Dell Threat Defense

Guida all'installazione e dell'amministratore

Con tecnologia Cylance

v17.06.16

2017-06-16

Sommario

PANORAMICA

Dell Threat Defense, con tecnologia Cylance, rileva e blocca i malware prima che possano colpire un dispositivo. Cylance usa un approccio matematico nell'identificazione dei malware, usando tecniche di apprendimento automatico invece di firme reattive, sistemi basati sull'attendibilità o sandbox. Questo approccio rende inutili nuovi malware, virus, bot e future varianti. Threat Defense analizza le potenziali esecuzioni dei file in cerca di malware nel sistema operativo.

Questa guida spiega l'utilizzo della Threat Defense Console, l'installazione di Threat Defense Agent e come configurare entrambi.

Funzionamento

Threat Defense è costituito da un piccolo agente, installato in ciascun host, che comunica con la console basata su cloud. L'agente rileva e impedisce l'esecuzione dei malware nell'host usando modelli matematici testati, non richiede una connettività continua al cloud o aggiornamenti continui della firma e lavora sia in reti aperte che isolate. Man mano che il panorama delle minacce si evolve, anche Threat Defense lo fa. Facendo costantemente pratica su enormi insiemi di dati reali, Threat Defense rimane sempre un passo avanti agli utenti non autorizzati.

- **Minaccia**: quando una minaccia viene scaricata nel dispositivo o c'è un tentativo di exploit.
- **Rilevamento delle minacce**: il modo in cui Threat Defense Agent identifica le minacce.
    - **Analisi dei processi**: analizza i processi in esecuzione nel dispositivo.
    - **Controllo delle esecuzioni:** analizza i processi solo quando vengono eseguiti. Include tutti i file che vengono eseguiti all'avvio, che sono impostati sull'esecuzione automatica e che vengono eseguiti manualmente dall'utente.
- **Analisi**: il modo in cui i file vengono identificati come dannosi o sicuri.
    - **Ricerca di punteggi di minacce nel cloud**: il modello matematico nel cloud usato per assegnare un punteggio alle minacce.
    - **Locale**: il modello matematico integrato nell'agente. Consente l'analisi quando il dispositivo non è connesso a Internet.
- **Azione**: ciò che fa l'agente quando un file viene identificato come una minaccia.
    - **Globale**: controlla le impostazioni dei criteri, tra cui *Quarantena globale* ed *Elenco file sicuri*.
    - **Locale**: verifica la presenza di file inseriti manualmente nei gruppi *In quarantena* e *Ignorato*.

Informazioni su questa guida

Dell consiglia agli utenti di familiarizzare con la console basata su cloud prima di installare l'agente negli endpoint. Comprendere in che modo vengono gestiti gli endpoint rende più semplice proteggerli e conservarli. Questo flusso di lavoro è un consiglio. Gli utenti possono avvicinarsi alla distribuzione nel proprio ambiente nel modo che più è loro congeniale.

Esempio: le zone contribuiscono a raggruppare i dispositivi nell'organizzazione. Per esempio, configurare una zona con una regola di zona che aggiunge automaticamente nuovi dispositivi a una zona in base a criteri selezionati (come sistema operativo, nome del dispositivo o nome del dominio).

Nota: le istruzioni per l'installazione dell'agente vengono date dopo le informazioni sui criteri e sulle zone. Se necessario, gli utenti possono iniziare con l'installazione dell'agente.

CONSOLE

Threat Defense Console è un sito Web al quale si accede per visualizzare le informazioni sulle minacce per l'organizzazione. La console rende semplice organizzare i dispositivi in gruppi (zone), configurare quali azioni intraprendere quando vengono individuate minacce in un dispositivo (criterio) e scaricare i file di installazione (agente).

Threat Defense Console supporta le seguenti lingue.

Francese	Tedesco	Italiano	Giapponese
Portoghese (Spagna)	Coreano	Spagnolo	Portoghese (Brasile)

Tabella 1: Lingue supportate in Threat Defense Console

Accesso

All'attivazione dell'account si riceve un messaggio di posta elettronica con le informazioni di accesso per Threat Defense Console. Fare clic sul collegamento nel messaggio di posta elettronica per andare alla pagina di accesso o andare a:

- Nord America: http://dellthreatdefense.com
- Europa: http://dellthreatdefense-eu.cylance.com

Criterio del dispositivo

Un criterio definisce il modo in cui l'agente gestisce i malware che incontra. Ad esempio, è possibile mettere automaticamente in *Quarantena* un malware o ignorarlo se si trova in una determinata cartella. Ciascun dispositivo deve essere in un criterio e solo un criterio può essere applicato a un dispositivo. Restringere un dispositivo ad un unico criterio elimina funzionalità che possono entrare in conflitto (come il blocco di un file che dovrebbe essere consentito per quel dispositivo). Se non viene assegnato alcun criterio, il dispositivo viene posto nel criterio predefinito.

Per il criterio predefinito è abilitato solo il Controllo delle esecuzioni, che analizza i processi solo quando vengono eseguiti. Questo fornisce una protezione base per il dispositivo, non interrompe le operazioni in atto nel dispositivo e fornisce tempo per testare le funzionalità del criterio prima di distribuirlo nell'ambiente di produzione.

Per aggiungere un criterio

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare i criteri.
2. Selezionare **Impostazioni > Criteri dispositivo**.
3. Fare clic su **Aggiungi nuovo criterio**.
4. Immettere un nome criterio e selezionare le opzioni del criterio.

5. Fare clic su **Crea**.

Azioni file

IMPOSTAZIONI > Criterio dispositivo > [selezionare un criterio] > Azioni file

Azioni file fornisce diverse opzioni per gestire i file rilevati da Threat Defense come *non sicuri* o *anomali*.

Suggerimento: per ulteriori informazioni sulla classificazione di file *non sicuri* o *anomali*, fare riferimento alla sezione Protezione - Minacce.

Quarantena automatica con Controllo delle esecuzioni

Questa funzione consente di mettere in *quarantena* o bloccare il file *non sicuro* o *anomalo* per impedirne l'esecuzione. *Mettendo il file in quarantena*, questo viene spostato dalla sua posizione originale alla directory della *quarantena*, ovvero **`C:\ProgramData\Cylance\Desktop\q`**.

Alcuni malware sono progettati per rilasciare altri file in determinate directory e continuano a farlo fino a quando il file viene rilasciato. Threat Defense modifica il file rilasciato in modo che non venga eseguito per far sì che questo tipo di malware non rilasci più in continuazione il file rimosso.

Suggerimento: Dell consiglia di testare la *quarantena automatica* su un numero ridotto di dispositivi prima di applicarla nell'ambiente di produzione. È necessario osservare i risultati dei test per garantire che non venga bloccata l'esecuzione di applicazioni fondamentali per l'attività.

Caricamento automatico

Dell consiglia agli utenti di abilitare il caricamento automatico per i file *non sicuri* e *anomali*. Threat Defense carica automaticamente qualsiasi file *non sicuro* o *anomalo* in Cylance Infinity Cloud per eseguire un'analisi più approfondita del file e fornire ulteriori dettagli.

Threat Defense carica e analizza solo file eseguibili di tipo Portable Executable (PE) sconosciuti. Se lo stesso file sconosciuto viene individuato in più dispositivi nell'organizzazione, Threat Defense carica solo un file per l'analisi, non un file per ciascun dispositivo.

Criterio Elenco file sicuri

Aggiungere file che sono considerati sicuri, al livello del criterio. L'agente non applicherà nessuna azione per le minacce ai file in questo elenco.

Per ulteriori informazioni su come gestire le eccezioni file (*in quarantena* o *sicuri*) ai vari livelli (*Locale*, *Criterio* o *Globale*), vedere l'Appendice B: Gestione delle eccezioni.

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare i criteri.
2. Selezionare **Impostazioni** > **Criteri dispositivo**.
3. Aggiungere un nuovo criterio o modificare un criterio esistente.
4. Fare clic su **Aggiungi file** in *Criterio Elenco file sicuri*.
5. Immettere le informazioni **SHA256**. Facoltativamente è possibile includere MD5 e il nome del file se è noto.
6. Selezionare una **categoria** per identificare meglio l'utilizzo di questo file.
7. Immettere un motivo per aggiungere il file al *Criterio Elenco file sicuri*.
8. Fare clic su **Invia**.

Impostazioni protezione

IMPOSTAZIONI > Criterio dispositivo > [selezionare un criterio] > Impostazioni protezione

Controllo delle esecuzioni

Threat Defense monitora sempre l'esecuzione di processi dannosi e avvisa quando si verificano tentativi di esecuzione da parte di file *non sicuri* o *anomali*.

Impedisci arresto del servizio dal dispositivo

Se selezionato, il servizio Threat Defense è protetto dall'arresto manuale o da parte di un altro processo.

Copia campioni di malware

Consente di specificare una condivisione di rete in cui copiare campioni di malware. Questo permette agli utenti di eseguire personalmente l'analisi dei file che Threat Defense considera *non sicuri* o *anomali*.

- Supporta le condivisioni di rete CIFS/SMB.
- Specificare un percorso di condivisione di rete. Esempio: **`c:\test`**.
- Tutti i file che rispondono ai criteri vengono copiati nella condivisione di rete, compresi i duplicati. Non viene eseguito alcun test di unicità.
- I file non vengono compressi.
- I file non sono protetti da password.

AVVERTENZA: I FILE NON SONO PROTETTI DA PASSWORD. PRESTARE ATTENZIONE IN MODO CHE NON VENGA ESEGUITO ALCUN FILE DANNOSO.

Controllo script

Controllo script protegge i dispositivi bloccando l'esecuzione di script attivi e script PowerShell dannosi.

1. Accedere alla console (http://dellthreatdefense.com).
2. Selezionare **Impostazioni** > **Criteri dispositivo**.
3. Selezionare un criterio e fare clic su **Impostazioni protezione**.
4. Selezionare la casella di controllo per abilitare **Controllo script**.
    a. **Avviso**: monitora gli script in esecuzione nell'ambiente. Consigliato per la distribuzione iniziale.
    b. **Blocca**: consente l'esecuzione degli script solo da cartelle specifiche. Usare dopo averlo testato in modalità Avviso.
    c. **Approva script in cartelle (e sottocartelle)**: le esclusioni delle cartelle di script devono specificare il relativo percorso della cartella.
    d. **Blocca utilizzo console PowerShell**: impedisce l'avvio della console PowerShell. Questa opzione offre ulteriore protezione contro l'utilizzo di one-liner PowerShell.

    Nota: se lo script avvia la console PowerShell e Controllo script è impostato in modo da bloccare la console PowerShell, lo script avrà esito negativo. Si consiglia agli utenti di modificare gli script per richiamare gli script PowerShell e non la console PowerShell.
5. Fare clic su **Salva**.

Registri agente

IMPOSTAZIONI > Criterio dispositivo > [selezionare un criterio] > Registri agente

Abilitare Registri agente nella console per caricare i file di registro e consentire la visualizzazione nella console.

1. Accedere alla console (http://dellthreatdefense.com).
2. Selezionare **Impostazioni** > **Criteri dispositivo**.
3. Selezionare un criterio e fare clic su **Registri agente**. Assicurarsi che il dispositivo selezionato per i file di registro sia assegnato a questo criterio.
4. Selezionare **Abilita caricamento automatico dei file di registro** e fare clic su **Salva**.
5. Fare clic sulla scheda **Dispositivi** e selezionare un dispositivo.
6. Fare clic su **Registri agente**. Vengono visualizzati i file di registro.
7. Fare clic su un file di registro. Il nome del file di registro è la data del registro.

Procedure consigliate per i criteri

Quando i criteri vengono creati per la prima volta, Dell consiglia di implementare le funzionalità dei criteri usando un approccio a fasi per assicurarsi che non vi siano ripercussioni su prestazioni e funzionamento. Creare nuovi criteri con più funzionalità abilitate man mano che si comprende meglio il funzionamento di Threat Defense nell'ambiente.

1. In fase di creazione di criteri iniziali, abilitare solo **Caricamento automatico**.
    a. L'agente usa Controllo delle esecuzioni e Monitoraggio dei processi per analizzare esclusivamente i processi in esecuzione.

       Include tutti i file che vengono eseguiti all'avvio, che sono impostati sull'esecuzione automatica e che vengono eseguiti manualmente dall'utente.

       L'agente invia solamente gli avvisi alla console. Nessun file viene bloccato o messo in *quarantena*.

    b. Controllare la console per eventuali avvisi di minaccia.

       L'obiettivo è trovare applicazioni o processi che devono essere eseguiti nell'endpoint e che sono considerati una minaccia (*anomali* o *non sicuri*).

       Configurare un criterio o un'impostazione della console per *consentirne* l'esecuzione se si verifica questa condizione (ad esempio, *escludere* le cartelle in un criterio, *ignorare* i file per tale dispositivo o aggiungere i file all'*Elenco file sicuri*).

    c. Usare questo criterio iniziale per un giorno per consentire l'esecuzione e l'analisi delle applicazioni e dei processi che vengono normalmente usati nel dispositivo.

IMPORTANTE: possono esserci applicazioni e processi che vengono eseguiti periodicamente in un dispositivo (ad esempio, una volta al mese) che possono essere considerati una minaccia. L'utente deve decidere se desidera eseguirli nel corso del criterio iniziale o ricordare di monitorare il dispositivo quando vengono eseguiti come pianificato.

2. In Impostazioni protezione, abilitare **Termina processi principali e processi secondari non sicuri in esecuzione** al termine di Controllo delle esecuzioni e Monitoraggio dei processi.

   Termina processi non sicuri e loro sottoprocessi in esecuzione termina i processi (e i sottoprocessi), indipendentemente dallo stato, quando viene rilevata una minaccia (EXE o MSI).

3. In Azioni file attivare **Quarantena automatica**.

   Quarantena automatica sposta eventuali file dannosi nella cartella *Quarantena*.

4. In Impostazioni protezione attivare **Controllo script**.

   In questo modo gli utenti sono protetti dagli script dannosi che vengono eseguiti nel dispositivo.

   Gli utenti possono approvare gli script da eseguire per cartelle specifiche.

   Le esclusioni delle cartelle di Controllo script devono specificare un percorso relativo della cartella (ad esempio, **`\Cases\ScriptsAllowed`**).

Zone

Una zona è un modo di organizzare e gestire i dispositivi. Ad esempio, i dispositivi possono essere suddivisi in base alla geografia o alla funzione. Se c'è un gruppo di dispositivi di importanza strategica, questi possono essere raggruppati insieme e alla zona può essere assegnata una priorità elevata. Inoltre, i criteri sono applicati al livello della zona, quindi i dispositivi possono essere raggruppati in una zona in base al criterio applicato a tali dispositivi.

Un'organizzazione ha una zona predefinita (Fuorizona) alla quale possono accedere solo gli amministratori. I nuovi dispositivi vengono assegnati alla Fuorizona, a meno che vi siano regole di zona che assegnano automaticamente i dispositivi alle zone.

È possibile assegnare manager e utenti di zona a una zona, consentendo loro di visualizzare in che modo tale zona è configurata. Questo consente anche ai manager e agli utenti di zona di accedere ai dispositivi per i quali sono responsabili. Deve essere creata almeno una zona per consentire a chiunque abbia un ruolo di manager o utente di zona di visualizzarlo.

Un dispositivo può appartenere a più zone, ma solo un criterio può essere applicato a un dispositivo. Consentire più zone fornisce una certa flessibilità nel modo in cui i dispositivi vengono raggruppati. Restringere un dispositivo a un unico criterio elimina funzionalità che possono entrare in conflitto (come il blocco di un file che dovrebbe essere *consentito* per quel dispositivo).

La presenza di dispositivi in più zone può verificarsi per i motivi seguenti:

- Il dispositivo viene aggiunto manualmente in più zone
- Il dispositivo è conforme alle regole di più di una zona
- Il dispositivo è già presente in una zona e in seguito è conforme alle regole di un'altra zona

Per i metodi di utilizzo delle zone consigliati, vedere Procedure consigliate per la gestione delle zone.

Per aggiungere una zona

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare le zone.
2. Fare clic su **Zone**.
3. Fare clic su **Aggiungi nuova zona**.
4. Immettere un Nome zona, selezionare un Criterio e selezionare un Valore. Una zona deve avere un criterio associato. Il valore è la priorità per la zona.
5. Fare clic su **Salva**.

Per aggiungere dispositivi a una zona

1. Accedere alla console (http://dellthreatdefense.com) con un account amministratore o manager di zona.
2. Fare clic su **Zone**.
3. Fare clic su una zona dal relativo *elenco*. I dispositivi attualmente presenti nella zona vengono visualizzati nell'*Elenco dei dispositivi della zona* nella parte inferiore della pagina.
4. Fare clic su **Aggiungi dispositivi alla zona**. Viene visualizzato un elenco di dispositivi.
5. Selezionare ciascun dispositivo da aggiungere alla zona e fare clic su **Salva**. Facoltativamente, selezionare **Applica criteri di zona ai dispositivi selezionati**. Aggiungere un dispositivo a una zona non comporta automaticamente l'applicazione del criterio della zona perché la zona potrebbe essere usata per organizzare i dispositivi, non per gestire il criterio per quei dispositivi.

Per rimuovere una zona

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono rimuovere le zone.
2. Fare clic su **Zone**.
3. Selezionare le caselle di controllo delle zone da rimuovere.
4. Fare clic su **Rimuovi**
5. Fare clic su **Sì** quando viene visualizzato il messaggio che chiede di confermare la rimozione della zona selezionata.

Proprietà delle zone

Le proprietà delle zone possono essere modificate secondo le necessità.

Informazioni sulla priorità delle zone

Alle zone possono essere assegnati diversi livelli di priorità (Bassa, Normale o Alta) che classificano la rilevanza o l'importanza dei dispositivi in tali zone. In diverse aree della dashboard, i dispositivi vengono visualizzati in base alla priorità per aiutare a identificare a quali dispositivi è necessario prestare immediatamente attenzione.

La priorità può essere impostata quando viene creata la zona o può essere modificata la zona per cambiare il valore della priorità.

Per modificare le proprietà delle zone

1. Accedere alla console (http://dellthreatdefense.com) come amministratore o manager di zona.
2. Fare clic su **Zone**.
3. Fare clic su una zona dal relativo *elenco*.
4. Immettere un nuovo nome nel campo **Nome** per modificare il nome della zona.
5. Selezionare un criterio diverso dal menu a discesa **Criterio** per modificare il criterio.
6. Selezionare un valore di priorità **Bassa**, **Normale** o **Alta**.
7. Fare clic su **Salva**.

Regola di zona

I dispositivi possono essere assegnati automaticamente a una zona in base a determinati criteri. Questo processo automatico è vantaggioso quando si aggiungono molti dispositivi alle zone. Quando vengono aggiunti nuovi dispositivi che corrispondono a una regola di zona, tali dispositivi vengono automaticamente assegnati a quella zona. Se è selezionata l'opzione **Applica ora a tutti i dispositivi esistenti**, tutti i dispositivi preesistenti che corrispondono alla regola vengono aggiunti a questa zona.

Nota: le regole di zona aggiungono automaticamente i dispositivi a una zona, ma non possono rimuoverli. Modificare l'indirizzo IP o il nome host del dispositivo non ne causa la rimozione da una zona. I dispositivi possono essere rimossi manualmente da una zona.

Esiste un'opzione per applicare il criterio di zona ai dispositivi che vengono aggiunti alla zona in quanto corrispondenti alla regola di zona. Ciò comporta la sostituzione del criterio esistente del dispositivo con il criterio di zona specificato. Occorre prestare attenzione quando si applica automaticamente un criterio in base alla regola di zona. Se non viene gestito correttamente, è possibile che un dispositivo venga assegnato al criterio sbagliato per la sua corrispondenza a una regola di zona.

Visualizzare la pagina Dettagli dispositivo nella console per visualizzare quale criterio è applicato a un dispositivo.

Per aggiungere una regola di zona

1. Accedere alla console (http://dellthreatdefense.com) come amministratore o manager di zona.
2. Fare clic su **Zone** e selezionare una zona dal relativo *elenco*.
3. Fare clic su **Crea regola** in Regola di zona.
4. Specificare i criteri per la zona selezionata. Fare clic sul segno più per aggiungere ulteriori condizioni. Fare clic sul segno meno per rimuovere una condizione.
5. Fare clic su **Salva**.

Criteri delle regole di zona

- **Quando viene aggiunto un nuovo dispositivo all'organizzazione**: qualsiasi nuovo dispositivo aggiunto all'organizzazione che corrisponde alla regola di zona viene aggiunto alla zona.
- **Quando viene modificato un attributo di un dispositivo**: quando gli attributi di un dispositivo esistente vengono modificati e corrispondono così alla regola di zona, quel dispositivo esistente viene aggiunto alla zona.
- **Indirizzo IPv4 nell'intervallo**: immettere un intervallo di indirizzo IPv4.
- **Nome del dispositivo**:
    - Inizia con: i nomi dei dispositivi devono iniziare con questo.
    - Contiene: i nomi dei dispositivi devono contenere questa stringa, ma può essere ovunque all'interno del nome.
    - Termina con: i nomi dei dispositivi devono terminare con questo.
- **Sistema operativo**:
    - È: il sistema operativo deve essere il sistema selezionato.
    - Non è: il sistema operativo non deve essere il sistema selezionato. Ad esempio, se l'unica regola di zona stabilisce che il sistema operativo non deve essere Windows 8, allora tutti i sistemi operativi, compresi dispositivi non Windows, vengono aggiunti alla zona.
- **Nome dominio**:
    - Inizia con: il nome dominio deve iniziare con questo.
    - Contiene: il nome dominio deve contenere questa stringa, ma può essere ovunque all'interno del nome.
    - Termina con: il nome dominio deve terminare con questo.
- **Nome distinto**:
    - Inizia con: il nome distinto deve iniziare con questo.
    - Contiene: il nome distinto deve contenere questa stringa, ma può essere ovunque all'interno del nome.
    - Termina con: il nome distinto deve terminare con questo.
- **Membro di (LDAP)**:
    - È: il membro di (gruppo) deve corrispondere a questo.
    - Contiene: il membro di (gruppo) deve contenere questo.
- **Seguenti condizioni soddisfatte**:
    - Tutte: tutte le condizioni nella regola di zona devono corrispondere per aggiungere il dispositivo.
    - Una qualsiasi: almeno una condizione nella regola di zona deve corrispondere per aggiungere il dispositivo.

- **Applicazione criterio di zona**:
    - Non applicare: non applicare il criterio di zona quando i dispositivi vengono aggiunti alla zona.
    - Applica: applica il criterio di zona quando i dispositivi vengono aggiunti alla zona.

      Avvertenza: applicare automaticamente un criterio di zona può incidere negativamente su alcuni dei dispositivi nella rete. Applicare automaticamente il criterio di zona *solo* se si è certi che la regola individuerà *solo* i dispositivi che *devono* avere questo particolare criterio di zona.
- **Applica ora a tutti i dispositivi esistenti**: applica la regola di zona a tutti i dispositivi nell'organizzazione. Non comporta l'applicazione del criterio di zona.

Informazioni sui Nomi distinti (DN)

Alcune cose da sapere sui Nomi distinti (DN, Distinguished Names) quando vengono usati nelle regole di zona.

- I caratteri jolly non sono consentiti, tuttavia la condizione "Contiene" ottiene gli stessi risultati.
- Gli errori e le eccezioni dei DN relative all'agente vengono raccolti nei file di registro.
- Se l'agente trova informazioni sui DN nel dispositivo, tali informazioni vengono automaticamente inviate alla console.
- Quando si aggiungono informazioni sui DN, devono essere formattate in modo appropriato, come indicato di seguito.
    - Esempio: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - Esempio: OU=Demo,OU=SEngineering,OU=Sales

Elenco dei dispositivi della zona

L'*Elenco dei dispositivi della zona* visualizza tutti i dispositivi assegnati a questa zona. I dispositivi possono appartenere a più zone. Utilizzare **Esporta** per scaricare un file CSV con le informazioni per tutti i dispositivi nell'*Elenco dei dispositivi della zona*.

Nota: se non ci sono le autorizzazioni per visualizzare una zona e viene comunque fatto clic sul collegamento della zona nella colonna delle zone, viene visualizzata una pagina di Risorsa non trovata.

Procedure consigliate per la gestione delle zone

Si può pensare alle zone come a dei tag, in cui ciascun dispositivo può appartenere a più zone (o avere più tag). Mentre non ci sono restrizioni sul numero di zone che possono essere create, le procedure consigliate identificano tre diverse appartenenze a zone tra esecuzione di test, criterio e granularità del ruolo utente all'interno dell'organizzazione.

Queste tre zone sono costituite da:

- Gestione degli aggiornamenti
- Gestione dei criteri
- Gestione dell'accesso basato sui ruoli

Organizzazione delle zone per la gestione degli aggiornamenti

Un uso comune delle zone è per contribuire alla gestione degli aggiornamenti dell'agente. Threat Defense supporta la versione più recente dell'agente e quella precedente. Questo consente all'azienda di supportare le finestre di blocco delle modifiche e di eseguire test approfonditi sulle nuove versioni dell'agente.

Esistono tre tipi di zona consigliati usati per dirigere e specificare l'esecuzione del test sull'agente e le fasi di produzione:

- **Aggiornamento della zona - Gruppo di prova**: queste zone devono avere dispositivi di test che rappresentano i dispositivi (e i software usati in quei dispositivi) in modo appropriato nell'organizzazione. Questo consente l'esecuzione di test dell'agente più recente e assicura che la distribuzione di tale agente ai dispositivi di produzione non interferisca con le procedure aziendali.
- **Aggiornamento della zona - Gruppo pilota**: questa zona può essere usata come zona di test secondaria o zona di produzione secondaria. Come zona di test secondaria consentirebbe l'esecuzione di test per nuovi agenti su un gruppo di dispositivi più grande prima dell'implementazione nella produzione. Come zona di produzione secondaria consentirebbe due versioni differenti dell'agente, ma poi si dovrebbero gestire due diverse zone di produzione.
- **Aggiornamento della zona - Produzione**: la maggior parte dei dispositivi deve trovarsi in zone assegnate alla produzione.

Nota: per aggiornare l'agente alla zona di produzione, vedere Aggiornamento dell'agente.

Aggiungere una zona di test o pilota

1. Accedere alla console (http://dellthreatdefense.com) con un account amministratore o manager di zona.
2. Selezionare **Impostazioni** > **Aggiornamento agente**.
3. Per zone di test o pilota:
    a. Fare clic su **Seleziona zone di test** o **Seleziona zone pilota**.
    b. Fare clic su una zona.

    Se la zona di produzione è impostata su **Aggiorna automaticamente**, le zone di test e pilota non sono disponibili. Modificare Aggiorna automaticamente nella zona di produzione in qualcosa di diverso per abilitare le zone di test e pilota.
4. Fare clic su **Selezionare la versione**.
5. Selezionare una versione dell'agente da applicare alla zona di test o pilota.
6. Fare clic su **Applica**.

Organizzazione delle zone per la gestione dei criteri

Un altro insieme di zone da creare contribuisce ad applicare criteri diversi a tipi di endpoint diversi. Prendere in considerazione i seguenti esempi:

- Zona criteri – Workstation
- Zona criteri – Workstation – Esclusioni
- Zona criteri – Server
- Zona criteri – Server – Esclusioni
- Zona criteri – Dirigenti – Protezione elevata

Dell consiglia di applicare un criterio per impostazione predefinita a tutti i dispositivi in questa zona criteri in ciascuna di queste zone. Prestare attenzione a non mettere un dispositivo in più zone criteri poiché questo può generare un conflitto su quale criterio viene applicato. Ricordare anche che il motore della regola di zona può contribuire ad organizzare automaticamente questi host basati su IP, nome host, sistema operativo e dominio.

Organizzazione delle zone per la gestione dell'accesso basato sui ruoli

L'accesso basato sui ruoli è usato per limitare l'accesso di un utente della console a un sottoinsieme di dispositivi che ha la responsabilità di gestire. Questo può comprendere la separazione per intervallo di IP, nomi host, sistema operativo o dominio. Prendere in considerazione i raggruppamenti per posizione geografica, tipo o entrambi.

Esempio:

- Zona RBAC – Desktop – Europa
- Zona RBAC – Server – Asia
- Zona RBAC – Tappeto rosso (Dirigenti)

Utilizzando gli esempi di zone precedenti, un manager di zona potrebbe essere assegnato a *Zona RBAC – Desktop – Europa* e avrebbe accesso solo ai dispositivi all'interno di tale zona. Se l'utente manager di zona cercasse di visualizzare altre zone, riceverebbe un messaggio di errore che indica che non ha le autorizzazioni per visualizzarle. Sebbene un dispositivo possa essere in più zone e il manager di zona sia in grado di visualizzare tale dispositivo, se cercasse di visualizzare le altre zone cui è associato il dispositivo non gli sarebbe consentito e visualizzerebbe il messaggio di errore.

In altre parti della console, come ad esempio la dashboard, il manager di zona per *Zona RBAC – Desktop – Europa* sarebbe inoltre limitato alle minacce e ad altre informazioni relative alla zona o ai dispositivi assegnati a tale zona.

Le stesse restrizioni si applicano agli utenti assegnati a una zona.

Gestione utenti

Gli amministratori hanno autorizzazioni globali e possono aggiungere o rimuovere utenti, assegnare utenti alle zone (come utenti o manager di zona), aggiungere o rimuovere dispositivi, creare criteri e creare zone. Gli amministratori possono anche eliminare dalla console utenti, dispositivi, criteri e zone in modo permanente.

Gli utenti e i manager di zona hanno solo accesso e autorizzazioni relativi alla zona cui sono assegnati. Questo si applica a dispositivi assegnati alla zona, minacce individuate in quei dispositivi e informazioni nella dashboard.

Per un elenco completo delle autorizzazioni utente concesse a ciascun utente, vedere l'Appendice C: Autorizzazioni utente.

Per aggiungere utenti

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare gli utenti.
2. Selezionare **Impostazioni > Gestione utenti**.
3. Immettere l'indirizzo di posta elettronica dell'utente.
4. Selezionare un ruolo nel menu a discesa Ruolo.
5. Quando si aggiunge un manager di zona o un utente, selezionare una zona a cui assegnarli.

6. Fare clic su **Aggiungi**. Viene inviato un messaggio di posta elettronica all'utente con un collegamento per creare una password.

Per modificare i ruoli utente

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare gli utenti.
2. Selezionare **Impostazioni** > **Gestione utenti**.
3. Fare clic su un utente. Viene visualizzata la pagina Dettagli utente.
4. Selezionare un ruolo e fare clic su **Salva**.

Per rimuovere utenti

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono creare gli utenti.
2. Selezionare **Impostazioni** > **Gestione utenti**.
3. Selezionare la casella di controllo dell'utente o degli utenti da rimuovere.
4. Fare clic su **Rimuovi**.
5. Fare clic su **Sì** quando viene visualizzato il messaggio che chiede di confermare la rimozione.

Informazioni relative alla rete

Configurare la rete per consentire a Threat Defense Agent di comunicare con la console tramite Internet. Questa sezione si occupa delle impostazioni firewall e delle configurazioni proxy.

Firewall

Per gestire i dispositivi non è necessario nessun software locale. I Threat Defense Agent sono gestiti da e rispondono alla console (interfaccia utente basata su cloud). La porta 443 (HTTPS) viene utilizzata per le comunicazioni e deve essere aperta sul firewall affinché gli agenti possano comunicare con la console. La console è ospitata da Amazon Web Services (AWS) e non è dotata di indirizzi IP fissi. Assicurarsi che gli agenti possano comunicare con i seguenti siti:

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com
- api2.cylance.com
- download.cylance.com

In alternativa, consentire il traffico HTTPS per *.cylance.com

Proxy

Il supporto proxy per Threat Defense viene configurato tramite una voce di registro. Quando viene configurato un proxy, l'agente usa l'indirizzo IP e la porta nella voce di registro per tutte le comunicazioni verso l'esterno ai server della console.

1. Accedere al registro.

   Nota: possono essere necessarie autorizzazioni elevate o la proprietà del registro a seconda della modalità con cui è stato installato l'agente (Modalità protetta abilitata oppure no).

2. Nell'editor del Registro di sistema, accedere a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Creare un nuovo valore stringa (REG_SZ):
   - Nome valore = ProxyServer
   - Dati valore = impostazioni proxy (ad esempio http://123.45.67.89:8080)

L'agente tenta di usare le credenziali dell'utente attualmente connesso per comunicare tramite Internet in ambienti autenticati. Se un server proxy autenticato è configurato e un utente non è connesso al dispositivo, l'agente non può autenticarsi nel proxy e non può comunicare con la console. In questo caso è necessario eseguire una delle due azioni seguenti:

- Configurare il proxy e aggiungere una regola per consentire tutto il traffico verso *.cylance.com.
- Usare un criterio proxy diverso, consentendo al proxy non autorizzato l'accesso agli host di Cylance (*.cylance.com).

In questo modo, se nessun utente è connesso al dispositivo, non è necessario che l'agente si autentichi e dovrebbe essere in grado di connettersi al cloud e comunicare con la console.

Dispositivi

Una volta che un agente è installato in un endpoint, diventa disponibile come un dispositivo nella console. Per iniziare a gestire dispositivi, assegnare un criterio (per gestire le *minacce* identificate), raggruppare i dispositivi (utilizzando le *zone*) ed eseguire azioni manualmente su ogni dispositivo (*Quarantena* e *Ignora*).

Gestione dei dispositivi

I dispositivi sono computer con un Threat Defense Agent. Gestire i dispositivi dalla console.

1. Accedere alla console (http://dellthreatdefense.com) come amministratore. Solo gli amministratori possono gestire i dispositivi.
2. Fare clic su **Dispositivi**.
3. Selezionare la casella di controllo di un dispositivo per consentire le seguenti azioni:
   - **Esporta**: crea e scarica un file CSV. Il file contiene informazioni sul dispositivo (nome, stato e criterio) per tutti i dispositivi nell'organizzazione.
   - **Rimuovi**: rimuove i dispositivi selezionati dal relativo *elenco*. Questa operazione non disinstalla l'agente dal dispositivo.
   - **Assegna criterio**: consente l'assegnazione dei dispositivi selezionati a un criterio.
   - **Aggiungi dispositivi alla zona**: consente di aggiungere i dispositivi selezionati a una o più zone.
4. Fare clic su un dispositivo per visualizzare la pagina Dettagli dispositivo.

- **Informazioni sul dispositivo**: visualizza informazioni come nome host, versione dell'agente e versione del sistema operativo.
- **Proprietà dispositivo**: consente di modificare il nome dispositivo, il criterio, le zone e il livello di registrazione.
- **Minacce e attività**: visualizza informazioni sulle minacce e altre attività relative al dispositivo.

5. Fare clic su **Aggiungi nuovo dispositivo** per visualizzare una finestra di dialogo con un token di installazione e collegamenti per scaricare il programma di installazione dell'agente.
6. Nella colonna Zone, fare clic su un nome di zona per visualizzare la pagina Dettagli zone.

Minacce e attività

Visualizza informazioni sulle minacce e altre attività relative al dispositivo selezionato.

Minacce

Visualizza tutte le minacce individuate nel dispositivo. Per impostazione predefinita, le minacce sono raggruppate per stato (*Non sicuro*, *Anomalo*, *In quarantena* e *Ignorato*).

- **Esporta**: crea e scarica un file CSV che contiene informazioni su tutte le minacce individuate nel dispositivo selezionato. Le informazioni sulle minacce comprendono informazioni come nome, percorso del file, punteggio Cylance e stato.
- **Quarantena**: *mette in quarantena* le minacce selezionate. Si tratta di una *quarantena locale*, ovvero questa minaccia viene *messa in quarantena* solo in questo dispositivo. Per *mettere in quarantena* una minaccia per tutti i dispositivi nell'organizzazione, accertarsi che la casella di controllo **Metti in quarantena questa minaccia anche ogni volta che viene trovata su qualsiasi dispositivo** sia selezionata (*quarantena globale*) quando un file viene *messo in quarantena*.
- **Ignora**: modifica lo stato della minaccia selezionata in *Ignorato*. È consentita l'esecuzione di un file *ignorato*. Si tratta di una *condizione locale*, ovvero il file è consentito solo in questo dispositivo. Per consentire questo file su tutti i dispositivi nell'organizzazione, selezionare la casella di controllo **Contrassegna come sicuro anche su tutti i dispositivi** (*Elenco file sicuri*) quando un file viene *ignorato*.

Tentativi di exploit

Visualizza tutti i tentativi di exploit nel dispositivo. Questo comprende le informazioni sul nome del processo, ID, tipo e azione intrapresa.

Registri agente

Visualizza i file di registro caricati dall'agente nel dispositivo. Il nome del file di registro è la data del registro.

Per visualizzare i file di registro dell'agente:

1. Caricare il file di registro corrente per un unico dispositivo.
   a. Fare clic su Dispositivi > Registri agente.
   b. Fare clic su **Carica file di registro corrente**. Questa operazione potrebbe richiedere alcuni minuti, in base alle dimensioni del file di registro.

OPPURE

1. Impostazioni dei criteri:
    a. Fare clic su Impostazioni > Criterio dispositivo > [selezionare un criterio] > Registri agente
    b. Fare clic su Abilita caricamento automatico dei file di registro.
    c. Fare clic su **Salva**.

Per visualizzare registri dettagliati, modificare il livello di registrazione dell'agente prima di caricare qualsiasi file di registro.

1. Nella console: **Dispositivi > [fare clic su un dispositivo]**, selezionare **Dettagliato** dal menu a discesa Livello di registrazione agente e fare clic su **Salva**. Dopo che i file di registro dettagliati sono stati caricati, Dell consiglia di modificare nuovamente il livello di registrazione agente in *Informazioni*.
2. Nel dispositivo, chiudere l'interfaccia utente di Threat Defense (fare clic con il pulsante destro del mouse sull'icona di Threat Defense nella barra delle applicazioni, quindi scegliere **Esci**).

OPPURE

1. Aprire la riga di comando come amministratore. Immettere la seguente riga di comando, quindi premere **Invio**.

    ```
    cd C:\Program Files\Cylance\Desktop
    ```

2. Immettere la seguente riga di comando, quindi premere **Invio**.

    ```
    Dell.ThreatDefense.exe –a
    ```

3. Viene visualizzata l'icona di Threat Defense nella barra delle applicazioni. Fare clic con il pulsante destro del mouse, scegliere **Registrazione**, quindi fare clic su **Tutto** (come Dettagliato nella console).

OPPURE (per Mac OS X)

1. Uscire dall'interfaccia utente attualmente in esecuzione.
2. Eseguire il seguente comando dal terminale.

    ```
    sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
    ```

3. Fare clic con il pulsante destro del mouse sulla nuova interfaccia utente quando si apre. Selezionare **Registrazione** > **Tutto**.

Controllo script

Visualizza tutte le attività rilevanti per Controllo script, come gli script negati.

Dispositivi duplicati

Quando il Threat Defense Agent viene installato per la prima volta in un dispositivo, viene creato un identificativo univoco usato dalla console per identificare e fare riferimento al dispositivo. Tuttavia, alcuni eventi, come l'utilizzo di un'immagine di macchina virtuale per creare più sistemi, possono causare la generazione di un secondo identificatore per lo stesso dispositivo. Selezionare il dispositivo e fare clic su **Rimuovi** se viene visualizzata una voce duplicata nella pagina Dispositivi nella console.

Per favorire l'identificazione di tali dispositivi, usare la funzione di ordinamento delle colonne nella pagina Dispositivi per ordinare e confrontare i dispositivi, generalmente per nome. In alternativa, l'*elenco dei dispositivi* può essere esportato come file .CSV e quindi visualizzato in Microsoft Excel o un'applicazione analoga con funzionalità avanzate di ordinamento/organizzazione.

Esempio di utilizzo di Microsoft Excel

1. Aprire il file CSV del dispositivo in Microsoft Excel.
2. Selezionare la colonna del nome dei dispositivi.
3. Dalla scheda Home, selezionare Formattazione condizionale > Regole evidenziazione celle > Valori duplicati.
4. Accertarsi che sia selezionata l'opzione **Duplica**, quindi selezionare un'opzione di evidenziazione.
5. Fare clic su **OK**. Gli elementi duplicati vengono evidenziati.

Nota: il comando Rimuovi rimuove solo il dispositivo dalla pagina Dispositivo. Questo non esegue un comando di disinstallazione per il Threat Defense Agent. È necessario disinstallare l'agente dall'endpoint.

Aggiornamento dell'agente

La manutenzione e la gestione dei Threat Defense Agent sono semplicissime. Gli agenti scaricano automaticamente gli aggiornamenti dalla console e la manutenzione della console viene effettuata da Cylance.

L'agente esegue un riscontro con la console ogni 1-2 minuti. La console riporta lo stato attuale dell'agente (*Online* oppure *Offline Non sicuro* o *Protetto*), le informazioni sulla versione, il sistema operativo e lo stato delle minacce.

Threat Defense rilascia mensilmente degli aggiornamenti all'agente. Questi aggiornamenti possono comprendere revisioni per la configurazione, nuovi moduli e modifiche al programma. Quando è disponibile un aggiornamento dell'agente (come riportato dalla console in Impostazioni > Aggiornamenti agente), l'agente scarica automaticamente l'aggiornamento e lo applica. Per controllare il traffico di rete durante gli aggiornamenti dell'agente, tutte le organizzazioni sono impostate per accogliere un massimo di 1000 aggiornamenti dei dispositivi contemporaneamente. Gli utenti possono inoltre disabilitare l'aggiornamento automatico, se preferiscono.

Nota: il supporto Dell può modificare il numero massimo di dispositivi aggiornabili contemporaneamente.

Aggiornamento in base alla zona

L'aggiornamento in base alla zona consente a un'organizzazione di valutare un nuovo agente in un sottoinsieme di dispositivi prima di distribuirlo nell'intero ambiente (Produzione). È possibile aggiungere temporaneamente una o più zone correnti a una delle due zone di test (test e pilota) che può usare un agente diverso da quello della Produzione.

Per configurare gli aggiornamenti in base alla zona:

1. Accedere alla console (http://dellthreatdefense.com) con un account amministratore.
2. Selezionare **Impostazioni > Aggiornamento agente**. Vengono visualizzate le tre versioni più recenti dell'agente.

   Se la zona di produzione è impostata su **Aggiorna automaticamente**, le zone di test e pilota non sono disponibili. Modificare Aggiorna automaticamente nella zona di produzione in qualcosa di diverso per abilitare le zone di test e pilota.
3. Selezionare una versione dell'agente specifica nell'elenco a discesa Produzione.
4. Per Produzione, selezionare anche Aggiorna automaticamente o Non aggiornare.
   a. **Aggiorna automaticamente** consente a tutti i dispositivi di produzione di eseguire automaticamente l'aggiornamento alla versione più recente nell'*elenco delle versioni dell'agente supportate*.

b. **Non aggiornare** impedisce l'aggiornamento dell'agente da parte di tutti i dispositivi di produzione.

5. Per la zona di test, selezionare una o più zone dall'elenco a discesa Zona, quindi selezionare una versione specifica dell'agente dall'elenco a discesa delle versioni.
6. Se lo si desidera, ripetere il punto 5 per la zona pilota.

Nota: quando un dispositivo viene aggiunto a una zona che fa parte della zona di test o pilota, quel dispositivo inizia ad usare la versione dell'agente della zona di test o pilota. Se un dispositivo appartiene a più di una zona, e una di tali zone appartiene alla zona di test o a quella pilota, la versione dell'agente della zona di test o pilota ha la priorità.

Per attivare l'aggiornamento di un agente

Per attivare un aggiornamento agente prima dell'intervallo orario successivo:

1. Fare clic con il pulsante destro del mouse sull'icona del Threat Defense Agent nella barra delle applicazioni e scegliere **Controlla aggiornamenti**.
2. Riavviare il servizio di Threat Defense. Questo forza un riscontro immediato con la console.

OPPURE

- Gli aggiornamenti possono essere avviati dalla riga di comando. Eseguire il comando seguente dalla directory di Cylance:

  ```
  Dell.ThreatDefense.exe – update
  ```

Dashboard

Una volta eseguito l'accesso alla Threat Defense Console viene visualizzata la pagina Dashboard. La Dashboard fornisce una panoramica delle minacce nell'ambiente e fornisce accesso a informazioni sulla console diverse da una pagina.

Statistiche sulle minacce

Le statistiche sulle minacce forniscono il numero di minacce identificate nelle *ultime 24 ore* e il *totale* per l'organizzazione. Fare clic su una *statistica di minaccia* per accedere alla pagina Protezione e visualizzare l'elenco delle minacce correlate alla statistica.

- **Minacce in esecuzione**: file identificati come minacce che sono attualmente in esecuzione in dispositivi dell'organizzazione.
- **Minacce in esecuzione automatica**: minacce che sono impostate per essere eseguite automaticamente.
- **Minacce messe in quarantena**: minacce *messe in quarantena* nelle ultime 24 ore e totale.
- **Esclusive per Cylance**: minacce identificate da Cylance, ma non da altre fonti di antivirus.

Percentuali di protezione

Visualizza le percentuali per Threat Protection e la protezione dei dispositivi.

- **Threat Protection**: la percentuale di minacce per le quali è stata intrapresa un'azione (Quarantena, Quarantena globale, Ignora ed Elenco file sicuri).
- **Protezione dispositivi**: la percentuale di dispositivi associati ad un criterio che ha la quarantena automatica abilitata.

Minacce per priorità

Visualizza il numero totale di minacce che richiedono un'azione (*Quarantena*, *Quarantena globale*, *Ignora* ed *Elenco file sicuri*). Le minacce vengono raggruppate per priorità (Alta, Media e Bassa). Questa panoramica visualizza il numero totale delle minacce che richiedono un'azione, suddivide quel totale per priorità, fornisce un totale della percentuale e il numero dei dispositivi che sono interessati.

Le minacce vengono elencate per priorità nell'angolo in basso a sinistra della pagina Dashboard. Viene specificato il numero totale delle minacce in un'organizzazione raggruppate per classificazione di priorità.

Una minaccia viene classificata come Bassa, Media o Alta in base al numero di attributi che possiede fra quelli riportati di seguito:

- Il file ha un punteggio Cylance superiore a 80.
- Il file è attualmente in esecuzione.
- Il file è stato eseguito precedentemente.
- Il file è impostato per l'esecuzione automatica.
- La priorità della zona in cui è stata rilevata la minaccia.

Questa classificazione aiuta gli amministratori a stabilire di quali minacce e dispositivi devono occuparsi prima. Fare clic sulla minaccia o sul numero dispositivo per visualizzare informazioni dettagliate su minacce e dispositivi.

Eventi di minaccia

Visualizza un grafico a linee con il numero di minacce individuate nell'arco degli ultimi 30 giorni. Le linee sono contrassegnate da colori diversi per i file *non sicuri, anomali, messi in quarantena, ignorati* e *cancellati*.

- Passare il mouse su un punto nel grafico per visualizzare i dettagli.
- Fare clic su uno dei colori nella legenda per mostrare o nascondere quella linea.

Classificazione delle minacce

Visualizza una mappa termica dei tipi di minacce rilevati nell'organizzazione, come virus o malware. Fare clic su un elemento nella mappa termica per passare alla pagina Protezione e visualizzare un elenco di minacce di quel tipo.

Elenchi dei primi cinque

Visualizza elenchi per le prime cinque minacce rilevate nel maggior numero di dispositivi, i primi cinque dispositivi con il maggior numero di minacce e le prime cinque zone con il maggior numero di minacce nell'organizzazione. Fare clic su un elemento dell'elenco per maggiori dettagli.

Gli elenchi dei primi cinque sulla dashboard evidenziano le minacce *pericolose* nell'organizzazione su cui non è stata eseguita alcuna azione, ad esempio quelle *messe in quarantena* o *ignorate*. Il più delle volte, questi elenchi dovrebbero essere vuoti. Sebbene sia consigliabile intervenire anche sulle minacce *anomale*, l'obiettivo degli elenchi dei primi cinque è quello di evidenziare le minacce critiche.

Protezione – Minacce

Threat Defense non si limita a classificare i file semplicemente come *non sicuri* o *anomali*. Advanced Threat Protection può fornire dettagli sulle caratteristiche statiche e dinamiche dei file. Questo consente agli amministratori non solo di bloccare eventuali minacce, ma di comprenderne il comportamento allo scopo di fornire loro delle risposte adeguate o di attenuarle.

Tipi di file

Non sicuro: un file con un punteggio compreso tra 60 e 100. Un file *Non sicuro* è un file in cui il motore di Threat Defense riscontra attributi profondamente simili a quelli di un malware.

Anomalo: un file con un punteggio compreso tra 1 e 59. Un file Anomalo presenta alcuni attributi di un malware ma meno rispetto a un file classificato *Non sicuro*; vi sono pertanto meno probabilità che il file in questione sia un malware.

Nota: occasionalmente, un file può essere classificato come *Non sicuro* o *Anomalo* anche se il punteggio mostrato non rientra nell'intervallo previsto per la classificazione. Ciò può essere dovuto a risultati aggiornati o ad analisi supplementari dei file dopo il rilevamento iniziale. Per le analisi più aggiornate, abilitare l'auto-caricamento nei criteri dei dispositivi.

Punteggio Cylance

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.

Visualizzazione delle informazioni sulle minacce

La scheda Protezione nella console visualizza informazioni dettagliate sulle minacce, i dispositivi in cui sono state individuate e le azioni intraprese in detti dispositivi per quelle minacce.

Nota: l'*elenco delle minacce* nella scheda Protezione presenta colonne configurabili. Fare clic sulla freccia GIÙ in una delle colonne per accedere al menu, quindi Mostra/Nascondi vari dettagli delle minacce. Il menu comprende un sottomenu per applicare filtri.

Per visualizzare i dettagli delle minacce

1. Accedere alla console (http://dellthreatdefense.com).
2. Fare clic sulla scheda **Protezione** per visualizzare un elenco delle minacce presenti nell'organizzazione.
3. Usare il filtro nella barra dei menu a sinistra per filtrare in base alla priorità (Alta, Media o Bassa) e allo stato (*In quarantena*, *Ignorato*, *Non sicuro* o *Anomalo*).

   Nota: i numeri che vengono visualizzati in rosso nel riquadro sinistro indicano minacce rilevanti che non sono state messe *in quarantena* o *ignorate*. Applicare un filtro a quegli elementi per visualizzare un elenco di file che devono essere analizzati.
4. Per aggiungere colonne in modo che possano essere visualizzate ulteriori informazioni sulle minacce, fare clic sulla freccia GIÙ accanto a uno dei nomi delle colonne, quindi selezionare un nome di colonna.
5. Per visualizzare informazioni aggiuntive su una minaccia specifica, fare clic sul collegamento del nome della minaccia (i dettagli vengono visualizzati in una nuova pagina) oppure fare clic in un punto qualunque della riga della minaccia (i dettagli vengono visualizzati in fondo alla pagina). Entrambe le visualizzazioni mostrano il medesimo contenuto, ma hanno stili di presentazione differenti. Le informazioni dettagliate in questione includono una panoramica dei metadati del file, un elenco di dispositivi in cui è presente la minaccia e rapporti probatori.

   a. Metadati dei file

      - Classificazione [assegnata dal team di gestione avanzata delle minacce e degli avvisi (ATAM, Advanced Threat and Alert Management) di Cylance]
      - Punteggio Cylance (livello di certezza)
      - Condanna dell'industria AV (rimanda a VirusTotal.com per il confronto con altri fornitori)
      - Data primo rilevamento, Data ultimo rilevamento
      - SHA256
      - MD5
      - Informazioni sui file (autore, descrizione, versione e così via)
      - Dettagli sulla firma

   b. Dispositivi

      L'*Elenco dei dispositivi della zona* relativo a una minaccia può essere filtrato in base allo stato della minaccia (*Non sicuro*, *In quarantena*, *Ignorato* e *Anomalo*). Fare clic sui collegamenti dei filtri dello stato per visualizzare i dispositivi che presentano la minaccia con lo stato indicato.

      - *Non sicuro*: il file è classificato come *Non sicuro*, ma non è stata eseguita alcuna azione.
      - *In quarantena*: il file è già stato messo *in quarantena* per via di un'impostazione dei criteri.
      - *Ignorato*: il file è stato *ignorato* o *inserito tra gli elementi consentiti* dall'amministratore.

- *Anomalo*: il file è classificato come *Anomalo*, ma non è stata eseguita alcuna azione.

c. Rapporti probatori

- **Indicatori di minaccia**: osservazioni su un file che il motore di Cylance Infinity ha analizzato. Questi indicatori aiutano a comprendere le motivazioni che sottendono la classificazione di un file e forniscono indicazioni approfondite sugli attributi e il comportamento di un file. Gli indicatori di minaccia sono raggruppati in categorie per offrire aiuto in base al contesto.
- **Dati dettagliati sulla minaccia**: Dati dettagliati sulla minaccia offre una sintesi generale delle caratteristiche statiche e dinamiche di un file, fra cui metadati supplementari del file, dettagli strutturali del file e comportamenti dinamici quali file rilasciati, chiavi di registro create o modificate e URL con i quali il file ha tentato di comunicare.

Per visualizzare gli indicatori delle minacce:

1. Accedere alla console (http://dellthreatdefense.com).
2. Fare clic su **Protezione** nel menu superiore per visualizzare un elenco delle minacce (o fare clic su **Dispositivi**, quindi selezionare un dispositivo).
3. Fare clic sul nome di una delle minacce. Viene visualizzata la pagina Dettagli minaccia.
4. Fare clic su **Rapporti probatori**.

Categorie degli indicatori di minaccia:

Ciascuna categoria rappresenta un'area che è stata individuata spesso in software dannosi ed è basata sull'analisi approfondita di oltre 100 milioni di binari. Il rapporto degli indicatori di minaccia indica quante di quelle categorie erano presenti nel file.

Anomalie
Il file presenta elementi che sono incoerenti o anomali in qualche modo. Spesso si tratta di incoerenze nella struttura del file.

Raccolta
Il file presenta prove di raccolta dati. Questo può comprendere l'enumerazione della configurazione del dispositivo o la raccolta di informazioni riservate.

Perdita di dati
Il file presenta prove di estrapolazione di dati. Questo può comprendere connessioni di rete verso l'esterno, prove che si comporti come un browser o altre comunicazioni di rete.

Inganno
Il file presenta prove di tentativi di ingannare. L'inganno può presentarsi sotto forma di sezioni nascoste, inclusione di codice per evitare il rilevamento o indicazioni di etichettatura impropria nei metadati o altre sezioni.

Distruzione
Il file presenta prove di funzionalità distruttive. La distruzione comprende la capacità di eliminare le risorse di un dispositivo come file e directory.

Varie
Tutti gli indicatori che non ricadono nelle altre categorie.

Nota: occasionalmente le sezioni Indicatori di minacce e Dati dettagliati sulla minaccia non presentano risultati o non sono disponibili. Questo accade quando il file non è stato caricato. La registrazione debug può fornire informazioni approfondite sul motivo per cui il file non è stato caricato.

Affrontare le minacce

Il tipo di azione da intraprendere per alcune minacce può dipendere dall'utente assegnato di un dispositivo. Le azioni applicate alle minacce possono essere applicate a livello del dispositivo o a livello globale. Di seguito sono elencate le diverse azioni che possono essere intraprese nei confronti di minacce rilevate o file:

- ***Quarantena***: mette in *quarantena* un file specifico per impedirne l'esecuzione nel dispositivo.

  Nota: È possibile mettere in quarantena una minaccia utilizzando la riga di comando di un dispositivo. Questa funzione è disponibile solo con Agente di Windows. Per ulteriori informazioni, vedere Messa in quarantena tramite la riga di comando.

- ***Quarantena globale***: mette in *quarantena globale* un file per impedirne l'esecuzione in qualsiasi dispositivo in tutta l'organizzazione.

  Nota: mettendo il file in *quarantena*, questo viene spostato dalla sua posizione originale alla directory della *quarantena* (**`C:\ProgramData\Cylance\Desktop\q`**).

- ***Ignora***: *ignora* un file specifico per consentirne l'esecuzione nel dispositivo specificato.

- ***Elenco file sicuri globale***: inserisce nell'*Elenco file sicuri globale* un file per consentirne l'esecuzione in qualsiasi dispositivo all'interno dell'intera organizzazione.

Nota: occasionalmente, Threat Defense può mettere in *quarantena* o segnalare un file "buono" (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 globale* può risultare utile in queste circostanze.

- ***Carica file***: caricare manualmente un file su Cylance Infinity per l'analisi. Se il caricamento automatico è abilitato, i nuovi file (che non sono stati analizzati da Cylance) vengono caricati automaticamente su Cylance Infinity. Se il file è presente su Cylance Infinity il pulsante Carica file non è disponibile (disattivato).
- ***Download del file***: scaricare un file per eseguire test personali. Questa funzionalità deve essere abilitata per l'organizzazione. L'utente deve essere un amministratore. È necessario che la minaccia venga rilevata usando la versione 1320 dell'agente o superiore.

  Nota: il file deve essere disponibile su Cylance Infinity e tutti e tre gli hash (SHA256, SHA1 e MD5) devono corrispondere tra Cylance Infinity e l'agente. In caso contrario il pulsante Scarica file non è disponibile.

Affrontare le minacce in un dispositivo specifico

1. Accedere alla console (http://dellthreatdefense.com) come amministratore o manager di zona.
2. Fare clic sulla scheda **Dispositivi**.
3. Cercare e selezionare il dispositivo.
4. In alternativa, potrebbe essere disponibile un collegamento al dispositivo dalla scheda Protezione se è elencato con una minaccia associata.
5. Tutte le minacce in quel dispositivo sono elencate in fondo alla pagina. Selezionare la minaccia da mettere in *quarantena* o *ignorare* il file sul dispositivo.

Affrontare globalmente le minacce

I file aggiunti all'*Elenco Quarantena globale* o all'*Elenco file sicuri globale* sono messi *in quarantena* o *consentiti* su tutti i dispositivi in tutte le zone.

1. Accedere alla console (http://dellthreatdefense.com) come amministratore.
2. Fare clic su **Impostazioni** > **Elenco globale**.
3. Fare clic su Quarantena globale o File sicuri.
4. Fare clic su **Aggiungi file**.
5. Aggiungere l'SHA256 (obbligatorio) del file, l'MD5, il nome e il motivo per cui si sposta nell'*Elenco globale*.
6. Fare clic su **Invia**.

Protezione – Controllo script

Threat Defense fornisce dettagli sugli script attivi e PowerShell che sono stati bloccati o per i quali è stato emesso un avviso. Con Controllo script abilitato, i risultati vengono visualizzati nella scheda Controllo script nella pagina Protezione. Questo fornisce dettagli sullo script e sui dispositivi interessati.

Per visualizzare i risultati di Controllo script

1. Accedere alla console (http://dellthreatdefense.com) come amministratore.
2. Fare clic su Protezione.
3. Fare clic su Controllo script.
4. Selezionare uno script nella tabella. In questo modo la tabella Dettagli si aggiorna con un elenco dei dispositivi interessati.

Descrizioni delle colonne di Controllo script

- **Nome file**: il nome dello script.
- **Interprete**: la funzionalità del controllo script che ha identificato lo script.
- **Ultimo rilevamento**: la data e l'ora in cui lo script è stato eseguito per l'ultima volta.
- **Tipo di unità**: il tipo di unità in cui è stato trovato lo script (esempio: disco rigido interno).
- **SHA256**: l'hash SHA 256 dello script.
- **Numero di dispositivi**: il numero di dispositivi interessati dallo script.
- **Avviso**: il numero di volte in cui è stato emesso un avviso per lo script. Può essere accaduto più volte per lo stesso dispositivo.
- **Blocca**: il numero di volte in cui lo script è stato bloccato. Può essere accaduto più volte per lo stesso dispositivo.

Descrizioni della colonna Dettagli

- **Nome del dispositivo**: il nome del dispositivo interessato dallo script. Fare clic sul nome del dispositivo per passare alla pagina Dettagli dispositivo.
- **Stato**: lo stato del dispositivo (online o offline).
- **Versione dell'agente**: il numero di versione dell'agente attualmente installato nel dispositivo.
- **Percorso file**: il percorso del file da cui è stato eseguito lo script.
- **Quando**: la data e l'ora in cui è stato eseguito lo script.
- **Nome utente**: il nome dell'utente connesso quando è stato eseguito lo script.
- **Azione**: l'azione intrapresa per lo script (Avviso o Blocca).

Elenco globale

L'*Elenco globale* permette a un file di essere contrassegnato per la *quarantena* o di *consentire* tali file su tutti i dispositivi nell'organizzazione.

- **Quarantena globale:** tutti gli agenti dell'organizzazione mettono in *quarantena* qualsiasi file nell'*Elenco Quarantena globale* individuato nel dispositivo.
- **Sicuro:** tutti gli agenti dell'organizzazione *consentono* qualsiasi file nell'*Elenco file sicuri* individuato nel dispositivo.
- **Non assegnato:** qualunque minaccia identificata nell'organizzazione che non viene assegnata né all'*Elenco Quarantena globale*, né all'*Elenco file sicuri*.

Modificare lo stato di una minaccia

Per modificare lo stato di una minaccia (*Quarantena globale*, *Sicuro* o *Non assegnato*):

1. Accedere alla console (http://dellthreatdefense.com) come amministratore.
2. Selezionare **Impostazioni** > **Elenco globale**.
3. Selezionare l'elenco corrente cui è assegnata la minaccia. Ad esempio, fare clic su Non assegnato per modificare una minaccia non assegnata in *Sicuro* o *Quarantena globale*.
4. Selezionare le caselle di controllo per le minacce da modificare e fare clic su un pulsante di stato.

a. Sicuro: sposta i file nell'*Elenco file sicuri*.

b. Quarantena globale: sposta i file nell'*Elenco Quarantena globale*.

c. Rimuovi dall'elenco: sposta i file nell'*Elenco dei file non assegnati*.

Aggiungere un file

Aggiungere manualmente un file all'*Elenco Quarantena globale* o all'*Elenco file sicuri*. Sono necessarie le informazioni sull'hash SHA256 per il file che si desidera aggiungere.

1. Accedere alla console (http://dellthreatdefense.com) come amministratore.
2. Selezionare **Impostazioni** > **Elenco globale**.
3. Selezionare l'elenco in cui aggiungere il file (*Quarantena globale* o *Sicuro*).
4. Fare clic su **Aggiungi file**.
5. Immettere le informazioni sull'hash SHA256. Facoltativamente è possibile immettere le informazioni su MD5 e il nome del file.
6. Immettere un motivo per l'aggiunta di questo file.
7. Fare clic su **Invia**.

Aggiungere all'elenco file sicuri per certificato

I clienti hanno la possibilità di inserire file nell'*Elenco file sicuri* per certificato firmato, che consente l'esecuzione senza interruzioni di qualsiasi software personalizzato correttamente firmato.

Nota: questa funzionalità attualmente funziona esclusivamente con i sistemi operativi Windows.

- Questa funzionalità consente ai clienti di definire un *Elenco file sicuri/elementi consentiti* per certificato firmato, rappresentato dall'identificazione SHA1 del certificato.
- Le informazioni del certificato sono estratte dalla console (Data e ora, Soggetto, Autorità emittente e Identificazione personale). Il certificato non viene caricato o salvato nella console.
- Data e ora del certificato rappresentano quando questo è stato creato.
- La console non controlla se il certificato è valido o scaduto.
- Se il certificato cambia (ad esempio, rinnovato o nuovo), deve essere aggiunto all'*Elenco file sicuri* nella console.

1. Aggiungere i dettagli del certificato all'Archivio dei certificati.
    a. Identificare l'identificazione personale del certificato per l'eseguibile di tipo Portable Executable (PE) firmato.
    b. Selezionare **Impostazioni** > **Certificati**.
    c. Fare clic su **Aggiungi certificato**.
    d. Fare clic su Cerca certificati da aggiungere o trascinare il certificato nella finestra del messaggio.
    e. Se si cercano i certificati, viene visualizzata la finestra Apri per consentire la selezione dei certificati.
    f. Facoltativamente, è possibile aggiungere delle note sul certificato.
    g. Fare clic su **Invia**. Autorità emittente, Soggetto, Identificazione personale e Note (se presenti) vengono aggiunti all'archivio.
2. Aggiungere il certificato all'*Elenco file sicuri*.

a. Selezionare **Impostazioni** > **Elenco globale**.

b. Fare clic sulla scheda **Sicuro**.

c. Fare clic su **Certificati**.

d. Fare clic su **Aggiungi certificato**.

e. Selezionare un certificato dall'*Elenco file sicuri*. Facoltativamente è possibile selezionare una categoria e aggiungere un motivo per cui viene aggiunto il certificato.

f. Fare clic su **Invia**.

Visualizzazione delle identificazioni personali per una minaccia

Nella scheda Protezione, in Dettagli minacce ora viene visualizzata l'identificazione personale del certificato. Dalla schermata, selezionare **Aggiungi al certificato** per aggiungere il certificato all'archivio.

Privilegi

Aggiungi al certificato è una funzione disponibile solo per gli amministratori. Se il certificato è già stato aggiunto all'archivio dei certificati, nella console viene visualizzato **Vai al certificato**. I certificati sono visibili esclusivamente dai manager di zona, che vedono l'opzione **Vai al certificato**.

Profilo

Il menu del profilo (angolo superiore destro) consente la gestione del proprio account, dei registri di controllo della console e l'accesso alla guida del prodotto.

Account

Modificare la password e le impostazioni di notifica tramite posta elettronica nella pagina Account.

1. Accedere alla console (http://dellthreatdefense.com).
2. Fare clic sul menu del profilo nell'angolo superiore destro e selezionare **Account**.
3. Per modificare la password:
    a. Fare clic su Modifica password.
    b. Immettere la password precedente.
    c. Immettere la nuova password e ripetere l'operazione per confermarla.
    d. Fare clic su Aggiorna.
4. Selezionare o deselezionare la casella di controllo per abilitare o disabilitare le Notifiche tramite posta elettronica. L'abilitazione e la disabilitazione della casella di controllo vengono salvate automaticamente. Notifiche tramite posta elettronica è disponibile solo per gli amministratori.

Registrazione di controllo

Elenco a discesa icona utente (angolo superiore destro della console)

Il Registro di controllo contiene informazioni sulle seguenti azioni eseguite dalla console:

- Accesso (Riuscito, Non riuscito)

- Criterio (Aggiungi, Modifica, Rimuovi)
- Dispositivo (Modifica, Rimuovi)
- Minaccia (In quarantena, Ignora, Quarantena globale, Elenco file sicuri)
- Utente (Aggiungi, Modifica, Rimuovi)
- Aggiornamento agente (Modifica)

Il Registro di controllo può essere visualizzato dalla console andando all'elenco a discesa del profilo nella parte in alto a destra della console e selezionando **Registro di controllo**. I registri di controllo sono disponibili solo per gli amministratori.

Impostazioni

Nella pagina Impostazioni vengono visualizzate le schede Applicazione, Gestione utente, Criterio dispositivo, Elenco globale e Aggiornamento agente. L'elemento di menu Impostazioni è disponibile solo per gli amministratori.

APPLICAZIONE

Threat Defense Agent

I dispositivi vengono aggiunti all'organizzazione installando Threat Defense Agent in ciascun endpoint. Una volta connessi alla console, applicare il criterio (per gestire le minacce identificate) e organizzare i dispositivi in base alle necessità dell'organizzazione.

Threat Defense Agent è progettato per usare una quantità minima delle risorse di sistema. L'agente tratta come una priorità i file o i processi che vengono eseguiti poiché questi eventi possono essere dannosi. I file che sono semplicemente su disco (archiviati ma non in esecuzione) assumono una priorità più bassa perché, sebbene possano essere dannosi, non costituiscono una minaccia immediata.

Agente di Windows

Requisiti di sistema

Per l'hardware dell'endpoint (CPU, GPU e così via), Dell consiglia di soddisfare o superare i requisiti consigliati del sistema operativo di destinazione. Di seguito sono descritte delle eccezioni (RAM, spazio su disco disponibile e requisiti software aggiuntivi).

Sistemi operativi	• Windows 7 *(32 bit e 64 bit)* • Windows Embedded Standard 7 *(32 bit)* e Windows Embedded Standard 7 Pro *(64 bit)* • Windows 8 e 8.1 *(32 bit e 64 bit)** • Windows 10 (*32 bit e 64 bit*)** • Windows Server 2008 e 2008 R2 *(32 bit e 64 bit)**** • Windows Server 2012 e 2012 R2 *(64 bit)**** • Windows Server 2016 - Standard, Data Center ed Essentials*****
RAM	• 2 GB
Spazio su disco rigido disponibile	• 300 MB
Software/requisiti aggiuntivi	• .NET Framework 3.5 (SP1) o superiore (solo *Windows*) • Browser Internet • Accesso Internet per accedere, eseguire l'accesso al programma di installazione e registrare il prodotto • Diritti di amministratore locale per installare il software
Altri requisiti	• TLS 1.2 è supportato con l'agente 1422 o versione successiva e richiede l'installazione di .NET Framework 4.5 o versioni successive

Tabella 2: Requisiti di sistema per Windows

*Non supportato: Windows 8.1 RT
**Windows 10 Anniversary Update richiede la versione 1402 o successiva dell'agente.
***Non supportati: Server Core (2008 e 2012) e Minimal Server (2012).
****Richiede la versione 1412 o successiva dell'agente.

Per scaricare il file di installazione

1. Accedere alla console (http://dellthreatdefense.com).
2. Selezionare **Impostazioni** > **Applicazione**.
3. Copiare il **token di installazione**.

   Il token di installazione è una stringa di caratteri generata in maniera casuale che abilita l'agente a creare rapporti per l'account assegnatogli nella console. Il token di installazione è necessario durante l'installazione, nella procedura di installazione guidata oppure come impostazione dei parametri di installazione.
4. Scaricare il programma di installazione.
   a. Selezionare il sistema operativo.
   b. Selezionare il tipo di file da scaricare.

      Per Windows, Dell consiglia di usare il file MSI per l'installazione dell'agente.

Suggerimento: se è impostata una regola di zona, i dispositivi possono essere assegnati automaticamente a una zona se il dispositivo corrisponde ai criteri della regola di zona.

Installare l'agente – Windows

Prima di installare Threat Defense assicurarsi che tutti i prerequisiti siano soddisfatti. Vedere Requisiti di sistema.

1. Fare doppio clic su DellThreatDefenseSetup.exe (o MSI) per avviare l'installazione.
2. Fare clic su **Installa** nella finestra di installazione di Threat Defense.
3. Immettere il token di installazione fornito da Threat Defense Tenant. Fare clic su **Avanti**.

   N.B. Se l'accesso al token di installazione non è disponibile, contattare l'amministratore di Threat Defense o consultare l'articolo della KB How To: Manage Threat Defense.
4. Facoltativamente è possibile modificare la cartella di destinazione di Threat Defense.

   Fare clic su **OK** per avviare l'installazione.
5. Fare clic su **Fine** per completare l'installazione. Selezionare la casella di controllo per avviare Threat Defense.

Parametri di installazione di Windows

L'agente può essere installato in maniera interattiva o non interattiva tramite l'oggetto criterio di gruppo, Microsoft System Center Configuration Manager (meglio noto come SCCM) e MSIEXEC. Gli MSI possono essere personalizzati con parametri integrati (come mostrato di seguito) oppure i parametri possono essere forniti dalla riga di comando.

Proprietà	Valore	Descrizione
PIDKEY	<Token di installazione>	Input automatico del token di installazione
LAUNCHAPP	0 o 1	0: l'icona dell'area di notifica e la cartella del menu Start sono nascoste in fase di esecuzione 1: l'icona dell'area di notifica e la cartella del menu Start non sono nascoste in fase di esecuzione (impostazione predefinita)

Proprietà	Valore	Descrizione
SELFPROTECTIONLEVEL	1 o 2	1: solo gli amministratori locali possono effettuare modifiche al registro e ai servizi 2: solo l'amministratore di sistema può effettuare modifiche al registro e ai servizi (impostazione predefinita)
APPFOLDER	<Cartella di installazione di destinazione>	Specifica la directory di installazione dell'agente Il percorso predefinito è C:\Program Files\Cylance\Desktop
VenueZone	"Zone_Name"	Richiede la versione 1382 o successiva dell'agente •Aggiunge dispositivi a una zona. •Se la zona non esiste, viene creata mediante il nome fornito. •Sostituire zone_name con il nome di una zona esistente o che si desidera creare. **Avvertenza**: l'aggiunta di spazi prima o dopo il nome della zona crea una nuova zona.

Tabella 3: Parametri di installazione per Windows

Il seguente esempio della riga di comando mostra come eseguire il Microsoft Windows Installer Tool (MSIEXEC) passandogli i parametri di installazione PIDKEY, APPFOLDER e LAUNCHAPP:

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

L'installazione è invisibile all'utente e il registro di installazione viene salvato in **`C:\temp`**. Quando l'agente è in esecuzione, sia l'icona dell'area di notifica sia la cartella Threat Defense del menu Start sono nascoste. È possibile trovare ulteriori informazioni relative a opzioni diverse della riga di comando accettate da MSIEXEC in KB 227091.

Installare l'agente di Windows usando Wyse Device Manager (WDM)

Questa sezione spiega come creare uno script di installazione, come creare un pacchetto RSP per WDM e come aggiungere il pacchetto a WDM per l'installazione in più thin client contemporaneamente senza l'interazione dell'utente.

Creare uno script di file batch che eseguirà l'installazione dalla riga di comando di Threat Defense. WDM esegue tale script durante la distribuzione.

1. Aprire il Blocco note. Usando i parametri della riga di comando visti in precedenza, immettere il seguente comando per eseguire l'installazione, sostituendo **`<INSTALLATION TOKEN>`** con il token fornito:
   `msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q`

   `C:\TDx86` viene utilizzato per la nostra directory, in quanto questa cartella viene copiata in questa posizione sul thin client durante l'installazione.

2. Salvare il file con estensione **`.bat`** nella cartella TDx86. Ad esempio, **`TDx86_Install.bat`**.

   Creare un pacchetto RSP mediante il quale l'applicazione Threat Defense può essere installata su più thin client contemporaneamente senza interazione da parte dell'utente.

3. Aprire Scriptbuilder in un computer che abbia WDM installato.
4. Immettere un Nome pacchetto e una Descrizione pacchetto.
    - In Categoria pacchetto selezionare Altri pacchetti.
    - In Sistema operativo selezionare Windows Embedded Standard 7.
5. Aggiungere Comandi di script per verificare che i sistemi di destinazione siano WES7 o WES7p.
    - In Comando di script selezionare Conferma sistema operativo (CO).
    - Per il valore SO del dispositivo, immettere il sistema operativo appropriato.
6. Per aggiungere elementi usare le doppie frecce.
7. Premere **OK** quando viene visualizzato il messaggio.
8. Aggiungere il comando per bloccare il thin client e impedire l'interazione dell'utente.
    - Selezionare **Comando script > Lockout User (LU)**. Non è necessario alcun valore. Tuttavia, in questo esempio viene emesso un **Valore Sì**, in modo che la schermata iniziale verrà rimossa in caso di errore o esito negativo del processo del programma di installazione.
9. Aggiungere un comando per copiare i file nel thin client.
    - Selezionare il comando script **X Copy (XC**).
    - Per il valore **Directory archivio** aggiungere **`*`** alla fine dell'elemento **`<regroot>\`** esistente.
    - Per il valore **Directory dispositivo** immettere il percorso in cui copiare i file sui thin client di destinazione. In questo esempio viene usato il Nome pacchetto.
10. Aggiungere un comando per eseguire lo script di installazione .bat.
    - Selezionare **Comando script > Execute on Device (EX)**.
    - Per il valore Nome file del dispositivo, immettere il percorso **`C:\TDx86\TDx86_install.bat`**. La cartella TDx86 viene copiata dal precedente comando XC.
    - Aggiungere **`+`** come valore di esecuzione sincrona. In questo modo si comunica a WDM di attendere fino al completamento del file in esecuzione per continuare.
11. Aggiungere un comando per eliminare i file copiati dal thin client.
    12. Aggiungere il comando di script Delete **Tree (DT)**.
12. Aggiungere comandi per disabilitare il blocco.
    13. Aggiungere il comando di script **End Lockout (EL**).
13. Per ricapitolare, il pacchetto di script dovrebbe essere simile a quello mostrato di seguito.
    a. Se si distribuisce Threat Defense in sistemi WES7P, aggiornare la sezione del sistema operativo in WES7P, altrimenti l'installazione del pacchetto non riesce.

14. Salvare il pacchetto.
    14. Fare clic su **Salva** e individuare la posizione della cartella **TDx86**. Se queste istruzioni sono state seguite, la cartella è sul desktop.
15. Chiudere Scriptbuilder.
16. Avviare **WyseDeviceManager** per aggiungere il pacchetto a WDM.
17. Passare a **WyseDeviceManager > Gestore pacchetti > Altri pacchetti**.
18. Selezionare **Azioni > Nuovo > Pacchetto** dalla barra dei menu.
19. Selezionare **Registra un pacchetto da un file di script (.RSP)** e fare clic su **Avanti**.
20. Individuare il percorso del file RSP creato al punto precedente e fare clic su **Avanti**.
21. Accertarsi che l'opzione **Attivo** sia selezionata, quindi fare clic su **Avanti.**
22. Fare clic su **Avanti** dopo aver predisposto WDM per registrare il pacchetto.
23. Fare clic su **Fine** quando il pacchetto sarà stato registrato.
24. Il pacchetto sarà visibile in **Altri pacchetti**.
25. Verificare il contenuto del pacchetto:
    a. Aprire Esplora risorse, accedere a **C:\inetpub\ftproot\Rapport** e individuare la cartella **TDx86**.
    b. Aprire la cartella TDx86 e verificare che comprenda il programma di installazione e il file .bat.

Ora in WDM è disponibile un pacchetto che è in grado di distribuire Threat Defense in più thin client WES7 senza l'interazione dell'utente.

Messa in quarantena tramite la riga di comando

È possibile mettere in quarantena un file utilizzando la riga di comando di un dispositivo. Ciò richiede la conoscenza dell'hash SHA256 per la minaccia.

Nota: Questa funzione è solo per Windows e richiede l'agente 1432 o versione successiva.

1. Sul dispositivo Windows, aprire la riga di comando. Esempio: Dal menu Start, cercare cmd.exe.
2. Richiamare Dell.ThreatDefense.exe e includere l'argomento **-q: <hash>**, dove <hash> è l'hash SHA256 per il file. Questo comando richiederà all'agente di inviare il file nella cartella di quarantena.

   Esempio della riga di comando (Dell Threat Defense installato nella posizione predefinita):

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

Agente di Mac OS X

Requisiti di sistema

Per l'hardware dell'endpoint (CPU, GPU e così via), Dell consiglia di soddisfare o superare i requisiti consigliati del sistema operativo di destinazione. Di seguito sono descritte delle eccezioni (RAM, spazio su disco disponibile e requisiti software aggiuntivi).

Sistemi operativi	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12*
RAM	• 2 GB
Spazio su disco rigido disponibile	• 300 MB

Tabella 4: Requisiti di sistema per Mac OS X

*Richiede la versione 1412 o successiva dell'agente.

Per scaricare il file di installazione

1. Accedere alla console (http://dellthreatdefense.com).
2. Selezionare **Impostazioni** > **Applicazione**.
3. Copiare il **token di installazione**.

   Il token di installazione è una stringa di caratteri generata in maniera casuale che abilita l'agente a creare rapporti per l'account assegnatogli nella console. Il token di installazione è necessario durante l'installazione, nella procedura di installazione guidata oppure come impostazione dei parametri di installazione.
4. Scaricare il programma di installazione.
   a. Selezionare il sistema operativo.
   b. Selezionare il tipo di file da scaricare.

Suggerimento: se è impostata una regola di zona, i dispositivi possono essere assegnati automaticamente a una zona se il dispositivo corrisponde ai criteri della regola di zona.

Installare l'agente – Mac OS X

Prima di installare Threat Defense assicurarsi che tutti i prerequisiti siano soddisfatti. Vedere Requisiti di sistema.

N.B. L'agente di Mac OS X sarà prodotto da Dell in una versione futura.

1. Fare doppio clic su **`DellThreatDefense.dmg`** per montare il programma di installazione.
2. Fare doppio clic sull'icona *Protect* dall'interfaccia utente di PROTECT per avviare l'installazione.
3. Fare clic su **Continua** per verificare che il sistema operativo e l'hardware soddisfino i requisiti.
4. Fare clic su **Continua** nella schermata Introduzione.
5. Immettere il token di installazione fornito da Threat Defense Tenant. Fare clic su **Continua**.

N.B. Se l'accesso al token di installazione non è disponibile, contattare l'amministratore di Threat Defense o consultare l'articolo della KB How To: Manage Threat Defense.

6. Facoltativamente è possibile modificare il percorso di installazione di Threat Defense.

   Fare clic su **Installa** per avviare l'installazione.

7. Immettere nome utente e password di un amministratore. Fare clic su **Installa software**.

8. Fare clic su **Chiudi** nella schermata di riepilogo.

Parametri di installazione per Mac OSX

È possibile installare Threat Defense Agent usando le opzioni della riga di comando in Terminale. Gli esempi riportati di seguito usano il programma di installazione PKG. Per DMG è sufficiente modificare l'estensione del file nel comando.

Nota: assicurarsi che gli endpoint di destinazione soddisfino i requisiti di sistema e che la persona che installa il software abbia le credenziali appropriate per l'installazione del software.

Proprietà	Valore	Descrizione
InstallToken		Token di installazione disponibile nella console
NoCylanceUI		L'icona dell'agente non deve essere visualizzata all'avvio. L'impostazione predefinita è Visibile.
SelfProtectionLevel	0 o 1	1: solo gli amministratori locali possono effettuare modifiche al registro e ai servizi. 2: solo l'amministratore di sistema può effettuare modifiche al registro e ai servizi (impostazione predefinita).
LogLevel	0, 1, 2 o 3	0: errore – vengono registrati solo i messaggi di errore. 1: avviso – vengono registrati i messaggi di avviso e di errore. 2: informazioni (predefinito) – vengono registrati i messaggi di errore, avviso e informazione. Questo può fornire dettagli durante la risoluzione dei problemi. 3: dettagliato – vengono registrati tutti i messaggi. Questo è il livello di registro consigliato durante la risoluzione dei problemi. Tuttavia, le dimensioni dei file di registro dettagliati possono diventare molto consistenti. Dell consiglia di attivare il livello Dettagliato durante la risoluzione dei problemi e di tornare al livello Informazioni al termine del processo.
VenueZone	"zone_name"	Richiede la versione 1382 o successiva dell'agente •Aggiunge dispositivi a una zona. •Se la zona non esiste, viene creata mediante il nome fornito. •Sostituire zone_name con il nome di una zona esistente o che si desidera creare.

Proprietà	Valore	Descrizione
		Avvertenza: l'aggiunta di spazi prima o dopo il nome della zona crea una nuova zona.

Tabella 5: Parametri di installazione per Mac OS X

Installare l'agente

Installare senza il token di installazione

```
sudo installer –pkg DellThreatDefense.pkg –target/
```

Installare con il token di installazione

```
echo [install_token] > cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Nota: sostituire **`[install_token]`** con il token di installazione. Il comando echo genera un file **`cyagent_install_token`**, un file di testo con un'opzione di installazione per riga. Questo file deve essere nella stessa cartella del pacchetto di installazione. Prestare attenzione alle estensioni file. L'esempio precedente mostra che il file di installazione cyagent_install_token non ha alcuna estensione. Le impostazioni predefinite in Mac OSX e macOS hanno le estensioni nascoste. La creazione manuale di questo file con Text Edit o un altro editor di testo può aggiungere automaticamente un'estensione file che dovrà essere rimossa.

Parametri di installazione facoltativi

Immettere quanto segue nel Terminale per creare un file (**cyagent_install_token**) che il programma di installazione utilizza per applicare le opzioni immesse. Ciascun parametro deve trovarsi su una riga a sé stante. Questo file deve essere nella stessa cartella del pacchetto di installazione.

Quello che segue è un esempio, nel file non sono necessari tutti i parametri. Il Terminale include tutto ciò che è racchiuso all'interno di virgolette singole nel file. Assicurarsi di premere Invio/A capo dopo ciascun parametro per mantenerli ognuno su una riga a sé stante nel file.

È anche possibile usare un editor di testo per creare il file che include ciascun parametro (su una riga a sé stante). Questo file deve essere nella stessa cartella del pacchetto di installazione.

Esempio:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Disinstallare l'agente

Senza password

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense
```

Con password

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense --
password=thisismypassword
```

Nota: sostituire **`thisismypassword`** con la password di disinstallazione creata nella console.

Servizio agente

Avviare il servizio

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

Interrompere il servizio

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

Verifica dell'installazione

Controllare i seguenti file per verificare che l'installazione dell'agente sia stata completata.

1. La cartella del programma è stata creata.
    - Predefinito di Windows: **`C:\Program Files\Cylance\Desktop`**
    - Predefinito di Mac OS X: **`/Applications/DellThreatDefense/`**
2. L'icona di Threat Defense è visibile nell'area di notifica del dispositivo di destinazione.

    Questo non si applica se viene usato il parametro LAUNCHAPP=0 (Windows) o NoCylanceUI (Mac OS X).
3. C'è una cartella Threat Defense nel menu Start/Tutti i programmi nel dispositivo di destinazione.

    Questo non si applica se viene usato il parametro LAUNCHAPP=0 (Windows) o NoCylanceUI (Mac OS X).
4. Il servizio Threat Defense è stato aggiunto ed è in esecuzione. Nel pannello Servizi di Windows del dispositivo di destinazione dovrebbe esserci un servizio di Threat Defense elencato come in esecuzione.
5. Il processo Dell.ThreatDefense.exe è in esecuzione. Nella scheda Processi di Gestione attività di Windows del dispositivo di destinazione dovrebbe essere elencato un processo Dell.ThreatDefense.exe.
6. Il dispositivo risponde alla console. Accedere alla console e fare clic sulla scheda Dispositivi, dovrebbe apparire il dispositivo di destinazione elencato come online.

Interfaccia utente dell'agente

L'interfaccia utente dell'agente è abilitata per impostazione predefinita. Fare clic sull'icona dell'agente nell'area di notifica per visualizzarla. In alternativa, è possibile installare l'agente in modo che nasconda l'icona dell'agente dall'area di notifica.

Scheda Minacce

Visualizza tutte le minacce individuate nel dispositivo e l'azione intrapresa. *Non sicuro* significa che non è stata eseguita alcuna azione sulla minaccia. *In quarantena* significa che la minaccia è stata modificata (per impedire l'esecuzione del file) ed è stata spostata nella cartella *Quarantena*. *Ignorato* significa che il file è considerato sicuro dall'amministratore e *Consentito* per l'esecuzione nel dispositivo.

Scheda Eventi

Visualizza qualsiasi evento di minaccia verificatosi nel dispositivo.

Scheda Script

Visualizza qualsiasi script dannoso che è stato eseguito nel dispositivo e le eventuali azioni intraprese nei confronti dello script.

Menu dell'agente

Il menu dell'agente fornisce accesso alla guida e agli aggiornamenti per Threat Defense. Fornisce anche accesso all'interfaccia utente avanzata che offre ulteriori opzioni di menu.

Menu dell'agente

Il menu dell'agente consente agli utenti di eseguire alcune azioni nel dispositivo. Fare clic con il pulsante destro del mouse sull'icona dell'agente per visualizzare il menu.

- **Controlla aggiornamenti**: l'agente verifica l'esistenza e installa eventuali aggiornamenti disponibili. Gli aggiornamenti sono limitati a quelli per la versione dell'agente consentita per la zona cui appartiene il dispositivo.
- **Verificare la disponibilità di aggiornamenti ai criteri**: l'agente verifica l'esistenza di aggiornamento ai criteri. Questo potrebbe consistere in modifiche ai criteri esistenti o in una diversa policy da applicare all'agente.

  Nota: Verificare la presenza di aggiornamenti ai criteri è supportato nella versione 1422 (o versione successiva) per Windows e nella versione 1432 (o versione successiva) per MacOS.
- **Informazioni su**: viene visualizzata una finestra di dialogo con la versione dell'agente, il nome del criterio assegnato al dispositivo, l'ultima volta in cui l'agente ha verificato la disponibilità di un aggiornamento e il token di installazione usato durante l'installazione.
- **Esci**: chiude l'icona dell'agente nell'area di notifica. Questo non disattiva nessuno dei servizi di Threat Defense.
- **Opzioni > Mostra notifiche**: selezionare questa opzione per visualizzare i nuovi eventi sotto forma di notifiche.

Abilitare le opzioni avanzate dell'interfaccia utente dell'agente

Threat Defense Agent fornisce alcune opzioni avanzate tramite l'interfaccia utente per offrire delle funzionalità nei dispositivi che non dispongono di connettività alla console. È necessario che il CylanceSVC.exe sia in esecuzione quando vengono abilitate le opzioni avanzate.

Windows

1. Se l'icona dell'agente è visibile nella barra delle applicazioni, fare clic con il pulsante destro del mouse sull'icona e scegliere **Esci**.
2. Avviare il prompt dei comandi e immettere il seguente comando. Al termine premere Invio.

   ```
   cd C:\Program Files\Cylance\desktop
   ```

   Se l'applicazione è stata installata in un percorso diverso, passare a quel percorso nel prompt dei comandi.
3. Immettere il seguente comando e al termine premere Invio.

   ```
   Dell.ThreatDefense.exe –a
   ```

   Viene visualizzata l'icona dell'agente nell'area di notifica.
4. Fare clic con il pulsante destro del mouse sull'icona. Vengono visualizzate le opzioni *Registrazione*, *Eseguire un rilevamento* e *Gestione minacce*.

Mac OSX/macOS

1. Se l'icona dell'agente è visibile nel menu superiore, fare clic con il pulsante destro del mouse sull'icona e scegliere **Esci**.
2. Aprire il Terminale ed eseguire
    a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

    Nota: questo è il percorso di installazione predefinito per Dell Threat Defense. Potrebbe essere necessario modificare il percorso in base all'ambiente in uso.
3. L'interfaccia utente dell'agente verrà ora visualizzata con opzioni aggiuntive.

Registrazione

Selezionare il livello di informazioni di registro da raccogliere dall'agente. L'impostazione predefinita è Informazioni. Dell consiglia di impostare il livello di registro su Tutto (Dettagliato) quando si esegue la risoluzione dei problemi. Quando la risoluzione dei problemi è stata completata, modificare nuovamente il livello su Informazioni (la registrazione di tutte le informazioni può generare file di registro molto grandi).

Esegui rilevamento

Consente agli utenti di specificare una cartella da analizzare per le minacce.

1. Selezionare **Esegui un rilevamento > Specifica cartella**.
2. Selezionare una cartella da analizzare e fare clic su **OK**. Eventuali minacce individuate vengono visualizzate nell'interfaccia utente dell'agente.

Gestione minacce

Consente agli utenti di eliminare i file *in quarantena* sul dispositivo.

1. Selezionare **Gestione minacce > Elimina messi in quarantena**.
2. Fare clic su **OK** per confermare.

Macchine virtuali

Ci sono alcuni suggerimenti da tenere presente quando si usa Threat Defense Agent in un'immagine di macchina virtuale.

Quando si crea un'immagine di macchina virtuale da usare come modello, disconnettere le impostazioni di rete della macchina virtuale prima di installare l'agente. Questo impedisce all'agente di comunicare con la console e di configurare i dettagli del dispositivo. In questo modo non si hanno dispositivi duplicati nella console.

Disinstallazione protetta da password

IMPOSTAZIONI > Applicazione

Per la disinstallazione dell'agente gli amministratori possono richiedere una password. Quando si disinstalla l'agente con una password:

- Se per l'installazione è stato usato il programma di installazione MSI, eseguire la disinstallazione usando l'MSI o tramite il Pannello di controllo.

- Se per l'installazione è stato usato l'EXE, usarlo anche per la disinstallazione. La disinstallazione tramite il Pannello di controllo non funziona se è stato usato il programma di installazione EXE ed è richiesta una password per la disinstallazione.
- Se si esegue la disinstallazione tramite la riga di comando, aggiungere la stringa di disinstallazione: **`UNINSTALLKEY = [MyUninstallPassword]`**.

Per creare una password di disinstallazione

1. Accedere alla console (http://dellthreatdefense.com) con un account amministratore.
2. Selezionare **Impostazioni** > **Applicazione**.
3. Selezionare la casella di controllo **Richiedi password per disinstallare agente**.
4. Immettere una password.
5. Fare clic su **Salva**.

Integrazioni

Threat Defense Console fornisce l'integrazione con alcuni programmi di terzi.

Syslog/SIEM

Threat Defense può integrarsi con il software Security Information Event Management (SIEM, Gestione delle informazioni e degli eventi di sicurezza) usando la funzionalità Syslog. Gli eventi Syslog sono registrati nello stesso momento in cui gli eventi dell'agente sono registrati nella console.

Per gli indirizzi IP più recenti per i messaggi Syslog, contattare il supporto Dell.

Tipi di evento

Registro di controllo

Selezionare questa opzione per inviare il registro di controllo delle azioni dell'utente eseguite nella console (sito Web) al server Syslog. Gli eventi del registro di controllo vengono sempre visualizzati nella schermata Registro di controllo, anche quando l'opzione non è selezionata.

Messaggio di esempio per il registro di controllo inoltrato a Syslog

Dispositivi

Selezionare questa opzione per inviare gli eventi del dispositivo al server Syslog.

- Quando viene registrato un nuovo dispositivo, si ricevono due messaggi per l'evento: Registrazione e SystemSecurity.

  Messaggio di esempio per l'evento registrazione del dispositivo

- Quando un dispositivo viene rimosso.

  Messaggio di esempio per l'evento rimozione del dispositivo

- Quando il criterio, la zona, il nome o il livello di registrazione di un dispositivo è stato modificato.

  Messaggio di esempio per l'evento aggiornamento del dispositivo

Minacce

Selezionare questa opzione per registrare eventuali minacce individuate di recente o modifiche osservate per le minacce esistenti, nel server Syslog. Le modifiche includono una minaccia *rimossa*, *in quarantena*, *ignorata* o *eseguita*.

Esistono cinque tipi di eventi di minaccia:

- **threat_found**: è stata individuata una nuova minaccia in uno stato *Non sicuro*.
- **threat_removed**: è stata *rimossa* una minaccia esistente.
- **threat_quarantined**: è stata individuata una nuova minaccia in uno stato di *quarantena*.
- **threat_waived**: è stata individuata una nuova minaccia nello stato *Ignorato*.
- **threat_changed**: il comportamento di una minaccia esistente è cambiato (esempi: punteggio, stato di quarantena, stato in esecuzione).
- **threat_cleared**: una minaccia è stata ignorata, aggiunta all'Elenco file sicuri o eliminata dalla quarantena su un dispositivo.

Messaggio di esempio di un evento di minaccia

Classificazione delle minacce

Ogni giorno centinaia di minacce vengono classificate come malware o Programmi potenzialmente indesiderati (PUP, Potentially Unwanted Programs). Se seleziona questa opzione, l'utente acconsente a ricevere una notifica quando si verificano questi eventi.

Messaggio di esempio di una classificazione di minaccia

SIEM (Security Information and Event Management, Gestione delle informazioni e degli eventi di sicurezza)
Specifica il tipo di server Syslog o SIEM cui devono essere inviati gli eventi.

Protocollo
Questo deve corrispondere a ciò che è configurato nel proprio server Syslog. Le opzioni sono UDP o TCP. Solitamente UDP è sconsigliato poiché non garantisce la consegna dei messaggi. Dell consiglia TCP (impostazione predefinita).

TLS/SSL
Disponibile solo se il protocollo specificato è TCP. TLS/SSL assicura che il messaggio di Syslog venga crittografato nel passaggio da Threat Defense al server Syslog. Dell incoraggia i clienti a selezionare questa opzione. Assicurarsi che il server Syslog sia configurato per rimanere in ascolto dei messaggi TLS/SSL.

IP/Dominio
Specifica l'indirizzo IP o il nome di dominio completo del server Syslog che ha impostato il cliente. Consultare gli esperti di rete interni per assicurarsi che le impostazioni per firewall e dominio siano configurate correttamente.

Porta
Specifica il numero di porta nei dispositivi per i quali il server Syslog rimane in ascolto in attesa di messaggi. Deve essere un numero tra 1 e 65535. I valori tipici sono: 512 per UDP, 1235 o 1468 per TCP e 6514 per TCP protetta (esempio: TCP con TLS/SSL abilitato).

Gravità
Specifica la gravità dei messaggi che devono essere visualizzati nel server Syslog. Si tratta di un campo soggettivo e può essere impostato sul livello preferito. Il valore della gravità non modifica i messaggi che vengono inoltrati a Syslog.

Struttura
Specifica il tipo di applicazione che registra il messaggio. Quella predefinita è Interna (o Syslog). Viene usata per categorizzare i messaggi quando vengono ricevuti dal server Syslog.

Esecuzione di test sulla connessione
Fare clic su **Connessione di test** per eseguire il test dell'IP/dominio, della porta e delle impostazioni del protocollo. Se vengono immessi valori validi, dopo poco viene visualizzato un messaggio che conferma che l'operazione è andata a *buon fine*.

Autenticazione personalizzata

Usare Provider di identità (IdP, Identity Providers) esterni per accedere alla console. Per questo è necessario configurare le impostazioni con il proprio IdP per ottenere un certificato X.509 e un URL per verificare l'accesso IdP. L'Autenticazione personalizzata gestisce Microsoft SAML 2.0. È stato appurato che questa funzionalità gestisce OneLogin, OKTA, Microsoft Azure e PingOne. Questa funzionalità offre anche un'impostazione Personalizzata e dovrebbe gestire altri provider di identità che seguono Microsoft SAML 2.0.

Nota: Autenticazione personalizzata non supporta Active Directory Federation Services (ADFS).

- **Autenticazione avanzata**: fornisce l'accesso con autenticazione a più fattori.
- **Single Sign-On**: fornisce l'accesso con single Sign-On (SSO).

  Nota: selezionare Autenticazione avanzata o Single Sign-On non influenza le impostazioni di Autenticazione personalizzata perché tutte le impostazioni di configurazione sono gestite dal provider di identità (IdP).
- **Consenti accesso password**: selezionare questa opzione per consentire l'accesso diretto alla console usando SSO. Questo consente i test delle impostazioni SSO senza perdere l'accesso alla console. Una volta eseguito l'accesso alla console tramite SSO, Dell consiglia di disabilitare questa funzionalità.
- **Provider:** selezionare il provider di servizi per l'autenticazione personalizzata.
- **Certificato X.509**: immettere le informazioni del certificato X.509.
- **URL di accesso**: immettere l'URL per l'autenticazione personalizzata.

Rapporto dati minacce

Un foglio di calcolo che contiene le seguenti informazioni sull'organizzazione:

- **Minacce**: elenca tutte le minacce individuate nell'organizzazione. Queste informazioni comprendono il nome e lo stato del file (*Non sicuro*, *Anomalo*, *Ignorato* e *In quarantena*).
- **Dispositivi**: elenca tutti i dispositivi nell'organizzazione sui quali è installato Threat Defense Agent. Queste informazioni comprendono il nome del dispositivo, la versione del sistema operativo, la versione dell'agente e il criterio applicato.
- **Indicatori di minaccia**: elenca ciascuna minaccia e le caratteristiche di minaccia associate.
- **Cancellato**: elenca tutti i file che sono stati *cancellati* nell'organizzazione. Queste informazioni comprendono i file che sono stati *ignorati*, aggiunti all'*Elenco file sicuri* o *eliminati* dalla cartella di *quarantena* su un dispositivo.
- **Eventi**: elenca tutti gli eventi relativi al grafico degli eventi di minaccia nella dashboard, per gli ultimi 30 giorni. Queste informazioni comprendono l'hash del file, il nome del dispositivo, il percorso del file e la data in cui si è verificato l'evento.

Quando questa funzionalità viene abilitata, il rapporto viene aggiornato automaticamente all'1:00 fuso orario del Pacifico (PST, Pacific Standard Time). Fare clic su **Rigenera rapporto** per generare manualmente un aggiornamento.

Il Rapporto dati minacce fornisce un URL e un token che possono essere usati per scaricare il rapporto senza necessità di accedere alla console. Secondo necessità, è anche possibile eliminare o rigenerare un token, che offre il controllo su chi ha accesso al rapporto.

RISOLUZIONE DEI PROBLEMI

Questa sezione fornisce un elenco di domande cui rispondere e file da raccogliere quando si esegue la risoluzione dei problemi con Threat Defense. Queste informazioni consentono al supporto Dell di assistere nella risoluzione dei problemi.

Inoltre, questa sezione contiene alcuni problemi comuni e le soluzioni suggerite.

Supporto

Parametri di installazione

- Qual è il metodo di installazione? Fornire i parametri usati.
    - Esempio – Windows: usare LAUNCHAPP=0 quando si installa dalla riga di comando per nascondere l'icona dell'agente e la cartella del menu Start in fase di esecuzione.
    - Esempio – Mac OS X: usare SelfProtectionLevel=1 quando si installa dalla riga di comando per disabilitare Protezione automatica nell'agente.
- Quali fasi dell'installazione è stato possibile verificare?
    - Esempio – Windows: è stato usato il programma di installazione MSI o EXE?
    - Esempio – Qualsiasi SO: sono state usate opzioni della riga di comando? Come la modalità non interattiva o nessuna interfaccia utente dell'agente.
- Abilitare la registrazione dettagliata per l'installazione.

Problemi relativi alle prestazioni

- Acquisire una schermata di Task Manager (Windows) o Activity Monitor (Mac OS X) che mostri i processi di Threat Defense e il consumo di memoria.
- Acquisire un backup dei processi di Threat Defense.
- Raccogliere i registri di debug.
- Raccogliere i risultati delle informazioni di sistema durante il problema.
    - Per Windows: msinfo32 o winmsd
    - Per Mac OS X: informazioni di sistema
- Raccogliere qualsiasi Registro eventi (Windows) o Informazione della console (Mac OS X) rilevante.

Problemi di aggiornamento, stato e connettività

- Assicurarsi che la porta 443 sia aperta nel firewall e che il dispositivo possa risolvere e connettersi ai siti Cylance.com.
- Il dispositivo è elencato nella pagina Dispositivi della console? È online oppure offline? Qual è la data/ora dell'ultima connessione?
- Il dispositivo usa un proxy per connettersi a Internet? Le credenziali sono configurate correttamente nel proxy?
- Riavviare il servizio di Threat Defense in modo che tenti di connettersi alla console.
- Raccogliere i registri di debug.
- Raccogliere i risultati delle informazioni di sistema durante il problema.
    - Per Windows: msinfo32 o winmsd
    - Per Mac OS X: informazioni di sistema

Abilitazione della registrazione debug

Per impostazione predefinita, Threat Defense memorizza i file di registro in **`C:\Program Files\Cylance\Desktop\log`**. Per la risoluzione dei problemi, è possibile configurare Threat Defense per produrre registri più dettagliati.

Incompatibilità di Controllo script

Problema:

Quando Controllo script è abilitato in alcuni dispositivi, può provocare conflitti con altri software in esecuzione in quei dispositivi. I conflitti sono generalmente dovuti all'agente che si inserisce in determinati processi che vengono richiamati da altri software.

Soluzione:

A seconda del software, questo problema può essere risolto aggiungendo esclusioni di processi specifici al criterio del dispositivo nella console. Un'altra opzione è di abilitare la modalità di compatibilità (chiave di registro) in ciascun dispositivo interessato. Tuttavia, se le esclusioni non sono efficaci, per ripristinare la normale funzionalità del dispositivo, Dell consiglia di disabilitare Controllo script nel criterio del dispositivo che interessa i dispositivi.

Nota: questa soluzione in modalità di compatibilità è disponibile per la versione 1370 dell'agente. A partire dalla versione 1382 dell'agente, il processo di aggiunta è stato aggiornato per la compatibilità con altri prodotti.

Modalità di compatibilità

Per abilitare la modalità di compatibilità aggiungere la chiave di registro riportata di seguito:

1. Usando l'editor del Registro di sistema, accedere a **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Fare clic con il pulsante destro del mouse su **Desktop**, scegliere **Autorizzazioni**, quindi assumere la proprietà e assicurarsi il **pieno controllo**. Fare clic su **OK**.
3. Fare clic con il pulsante destro del mouse su **Desktop**, quindi selezionare **Nuovo** > **Valore binario**.
4. Denominare il file **CompatibilityMode**.
5. Aprire le impostazioni di registro e modificare il valore in **01**.
6. Fare clic su **OK**, quindi chiudere l'editor del Registro di sistema.
7. Potrebbe essere necessario un riavvio del dispositivo.

Opzioni riga di comando

Usando Psexec:

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

Per eseguire un comando in più dispositivi, usare **`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}
```

APPENDICE A: GLOSSARIO

Anomalo	Un file sospetto con un punteggio più basso (da 1 a 59) con probabilità più basse di essere un malware
Amministratore	Gestore tenant per Threat Defense
Agente	Host dell'endpoint di Threat Defense che comunica con la console
Registro di controllo	Registro che registra le azioni eseguite da Threat Defense Console
Quarantena automatica	Impedisce automaticamente l'esecuzione di tutti i file *non sicuri* e/o *anomali*
Caricamento automatico	Carica automaticamente qualsiasi file Portable Executable (PE) sconosciuto, rilevato come *non sicuro* o *anomalo*, in Cylance Infinity Cloud per l'analisi
Console	Interfaccia utente per la gestione di Threat Defense
Criterio del dispositivo	Criterio di Threat Defense che può essere configurato dall'amministratore dell'organizzazione che definisce la modalità di gestione delle minacce in tutti i dispositivi
Quarantena globale	Impedisce l'esecuzione di un file a livello globale (in tutti i dispositivi di un'organizzazione)
Elenco File globalmente sicuri	Consente l'esecuzione di un file a livello globale (in tutti i dispositivi di un'organizzazione)
Infinity	Il modello matematico usato per assegnare punteggi ai file
Organizzazione	L'account di un tenant che usa il servizio di Threat Defense
Quarantena	Impedisce l'esecuzione di un file a livello locale (in un dispositivo specifico)
Minacce	File potenzialmente dannosi rilevati da Threat Defense, classificati come *non sicuri* o *anomali*
Non sicuro	Un file sospetto con un punteggio alto (da 60 a 100) con elevate probabilità di essere un malware
Ignora	Consente l'esecuzione di un file a livello locale (in un dispositivo specifico)
Zona	Un modo per organizzare e raggruppare dispositivi all'interno di un'organizzazione in base a priorità, funzionalità e così via
Regola di zona	Funzionalità che abilita l'assegnazione automatica dei dispositivi a zone specifiche in base a indirizzo IP, sistema operativo e nomi dei dispositivi

APPENDICE B: GESTIONE DELLE ECCEZIONI

In alcuni casi, gli utenti devono mettere manualmente in *quarantena* o *consentire* (*ignorare*) un file. Threat Defense fornisce metodi per gestire le eccezioni per ciascun dispositivo (*Locale*), per un gruppo di dispositivi (*Criterio*) o per l'intera organizzazione (*Globale*).

File

Locale: mette in *quarantena* o *ignora* (*Elenco file sicuri*) un file sul dispositivo. Utile per *bloccare* o *consentire* un file finché non sarà possibile analizzarlo. Anche *ignorare* un file su un dispositivo risulta utile se tale dispositivo è l'unico in cui il file potrà essere *eseguito*. Dell consiglia di utilizzare *Criterio* o *Globale* se questa azione deve essere eseguita su più dispositivi.

Criterio: inserisce un file nell'*Elenco file sicuri* su tutti i dispositivi assegnati a un criterio. Utile per consentire un file per un gruppo di dispositivi (ad esempio, consentire a dispositivi IT di eseguire strumenti che potrebbero essere usati a scopi dannosi, come PsExec). Non è possibile mettere in *quarantena* un file a livello di Criterio.

Globale: mette in *quarantena* o inserisce nell'*Elenco file sicuri* un file per l'organizzazione. Mette in *quarantena* un file dannoso noto nell'organizzazione. Inserisce nell'*Elenco file sicuri* un file ritenuto sicuro e utilizzato nell'organizzazione, ma contrassegnato dall'agente come dannoso.

Script

Criterio: Controllo script consente l'approvazione di script da eseguire da una cartella designata. Consentire agli script di essere eseguiti per una cartella consente anche gli script nelle sottocartelle.

Certificati

Globale: aggiunge certificati alla console, quindi li aggiunge all'*Elenco file sicuri*. Questo consente l'esecuzione nell'organizzazione delle applicazioni firmate da questo certificato.

Per aggiungere un certificato, selezionare **Impostazioni > Certificati**, quindi fare clic su **Aggiungi certificato**.

Per aggiungere il certificato all'*Elenco file sicuri*, selezionare **Impostazioni > Elenco globale**, selezionare la scheda **Sicuro**, selezionare la scheda **Certificati**, quindi fare clic su **Aggiungi certificato**.

APPENDICE C: AUTORIZZAZIONI UTENTE

Le azioni che un utente può eseguire dipendono dalle autorizzazioni utente (ruolo) che gli sono state assegnate. In generale, gli amministratori possono eseguire azioni in qualunque punto dell'organizzazione. Il campo di azione di manager di zona e utenti è limitato alle zone alle quali sono assegnati. Questa limitazione comprende solo la capacità di accedere ai dispositivi all'interno di una zona e la sola visualizzazione dei dati sulle minacce relativi a quei dispositivi. Se un manager di zona o un utente non riesce a visualizzare un dispositivo o una minaccia, è probabile che il dispositivo non appartenga a nessuna delle zone assegnategli.

	UTENTE	MANAGER DI ZONA	AMMINISTRATORE
Aggiornamento dell'agente			
Visualizzazione/Modifica			x
Registrazione di controllo			
Visualizzazione			x
Dispositivi			
Aggiunta dispositivi – Globale			x
Aggiunta dispositivi a una zona			x
Rimozione dispositivi – Globale			x
Rimozione dispositivi da una zona		x	x
Modifica nome del dispositivo		x	x
Zone			
Creazione zona			x
Eliminazione zona			x
Modifica nome zona – Qualunque			x
Modifica nome zona assegnata		x	x
Criterio			
Creazione criterio – Globale			x
Creazione criterio per una zona			x
Aggiunta criterio – Globale			x
Aggiunta criterio a una zona		x	x
Rimozione criterio – Globale			x
Rimozione criterio da una zona		x	x
Minacce			
Mettere in quarantena file – Globale			x
Mettere in quarantena file in una zona	x	x	x
Ignorare file – Globale			x
Ignorare file in una zona	x	x	x
Quarantena globale/Sicuri			x
Impostazioni			
Generazione o eliminazione token di installazione			x
Generazione o eliminazione URL di invito			x
Copia del token di installazione	x	x	x
Copia dell'URL di invito			x
Gestione utenti			
Assegnazione utenti a qualsiasi zona			x
Assegnazione utenti a zona gestita		x	x
Assegnazione manager di zona – Globale			x

Assegnazione manager di zona a zone gestite	X	X
Eliminazione utenti dalla console		X
Rimozione utenti dalla zona – Globale		X
Rimozione utenti dalla zona gestita	X	X

APPENDICE D: FILTRO DI SCRITTURA BASATO SU FILE

Dell Threat Defense Agent può essere installato su un sistema su cui è in esecuzione Windows Embedded Standard 7 (Thin Client). Sui dispositivi integrati, la scrittura nell'archiviazione del sistema potrebbe non essere consentita. In questo caso, il sistema può utilizzare un filtro di scrittura basato su file per reindirizzare le scritture nell'archiviazione del sistema alla cache nella memoria del sistema. In questo modo, l'agente potrebbe perdere le modifiche a ogni riavvio del sistema.

Quando si utilizza l'agente in un sistema incorporato, utilizzare la procedura descritta di seguito:

1. Prima di installare l'agente, disabilitare il filtro di scrittura basato su file utilizzando il comando: `fbwfmgr /disable`.
2. Riavviare il sistema. In questo modo avrà effetto la disattivazione del filtro.
3. Installare Dell Threat Defense Agent.
4. Dopo aver installato l'agente, riattivare il filtro di scrittura basato su file utilizzando il comando: `fbwfmgr /enable`.
5. Riavviare il sistema. In questo modo avrà effetto l'attivazione del filtro.
6. Nel filtro di scrittura basato su file escludere le seguenti cartelle:
    a. C:\Program Files\Cylance\Desktop - L'esclusione di questa cartella consente di mantenere gli aggiornamenti dell'agente in seguito al riavvio del sistema.
7. Utilizzare il seguente comando per escludere la cartella Desktop: `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. Si presuppone che l'installazione venga eseguita nella directory predefinita. Modificare l'esclusione per la cartella in cui è stato installato l'agente.
8. Se si decide di archiviare le minacce nel computer per eseguire test rispetto all'agente, assicurarsi di escludere anche la posizione di archiviazione dal filtro di scrittura basato su file (ad esempio, `C:\Samples`).

APPENDICE E: ARTICOLI DI BASE DI CONOSCENZA

Per ulteriori informazioni, fare riferimento a questi articoli della Knowledge Base:

Rilasciare note dalla versione:

http://www.dell.com/support/article/it/it/19/SLN305419/?lang=IT

Conoscenza generale e amministrazione:

http://www.dell.com/support/article/it/it/19/SLN302194/?lang=IT

Requisiti generali di sistema:

http://www.dell.com/support/article/it/it/19/SLN301914/?lang=IT

Esclusioni che potrebbero essere necessarie per altri virus antivirus:

http://www.dell.com/support/article/it/it/19/SLN301134/?lang=IT

Data Security Forum Comunitari:

http://en.community.dell.com/techcenter/security/datasecurity/f