern potrebbe non essere aggiornato. Fare clic con il pulsante destro sull'icona dell'agent nella barra delle applicazioni di Windows e selezionare **Aggiorna ora**.

Funzione	Icona	Significato
Percorso		In ufficio (rete interna)
		Fuori ufficio (rete esterna)
Scansione in tempo reale		Attivo
		Disattivo
POP3 Mail Scan		Attivo
		Disattivo
Smart Scan		Connesso a Trend Micro Smart Protection Network
		Impossibile connettersi a Smart Protection Network. La protezione risulta ridotta poiché i Security Agent non sono in grado di inviare query di scansione. **Nota** Verificare che TMiCRCScanService di Smart Scan Service sia in esecuzione e che Security Agent siano connessi a Security Server.
		La funzione Smart Scan è disattivata. Utilizzo della scansione convenzionale

Funzione	Icona	Significato
• Firewall • Reputazione Web • Filtro URL • Monitoraggio del comportamento • Controllo dispositivo • Intelligenza computazionale predittiva		Attivo
		Disattivo

Appendice B

Supporto dell'IPv6 in Worry-Free Business Security

La lettura di questa appendice è necessaria per gli utenti che intendono implementare Worry-Free Business Security in un ambiente che supporta l'indirizzamento IPv6. Questa appendice contiene informazioni sull'entità del supporto IPv6 in Worry-Free Business Security.

Trend Micro presume che il lettore conosca bene i concetti relativi a IPv6 e le attività necessarie per configurare una rete che supporti l'indirizzamento IPv6.

Supporto IPv6 per Worry-Free Business Security e i Security Agent

Il supporto IPv6 per Worry-Free Business Security è stato introdotto nella versione 8.0. Nelle versioni precedenti di Worry-Free Business Security, l'indirizzamento IPv6 non era supportato. Il supporto IPv6 viene attivato automaticamente dopo l'installazione o l'aggiornamento di Security Server, Security Agent e Messaging Security Agent che soddisfano i requisiti IPv6.

Requisiti IPv6 del Security Server

Di seguito sono elencati i requisiti IPv6 per il Security Server:

- Se il server deve gestire agent IPv4 e IPv6, deve disporre sia dell'indirizzo IPv4 che IPv6 e deve essere identificato tramite il nome host. Se il server viene identificato tramite il suo indirizzo IPv4, gli agent IPv6 puri non possono collegarsi al server. Lo stesso problema si verifica se client IPv4 puri si collegano a un server identificato tramite il suo indirizzo IPv6.
- Se il server deve gestire solo agent IPv6, il requisito minimo è un indirizzo IPv6. Il server può essere identificato tramite il nome host o l'indirizzo IPv6. Se il server viene identificato tramite il nome host, è preferibile utilizzare il suo nome di dominio completo (FQDN). Infatti, in un ambiente IPv6 puro, un server WINS non può tradurre un nome host nel suo corrispondente indirizzo IPv6.
- Verificare che l'indirizzo IPv6 o IPv4 della macchina host possa essere recuperato usando, ad esempio, il comando "`ping`" o "`nslookup`".
- Per installare il Security Server su un computer IPv6 puro, configurare un server proxy dual-stack in grado di convertire tra indirizzi IPv4 e IPv6 (come DeleGate). Posizionare il server proxy tra il Security Server e la rete Internet, al fine di consentire al server di collegarsi ai servizi gestiti da Trend Micro, ad esempio il server ActiveUpdate, il sito Web di registrazione online e Smart Protection Network.

Requisiti del Messaging Security Agent

Il Messaging Security Agent (solo Advanced) deve essere installato su un server Microsoft Exchange dual-stack o IPv6 puro.

Preferibilmente, il Messaging Security Agent dovrebbe disporre di indirizzi IPv4 e IPv6, in quanto alcune delle entità alle quale si connette supportano solo l'indirizzamento IPv4.

Limitazioni del server IPv6 puro

La tabella seguente elenca le limitazioni che si applicano al Security Server dotato solo di indirizzo IPv6.

TABELLA B-1. Limitazioni del server IPv6 puro

VOCE	LIMITAZIONE
Gestione di agent	Un server IPv6 puro non è in grado di: • Implementare agent sui client IPv4 puri • Gestire i agent IPv4 puri.
Aggiornamenti e gestione centralizzata	Un server IPv6 puro non è in grado di eseguire l'aggiornamento da origini IPv4 pure, come: • Server ActiveUpdate di Trend Micro • Qualsiasi origine aggiornamenti personalizzata IPv4 pura
Registrazione del prodotti, attivazione e rinnovo	Un server IPv6 puro non è in grado di connettersi al server per la registrazione online di Trend Micro per registrare il prodotto, ottenere la licenza e attivare o rinnovare la licenza.
Connessione proxy	Un server IPv6 puro non è in grado di stabilire la connessione attraverso un server proxy IPv4 puro.

Voce	Limitazione
Soluzioni plug-in	Un server IPv6 puro dispone di Plug-in Manager, ma non è in grado di implementare le soluzioni plug-in a: • Agent IPv4 puri o host IPv4 puri (a causa dell'assenza di una connessione diretta) • Agent IPv6 puri o host IPv6 puri in quanto nessuna delle soluzioni plug-in supporta l'IPv6.

È possibile superare molte di queste limitazioni impostando un server proxy dual-stack in grado di convertire gli indirizzi IPv4 in IPv6 e viceversa (come DeleGate). Posizionare il server proxy tra il Security Server e le entità alle quali si connette o che serve.

Limitazioni del Security Agent IPv6 puro

La tabella seguente elenca le limitazioni che si applicano quando il Security Agent ha un solo indirizzo IPv6.

Tabella B-2. Limitazioni del Security Agent IPv6 puro

Voce	Limitazione
Security Server principale	Gli agent IPv6 puri non possono essere gestiti da un Security Server IPv4 puro.
Aggiornamenti	Un Security Agent IPv6 puro non può eseguire l'aggiornamento da fonti aggiornamento IPv4 pure come: • Server ActiveUpdate di Trend Micro • Un Security Server IPv4 • Un Update Agent IPv4 puro • Qualsiasi origine aggiornamenti personalizzata IPv4 pura
Query di scansione e Smart Feedback	Un Security Agent IPv6 puro non è in grado di inviare query a Trend Micro Smart Protection Network e non può utilizzare il servizio Smart Feedback.

Voce	Limitazione
Soluzioni plug-in	Gli agent IPv6 puri non sono in grado di installare le soluzioni plug-in, in quanto nessuna di queste supporta IPv6.
Connessione proxy	Un client Security Agent IPv6 puro non può connettersi mediante un server proxy IPv4 puro.

È possibile superare molte di queste limitazioni impostando un server proxy dual-stack in grado di convertire gli indirizzi IPv4 in IPv6 e viceversa (come DeleGate). Posizionare il server proxy tra i Security Agent e le entità a cui sono connessi.

Configurazione indirizzi IPv6

La console Web consente di configurare un indirizzo IPv6 o un intervallo di indirizzi IPv6. Di seguito sono riportate alcune istruzioni per la configurazione.

- Worry-Free Business Security accetta presentazioni di indirizzi IPv6 standard.

  Ad esempio:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Worry-Free Business Security accetta inoltre indirizzi IPv6 con collegamento locale, come:

  `fe80::210:5aff:feaa:20a2`

AVVERTENZA!

Quando si specifica un indirizzo IPv6 con collegamento locale è necessario essere prudenti in quanto, anche se Worry-Free Business Security accetta l'indirizzo, potrebbe non funzionare come previsto in determinate circostanze. Ad esempio, non è possibile aggiornare i Security Agent da una fonte aggiornamenti se la fonte si trova in un altro segmento di rete ed è identificata dal corrispondente indirizzo IPv6 con collegamento locale.

- Quando l'indirizzo IPv6 fa parte di un URL, racchiuderlo tra parentesi quadre ([]).
- Per gli intervalli di indirizzi IPv6, generalmente sono necessari un prefisso e una lunghezza di prefisso. Per le configurazioni in cui il server esegue query degli indirizzi IP, si applicano le limitazioni della lunghezza del prefisso per evitare che si verifichino problemi di prestazioni quando il server esegue query su un numero elevato di indirizzi IP. Ad esempio, per la funzionalità Gestione server esterni, la lunghezza del prefisso deve essere compresa tra 112 (65.536 indirizzi IP) e 128 (2 indirizzi IP).
- Alcune impostazioni relative agli indirizzi o agli intervalli di indirizzi IPv6 vengono implementate sui Security Agent ma i Security Agent le ignorano. Ad esempio, se si configura l'elenco delle origini Smart Protection e si include uno Smart Protection Server identificato dal corrispondente indirizzo IPv6, i Security Agent IPv4 puri ignoreranno il server e si collegheranno alle altre origini Smart Protection.

Schermate che visualizzano gli indirizzi IP

In questa argomento sono enumerate le posizioni della console Web in cui sono visualizzati gli indirizzi IP.

- Struttura dei gruppi di protezione

  Ogni volta che compare la Struttura dei gruppi di protezione, gli indirizzi IPv6 degli agent IPv6 compaiono sotto alla colonna **Indirizzo IP**. Per gli agent dual-stack, gli indirizzi IPv6 sono visualizzati se sono stati utilizzati per la registrazione al server.

Nota

L'indirizzo IP utilizzato dagli agent dual-stack durante la registrazione sul server è visibile nella sezione **Indirizzo IP preferito** in **Amministrazione** > **Impostazioni globali** > **scheda Desktop/Server**.

Quando si esportano le impostazioni dell'agent in un file, gli indirizzi IPv6 si trovano anche nel file esportato.

- Registri

  Gli indirizzi IPv6 degli agent dual-stack e IPv6 puri sono visualizzati nei registri.

Appendice C

Assistenza tecnica

Ulteriori informazioni sui seguenti argomenti:

- *Risorse per la risoluzione dei problemi a pagina C-2*
- *Come contattare Trend Micro a pagina C-3*
- *Invio di contenuti sospetti a Trend Micro a pagina C-4*
- *Altre risorse a pagina C-6*

Risorse per la risoluzione dei problemi

Prima di contattare l'assistenza tecnica, consultare le seguenti risorse online di Trend Micro.

Utilizzo del portale di supporto

Il portale Assistenza Trend Micro è una risorsa online attiva 24 ore su 24, sette giorni su sette, che contiene le informazioni più aggiornate su problemi sia comuni che insoliti.

Procedura

1. Accedere a https://success.trendmicro.com.
2. Effettuare la selezione tra i prodotti disponibili o fare clic sull'apposito pulsante per avviare la ricerca di soluzioni.
3. Per cercare le soluzioni possibili, utilizzare la casella **Cerca assistenza**.
4. Se non viene individuata alcuna soluzione, fare clic su **Contatta supporto** e selezionare il tipo di supporto necessario.

   Suggerimento

   Per segnalare un caso di assistenza online, visitare la pagina al seguente URL:

   https://success.trendmicro.com/smb-new-request

   Il caso viene esaminato da un addetto all'assistenza tecnica di Trend Micro e la risposta giungerà nell'arco di 24 al massimo.

Enciclopedia delle minacce

La maggior parte delle minacce informatiche di oggi è costituita da minacce miste, ovvero dalla combinazione di due o più tecnologie ideata per

bypassare i protocolli di sicurezza dei computer. Trend Micro ostacola queste minacce complesse con prodotti pensati per creare una strategia di difesa personalizzata. L'Enciclopedia delle minacce fornisce un elenco esauriente di nomi e sintomi delle varie miscele di minacce, incluse minacce informatiche conosciute, spam, URL dannosi, nonché vulnerabilità conosciute.

Per ulteriori informazioni, vedere https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware:

- Minacce informatiche e codici mobili dannosi attualmente attivi o in circolazione
- Pagine informative sulle minacce correlate, per una descrizione degli attacchi Web completa.
- Avvisi sulle minacce Internet riguardanti gli attacchi mirati e le minacce per la sicurezza
- Informazioni sull'andamento online e sugli attacchi Web
- Resoconti settimanali sulle minacce informatiche

Come contattare Trend Micro

È possibile contattare gli addetti di Trend Micro via telefono o e-mail:

Indirizzo	TREND MICRO Italy S.r.l. Edison Park Center Viale Edison 110 - Edificio C 20099 Sesto San Giovanni (MI) Italia
Telefono	+39 02 925931
Sito Web	https://www.trendmicro.com
Indirizzo e-mail	support@trendmicro.com

- Uffici di assistenza nel mondo:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Come contattare Trend Micro:

  http://www.trendmicro.it/informazioni/contatti/index.html

- Documentazione dei prodotti Trend Micro

  https://docs.trendmicro.com

Semplificazione della chiamata all'assistenza tecnica

Per migliorare la risoluzione dei problemi, tenere a disposizione le seguenti informazioni:

- Passaggi che hanno causato il problema
- Informazioni sulla rete o sulle apparecchiature
- Marca e modello del computer ed eventuale hardware aggiuntivo o dispositivi collegati
- Quantità di memoria e spazio libero su disco
- Sistema operativo e versione del service pack
- Versione dell'Agent installato
- Numero di serie o codice di attivazione
- Descrizione dettagliata dell'ambiente di installazione
- Testo esatto di eventuali messaggi di errore ricevuti

Invio di contenuti sospetti a Trend Micro

Sono disponibili numerose opzioni per inviare contenuti sospetti a Trend Micro per ulteriore analisi.

Email Reputation Services

Inviare una query per la reputazione di un indirizzo IP specific e indicare un agente di trasferimento del messaggio da includere nell'elenco approvali globale:

https://servicecentral.trendmicro.com/en-us/ers/

Consultare il seguente articolo della Knowledge Base per esempi dei messaggi da inviare a Trend Micro:

https://success.trendmicro.com/solution/1112106

Servizi di reputazione file

Raccogliere le informazioni di sistema e inviare il contenuto del file dannoso a Trend Micro:

https://success.trendmicro.com/solution/1059565

Annotare il numero di pratica per riferimenti futuri.

Servizi di reputazione Web

Inviare una query sulla classificazione della sicurezza e sul tipo di contenuto di un URL sospettato di phishing o di altri cosiddetti "vettori di infezioni" (fonte intenzionale di minacce Internet quali spyware e minacce informatiche).

https://global.sitesafety.trendmicro.com/

se la classificazione assegnata è corretta, reinviare una nuova richiesta di classificazione a Trend Micro.

Altre risorse

Oltre alle soluzioni e all'assistenza, online sono disponibili molte altre risorse per rimanere aggiornati, conoscere le innovazioni ed essere informati sulle ultime novità che riguardano la sicurezza.

Centro di download

Periodicamente, Trend Micro rilascia una patch per il problema noto riportato oppure un aggiornamento applicabile ad un servizio o a un prodotto specifico. Per consultare le patch disponibili, accedere a:

https://www.trendmicro.com/download/

Se una patch non è stata applicata (ogni patch ha una data) aprire il file Readme e determinare se si tratta di una patch rilevante per l'ambiente di riferimento. Il file Readme contiene inoltre le istruzioni per l'installazione.

Riscontri sulla documentazione

Trend Micro si impegna continuamente a migliorare la propria documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, visitare il seguente sito:

https://docs.trendmicro.com/en-us/survey.aspx

Appendice D

Nozioni e terminologia prodotti

Gli elementi contenuti in questa appendice forniscono ulteriori informazioni su prodotti e tecnologie Trend Micro.

Patch critica

Una patch critica risolve i problemi di sicurezza e può essere implementata su tutti i clienti. Le patch critiche Windows includono un programma di installazione al contrario delle patch non Windows che di solito dispongono di uno script di installazione.

Hotfix

Una hot fix è un accorgimento o una soluzione a un problema specifico riscontrato dagli utenti. Le hot fix sono specifiche per determinati problemi e pertanto non vengono distribuiti a tutti i clienti. Le hot fix Windows comprendono un programma di installazione a differenza delle hot fix non Windows che non lo comprendono (di solito è necessario interrompere i daemon, copiare il file per sovrascriverne la controparte nell'installazione personale e riavviare i daemon).

IntelliScan

IntelliScan è un metodo di identificazione dei file da analizzare. Per i file eseguibili (ad esempio `.exe`), il tipo di file effettivo viene determinato in base al suo contenuto. Per i file non eseguibili (ad esempio `.txt`), il tipo di file effettivo viene determinato in base all'intestazione del file.

L'utilizzo di IntelliScan offre i vantaggi illustrati di seguito:

- Ottimizzazione delle prestazioni: IntelliScan non influisce sulle applicazioni del agente perché utilizza risorse di sistema minime.
- Periodo di scansione più breve: IntelliScan utilizza l'identificazione del tipo di file effettivo; sottopone a scansione solo i file che sono vulnerabili alle infezioni. Il tempo di scansione risulta quindi sensibilmente ridotto rispetto alla scansione di tutti i file.

IntelliTrap

IntelliTrap è la tecnologia euristica di Trend Micro utilizzata per individuare le minacce che si servono della compressione in tempo reale associata ad altre caratteristiche delle minacce informatiche, come i packer. Tra queste minacce ricordiamo virus/malware, worm, cavalli di Troia, backdoor e bot. Gli sviluppatori di virus spesso cercano di aggirare il filtro di virus/minacce informatiche utilizzando diversi sistemi di compressione. IntelliTrap è una tecnologia per motore di scansione in tempo reale, basata su regole e sul riconoscimento di pattern, che è in grado di rilevare e rimuovere virus/malware noti contenuti nei file compressi fino a 17 livelli di profondità creati con uno fra i 16 tipi di compressione più diffusi.

Nota

IntelliTrap utilizza lo stesso motore della scansione antivirus. Di conseguenza, le regole di gestione e scansione dei file per IntelliTrap coincidono con quelle definite dall'amministratore per la scansione antivirus.

L'agent inserisce i rilevamenti di bot e altre minacce informatiche nel registro di IntelliTrap. È possibile esportare i contenuti del registro di IntelliTrap per includerli nei rapporti.

Quando esegue la verifica per rilevare bot e altre minacce informatiche, IntelliTrap utilizza i seguenti componenti:

- Motore di scansione virushzw100
- Pattern IntelliTrap
- Pattern eccezioni IntelliTrap

Sistema di rilevamento anti-intrusione

Il sistema di rilevamento anti-intrusione (IDS) facilita l'identificazione dei pattern nei pacchetti di rete che possono indicare un attacco al dispositivo.

Il sistema di rilevamento anti-intrusione (IDS) aiuta a impedire le seguenti intrusioni note:

Intrusione	Descrizione
frammento troppo grande	Attacco DoS (Denial of Service) in cui un hacker dirige un pacchetto TCP/UDP di dimensioni eccessive sul dispositivo di destinazione. Può causare l'overflow del buffer, che può causare il blocco o il riavvio del dispositivo.
Ping of Death	Attacco DoS (Denial of Service) in cui un hacker dirige un pacchetto ICMP/ICMPv6 di dimensioni eccessive sul dispositivo di destinazione. Può causare l'overflow del buffer, che può causare il blocco o il riavvio del dispositivo.
conflitto ARP	Tipo di attacco in cui un hacker invia una richiesta ARP (Address Resolution Protocol) a un dispositivo di destinazione utilizzando lo stesso indirizzo IP come origine e come destinazione. Il dispositivo oggetto dell'attacco comincia a inviare continuamente una risposta ARP (il suo indirizzo MAC) a se stesso, con conseguente blocco del dispositivo.
flooding SYN	Attacco DoS (Denial of Service) in cui un programma invia al dispositivo più pacchetti di sincronizzazione (SYN) TCP, causando un invio continuo di risposte di riconoscimento della sincronizzazione (SYN/ACK) da parte del dispositivo. Ciò può esaurire la memoria del dispositivo e causare guasti del dispositivo.
frammenti sovrapposti	In modo analogo al teardrop, questo attacco DoS (Denial of Service) invia al dispositivo frammenti TCP sovrapposti. Questo causa la sovrascrittura delle informazioni di intestazione del primo frammento TCP che potrebbe così oltrepassare un firewall. Il firewall, a questo punto, potrebbe consentire l'accesso ai successivi frammenti contenenti il codice maligno permettendo loro di raggiungere il dispositivo di destinazione.
Teardrop	Questo attacco DoS (Denial of Service) simile all'attacco a frammenti sovrapposti, utilizza dei frammenti IP. Un valore di offset errato all'interno del secondo o di altri frammenti IP può causare il blocco del sistema operativo del dispositivo ricevente nel momento in cui tenta di riassemblare i frammenti.
attacco frammento minuscolo	Tipo di attacco in cui un frammento TCP di dimensioni minime forza le informazioni di intestazione del primo pacchetto TCP all'interno del frammento successivo. In questo modo potrebbero essere ignorati i frammenti successivi che potrebbero contenere dati dannosi.

Intrusione	Descrizione
IGMP frammentato	Attacco DoS (Denial of Service) che invia pacchetti IGMP frammentati a un dispositivo di destinazione, che non riesce a elaborarli correttamente. Ciò può bloccare il dispositivo o rallentarne le attività.
attacco LAND	Tipo di attacco che invia al dispositivo pacchetti di sincronizzazione (SYN) IP contenenti lo stesso indirizzo come origine e come destinazione facendo in modo che il dispositivo invii la risposta di riconoscimento della sincronizzazione (SYN/ACK) a se stesso. Ciò può bloccare il dispositivo o rallentarne le attività.

Parole chiave

In Worry-Free Business Security, le parole chiave comprendono le voci riportate di seguito e vengono utilizzate per filtrare i messaggi:

- Parole (pistole, bombe e così via)
- Numeri (1,2,3 e così via)
- Caratteri speciali (&, # , + e così via)
- Frasi brevi (pesce blu, telefono rosso, casa grande e così via)
- Parole o frasi collegate con operatori logici (mele .AND. arance)
- Parole o frasi che utilizzano espressioni regolari (.REG. a.*e corrisponde a "ace", "ape" e "avanzate", ma non a "avv", "api" o "antivirus")

Worry-Free Business Security può importare un elenco di parole chiave esistente da un file di testo (`.txt`). Le parole chiave importate vengono visualizzate nell'elenco di parole chiave.

Operatori sulle parole chiave

Gli operatori sono comandi in grado di unire più parole. Gli operatori possono ampliare o restringere i risultati di un criterio. Racchiudere gli operatori tra punti (.). Ad esempio:

```
mele .AND. arance e mele .NOT. arance
```

Nota

L'operatore contiene un punto immediatamente prima e dopo. È presente uno spazio tra il punto finale e la parola chiave.

TABELLA D-1. Uso degli operatori

OPERATORE	FUNZIONAMENTO	ESEMPIO
qualsiasi parola chiave	Il Messaging Security Agent cerca i contenuti che corrispondono alla parola	Immettere la parola e aggiungerla all'elenco delle parole chiave
OR	Il Messaging Security Agent cerca eventuali parole chiave separate da OR Ad esempio, mela OR arancia. L'agent cerca la parola mela o arancia. Se nei contenuti è presente una di queste parole, viene rilevata una corrispondenza.	Digitare "`.OR.`" tra tutte le parole che si desidera includere. Ad esempio, "mela .OR. arancia"
AND	Il Messaging Security Agent cerca tutte le parole chiave separate da AND Ad esempio, mela AND arancia. L'agent cerca sia la parola mela che la parola arancia. Se nei contenuti non sono presenti entrambe le parole, non viene rilevata alcuna corrispondenza.	Digitare "`.AND.`" tra tutte le parole che si desidera includere. Ad esempio, "mela .AND. arancia"

Operatore	Funzionamento	Esempio
NOT	Il Messaging Security Agent esclude dalla ricerca le parole chiave che seguono NOT. Ad esempio, .NOT. succo. L'agent cerca i contenuti che non contengono la parola succo. Se il messaggio contiene "spremuta d'arancia", viene rilevata una corrispondenza, ma se contiene "succo d'arancia", non ne viene rilevata alcuna.	Digitare "`.NOT.`" prima della parola che si desidera escludere. Ad esempio, ".NOT. succo"
WILD	Il simbolo del carattere jolly sostituisce la parte mancante di una parola. Vengono rilevate tutte le corrispondenze con qualsiasi parola contenga la parte non sostituita dal carattere jolly. **Nota** Il Messaging Security Agent non supporta l'utilizzo del carattere "?" nel comando con carattere jolly ".WILD.".	Digitare "`.WILD.`" prima delle parti della parola che si desidera includere. Ad esempio, se si desidera individuare tutte le parole che contengono "valu", digitare "`.WILD.valu`". Le parole Valumart, valutazione e valutario vengono considerate corrispondenze.
REG	Per specificare un'espressione regolare, aggiungere un operatore .REG. prima del modello (ad esempio, .REG. a.*e). Vedere *Espressioni regolari a pagina D-10*.	Digitare "`.REG.`" prima del modello della parola che si desidera rilevare. Ad esempio, ".REG. a.*e" corrisponde a: "ace", "ape" e "salmastre", ma non "avv", "api" o "antivirus"

Uso efficace delle parole chiave

Messaging Security Agent mette a disposizione degli utenti funzioni semplici e potenti per creare filtri estremamente specifici. Durante la creazione delle regole di filtro del contenuto, è importante ricordare che:

- Per impostazione predefinita, Messaging Security Agent cerca corrispondenze esatte con le parole chiave. Utilizzare le espressioni regolari per cercare corrispondenze parziali delle parole chiave. Vedere *Espressioni regolari a pagina D-10*.
- Il Messaging Security Agent analizza diversamente più parole chiave sulla stessa riga, più parole chiave di cui ciascuna su righe diverse e più parole chiave separate da virgola, punto, trattino o altri segni di punteggiatura. Per ulteriori informazioni sull'uso delle parole chiave su più righe, vedere la tabella seguente.
- È possibile impostare Messaging Security Agent in modo che cerchi sinonimi delle parole chiave.

TABELLA D-2. Modalità di utilizzo delle parole chiave

SITUAZIONE	ESEMPIO	CORRISPONDENZA/MANCATA CORRISPONDENZA
Due parole in una stessa riga	pistole bombe	Corrispondenza: "Fare clic qui per acquistare pistole, bombe e altre armi." Mancata corrispondenza: "Fare clic qui per acquistare pistole e bombe."
Due parole separate da una virgola	pistole, bombe	Corrispondenza: "Fare clic qui per acquistare pistole, bombe e altre armi." Mancata corrispondenza: "Fare clic qui per acquistare pistole usate, bombe nuove e altre armi."

Situazione	Esempio	Corrispondenza/Mancata corrispondenza
Più parole su righe multiple	pistole bombe armi e munizioni	Se si seleziona **Qualsiasi parola chiave specificata** Corrispondenza: "Pistole in vendita" Altra corrispondenza: "Acquista pistole, bombe e altre armi." Se si seleziona **Tutte le parole chiave specificate** Corrispondenza: "Acquista pistole bombe armi e munizioni" Mancata corrispondenza: "Acquista pistole bombe armi munizioni." Altra mancata corrispondenza: "Acquista pistole, bombe, armi e munizioni"
Più parole chiave sulla stessa riga	pistole bombe armi munizioni	Corrispondenza: "Acquista pistole bombe armi munizioni" Mancata corrispondenza: "Acquista munizioni per le tue pistole e armi e nuove bombe"

Patch

La patch è un gruppo di hotfix e patch di protezione che consente di risolvere più problemi di un programma. Trend Micro rende disponibili le patch regolarmente. Le patch Windows includono un programma di installazione al contrario delle patch non Windows che di solito dispongono di uno script di installazione.

Espressioni regolari

Le espressioni regolari vengono utilizzate per effettuare la ricerca di stringhe. Consultare le seguenti tabelle per alcuni esempi di espressioni regolari. Per specificare un'espressione regolare, aggiungere un operatore ".REG." prima del modello.

In Internet, sono disponibili diversi siti Web ed esercitazioni online. Uno di questi siti è PerlDoc, all'indirizzo:

http://www.perl.com/doc/manual/html/pod/perlre.html

AVVERTENZA!

Le espressioni regolari sono un potente strumento di ricerca delle stringhe. Per questo motivo, Trend Micro consiglia agli amministratori che decidono di utilizzarle di acquisire familiarità e dimestichezza con la sintassi delle espressioni regolari. Le espressioni regolari scritte con una sintassi errata possono avere un impatto decisamente negativo sulle prestazioni. Trend Micro suggerisce di cominciare con espressioni regolari semplici che non utilizzano una sintassi complessa. Quando si introducono delle nuove regole, utilizzare l'azione di archiviazione e osservare il modo in cui il Messaging Security Agent gestisce i messaggi che utilizzano la regola introdotta. Quando si è certi che la regola non ha conseguenze impreviste, è il momento di modificare l'azione.

Esempi di espressione regolare

Consultare le seguenti tabelle per alcuni esempi di espressioni regolari. Per specificare un'espressione regolare, aggiungere un operatore ".REG." prima del modello.

TABELLA D-3. Conteggio e raggruppamento

ELEMENTO	SIGNIFICATO	ESEMPIO
.	Il punto rappresenta qualsiasi carattere salvo quello per passare a una nuova riga.	do. rileva don, dovere, dorato, dos, dot, ecc. d.e rileva dove, dolore, ecc.

Elemento	Significato	Esempio
*	L'asterisco indica nessuna o varie occorrenze dell'elemento precedente.	no* rileva n, no, noo, nooo, noooo, ecc.
+	Il più indica una o varie occorrenze dell'elemento precedente.	no+ rileva no, noo, nooo, noooo, ecc. ma non n
?	Il punto interrogativo indica nessuna o una occorrenza dell'elemento precedente.	no?n rileva nn o non ma non noon, nooon ecc.
( )	Le parentesi permettono di considerare tutti i caratteri inclusi al loro interno come un'unica entità.	d(opo)+ rileva o dopoopo o dopoopoopo ecc. Il carattere + viene applicato alla sottostringa tra parentesi affinché la regex cerchi la d seguita da una o più occorrenze della stringa "opo".
[ ]	Le parentesi quadre indicano un insieme o una serie di caratteri.	d[aeiou]+ rileva da, de, di, do, du, daa, dae, dai, ecc. Il carattere + viene applicato all'insieme di caratteri tra parentesi quadre affinché la regex cerchi la d seguita da una o più occorrenze dei caratteri presenti [aeiou]. d[A-Z] rileva dA, dB, dC, e così via fino a dZ. L'insieme di caratteri tra parentesi quadre rappresenta la serie di tutte le lettere maiuscole comprese tra A e Z.
[^]	Il carattere accento circonflesso racchiuso tra parentesi quadre nega logicamente l'insieme o l'intervallo specificati; in tal modo la regex trova la corrispondenza tra qualsiasi carattere che non sia incluso nell'insieme o nell'intervallo.	d[^aeiouy] trova db, dc o dd, d9, d#--d seguiti da qualsiasi carattere singolo ad eccezione di una vocale.

Elemento	Significato	Esempio
{ }	I caratteri parentesi graffa specificano un numero determinato di occorrenze dell'elemento precedente. Un singolo valore all'interno delle parentesi graffe significa che verrà individuato soltanto il numero di occorrenze specificato. Una coppia di numeri separati da una virgola rappresenta un insieme di occorrenze valide del carattere precedente. Una singola cifra seguita da una virgola significa che non esiste alcun limite superiore.	da{3} trova daaa--d seguito da 3 occorrenze e non più di 3 di "a". da{2,4} trova daa, daaa, daaaa e daaaa (ma non daaaaa)--d seguiti da 2, 3 o 4 occorrenze di "a". da{4,} trova daaaa, daaaaa, daaaaaa ecc.--d seguiti da almeno 4 occorrenze di "a".

Tabella D-4. Classi di caratteri (stenografia)

Elemento	Significato	Esempio
\d	Qualsiasi carattere numerico; a livello di funzione, equivale a [0-9] o [[:digit:]].	\d trova 1, 12, 123 ecc. ma non 1b7--uno o più caratteri numerici.
\D	Qualsiasi carattere non numerico; a livello di funzione, equivale a [^0-9] o [^[:digit:]].	\D trova a, ab, ab& ma non 1, ossia uno o più caratteri esclusi 0, 1, 2, 3, 4, 5, 6, 7, 8 o 9.
\w	Qualsiasi lettera, vale a dire qualsiasi carattere alfanumerico; a livello di funzione, equivale a [_A-Za-z0-9] o [_[:alnum:]]	\w trova a, ab, a1 ma non !&--una o più lettere maiuscole o minuscole o cifre ma non la punteggiatura o altri caratteri speciali.
\W	Qualsiasi carattere non alfanumerico; a livello di funzione, equivale a [^_A-Za-z0-9] o [^_[:alnum:]].	\W trova *, & ma non ace o a1--uno o più caratteri eccetto lettere maiuscole o minuscole e cifre.
\s	Qualsiasi carattere spazio vuoto; spazio, nuova riga, tabulatore, spazio unificatore ecc.; a livello di funzione, equivale a [[:space]].	verdura\\s trova "verdura" seguito da un carattere spazio vuoto. Quindi la frase "Sono un fan della musica rock" avvia la regex, mentre "Siamo fans della musica rock" no.

Elemento	Significato	Esempio
\S	Uno spazio non vuoto; qualsiasi carattere diverso da uno spazio, da una nuova riga, da un carattere tabulatore, da uno spazio unificatore ecc.; a livello di funzione, equivale a [^[:space]].	verdura\\S trova "verdura" seguito da un carattere diverso da spazio vuoto. Quindi la frase "Siamo fans della musica rock" avvia la regex, mentre "Sono un fan della musica rock" no.

Tabella D-5. Classi di caratteri

Elemento	Significato	Esempio
[:alpha:]	Qualsiasi carattere alfabetico	.REG. [[:alpha:]] trova abc, def, xxx ma non 123 o @#$.
[:digit:]	Qualsiasi cifra; a livello di funzione, equivale a \d	.REG. [[:digit:]] trova 1, 12, 123 ecc.
[:alnum:]	Qualsiasi "lettera", vale a dire qualsiasi carattere alfanumerico; a livello di funzione, equivale a \w.	.REG. [[:alnum:]] trova abc, 123 ma non ~!@.
[:space:]	Qualsiasi carattere spazio vuoto; spazio, nuova riga, carattere tabulatore, spazio unificatore ecc.; a livello di funzione, equivale a \s.	.REG. (fan)[[:space:]] trova "fan" seguito da un carattere spazio vuoto. Quindi la frase "Sono un fan della musica rock" avvia la regex, mentre "Siamo fans della musica rock" no.
[:graph:]	Qualsiasi carattere esclusi gli spazi, i caratteri di controllo e caratteri simili.	.REG. [[:graph:]] trova 123, abc, xxx, >< ma non lo spazio o i caratteri di controllo.
[:print:]	Qualsiasi carattere (simile a [:graph:]) ma comprende il carattere spazio.	.REG. [[:print:]] trova 123, abc, xxx, >< e i caratteri spazio.
[:cntrl:]	Qualsiasi carattere di controllo (ad es. CTRL + C, CTRL + X)	.REG. [[:cntrl:]] trova 0x03, 0x08 ma non abc, 123, !@#.
[:blank:]	Caratteri spazio e tabulatore	.REG. [[:blank:]] trova i caratteri spazio e tabulatore ma non 123, abc, !@#

Elemento	Significato	Esempio
[:punct:]	Caratteri punteggiatura.	.REG. [[:punct:]] trova ; : ? ! ~ @ # $ % & * ‘ “ ecc. ma non 123, abc
[:lower:]	Qualsiasi carattere alfabetico minuscolo (Nota: Selezionare l'opzione 'Attiva corrispondenza maiuscole/minuscole', altrimenti il funzionamento è identico a quello di [:alnum:])	.REG. [[:lower:]] trova abc, Def, sTress, Do, ecc. ma non ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Qualsiasi carattere alfabetico maiuscolo (Nota: Selezionare l'opzione 'Attiva corrispondenza maiuscole/minuscole', altrimenti il funzionamento è identico a quello di [:alnum:])	.REG. [[:upper:]] trova ABC, DEF, STRESS, DO ecc. ma non abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Cifre consentite in un numero esadecimale (0-9a-fA-F).	.REG. [[:xdigit:]] trova 0a, 7E, 0f ecc.

Tabella D-6. Ancoraggi di pattern

Elemento	Significato	Esempio
^	Indica l'inizio di una stringa.	^(benché) trova qualsiasi blocco di testo che comincia con "benché". Quindi, la frase "benché io sia un fan della musica" avvia la regex mentre "Io sono un fan della musica benché" no.
$	Indica la fine di una stringa.	(benché)$ trova qualsiasi blocco di testo che finisce con "benché". Quindi, la frase "benché io sia un fan della musica" non avvia la regex mentre "Io sono un fan della musica benché" sì.

TABELLA D-7. Sequenze di escape e stringhe letterali

ELEMENTO	SIGNIFICATO	ESEMPIO
\	Per trovare alcuni caratteri che hanno un significato particolare nelle espressioni regolari (ad esempio "+").	(1) .REG. C\\C\+\+ trova 'C\C++'. (2) .REG. * trova *. (3) .REG. \? trova ?.
\t	Indica un carattere tabulatore.	(pane)\\t trova qualsiasi blocco di testo che contiene la sottostringa "pane" immediatamente seguita da un carattere tabulatore (ASCII 0x09).
\n	Indica il carattere della nuova riga. **Nota** piattaforme diverse hanno modi diversi di rappresentare il carattere di nuova riga. In Windows, una nuova riga è rappresentata da una coppia di caratteri, un ritorno a capo seguito da un salto di riga. In Unix e Linux, una nuova riga è semplicemente un salto di riga, e nei Macintosh una nuova riga è semplicemente un ritorno a capo.	(pane)\n\n trova qualsiasi blocco di testo che contenga la sottostringa "pane" immediatamente seguita da due caratteri di nuova riga (ASCII 0x0A).
\r	Indica un carattere ritorno a capo.	(pane)\r trova qualsiasi blocco di testo che contenga la sottostringa "pane" immediatamente seguita da un carattere ritorno a capo (ASCII 0x0D).

Elemento	Significato	Esempio
\b	Indica un carattere backspace. OR Segnala limiti.	(pane)\b trova qualsiasi blocco di testo che contenga la sottostringa “pane” immediatamente seguita da un carattere backspace (ASCII 0x08). Un limite di parola (\b) è un punto tra due caratteri con \w da un lato e \W dall'altro (in qualsiasi ordine), ritenendo i caratteri immaginari all'inizio e alla fine della stringa corrispondenti a \W. (nelle classi di caratteri \b rappresenta il backspace piuttosto che un limite di parola). Ad esempio, la seguente espressione regolare può corrispondere al codice fiscale: .REG. \b\d{3}-\d{2}-\d{4}\b
\xhh	Indica un carattere ASCII con un determinato codice esadecimale (dove hh rappresenta un valore esadecimale a due cifre).	\x7E(\w){6} trova qualsiasi blocco di testo contenente una "parola" composta esattamente da sei caratteri alfanumerici preceduti da un carattere ~ (tilde). Quindi, vengono trovate le parole '~ab12cd', '~Pa3499' ma non la parola '~oops'.

Generatore di espressioni regolari

Quando si stabilisce come configurare le regole per Prevenzione della perdita di dati, considerare che il generatore dell'espressione regolare è in grado di creare solo espressioni semplici in base alle seguenti regole e limitazioni:

- Solo i caratteri alfanumerici possono essere variabili.
- Tutti gli altri caratteri, quali [-], [/] e così via possono essere solo costanti.

- Gli intervalli di variabili possono essere solo A-Z e 0-9; non è possibile stabilire altri limiti, ad esempio A-D.
- Le espressioni regolari generate da questo strumento sono indipendenti dall'uso di maiuscole e minuscole.
- Le espressioni regolari generate da questo strumento possono effettuare solo corrispondenze positive, non negative ("se non corrisponde").
- Le espressioni basate sul campione possono corrispondere solo al numero esatto di caratteri e spazi riportati nel campione. Lo strumento non è in grado di generare la corrispondenza "uno o più" di un determinato carattere o stringa.

Sintassi con espressioni complesse

Una parola chiave è composta da token, cioè le più piccole unità utilizzate per individuare corrispondenze tra l'espressione e il contenuto. Un token può essere un operatore, un simbolo logico o l'operando, vale a dire l'argomento o il valore su cui agisce l'operatore.

Gli operatori includono .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., ".(." e " .)." L'operando e l'operatore devono essere separati da uno spazio. Un operando può contenere vari token. Vedere *Parole chiave a pagina D-5*.

Espressioni regolari all'opera

L'esempio seguente descrive il funzionamento del filtro di contenuti delle tessere sanitarie, uno dei filtri predefiniti:

[Formato] .REG. \b\d{3}-\d{2}-\d{4}\b

L'espressione precedente utilizza \b, un carattere backspace, seguito da \d, qualsiasi cifra e da {x}, che indica il numero di cifre, e infine da -, il trattino. Questa espressione trova il codice fiscale. La tabella seguente descrive le stringhe che trovano l'espressione regolare esemplificativa:

TABELLA D-8. Numeri che corrispondono all'espressione regolare per i codici fiscali

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Corrisponde

333224444	Non corrisponde
333 22 4444	Non corrisponde
3333-22-4444	Non corrisponde
333-22-44444	Non corrisponde

Se si modifica l'espressione come segue,

[Formato] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

la nuova espressione trova questa sequenza:

333 22 4444

Elenco di esclusione scansione

Elenco di esclusione scansione per Security Agent

Questo elenco di esclusione contiene tutti i prodotti Trend Micro che vengono esclusi dalla scansione per impostazione predefinita.

TABELLA D-9. Elenco di esclusione Security Agent

NOME DEL PRODOTTO	PERCORSO DI INSTALLAZIONE
InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion` `ProgramDirectory=`
ScanMail eManager (ScanMail per Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion` `ProgramDirectory=`

Nome del prodotto	Percorso di installazione
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Directory programma= C:\Programmi\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=

Nome del prodotto	Percorso di installazione
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

Nome del prodotto	Percorso di installazione
ScanMail per Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

Nome del prodotto	Percorso di installazione
ScanMail per Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= Ottenere il percorso al file exclusion.txt da HKEY_LOCAL_MACHINE\\SOFTWARE\\TrendMicro\\ScanMail for Microsoft Exchange\\CurrentVersion\\HomeDir Passare al percorso HomeDir (ad esempio, C:\Programmi\Trend Micro\Messaging Security Agent\) Aprire exclusion.txt C:\Programmi\Trend Micro\Messaging Security Agent \Temp\ C:\Programmi\Trend Micro\Messaging Security Agent \storage\quarantine\ C:\Programmi\Trend Micro\Messaging Security Agent \storage\backup\ C:\Programmi\Trend Micro\Messaging Security Agent \storage\archive\ C:\Programmi\Trend Micro\Messaging Security Agent \SharedResPool

Elenco esclusione scansione per Messaging Security Agent (solo Advanced)

Per impostazione predefinita, quando Messaging Security Agent è installato su un server Microsoft Exchange (2000 o versione successiva), non esegue la scansione dei database Microsoft Exchange, dei file di registro Microsoft

Exchange, delle cartelle del server virtuale o dell'unità M:\. L'elenco esclusione viene salvato in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Programmi\Exchsrvr\mdbdata\

priv1.stm|C:\Programmi\Exchsrvr\mdbdata\

priv1.edb|C:\Programmi\Exchsrvr\mdbdata\

pub1.stm|C:\Programmi\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Programmi\Exchsrvr\mdbdata\

|C:\Programmi\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Programmi\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Programmi\Exchsrvr\Mailroot\vsi 1\BadMail\
```

Per altre cartelle Microsoft Exchange consigliate, aggiungerle manualmente all'elenco di esclusione dalla scansione. Vedere http://support.microsoft.com/kb/245822/.

Esclusioni SBS 2003

Per SBS 2003, aggiungere manualmente:

Esclusioni Microsoft Exchange	
Database del server Microsoft Exchange	`C:\Programmi\Exchsrvr\MDBDATA`
File MTA di Microsoft Exchange	`C:\Programmi\Exchsrvr\Mtadata`
File del registro rilevamento messaggi di Microsoft Exchange	`C:\Programmi\Exchsrvr\server_name.log`
Mailroot SMTP di Microsoft Exchange	`C:\Programmi\Exchsrvr\Mailroot`
File di lavoro di Microsoft Exchange	`C:\Programmi\Exchsrvr\MDBDATA`

Servizio di replica del sito	C:\Programmi\Exchsrvr\srsdata C:\Programmi\Exchsrvr\conndata
Esclusioni IIS	
File di sistema IIS	C:\WINDOWS\system32\inetsrv
Cartella di compressione IIS	C:\WINDOWS\IIS Temporary Compressed Files
Esclusioni del controller di dominio	
File del database ActiveDirectory	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
File del database NTFRS	C:\WINDOWS\ntfrs
Esclusioni servizi Windows SharePoint	
Cartella SharePoint temporanea	C:\windows\temp\FrontPageTempDir
Esclusioni cartella desktop client	
Negozio Windows Update	C:\WINDOWS\SoftwareDistribution\DataStore
Ulteriori esclusioni	
Database di memorizzazione removibile (utilizzato da SBS Backup)	C:\Windows\system32\NtmsData
Messaggio non recapitato connettore POP3 SBS	C:\Programmi\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail

Posta in entrata connettore POP3 SBS	`C:\Programmi\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail`
Negozio Windows Update	`C:\WINDOWS\SoftwareDistribution\DataStore`
Negozio DHCP Database	`C:\WINDOWS\system32\dhcp`
Negozio WINS Database	`C:\WINDOWS\system32\wins`

Service Pack

Un service pack è un consolidamento di hot fix, patch e miglioramenti alle funzioni ed è significativo al punto da rappresentare un aggiornamento del prodotto. Sia i service pack Windows che non Windows includono un programma di installazione e uno script di installazione.

Porta dei cavalli di Troia

Le porte per cavalli di Troia vengono comunemente usate dai programmi cavalli di Troia per collegarsi ai client. Durante un'infezione, Worry-Free Business Security blocca i numeri di porta seguenti che possono essere utilizzati dai programmi cavalli di Troia:

TABELLA D-10. Porte dei cavalli di Troia

NUMERO DI PORTA	PROGRAMMA CAVALLO DI TROIA	NUMERO DI PORTA	PROGRAMMA CAVALLO DI TROIA
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks

Numero di porta	Programma cavallo di Troia	Numero di porta	Programma cavallo di Troia
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

File non disinfettabili

Il motore di scansione virus non è in grado di disinfettare i seguenti file:

Tabella D-11. Soluzioni per i file non disinfettabili

File non disinfettabile	Spiegazione e soluzione
File infettati da cavalli di Troia	I cavalli di Troia sono dei programmi che eseguono operazioni non previste o non autorizzate in genere con intenti dannosi, come visualizzare messaggi, eliminare file e formattare dischi. I cavalli di Troia non infettano i file, quindi non è necessario eseguire la disinfezione. Soluzione: motore Damage Cleanup e motore Damage Cleanup consentono di rimuovere i cavalli di Troia.
File infettati da worm	Un worm è un programma (o gruppo di programmi) autonomo in grado di diffondere copie funzionanti di se stesso o di suoi segmenti ad altri sistemi di client. La propagazione avviene in genere mediante le connessioni alla rete o gli allegati e-mail. I worm non possono essere disinfettati dal momento che ciascun file è un programma autonomo. Soluzione: Trend Micro raccomanda di eliminare i worm.
File infetti protetti da scrittura	Soluzione: rimuovere la protezione da scrittura, per permettere la disinfezione del file.
File protetti tramite password	File protetti da password (per esempio file compressi o file Microsoft Word protetti da password). Soluzione: rimuovere la protezione della password, per permettere la disinfezione del file.
File di backup	I file con l'estensione RB0~RB9 sono copie di backup dei file infetti. Il processo di disinfezione effettua il backup dei file infetti per disporre di una copia del file originale qualora venisse danneggiato da virus/malware nel corso della disinfezione. Soluzione: se la disinfezione è avvenuta correttamente, non è necessario conservare le copie di backup del file infetto. Se il funzionamento del client non presenta problemi, si può eliminare il file di backup.
File infetti presenti nel Cestino	Il sistema potrebbe non consentire la rimozione dei file infetti dal Cestino, perché il sistema non è in esecuzione. Soluzione:

File non disinfettabile	Spiegazione e soluzione

	1. Riavviare il client in modalità MS-DOS.
	2. Aprire il prompt dei comandi.
	3. Per eliminare i file, digitare le seguenti stringhe:
	`cd \`
	`cd recycled`
	`del *.* /S`
	L'ultimo comando immesso elimina tutti i file presenti nel Cestino.

File infetti contenuti nella cartella Temp di Windows o nella cartella dei file temporanei di Internet Explorer	Il sistema potrebbe non consentire di disinfettare i file infetti contenuti nella cartella Temp di Windows o nella cartella dei file temporanei di Internet Explorer poiché il client li sta utilizzando. I file che si desidera disinfettare potrebbero essere dei file temporanei necessari per il corretto funzionamento di Windows.
	Soluzione:
	1. Riavviare il client in modalità MS-DOS.
	2. Se il file infetto si trova nella cartella Temp di Windows:
	a. Aprire il prompt dei comandi e accedere alla cartella Temp di Windows (che si trova in `C:\Windows\Temp` per impostazione predefinita).
	b. Per eliminare i file, digitare le seguenti stringhe:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	L'ultimo comando immesso consente di eliminare tutti i file presenti nella cartella Temp di Windows.
	c. Riavviare il client in modalità normale
	3. Se il file infetto si trova nella cartella dei file temporanei di Internet Explorer:
	a. Aprire un prompt dei comandi e accedere alla cartella dei file temporanei di Internet Explorer (che si trova in `C:\Utenti`

File non disinfettabile	Spiegazione e soluzione

	\<nome utente\>\AppData\Local\Microsoft\Windows\Temporary Internet Files per impostazione predefinita).
	b. Per eliminare i file, digitare le seguenti stringhe:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	L'ultimo comando immesso consente di eliminare tutti i file presenti nella cartella temporanea di Internet Explorer.
	c. Riavviare il client in modalità normale

File compressi utilizzando un formato di compressione non supportato.	Soluzione: Decomprimere i file.
File bloccati o file temporaneamente in esecuzione.	Soluzione: Sbloccare i file o attendere l'esecuzione dei file.
File danneggiati	Soluzione: Eliminare i file.

Indice

A

ActiveAction, 7-16
Assistenza
    risoluzione rapida dei problemi, C-4
attacco frammento minuscolo, D-4
attacco LAND, D-5
AutoPcc.exe, 3-7, 3-8, 3-11, 3-12
azioni di scansione
    spyware/grayware, 7-15

C

cavallo di Troia, programma, 1-10, 8-6
client, installazione
    Client Packager, 3-13
    Impostazione script di accesso, 3-11
    Utilizzo di Vulnerability Scanner, 3-21
Client Packager, 3-8, 3-13, 3-15
    deployment, 3-16
    impostazioni, 3-14
Codice dannoso ActiveX, 1-10
codice dannoso Java, 1-10
complessità delle password, 6-61
componenti, 8-4
conflitto ARP, D-4
console Web, 2-4, 2-5
    informazioni, 2-4
    requisiti, 2-5
criteri di sicurezza
    password, complessità
        requisiti, 6-61

D

Damage Cleanup Services, 3-4
directory di quarantena, 5-18, 14-19
disinstallazione
    uso del programma di disinstallazione, 3-41
documentazione, xiv
Driver del monitoraggio del comportamento, 8-9
Driver Early Boot Cleanup, 8-8
duplicazione dei componenti, 8-12

E

Enciclopedia dei virus, 1-9

F

file COM infettante, 1-10
file crittografati, 14-19
file EXE infettante, 1-10
firewall
    vantaggi, 5-29
flooding SYN, D-4
frammenti sovrapposti, D-4
frammento troppo grande, D-4

H

hot fix, 8-10

I

IDS, D-3
IGMP frammentato, D-5
Impostazione script di accesso, 3-7, 3-8, 3-11, 3-12
Impostazioni DHCP, 3-24
Installazione di Security Agent

dalla console Web, 3-17
installazione remota, 3-8

J
Joke, programma, 1-9

M
Metodi di installazione del Security Agent, 3-7
metodo di scansione, 3-14
Modello Damage Cleanup, 8-6
Motore avanzato scansione minacce, 8-7
Motore Damage Cleanup, 8-6
Motore di intelligence contestuale, 8-7
Motore di scansione antivirus, 8-5
Motore di scansione spyware/grayware, 8-8

N
nuove caratteristiche, 1-2

O
operazioni pre-installazione, 3-9, 3-18, 3-21

P
packer, 1-10
pagina di installazione sul Web, 3-7
patch, 8-10
patch di sicurezza, 8-10
Pattern antivirus, 8-5, 8-17
Pattern avanzato correlazione minacce, 8-7
Pattern comune per firewall, 8-8
Pattern Damage Recovery, 8-9
Pattern di configurazione monitoraggio del comportamento, 8-9
Pattern di monitoraggio della scansione del programma, 8-10
Pattern di prevenzione contro gli attacchi al browser, 8-10
Pattern di rilevamento monitoraggio del comportamento, 8-9
Pattern eccezioni IntelliTrap, 8-5
Pattern firma digitale, 8-9
Pattern implementazione dei criteri, 8-9
pattern incrementale, 8-12
Pattern intelligenza contestuale, 8-7
Pattern IntelliTrap, 8-5
Pattern spyware/grayware, 8-8
Pattern unificato relativo allo Script Analyzer, 8-10
Ping of Death, D-4
Plug-in Manager, 3-4
probabile virus/malware, 1-9
programmi, 8-4
protezione dispositivi esterni, 8-9

R
reputazione file, 1-4
reputazione Web, 1-4, 3-4, 5-2
Responsabile delle query di intelligence contestuale, 8-7
rilevamento rootkit, 8-9
rischi per la sicurezza, 1-11, 1-12
spyware/grayware, 1-11, 1-12
riscontri sulla documentazione, C-6

S
scansione convenzionale, 5-4
scansione spyware/grayware
operazioni, 7-15
script di prova EICAR, 1-10

server, aggiornamento
    aggiornamento pianificato, 8-15
    duplicazione dei componenti, 8-12
    manuale, 8-14
Servizio principale monitoraggio del comportamento, 8-9
Sistema di rilevamento anti-intrusione, D-3
smart protection, 1-3, 1-4
    Smart Protection Network, 1-3
Smart Protection
    Servizi di reputazione file, 1-4
    Servizi di reputazione Web, 1-4
Smart Protection Network, 1-3
smart scan, 5-4
spyware/grayware, 1-11, 1-12
    adware, 1-11
    applicazioni per decifratura password, 1-12
    dialer, 1-11
    programmi Joke, 1-11
    spyware, 1-11
    strumenti per hacker, 1-11
    strumento di accesso remoto, 1-11
Supporto IPv6, B-2
    limitazioni, B-3, B-4
    visualizzazione indirizzi IPv6, B-6

T

Teardrop, D-4
tipi di scansione, 3-4

U

Update Agent, 3-4

V

virus/minacce informatiche, 1-9, 1-10
    cavallo di Troia, programma, 1-10
    Codice dannoso ActiveX, 1-10
    codice dannoso Java, 1-10
    file COM ed EXE infettante, 1-10
    Joke, programma, 1-9
    packer, 1-10
    probabile virus/malware, 1-9
    tipi, 1-9, 1-10
    virus da macro, 1-10
    virus del settore boot, 1-10
    virus di prova, 1-10
    virus VBScript, JavaScript o HTML, 1-10
    worm, 1-10
virus da macro, 1-10
virus del settore boot, 1-10
virus di prova, 1-10
virus di rete, 5-29
virus HTML, 1-10
virus JavaScript, 1-10
virus VBScript, 1-10
Vulnerability Scanner, 3-8, 3-21
    Impostazioni DHCP, 3-24
    impostazioni ping, 3-31
    recupero descrizione del computer, 3-30

W

WFBS
    documentazione, xiv
worm, 1-10

TREND MICRO INCORPORATED

TREND MICRO Italy S.r.l. Edison Park Center Viale Edison 110 -
Edificio C 20099 Sesto San Giovanni (MI) Italia
Telefono: +39 02 925931 Fax: +39 02 92593401 info@trendmicro.com

www.trendmicro.com

Item Code: WFIM108702/190701