Guida per l'utente

HP Sure Sense

Prima edizione: giugno 2019

Numero di parte del documento: L63508-061

Sommario

1 Informazioni introduttive

HP Sure Sense utilizza modelli di deep learning (apprendimento approfondito) per rilevare file dannosi ed evitare che attacchi di malware, zero-day, ransomware e Advanced Persistent Threat (APT) danneggino il computer.

HP Sure Sense utilizza i seguenti componenti:

- **Modello di previsione:** un modello di previsione leggero di deep learning. Rileva in modo autonomo le minacce cibernetiche e consente la protezione da zero-day e APT.
- **Servizi cloud di reputazione file:** un database basato su cloud contenente informazioni su file noti che aggiunge un secondo livello di classificazione. Se questa opzione è abilitata, i file hash per PE (Portable Executable) vengono inviati ai servizi di reputazione file nel cloud.
- **Content Delivery Network:** rete per la consegna dei contenuti; un sistema che distribuisce il modello di previsione e gli aggiornamenti software più recenti per HP Sure Sense.

Schede del menu principale

Il menu principale include le seguenti schede:

- **Status** (Stato): consente di visualizzare lo stato di protezione, il riepilogo delle minacce e altre informazioni.
- **Alert Log** (Registro avvisi): consente di visualizzare una tabella che elenca gli eventi e i registri di protezione. Contiene informazioni su sicurezza, aggiornamenti e gestione. In questa pagina, è possibile visualizzare maggiori dettagli sugli avvisi di protezione e intraprendere ulteriori azioni.
- **Quarantine** (Quarantena): consente di visualizzare una tabella contenente tutti i file in quarantena. Ogni voce si basa su un valore hash univoco. Le voci comprendono informazioni relative ai file e alla posizione originale del file. È possibile ripristinare i file in quarantena dalla colonna **Action** (Azione).
- **Settings** (Impostazioni): consente di configurare se visualizzare o meno le notifiche, impostare le lingue della console e gestire altre preferenze. Per visualizzare o modificare le **Advanced Settings** (Impostazioni avanzate): selezionare **Edit** (Modifica) e immettere le credenziali dell'amministratore.

Scansione completa

La scansione completa analizza tutti i file esistenti sulle unità locali del computer. Qualsiasi file identificato come dannoso viene bloccato e messo in quarantena.

Protezione avanzata dalle minacce

Quando la protezione avanzata dalle minacce è abilitata, monitora il comportamento di tutti i processi in corso per identificare eventuali malware. Se un processo viene identificato come ransomware, viene terminato.

2 Processi di sicurezza

Prevenzione dei malware

Tutti i file aggiunti alle unità locali del computer vengono automaticamente scansionati e analizzati. Se un file viene identificato come dannoso, si verificano le seguenti azioni:

- Il file viene bloccato e messo in quarantena. Il processo di quarantena copia il file nella cartella di quarantena, elimina il file dalla sua posizione originale e lo aggiunge alla tabella di quarantena.
- Viene aggiunto un evento alla pagina **Alert Log** (Registro avvisi). Viene visualizzata una notifica per indicare che la minaccia è stata bloccata. Se si fa clic sulla notifica, viene visualizzata la pagina **Quarantine** (Quarantena) con la relativa voce evidenziata.

NOTA: I file dannosi sui dispositivi di archiviazione esterni vengono bloccati e la loro esecuzione interrotta, ma non vengono messi in quarantena.

Ripristino ed eliminazione dei file in quarantena

I file spostati nella cartella di quarantena possono essere ripristinati o eliminati in base alle necessità. I file ripristinati vengono spostati nelle rispettive posizioni originali e ne è consentita l'esecuzione. L'eliminazione di un file in quarantena rimuove la voce dalla tabella di quarantena ed elimina il file dalla cartella di quarantena. Non modifica la classificazione del file e tutte le nuove istanze del file vengono bloccate e messe in quarantena.

Per eliminare o ripristinare i file in quarantena:

1. Aprire la pagina **Quarantine** (Quarantena).
2. Selezionare il file da eliminare. Selezionare l'icona **Action** (Azione).
3. Selezionare una delle opzioni: **Restore File** (Ripristina file), **Delete File** (Elimina file) o **File Details** (Dettagli file).

IMPORTANTE: Prima di ripristinare un file in quarantena, verificare che il file non sia un malware.

Per eliminare tutti i file contemporaneamente:

▲ Dalla pagina **Quarantine** (Quarantena), selezionare l'icona del cestino alla destra della casella di ricerca.

Aggiunta e rimozione di file attendibili

I file attendibili sono file bloccati e successivamente ripristinati dall'utente, che ne ha consentito l'esecuzione. È possibile aggiungere file attendibili all'elenco dei file attendibili dalla pagina **Quarantine** (Quarantena) o dalla pagina **Alert Log** (Registro avvisi). È possibile aggiungere processi all'elenco dei file attendibili solamente dalla pagina **Alert Log** (Registro avvisi).

I file aggiunti all'elenco dei file attendibili vengono ripristinati nelle cartelle originali ed eliminati dalla cartella di quarantena. I processi aggiunti all'elenco dei file attendibili possono essere eseguiti e il loro comportamento non viene più monitorato per individuare eventuali ransomware. I file e i processi aggiunti all'elenco dei file attendibili non vengono scansionati.

Per aggiungere un file o un processo attendibile:

1. Aprire la pagina **Alert Log** (Registro avvisi).
2. Selezionare l'icona Actions (Azioni) nella voce del file o processo da aggiungere.
3. Per aggiungere un file, selezionare **Restore File** (Ripristina file).

   Per aggiungere un processo, selezionare **Add to Trusted Files** (Aggiungi a file attendibili).

IMPORTANTE: Prima di aggiungere un file o un processo all'elenco dei file attendibili, verificare che non sia un malware.

Per rimuovere un file o un processo attendibile dall'elenco dei file attendibili:

1. Dalla pagina **Settings** (Impostazioni), selezionare **Edit Trusted Files** (Modifica file attendibili).
2. Selezionare il file o il processo da rimuovere, quindi selezionare l'icona **Actions** (Azioni).
3. Per rimuovere un file, selezionare **Quarantine File** (Metti file in quarantena).

   Per rimuovere un processo, selezionare **Remove From List** (Rimuovi da elenco).

Esclusioni

Le cartelle e i processi possono essere esclusi dalla scansione mediante l'opzione **Exclusions** (Esclusioni).

IMPORTANTE: Prima di aggiungere una cartella all'elenco delle esclusioni, HP consiglia quanto segue:

- Aggiungere unicamente cartelle in sola lettura per minimizzare il rischio di aggressioni e abusi delle cartelle attendibili.
- Non aggiungere cartelle temporanee. I malware tendono a scrivere moduli su cartelle temporanee. Questo consiglio è inoltre pertinente per le cartelle di sistema come `Windows` o `system32`.
- Se una soluzione specifica continua a restituire falsi positivi, consultare il fornitore della soluzione per ulteriori raccomandazioni.

Per accedere all'elenco delle esclusioni:

1. Aprire la pagina **Settings** (Impostazioni), quindi scorrere verso il basso fino a **Advanced Settings** (Impostazioni avanzate).
2. Selezionare **Edit Exclusions** (Modifica esclusioni).

A Disinstallazione di HP Sure Sense

Se HP Sure Sense è attualmente installato e si richiede una nuova installazione, è necessario rimuovere prima la versione corrente. Il metodo di disinstallazione si basa sul modo in cui HP Sure Sense è stato installato.

Se HP Sure Sense è stato installato manualmente mediante l'installazione guidata:

- Eseguire il programma di installazione e selezionare **Uninstall** (Disinstalla).

Se HP Sure Sense era preinstallato sul dispositivo:

1. Da **Impostazioni di Windows**, andare a **App e funzionalità**.
2. Disinstallare il programma di installazione di HP Sure Sense.