Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: un messaggio di ATTENZIONE evidenzia la possibilità che si verifichi un danno all'hardware o una perdita di dati ed indica come evitare il problema.

AVVERTENZA: un messaggio di AVVERTENZA evidenzia un potenziale rischio di danni alla proprietà, lesioni personali o morte.

Contents

1

Introduction

Before you perform tasks explained in this guide, the following components must be installed:

- Endpoint Security Suite Enterprise - refer to *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*
- Security Management Server or Security Management Server Virtual Server - refer to *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Server Quick Start and Installation Guide*

This guide explains basic administration of Advanced Threat Prevention and should be used with *AdminHelp*, available in the Management Console.

Contattare Dell ProSupport for Software

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24x7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono al di fuori degli Stati Uniti, vedere Numeri di telefono internazionali di Dell ProSupport for Software.

2

Guida introduttiva

Questo capitolo comprende le procedure consigliate per iniziare ad amministrare Advanced Threat Prevention.

Le procedure consigliate per iniziare ad amministrare Advanced Threat Prevention includono le seguenti fasi:

- Eseguire il provisioning del tenant di Advanced Threat Prevention
  - Necessario per implementare Advanced Threat Prevention
  - Le licenze di Advanced Threat Prevention devono essere presenti nel Dell Server
- Configurare l'aggiornamento automatico dell'agente di Advanced Threat Prevention
  - Iscrizione agli aggiornamenti automatici di Advanced Threat Prevention (opzionale)
  - Gli aggiornamenti vengono rilasciati ogni mese
- Assegnare o modificare i ruoli amministrativi
  - Eseguire il provisioning o il ripristino del servizio Advanced Threat Prevention
  - Eseguire il backup e scaricare i certificati del servizio Advanced Threat Prevention esistenti
  - Visualizzare, modificare ed eseguire il commit dei criteri
- Impostare le notifiche
  - Impostare le notifiche di posta elettronica e della dashboard per gli avvisi Advanced Threat Prevention (opzionale)
  - Notifiche personalizzate in base alle esigenze dell'azienda

Provisioning di un tenant

Deve essere eseguito il provisioning di un tenant nel Dell Server prima che diventi attiva l'applicazione dei criteri di Advanced Threat Prevention.

Prerequisiti

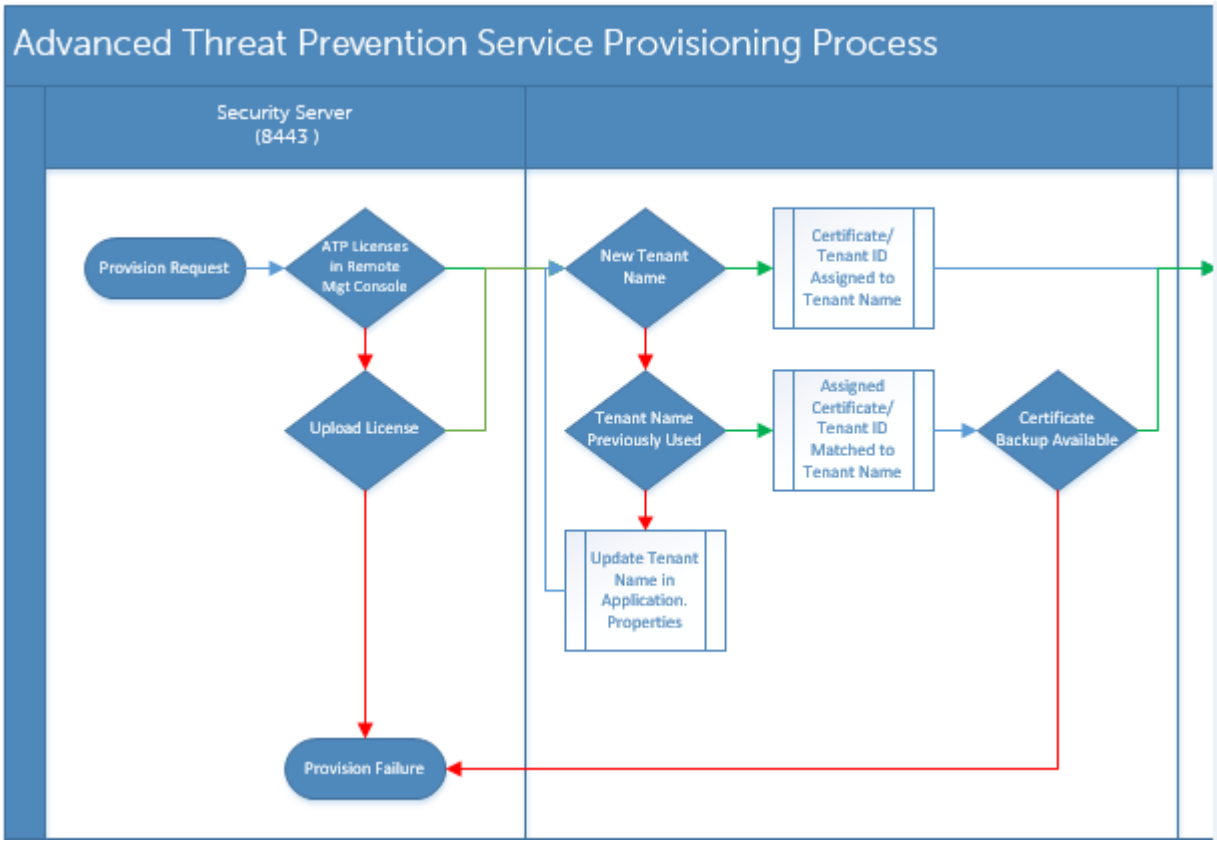
- Deve essere eseguito da un amministratore con il ruolo di amministratore di sistema.
- Deve essere dotato di connettività ad Internet per eseguire il provisioning sul Dell Server.
- Deve essere dotato di connettività a Internet nel client per visualizzare l'integrazione del servizio online di Advanced Threat Prevention nella Management Console.
- Il provisioning è basato su un token generato da un certificato durante il provisioning.
- Le licenze di Advanced Threat Prevention devono essere presenti nel Dell Server.

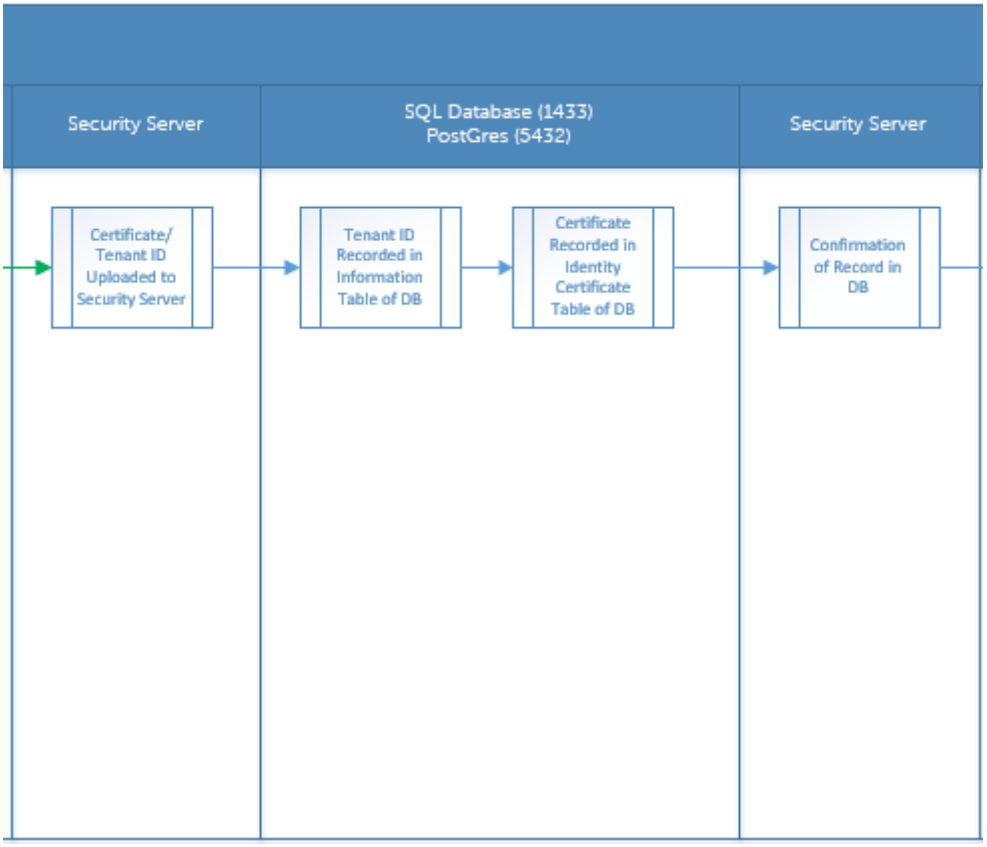
Eseguire il provisioning di un tenant

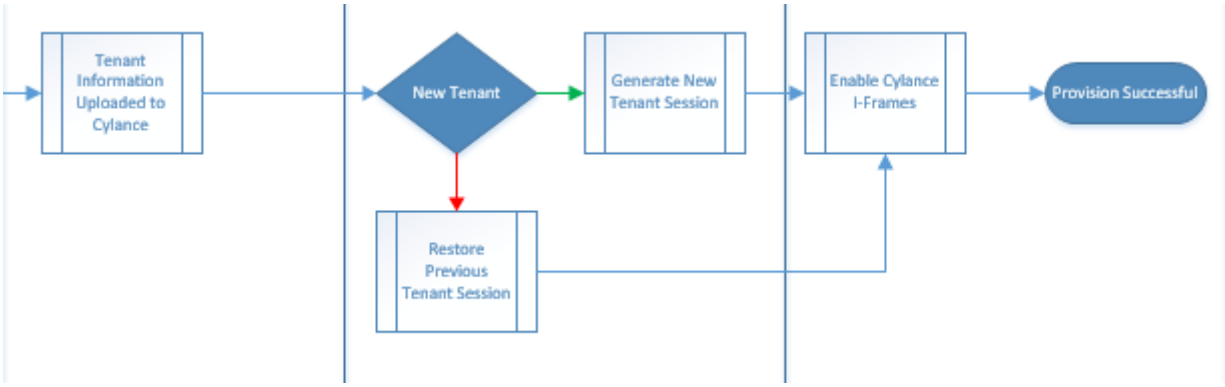
1. Eseguire l'accesso alla Management Console come amministratore Dell.
2. Nel riquadro sinistro della Management Console, fare clic su **Gestione > Gestione dei servizi**.
3. Fare clic su **Imposta il servizio Advanced Threat Protection**. Se si verifica un guasto a questo punto, importare le licenze di Advanced Threat Prevention.
4. La procedura guidata di installazione si avvia quando le licenze vengono importate. Fare clic su **Avanti** per iniziare.
5. Leggere e accettare l'EULA e fare clic su **Avanti**.
6. Fornire le credenziali di identificazione al Dell Server per il provisioning del tenant. Fare clic su **Avanti**. *Il provisioning di un tenant esistente che è prodotto da Cylance non è supportato.*
7. Scaricare il certificato. Questa operazione è necessaria per il ripristino in caso di emergenza con il Dell Server. Il certificato non viene automaticamente sottoposto a backup. Eseguire il backup del certificato in una posizione sicura su un altro computer. Selezionare la casella di controllo per confermare che è stato eseguito il backup del certificato e fare clic su **Avanti**.
8. La configurazione è stata completata. Fare clic su **OK**.

Provisioning e comunicazione agente

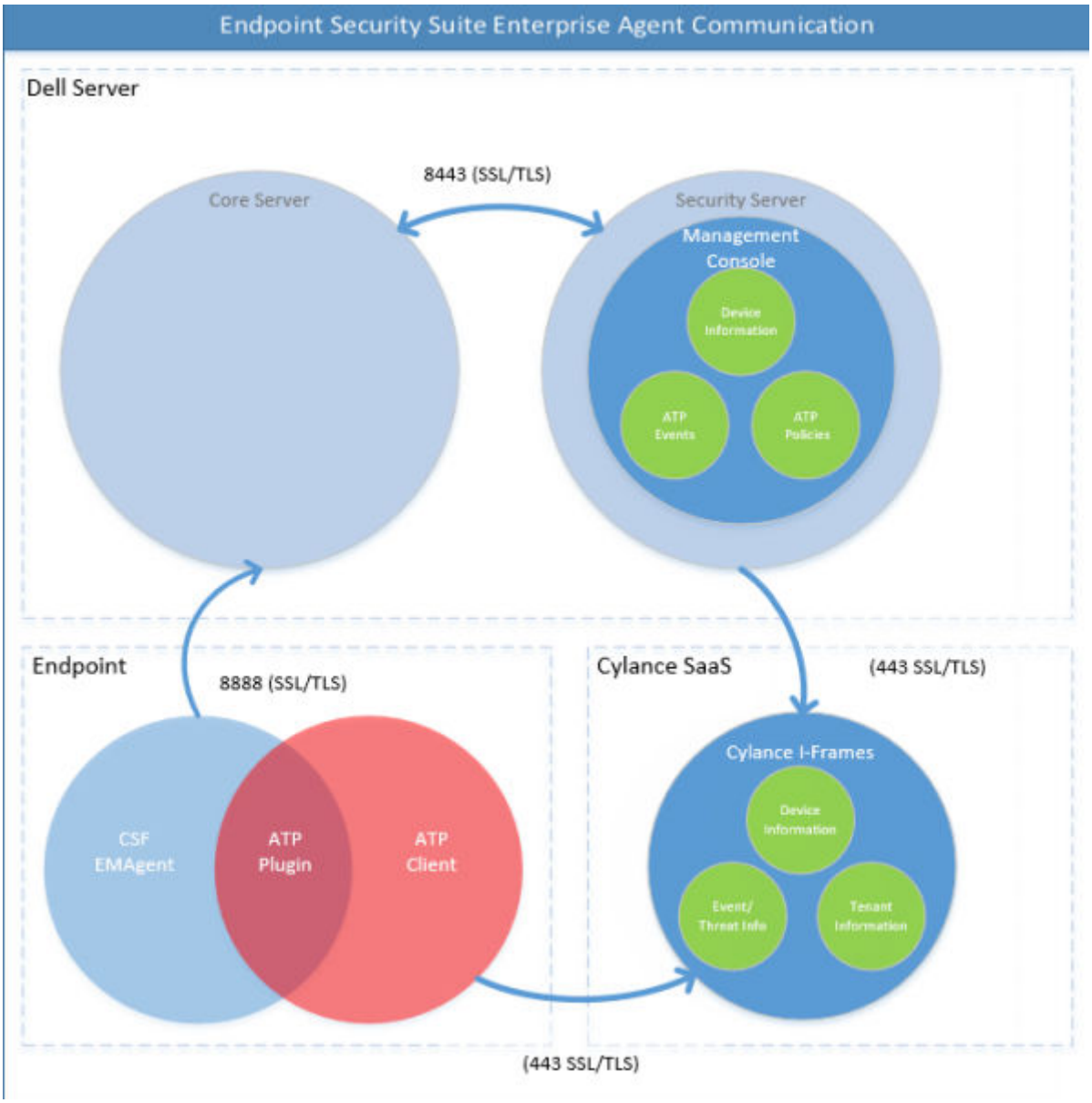
I diagrammi seguenti illustrano il processo di provisioning del servizio Advanced Threat Prevention.



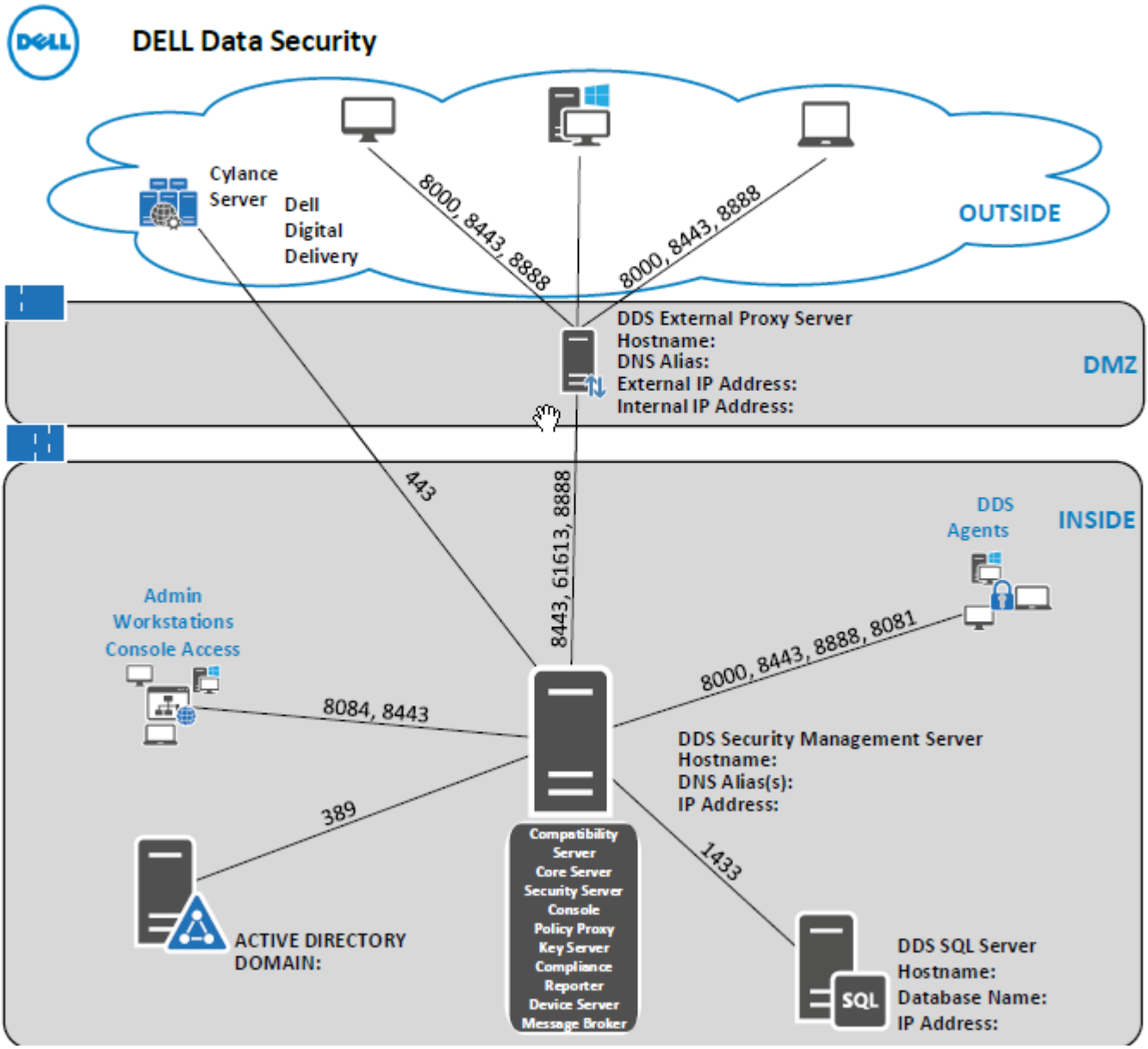




Il diagramma seguente illustra il processo di comunicazione dell'agente di Advanced Threat Prevention.



Il seguente diagramma mostra l'architettura e gli strumenti di comunicazione di un server Dell.



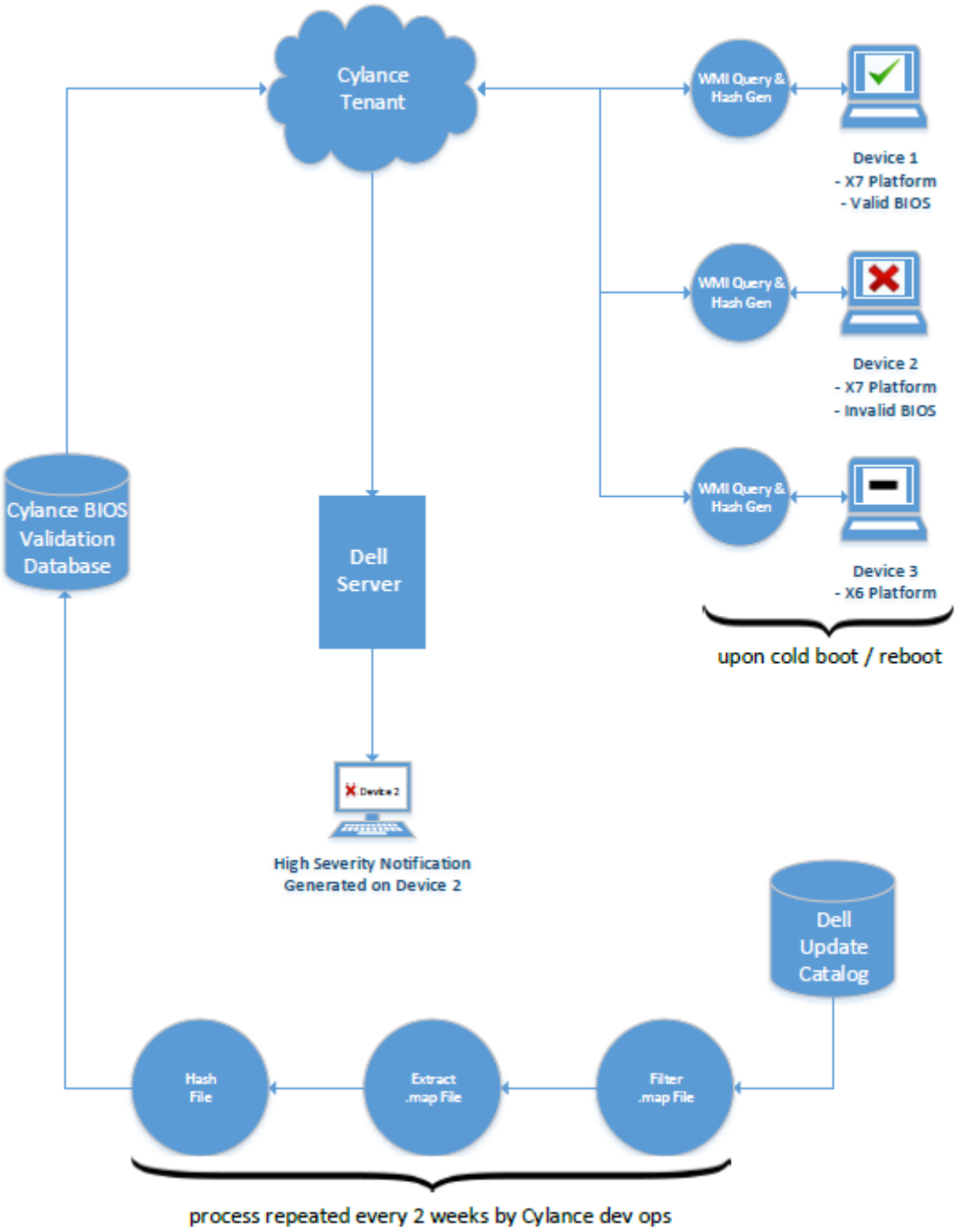
Abilitare la verifica dell'integrità dell'immagine del BIOS

Il criterio per la verifica dell'integrità dell'immagine del BIOS è attivato per impostazione predefinita quando l'opzione principale di Advanced Threat Prevention è abilitata.

Per una panoramica del processo di verifica dell'integrità dell'immagine del BIOS, consultare Processo di verifica dell'integrità dell'immagine del BIOS.

Processo di verifica

Il diagramma seguente illustra il processo di verifica dell'integrità dell'immagine del BIOS.



Se il criterio *Abilita verifica BIOS* è selezionato nella Console di gestione, il tenant di Cylance convalida un hash del BIOS sui computer endpoint al fine di garantire che il BIOS non sia stato modificato dalla versione di fabbrica Dell, che è un possibile vettore di attacco. Se viene rilevata una minaccia, viene passata una notifica al Dell Server e l'amministratore IT viene avvisato nella Remote Management Console. Per una panoramica del processo, consultare Processo di verifica dell'integrità dell'immagine del BIOS.

N.B.: Con questa funzione non è possibile utilizzare un'immagine di fabbrica personalizzata in quanto il BIOS è stato modificato.

Modelli di computer Dell che supportano la verifica dell'integrità dell'immagine del BIOS	
• Latitude 3470 • Latitude 3570 • Latitude 7275	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440

Modelli di computer Dell che supportano la verifica dell'integrità dell'immagine del BIOS		
• Latitude 7370 • Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Precision Mobile Workstation 3510 • Precision Mobile Workstation 5510 • Precision Workstation 3620 • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Configurare l'aggiornamento automatico dell'agente di Advanced Threat Prevention

Nella Management Console, è possibile registrarsi per ricevere gli aggiornamenti automatici dell'agente di Advanced Threat Prevention. La registrazione per ricevere gli aggiornamenti automatici dell'agente consente ai client di scaricare e applicare automaticamente gli aggiornamenti dal servizio Advanced Threat Prevention. Gli aggiornamenti vengono rilasciati ogni mese.

N.B.:

Gli aggiornamenti automatici dell'agente vengono supportati con Dell Server v9.4.1 o versione successiva.

Ricevere gli aggiornamenti automatici dell'agente

Per registrarsi per ricevere gli aggiornamenti automatici dell'agente:

1. Nel riquadro sinistro della Management Console, fare clic su **Gestione** > **Gestione dei servizi**.
2. Nella scheda *Minacce avanzate*, sotto *Aggiornamento automatico agente*, fare clic su **Attivato** e quindi su **Salva preferenze**.

   L'operazione può richiedere alcuni minuti per completare le informazioni e visualizzare gli aggiornamenti automatici.

Interrompere la ricezione degli aggiornamenti automatici dell'agente

Per interrompere la ricezione degli aggiornamenti automatici dell'agente:

1. Nel riquadro sinistro della Management Console, fare clic su **Gestione** > **Gestione dei servizi**.
2. Nella scheda *Minacce avanzate*, sotto *Aggiornamento automatico agente*, fare clic su **Disattivato**, quindi su **Salva preferenze**.

Assegnare o modificare i ruoli amministrativi

Visualizzare o modificare i privilegi di amministratore esistenti dalla pagina Amministratori nella Management Console.

Ruoli dell'amministratore

L'accesso dell'amministratore è integrato con Active Directory per semplificare il processo di gestione degli amministratori e consentire l'utilizzo dell'infrastruttura di autenticazione utenti esistente. Agli amministratori vengono assegnati ruoli che definiscono il livello di accesso consentito a ogni amministratore. Ad esempio, ad alcuni amministratori potrebbe essere consentito solo il ripristino assistito dall'helpdesk, mentre altri potrebbero disporre dell'accesso completo per modificare i criteri di protezione. È possibile assegnare ruoli amministratore ai gruppi di Active Directory per modificare rapidamente il livello di accesso amministratore degli utenti apportando una semplice modifica all'appartenenza ai gruppi AD. Agli utenti non di dominio può essere concesso solo l'accesso per la creazione di rapporti tramite Compliance Reporter.

Per effettuare le seguenti operazioni, è richiesto il ruolo di amministratore di sistema:

- Eseguire il provisioning o il ripristino del servizio Advanced Threat Prevention
- Iscriversi agli aggiornamenti automatici di Advanced Threat Prevention
- Impostare le notifiche di posta elettronica o della dashboard per gli avvisi Advanced Threat Prevention

- Eseguire il backup e scaricare i certificati del servizio Advanced Threat Prevention esistenti

N.B.: Per visualizzare, modificare o eseguire il commit dei criteri, è richiesto il ruolo di amministratore della sicurezza.

Per visualizzare o modificare i privilegi di amministratore esistenti, seguire la procedura seguente:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Amministratori**.
2. Ricercare o selezionare la riga in cui viene visualizzato il nome utente dell'amministratore appropriato per visualizzarne i dettagli utente.
3. Visualizzare o modificare i ruoli dell'amministratore nel riquadro destro.
4. Fare clic su **Salva**.

N.B.: Dell raccomanda di assegnare i ruoli dell'amministratore a livello di gruppo piuttosto che a livello di utente.

Per visualizzare, assegnare o modificare i ruoli dell'amministratore a livello di gruppo, attenersi alla procedura seguente:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Gruppi di utenti**.
2. Ricercare o selezionare un nome gruppo, quindi fare clic sulla scheda **Amministrazione**. Viene visualizzata la pagina con i dettagli del gruppo di utenti.
3. Selezionare o deselezionare i ruoli dell'amministratore assegnati al gruppo.
4. Fare clic su **Salva**.

Se si rimuove un Gruppo con privilegi di amministratore e successivamente si aggiunge nuovamente il Gruppo, questo resta un Gruppo amministratore.

Per visualizzare, assegnare o modificare i ruoli dell'amministratore a livello di utente, attenersi alla procedura seguente:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Utenti**.
2. Ricercare o selezionare un nome utente, quindi fare clic sulla scheda Amministratore.
3. Selezionare o deselezionare i ruoli dell'amministratore assegnati all'utente.
4. Fare clic su **Salva**.

Ruoli dell'amministratore - Assegnare o modificare i ruoli per l'utente e fare clic su **Salva**.

Ruoli del gruppo ereditati - Un elenco in sola lettura dei ruoli che l'utente ha ereditato da un gruppo. Per modificare i ruoli, fare clic sulla scheda **Gruppi di utenti** per l'utente e selezionare il nome del gruppo.

Ruoli designati - Diritti di amministratore delegati a un utente.

Impostare le notifiche

Nella Remote Management Console, è possibile registrarsi per ricevere le notifiche. L'elenco Notifiche fornisce un riepilogo configurabile di notizie, avvisi ed eventi da visualizzare nella dashboard o da inviare come notifiche tramite posta elettronica.

Tipi di notifica

È possibile selezionare i tipi di notifiche da includere nell'elenco. Le notifiche dei tipi rimanenti vengono nascoste. Le notifiche di **Threat Protection** e **Advanced Threat Event** sono relative ad Advanced Threat Prevention.

I tipi includono:

- **Aggiornamento**: notizie sui prossimi aggiornamenti dei prodotti. Per visualizzare e ricevere aggiornamenti sui prodotti, è necessario registrarsi per riceverli. Selezionare **Gestione servizi > Notifiche prodotto**, fare clic su **Attivato**, quindi fare clic su **Salva preferenze**.
- **Config**: notizie sulle modifiche alla configurazione.
- **Knowledge base**: riepiloghi e collegamenti ad articoli della knowledge base con informazioni tecniche approfondite quali, ad esempio, soluzioni alternative e metodi di configurazione.
- **Annuncio**: notizie sulle prossime uscite e sui nuovi prodotti.
- **Licenza**: avvisa quando la disponibilità del volume di licenze è bassa, oppure quando il numero di licenze di accesso client è stato superato.
- **Protezione dalle minacce**: un avviso di minaccia di Advanced Threat Prevention.
- **Evento di minaccia avanzato**: un evento rilevato da Advanced Threat Prevention. Il riepilogo contiene un elenco degli eventi critici, principali, minori, di avvertenza e di informazione, con collegamenti a informazioni più dettagliate.
- **Evento di minaccia**: un evento rilevato da Threat Protection.
- **Certificato**: notifica di scadenza del certificato.
- **Eccezioni Dell Server** - Un problema di comunicazione del server Dell sta compromettendo l'invio delle seguenti notifiche: Threat Protection, Aggiornamento, Config, Knowledge Base e Annuncio.

Dopo aver selezionato uno o più tipi, fare clic sullo spazio neutro sull'elenco per applicare le selezioni.

Selezionare **Cancella elementi selezionati** per reimpostare le selezioni in questo elenco.

Livelli di priorità

N.B.: I livelli di priorità delle notifiche non sono correlati ai livelli di priorità visualizzati nella dashboard tranne che nell'area delle notifiche.

Le priorità sono: Critica, Alta, Media e Bassa. Questi livelli di priorità sono relativi solo l'uno all'altro nell'ambito di una tipologia di notifica.

È possibile selezionare i livelli di priorità di notifiche da includere nell'area delle notifiche della dashboard o nell'elenco delle notifiche tramite posta elettronica. Le notifiche dei restanti livelli di priorità non sono incluse nella dashboard o nell'elenco delle notifiche tramite posta elettronica.

Selezionare **Cancella elementi selezionati** per reimpostare le selezioni in questo elenco. Verranno visualizzate tutte le notifiche (a meno che siano state filtrate altrove).

3

Criteri

Questo capitolo descrive la gestione dei criteri per Advanced Threat Prevention.

- Abilitare Advanced Threat Prevention
- Impostazioni dei criteri consigliate
- Eseguire il commit delle modifiche ai criteri

Per un elenco completo e una descrizione dei criteri di Advanced Threat Prevention, consultare la *guida dell'amministratore*, disponibile nella Management Console.

Abilitare Advanced Threat Prevention

Il criterio Advanced Threat Prevention è **disattivato** per impostazione predefinita e deve essere **attivato** per abilitare i criteri di Advanced Threat Prevention. I criteri di Advanced Threat Prevention sono applicabili a livello di azienda, gruppo di endpoint ed endpoint.

Per abilitare il criterio Advanced Threat Prevention a livello aziendale, seguire questi passaggi:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Azienda**.
2. Fare clic su **Threat Prevention**.
3. Attivare/disattivare l'opzione principale di Advanced Threat Prevention selezionando **Off**/**On**.

Per abilitare il criterio Advanced Threat Prevention a livello di gruppo di endpoint, seguire questi passaggi:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Gruppo di endpoint**.
2. Fare clic su **Threat Prevention**.
3. Attivare/disattivare l'opzione principale di Advanced Threat Prevention selezionando **Off**/**On**.

Per abilitare il criterio Advanced Threat Prevention a livello di endpoint, seguire questi passaggi:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Endpoint**.
2. Fare clic su **Threat Prevention**.
3. Attivare/disattivare l'opzione principale di Advanced Threat Prevention selezionando **Off**/**On**.

Impostazioni dei criteri consigliate

- Per l'elenco più aggiornato delle impostazioni dei criteri consigliate, vedere l'articolo della KB SLN301562.

Eseguire il commit delle modifiche ai criteri

Per eseguire il commit dei criteri modificati e salvati:

1. Nel riquadro sinistro della Management Console, fare clic su **Gestione > Esegui commit**.
2. In Commento, immettere una descrizione della modifica.
3. Fare clic su **Commit criteri**.

Quando un amministratore fa clic su **Commit criteri** si verifica la pubblicazione o il commit del criterio. Vengono visualizzate le seguenti informazioni:

- Modifiche dei criteri in sospeso - Il numero delle modifiche dei criteri pronte per il commit.
- Data del commit - Data e ora in cui è stato eseguito il commit dei criteri.
- Modificato da - Nome utente dell'amministratore che ha eseguito il commit dei criteri.
- Commento - Eventuali commenti aggiunti durante il commit dei criteri.
- Versione - Il numero di salvataggi dei criteri dall'ultimo commit dei criteri più la versione precedente.

4

Minacce

Questo capitolo descrive come identificare e gestire le minacce rilevate in un ambiente aziendale dopo l'installazione di Advanced Threat Prevention.

Identificare una minaccia

Notifiche di posta elettronica e dashboard

Se sono state impostate notifiche di posta elettronica per Threat Protection e Advanced Threat Event, un amministratore riceverà una notifica relativa a eventi e minacce Advanced Threat Prevention.

Il riepilogo delle notifiche della dashboard nella Management Console mostra le minacce e gli eventi Advanced Threat Prevention, come i tipi di notifica Threat Protection e Advanced Threat Events.

- Tipo di protezione da minacce - Un avviso di minaccia da Advanced Threat Prevention.
- Tipo di evento di minaccia avanzato - Un evento rilevato da Advanced Threat Prevention. Un evento non è necessariamente una minaccia.

La tabella seguente descrive in dettaglio le etichette, la gravità e le informazioni sulle minacce.

Etichetta	Gravità	Dettagli
ThreatFound	Critico	Indica che su un dispositivo è stato identificato un eseguibile portatile (PE), ma che non è stato bloccato o messo in quarantena sull'endpoint, indicando quindi una minaccia attiva sul sistema.
ThreatBlocked	Avviso	Indica che un eseguibile portatile è stato identificato sul dispositivo, ma la sua esecuzione è stata bloccata. Questa minaccia non è stata messa in quarantena, probabilmente perché il criterio di quarantena automatica non è stato abilitato oppure perché il file si trova in una posizione in cui non è possibile eseguire la scrittura con l'Account di SISTEMA locale (share di rete, dispositivo USB che è stato rimosso, ecc.).
ThreatTerminated	Avviso	Indica che un eseguibile portatile (PE) è stato identificato sul dispositivo e il relativo processo è stato terminato, poiché era in stato di esecuzione attiva. Ciò non indica che anche il file è stato messo in quarantena, poiché il PE potrebbe essere stato eseguito da un'altra posizione. Si consiglia di cercare un altro evento correlato a questo endpoint ed eseguibile per convalidare che la minaccia sia stata contrastata correttamente.
MemoryViolationBlocked	Avviso	Indica che un eseguibile o uno script ha tentato l'esecuzione, ma ha violato il criterio Protezione della memoria o Controllo script. L'esecuzione dell'eseguibile o dello script è stata bloccata di conseguenza. In genere, questo indica che il criterio correlato di Protezione della memoria o Controllo script indicato è stato impostato su Blocca.

Etichetta	Gravità	Dettagli
MemoryViolationTerminated	Avviso	Indica che un eseguibile o uno script era in stato di esecuzione attiva, ma ha violato il criterio Protezione della memoria o Controllo script. L'esecuzione dell'eseguibile o dello script è stata interrotta di conseguenza. In genere, questo indica che il criterio correlato di Protezione della memoria o Controllo script indicato è stato impostato su Termina.
MemoryViolation	Avviso	Indica che un eseguibile o uno script ha violato il criterio Protezione della memoria o Controllo script. Non è stata intrapresa nessuna azione contro l'eseguibile o lo script, probabilmente a causa del criterio impostato su Consenti.
ThreatRemoved	Informazioni	Indica che un eseguibile portatile (PE) contrassegnato in precedenza, considerato una minaccia, è stato rimosso dall'endpoint. Ciò potrebbe indicare che il PE è stato rimosso dalla quarantena o è stato rimosso dalla posizione iniziale. Questo si può riscontrare facilmente con i PE che sono stati rilevati inizialmente su supporti rimovibili (USB, CD-ROM, ecc.)
ThreatQuarantined	Informazioni	Indica che un eseguibile portatile (PE) è stato identificato come potenziale minaccia e che in seguito è stato correttamente messo in quarantena. Ciò indica che è abilitato il criterio di quarantena automatica delle minacce in base alla classificazione come Anomalo (punteggio Cylance compreso tra 0 e 60) o Non sicuro (punteggio Cylance compreso tra 60 e 100).
ThreatWaived	Informazioni	Indica che un eseguibile portatile (PE) identificato come potenziale minaccia è stato ignorato in base all'Elenco file sicuri globale o a una funzione Ignora locale. Ciò potrebbe anche indicare che l'hash SHA256 è stato aggiunto ai criteri "Ignora" o "Elenco file sicuri globale" all'interno di Dell Security Management Server.
ThreatChanged	Informazioni	Indica quando il punteggio Cylance di un eseguibile portatile (PE) è cambiato. Ciò accade in genere a causa del punteggio in due fasi eseguito da Cylance. L'analisi dell'engine di punteggio locale della minaccia potrebbe non corrispondere all'analisi dell'engine cloud Cylance. In questi casi, poiché l'engine cloud Cylance contiene dati aggiuntivi, viene utilizzato il punteggio derivato dall'engine cloud Cylance. Ciò può anche indicare che un aggiornamento di Cylance ha determinato l'inizializzazione di una nuova analisi dei file precedentemente considerati minacce e che è stato calcolato un nuovo punteggio per cui questo PE non è più considerato una minaccia.
ProtectionStatusChanged	Informazioni	Indica che uno stato di protezione dell'endpoint ha subito delle modifiche. Si attiva quando Dell Encryption Management Agent si riconnette ai servizi Cylance tramite i plug-in Cylance. Si attiva generalmente quando un endpoint viene riavviato, in quanto vi è un breve periodo in cui CSF potrebbe non essere collegato ai plug-in di Cylance durante l'avvio.

Cliccare su una notifica per maggiori dettagli. Il riepilogo include collegamenti alle ulteriori minacce o ai dettagli dell'evento.

Scheda Minacce avanzate

La scheda Minacce avanzate fornisce una visualizzazione dinamica delle informazioni dettagliate sugli eventi per l'azienda nel suo complesso, incluso un elenco dei dispositivi su cui si sono verificati gli eventi e delle azioni intraprese sui dispositivi in relazione a tali eventi.

Per accedere alla scheda Minacce avanzate aziendali, attenersi alla seguente procedura:

1. Nel riquadro sinistro, cliccare su **Popolamenti > Azienda**.
2. Selezionare la scheda **Minacce avanzate**.

Le informazioni su eventi, dispositivi e azioni sono organizzate nelle schede seguenti:

- **Protezione** - Elenca i file potenzialmente dannosi e gli script e i dettagli, inclusi i dispositivi su cui si trovano i file e gli script.
- **Agenti** - Fornisce informazioni sui dispositivi che eseguono il client Advanced Threat Prevention, nonché la possibilità di esportare le informazioni o rimuovere i dispositivi dall'elenco.
- **Elenco globale** - Elenca i file negli elenchi quarantena globale e dei file sicuri e fornisce la possibilità di spostare i file in questi elenchi.
- **Opzioni** - Consente l'integrazione con Security Information Event Management (SIEM, Gestione delle informazioni e degli eventi di sicurezza).
- **Certificato**: consente il caricamento del certificato. Dopo il caricamento, i certificati vengono visualizzati nella scheda Elenco globale e possono essere inseriti nell'Elenco file sicuri.

Le tabelle nelle schede possono essere organizzate nei modi seguenti:

- Aggiungere o eliminare le colonne dalla tabella: cliccare sulla freccia accanto a qualsiasi intestazione delle colonne, selezionare **Colonne**, quindi selezionare le colonne da visualizzare. Deselezionare la casella di controllo delle colonne da nascondere.
- Per ordinare i dati - Cliccare su un'intestazione di colonna.
- Per raggruppare per colonna - Trascinare in alto l'intestazione di colonna finché non diventa verde.

Scheda Eventi di minaccia avanzati

La scheda Eventi di minaccia avanzati mostra informazioni sugli eventi per l'intera azienda in base alle informazioni disponibili nel Dell Server.

La scheda viene visualizzata se il servizio Advanced Threat Prevention viene sottoposto a provisioning e le licenze sono disponibili.

Per esportare i dati dalla scheda Eventi di minaccia avanzati, cliccare su **Esporta** e selezionare il formato file **Excel** o **CSV**.

N.B.: I file di Excel sono limitati a 65.000 righe. I CSV non hanno limiti di dimensioni.

Punteggio Cylance e aggiornamenti del modello di minaccia

Viene attribuito un punteggio Cylance a ciascun file reputato Anomalo o Non sicuro. Il punteggio rappresenta il livello di certezza che il file è un malware. Quanto più alto è il numero tanto più elevato è il livello di certezza.

Il modello di minaccia predittivo utilizzato per proteggere i dispositivi riceve aggiornamenti periodici per migliorare le percentuali di rilevamento.

Nelle due colonne sulla pagina Protezione nella Management Console è illustrato come un nuovo modello di minaccia influenza l'organizzazione. Visualizzare e confrontare le colonne Stato di produzione e Nuovo stato per osservare quali file nei dispositivi possono essere influenzati da una modifica del modello.

Per visualizzare le colonne Stato di produzione e Nuovo stato:

1. Nel riquadro sinistro, cliccare su **Popolamenti > Azienda**.
2. Selezionare la scheda **Minacce avanzate**.
3. Cliccare sulla scheda **Protezione**.
4. Cliccare sulla freccia GIÙ sull'intestazione di una colonna nella tabella.
5. Passare il mouse su **Colonne**.
6. Selezionare le colonne **Stato di produzione** e **Nuovo stato**.

Stato di produzione - Stato del modello corrente (sicuro, anomalo o non sicuro) per il file.

Nuovo stato - Stato del modello per il file nel nuovo modello.

Ad esempio, un file che è stato considerato sicuro nel modello corrente potrebbe diventare Non sicuro nel nuovo modello. Se l'organizzazione necessita di tale, è possibile aggiungerlo all'elenco sicuro. Un file che non è mai stato rilevato o senza punteggio del modello corrente potrebbe essere considerato non sicuro per il nuovo modello. Se l'organizzazione necessita di tale, è possibile aggiungerlo all'elenco sicuro.

Solo i file presenti sul dispositivo nell'organizzazione e che hanno subito una modifica del punteggio Cylance vengono visualizzati. Alcuni file potrebbe avere subito una modifica di punteggio e restare comunque nel proprio stato corrente. Ad esempio, se il punteggio Cylance per un file passa da 10 a 20, lo stato del file potrebbe restare Anomalo e il file viene visualizzato nell'elenco del modello aggiornato (se questo file è presente sui dispositivi dell'organizzazione).

Confrontare il modello corrente con il nuovo modello

È ora possibile esaminare le differenze tra il modello corrente e il nuovo modello.

I due scenari che è necessario conoscere sono:

Stato di produzione = Sicuro, Nuovo stato = anomalo o non sicuro

- L'organizzazione considera il file come sicuro

- L'organizzazione ha lo stato Anomalo e/o Non sicuro impostato su Auto-quarantena

Negli scenari riportati sopra si consiglia di rendere sicuri i file da consentire nell'organizzazione.

Identificare le classificazioni

Per identificare le classificazioni che potrebbero avere un impatto negativo sull'organizzazione, Dell consiglia di adottare l'approccio seguente:

1. Applicare un filtro alla colonna Nuovo stato per visualizzare tutti i file non sicuri, anomali e in quarantena.
2. Applicare un filtro alla colonna Stato di produzione per visualizzare tutti i file sicuri.
3. Applicare un filtro alla colonna Classificazione per mostrare solo i file attendibili e le minacce locali.

Attendibili: i file locali sono stati analizzati da Cylance e sono risultati sicuri. Rendere sicuri questi elementi dopo la verifica.
Se sono presenti numerosi file nell'elenco filtrato, potrebbe essere necessario assegnare priorità utilizzando più attributi. Ad esempio, aggiungere un filtro alla colonna Rilevato da per esaminare le minacce rilevate dal Controllo delle esecuzioni. Queste sono state rilevate quando un utente ha tentato di eseguire un'applicazione e richiedono un'attenzione più urgente rispetto ai file inattivi rilevati dal Rilevamento delle minacce in background o dall'Analizzatore file.

Le informazioni per il confronto tra i modelli provengono dal database, non dai dispositivi. Pertanto, per il confronto tra i modelli non viene rieseguita un'analisi. Tuttavia, quando è disponibile un nuovo modello e è installato l'agente corretto, viene rieseguita un'analisi dell'organizzazione e vengono applicate tutte le modifiche del modello.

Consultare la *guida dell'amministratore* per ulteriori informazioni.

Visualizzare Protezione Web ed Eventi del firewall

Le minacce sono suddivise in categorie di eventi quali Malware/Exploit, Filtro Web, Firewall oppure Senza categoria. L'elenco di eventi di minacce può essere ordinato in funzione di una qualsiasi delle intestazioni colonna. Si possono visualizzare gli eventi di minaccia per l'intera azienda o per uno specifico endpoint. Per visualizzare gli eventi di minacce per uno specifico endpoint, dalla scheda Eventi di minaccia aziendali, selezionare il dispositivo nella colonna ID dispositivo.

Per visualizzare gli eventi di minaccia nell'azienda, attenersi alla seguente procedura:

1. Nel riquadro sinistro, cliccare su **Popolamenti > Azienda**.
2. Cliccare sulla scheda **Eventi di minaccia**.
3. Selezionare il livello di gravità desiderato e il periodo di tempo per il quale mostrare gli eventi.

Per visualizzare le minacce in uno specifico endpoint, attenersi alla seguente procedura:

1. Nel riquadro sinistro, cliccare su **Popolamenti > Endpoint**.
2. Ricercare o selezionare un nome host, quindi cliccare sulla scheda **Eventi di minaccia**.

Gestire una minaccia

È possibile mettere in quarantena, aggiungere all'elenco file sicuri, ignorare ed esportare le minacce.

Eseguire queste azioni a livello aziendale:

- Esportare una minaccia o uno script che ha attivato un avviso
- Mettere in quarantena una minaccia
- Aggiungere una minaccia all'elenco di file sicuri
- Modificare manualmente l'elenco globale

Per gestire una minaccia identificata a livello aziendale:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Azienda**.
2. Selezionare la scheda **Minacce avanzate**.
3. Selezionare Protezione.

Dalla tabella Controllo script, è possibile esportare uno script elencato nella tabella come potenziale minaccia.

Gestire le minacce avanzate aziendali

La scheda Protezione fornisce informazioni su file e script potenzialmente dannosi.

Tabella delle minacce

Dalla tabella delle minacce, è possibile esportare o mettere una minaccia in quarantena o nell'elenco dei file sicuri. È inoltre possibile aggiungere manualmente una minaccia all'elenco Quarantena globale.

La tabella elenca tutti gli eventi rilevati all'interno dell'organizzazione. Un evento può anche essere una minaccia, ma non necessariamente.

Visualizzare informazioni aggiuntive su una minaccia specifica facendo clic sul collegamento del nome della minaccia (per visualizzare i dettagli visualizzati in una nuova pagina) oppure facendo clic in un punto qualunque della riga della minaccia per visualizzare i dettagli in fondo alla pagina.

Per visualizzare ulteriori informazioni sulle minacce nella tabella, fare clic sulla freccia GIÙ sull'intestazione di una colonna per selezionare e aggiungere le colonne. Nelle colonne, vengono visualizzati i metadati relativi al file, come, ad esempio, classificazioni, punteggio Cylance (livello di fiducia), rilevamento di settore AV (collegamenti a VirusTotal.com per il confronto con gli altri fornitori), data primo individuato, SHA256, MD5, informazioni file (autore, descrizione, versione) e dettagli firma.

Comandi

- **Esporta** - Esporta i dati selezionati in un file CSV. Selezionare le righe da esportare, quindi fare clic su **Esporta**.
- **Quarantena globale** - Aggiunge un file all'elenco Quarantena globale. La minaccia viene messa definitivamente in quarantena da tutti i dispositivi.
- **Sicuro** - Aggiunge un file all'elenco file sicuri. Il file viene trattato definitivamente come sicuro in tutti i dispositivi.

  N.B.: Occasionalmente, un file "buono" può essere segnalato come non sicuro (questo potrebbe avvenire se le caratteristiche del file sono particolarmente simili a quelle di file dannosi). Ignorare il file o inserirlo nell'elenco dei file sicuri può risultare utile in queste circostanze.

- **Modifica elenco globale** - Aggiunge o rimuove i file dall'elenco Quarantena globale.
- **Ignora** - Aggiunge un file all'elenco dei file ignorati di un computer. L'esecuzione di questo file è consentita sul computer.

Gestire le minacce avanzate dell'endpoint

Per gestire una minaccia identificata su un computer specifico:

1. Nel riquadro sinistro, fare clic su **Popolamenti > Azienda**.
2. Selezionare la scheda **Minacce avanzate**.
3. Selezionare gli agenti.
4. Selezionare il nome di un agente specifico e selezionare il comando appropriato: **Esporta**, **Quarantena** o **Ignora** per esportare, mettere in quarantena o ignorare una minaccia.

5

Modalità disconnessa

La modalità disconnessa consente al Dell Server di gestire gli endpoint di Advanced Threat Prevention senza connessione client a Internet o a una rete esterna. La modalità disconnessa consente inoltre al Dell Server di gestire i client senza connessione Internet o un servizio Advanced Threat Prevention sottoposto a provisioning e ospitato. Il Dell Server acquisisce tutti i dati di eventi e minacce in modalità disconnessa.

Per stabilire se un Dell Server è in esecuzione in modalità disconnessa, fare clic sull'icona dell'ingranaggio in alto a destra nella Remote Management Console e selezionare Informazioni. La schermata Informazioni indica che un Dell Server è in modalità disconnessa, sotto la versione del Dell Server.

La modalità disconnessa è diversa da un'installazione connessa standard del Dell Server per i punti riportati di seguito.

Attivazione del client

Un token di installazione viene generato quando l'amministratore carica una licenza di Advanced Threat Prevention, che consente di attivare il client Advanced Threat Prevention.

Management Console

Gli elementi seguenti **non sono disponibili** nella Console di gestione quando il Dell Server è in esecuzione in modalità disconnessa:

- Le seguenti sono aree specifiche per Advanced Threat Prevention: Minacce avanzate per priorità, (Minacce avanzate) Eventi per classificazione, Prime dieci minacce avanzate ed Eventi Advanced Threat Prevention.
- Scheda **Azienda > Minacce avanzate**, che mostra una visualizzazione dinamica delle informazioni dettagliate sugli eventi per l'azienda nel suo complesso, incluso un elenco dei dispositivi in cui si sono verificati gli eventi e delle azioni intraprese in detti dispositivi in relazione a tali eventi.
- (Riquadro di navigazione a sinistra) Gestione dei servizi, che consente l'attivazione del servizio Advanced Threat Prevention e la registrazione alle notifiche sul prodotto.

Per supportare la modalità disconnessa, la seguente voce **è disponibile** nella Management Console:

- Scheda **Azienda > Eventi di minaccia avanzati**, che elenca le informazioni sugli eventi per l'intera azienda sulla base delle informazioni disponibili nel Dell Server in modalità disconnessa.

Funzionalità

Le funzionalità seguenti non sono disponibili nella Management Console quando il Dell Server è in esecuzione in modalità disconnessa:

- Upgrade, aggiornamento e migrazione di Security Management Server
- Aggiornamento automatico di Security Management Server Virtual: l'aggiornamento deve essere eseguito manualmente
- Aggiornamento del profilo cloud
- Aggiornamento automatico di Advanced Threat Prevention
- Caricamento di file eseguibili non sicuri o anomali per l'analisi di Advanced Threat Prevention
- Caricamento di file di Advanced Threat Prevention e caricamento di file di registro

La seguente funzionalità differisce:

- Il Dell Server invia l'elenco file sicuri globale, l'elenco file in quarantena e l'elenco file sicuri agli agenti.
- L'elenco file sicuri globale viene importato nel Dell Server tramite il criterio Consenso globale.
- L'elenco file in quarantena viene importato nel Dell Server tramite il criterio Elenco file in quarantena.
- L'elenco file sicuri in quarantena viene importato nel Dell Server tramite il criterio Elenco file sicuri.

Questi criteri sono disponibili solo in modalità disconnessa. Per ulteriori informazioni su questi criteri, consultare la *guida dell'amministratore*, disponibile nella Remote Management Console.

Per ulteriori informazioni sulla modalità disconnessa, consultare "Modalità disconnessa" nella *Guida dell'amministratore*, disponibile nella Management Console.

Identificare e gestire le minacce in modalità disconnessa

Per gestire le minacce in modalità disconnessa, è necessario prima impostare i seguenti criteri di Advanced Threat Prevention vigenti nella propria organizzazione:

- Permesso globale
- Elenco quarantena
- Elenco file sicuri

Questi criteri vengono inviati al client di Advanced Threat Prevention solo se il Dell Server rileva un token di installazione in modalità disconnessa, preceduto dal prefisso "DELLAG".

Consultare la *guida dell'amministratore* per alcuni esempi di questi criteri.

Per visualizzare i file che Advanced Threat Prevention identifica come potenziali minacce, accedere alla scheda **Azienda > Eventi di minaccia avanzati**. Questa scheda contiene un elenco delle informazioni dettagliate sugli eventi per l'intera azienda e le azioni intraprese, come ad esempio Bloccato o Terminato.

6

Risoluzione dei problemi

Ripristinare Advanced Threat Prevention

Ripristinare il servizio

Per eseguire il ripristino del servizio Advanced Threat Prevention, sarà necessario il certificato del quale è stato precedentemente eseguito il backup.

1. Nel riquadro sinistro della Management Console, fare clic su **Gestione > Gestione dei servizi**.
2. Fare clic su **Ripristina servizio Advanced Threat Prevention**.
3. Attenersi alle istruzioni fornite per il ripristino guidato del servizio e, quando richiesto, caricare il certificato del servizio Advanced Threat Prevention.

Trovare il codice prodotto con Windows PowerShell

- Utilizzando questo metodo è possibile identificare facilmente il codice di prodotto, se il codice di prodotto viene modificato in futuro.

  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

  L'output risulterà con il percorso completo e il nome del file .msi (il nome esadecimale del file convertito).

Advanced Threat Prevention

- Per far monitorare HKLM\SOFTWARE\Dell\Dell Data Protection al plug-in Advanced Threat Prevention per modificare il valore LogVerbosity e aggiornare il livello di registro del client di conseguenza, impostare il seguente valore.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Errore irreversibile: 1

  Errore 3

  Avviso 5

  Info 10

  Dettagliata 12

  Traccia 14

  Debug 15

  Il valore del registro viene selezionato all'avvio del servizio Advanced Threat Prevention o quando cambia il valore. Se il valore del registro non esiste, non vi è alcun cambiamento a livello di registrazione.

  Usare questa impostazione di registro solo per esecuzione di test/debug, in quanto controlla i dettagli di registro per altri componenti, inclusi la crittografia e l'Encryption Management Agent.

- La Modalità di compatibilità consente l'esecuzione delle applicazioni nel computer client mentre i criteri Protezione della memoria oppure Protezione della memoria e Controllo script sono abilitati. L'abilitazione della modalità di compatibilità richiede l'aggiunta di un valore di registro nel computer client.

  Per abilitare la modalità di compatibilità, attenersi alla seguente procedura:

1. Nella Management Console, disabilitare il criterio *Protezione della memoria abilitata*. Se il criterio *Controllo script* è abilitato, disabilitarlo.
2. Aggiungere il valore di registro CompatibilityMode.
   a. Usando l'editor del Registro di sistema nel computer client, andare a `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Fare clic con il pulsante destro del mouse su **Desktop**, fare clic su **Autorizzazioni**, quindi assumere la proprietà e assicurarsi il pieno controllo.
   c. Fare clic con il pulsante destro del mouse su **Desktop**, quindi selezionare **Nuovo Valore binario**.
   d. Per il nome, digitare `CompatibilityMode`.
   e. Aprire le impostazioni di registro e modificare il valore in `01`.
   f. Fare clic su **OK**, quindi chiudere l'editor del Registro di sistema.

   Per aggiungere il valore di registro con un comando, è possibile usare una delle seguenti opzioni della riga di comando da eseguire nel computer client:

   - Per un computer - Psexec:

     ```
     psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
     CompatibilityMode /t REG_BINARY /d 01
     ```

   - (Per più computer) Invoke-Command cmdlet:

     ```
     $servers = "testComp1","testComp2","textComp3"

     $credential = Get-Credential -Credential {UserName}\administrator

     Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
     -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
     01}
     ```

3. Nella Management Console, abilitare nuovamente il criterio *Protezione della memoria abilitata*. Se il criterio *Controllo script* era abilitato in precedenza, abilitarlo nuovamente.