Benutzerhandbuch

HP Sure Sense

Erste Ausgabe: Juni 2019

Dokumentennummer: L63508-041

Inhaltsverzeichnis

1 Erste Schritte

HP Sure Sense nutzt Deep Learning-Modelle, um bösartige Dateien zu finden und um zu verhindern, dass Ihr Computer durch Malware, Zero-Day-Angriffe, Ransomware und APT-Angriffe (Advanced Persistent Threat) beschädigt wird.

HP Sure Sense verwendet die folgenden Komponenten:

- **Vorhersagemodell:** Ein einfaches Deep Learning-Vorhersagemodell. Es erkennt selbstständig Cyber-Bedrohungen und aktiviert Zero-Day- und APT-Schutz.
- **Dateireputations-Clouddienste:** Eine cloudbasierte Datenbank mit Informationen zu bekannten Dateien, die eine zweite Ebene zur Klassifizierung ergänzt. Wenn diese Option aktiviert ist, wird der Hash für PE-Dateien (Portable Executable) an die Dateireputationsdienste in der Cloud gesendet.
- **Content Delivery Network:** Ein System, das das aktuelle Vorhersagemodell und Software-Updates für HP Sure Sense verteilt.

Registerkarten des Hauptmenüs

Das Hauptmenü umfasst die folgenden Registerkarten:

- **Status**: Zeigt den Schutzstatus, eine Zusammenfassung der Bedrohungen und weitere Informationen an.
- **Warnungsprotokoll**: Zeigt eine Tabelle an, die Sicherheitsereignisse und Protokolle auflistet. Sie enthält Informationen über Sicherheit, Updates und Verwaltung. Auf dieser Seite können Sie weitere Informationen zu Sicherheitswarnungen anzeigen und weitere Maßnahmen ergreifen.
- **Quarantäne**: Zeigt eine Tabelle an, die alle Dateien in Quarantäne auflistet. Jeder Eintrag basiert auf einem eindeutigen Hash-Wert. Die Einträge enthalten Informationen zu den Dateien und zum ursprünglichen Speicherort der Datei. Sie können Dateien in Quarantäne über die Spalte **Aktion** wiederherstellen.
- **Einstellungen**: Ermöglicht es Ihnen, die Anzeige von Benachrichtigungen zu konfigurieren, Konsolensprachen festzulegen und andere Einstellungen zu verwalten. So zeigen Sie **Erweiterte Einstellungen** an oder ändern diese: Wählen Sie **Bearbeiten** aus und geben Sie die Anmeldeinformationen des Administrators ein.

Vollständige Prüfung

Bei der vollständigen Prüfung werden alle vorhandenen Dateien auf lokalen Laufwerken des Computers analysiert. Jede als bösartig gekennzeichnete Datei wird gesperrt und in Quarantäne gestellt.

Erweiterter Bedrohungsschutz

Wenn der erweiterte Bedrohungsschutz aktiviert ist, wird das Verhalten aller aktiven Prozesse auf Malware überwacht. Wenn ein Prozess als Ransomware erkannt wird, wird der Prozess abgebrochen.

2 Sicherheitsverfahren

Verhindern von Malware

Alle Dateien, die zu den lokalen Laufwerken des Computers hinzugefügt werden, werden automatisch geprüft und analysiert. Wenn eine Datei als bösartig erkannt wird, werden die folgenden Aktionen ausgeführt:

- Die Datei wird gesperrt und in Quarantäne gestellt. Beim Quarantänevorgang wird die Datei in den Quarantäneordner kopiert, aus ihrem ursprünglichen Speicherort gelöscht und der Quarantänetabelle hinzugefügt.
- Der Seite **Warnungsprotokoll** wird ein Ereignis hinzugefügt. Eine Benachrichtigung wird angezeigt, die angibt, dass die Bedrohung verhindert wurde. Wenn Sie auf die Benachrichtigung klicken, wird die Seite **Quarantäne** geöffnet, auf der der entsprechende Eintrag hervorgehoben ist.

HINWEIS: Bösartige Dateien auf externen Speichergeräten werden gesperrt und ihre Ausführung wird verhindert, sie werden jedoch nicht in Quarantäne gestellt.

Wiederherstellen und Löschen von Dateien in Quarantäne

Dateien, die in den Quarantäneordner verschoben wurden, können bei Bedarf wiederhergestellt oder gelöscht werden. Wiederhergestellte Dateien werden an ihre ursprünglichen Speicherorte verschoben und dürfen ausgeführt werden. Durch das Löschen einer Datei in Quarantäne wird der Eintrag aus der Quarantänetabelle entfernt und die Datei wird aus dem Quarantäneordner gelöscht. Die Klassifizierung der Datei wird dadurch nicht verändert und alle neuen Instanzen der Datei werden gesperrt und in Quarantäne gestellt.

So löschen Sie Dateien in Quarantäne oder stellen sie wieder her:

1. Öffnen Sie die Seite **Quarantäne**.
2. Wählen Sie die Datei aus, die gelöscht werden soll. Wählen Sie das Symbol **Aktion** aus.
3. Wählen Sie die Option **Datei wiederherstellen**, **Datei löschen** oder **Dateidetails** aus.

WICHTIG: Stellen Sie sicher, dass die Datei keine Malware ist, bevor Sie eine Datei in Quarantäne wiederherstellen.

So löschen Sie alle Dateien auf einmal:

▲ Wählen Sie auf der Seite **Quarantäne** das Papierkorb-Symbol rechts neben dem Suchfeld aus.

Hinzufügen und Entfernen von vertrauenswürdigen Dateien

Vertrauenswürdige Dateien sind Dateien, die gesperrt und dann wiederhergestellt wurden und vom Benutzer ausgeführt werden dürfen. Sie können vertrauenswürdige Dateien der Liste der vertrauenswürdigen Dateien auf der Seite **Quarantäne** oder der Seite **Warnungsprotokoll** hinzufügen. Sie können nur auf der Seite **Warnungsprotokoll** Prozesse zur Liste der vertrauenswürdigen Dateien hinzufügen.

Dateien, die der Liste der vertrauenswürdigen Dateien hinzugefügt werden, werden in ihren ursprünglichen Ordnern wiederhergestellt und aus dem Quarantäneordner gelöscht. Prozesse, die der Liste der vertrauenswürdigen Dateien hinzugefügt werden, dürfen ausgeführt werden und werden nicht mehr auf Ransomware-Verhalten überwacht. Dateien und Prozesse, die der Liste der vertrauenswürdigen Dateien hinzugefügt werden, werden nicht geprüft.

So fügen Sie eine vertrauenswürdige Datei oder einen Prozess hinzu:

1. Öffnen Sie die Seite **Warnungsprotokoll**.
2. Wählen Sie das Symbol „Aktionen“ im Eintrag der Datei oder des Prozesses aus, die bzw. den Sie hinzufügen möchten.
3. Wählen Sie zum Hinzuzufügen einer Datei **Datei wiederherstellen** aus.

   Wählen Sie zum Hinzufügen eines Prozesses **Zu vertrauenswürdigen Dateien hinzufügen** aus.

WICHTIG: Stellen Sie vor dem Hinzufügen einer Datei oder eines Prozesses zur Liste der vertrauenswürdigen Dateien sicher, dass es sich nicht um Malware handelt.

So entfernen Sie eine vertrauenswürdige Datei oder einen Prozess aus der Liste der vertrauenswürdigen Dateien:

1. Wählen Sie auf der Seite **Einstellungen** die Option **Vertrauenswürdige Dateien bearbeiten** aus.
2. Wählen Sie die Datei oder den Prozess aus, die bzw. den Sie entfernen möchten, und wählen Sie dann das Symbol **Aktionen** aus.
3. Um eine Datei zu entfernen, wählen Sie **Quarantänedatei** aus.

   Um einen Prozess zu entfernen, wählen Sie **Aus Liste entfernen** aus.

Ausschlüsse

Mit der Option **Ausschlüsse** können Ordner und Prozesse von der Prüfung ausgeschlossen werden.

WICHTIG: Bevor Sie einen Ordner zur Ausschlussliste hinzufügen, empfiehlt HP Folgendes:

- Fügen Sie nur schreibgeschützte Ordner hinzu, um die Gefahr zu minimieren, dass vertrauenswürdige Ordner von Angreifern missbraucht werden.
- Fügen Sie keine temporären Ordner hinzu. Malware schreibt häufig Module in temporäre Ordner. Diese Empfehlung gilt auch für Systemordner wie `Windows` oder `system32`.
- Wenn eine bestimmte Lösung weiterhin falsch positive Ergebnisse zurückgibt, bitten Sie den Hersteller der Lösung um Empfehlungen.

So greifen Sie auf die Ausschlussliste zu:

1. Öffnen Sie die Seite **Einstellungen** und führen Sie einen Bildlauf nach unten zu **Erweiterte Einstellungen** durch.
2. Wählen Sie **Ausnahmen bearbeiten** aus.

A Deinstallieren von HP Sure Sense

Wenn HP Sure Sense derzeit installiert ist und eine neue Installation erforderlich ist, müssen Sie zuerst die aktuelle Version entfernen. Die Methode für die Deinstallation basiert darauf, wie HP Sure Sense installiert wurde.

Wenn HP Sure Sense manuell mithilfe des Installationsassistenten installiert wurde:

- Führen Sie das Installationsprogramm aus und wählen Sie **Deinstallieren** aus.

Wenn HP Sure Sense auf Ihrem Gerät vorinstalliert war:

1. Wechseln Sie unter **Windows-Einstellungen** zu **Apps und Features**.
2. Deinstallieren Sie das HP Sure Sense-Installationsprogramm.