Guía del usuario

HP Sure Sense

Primera edición: junio de 2019

Referencia del documento: L63508-E51

Tabla de contenido

1 Primeros pasos

HP Sure Sense utiliza modelos de aprendizaje profundo para detectar archivos maliciosos y evitar que los ataques de malware, día cero, ransomware y Advanced Persistent Threat (APT) dañen su equipo.

HP Sure Sense utiliza los siguientes componentes:

- **Modelo de predicción:** un modelo de predicción de aprendizaje profundo ligero. Detecta de forma autónoma las amenazas cibernéticas y habilita la protección de día cero y APT.
- **Servicios en la nube sobre reputación de archivos:** una base de datos basada en la nube con información sobre archivos conocidos que agrega una segunda capa de clasificación. Cuando esta opción está activada, los archivos hash de PE (Portable Executable) se envían a los servicios de reputación de archivos de la nube.
- **Red de entrega de contenido:** un sistema que distribuye el último modelo de predicción y actualizaciones de software para HP Sure Sense.

Fichas del menú principal

El menú principal incluye las siguientes fichas:

- **Estado**: muestra el estado de la protección, el resumen de amenazas e información adicional.
- **Registro de alerta**: muestra una tabla que enumera los registros y los eventos de seguridad. Incluye información sobre seguridad, actualizaciones y administración. Desde esta página, puede ver detalles adicionales sobre las alertas de seguridad y tomar más acciones.
- **Cuarentena**: muestra una tabla que enumera todos los archivos en cuarentena. Cada entrada se basa en un valor hash único. Las entradas incluyen información relacionada con los archivos y la ubicación original del archivo. Puede restaurar los archivos en cuarentena desde la columna **Acción**.
- **Configuración**: le permite configurar si se muestran las notificaciones, definir los idiomas de la consola y administrar otras preferencias. Para ver o cambiar la **Configuración avanzada**: seleccione **Editar** e introduzca las credenciales de administrador.

Exploración completa

La exploración completa analiza todos los archivos existentes en las unidades locales del equipo. Todos los archivos identificados como maliciosos se bloquean y ponen en cuarentena.

Protección mejorada contra amenazas

Cuando la protección mejorada contra amenazas está habilitada, supervisa el comportamiento de todos los procesos de ejecución de malware. Si se identifica un proceso como ransomware, el proceso se termina.

2 Procesos de seguridad

Prevención de malware

Todos los archivos agregados a las unidades locales del equipo se exploran y analizan automáticamente. Cuando se identifica un archivo como malicioso, se producen las siguientes acciones:

- El archivo se bloquea y se pone en cuarentena. El proceso de cuarentena copia el archivo en la carpeta de cuarentena, elimina el archivo de su ubicación original y agrega el archivo a la tabla de cuarentena.
- Se agrega un evento a la página **Registro de alertas**. Se muestra una notificación para indicar que se ha prevenido la amenaza. Si hace clic en la notificación, la página **Cuarentena** se abrirá con la entrada correspondiente resaltada.

NOTA: Los archivos maliciosos de los dispositivos de almacenamiento externos se bloquean y se evita su ejecución, pero no se ponen en cuarentena.

Restauración y eliminación de archivos en cuarentena

Los archivos que se mueven a la carpeta de cuarentena pueden restaurarse o eliminarse según sea necesario. Los archivos restaurados se mueven a sus ubicaciones originales y se permite su ejecución. Al eliminar un archivo en cuarentena, se elimina la entrada de la tabla de cuarentena y se elimina el archivo de la carpeta de cuarentena. No cambia la clasificación del archivo y cualquier nueva instancia del archivo se bloquea y pone en cuarentena.

Para eliminar o restaurar archivos en cuarentena:

1. Abra la página **Cuarentena**.
2. Seleccione el archivo que desea eliminar. Seleccione el icono de **Acciones**.
3. Seleccione entre las opciones **Restaurar archivo**, **Eliminar archivo** o ver **Detalles del archivo**.

IMPORTANTE: Antes de restaurar un archivo en cuarentena, verifique que el archivo no sea malware.

Para eliminar todos los archivos a la vez:

▲ En la página **Cuarentena**, seleccione el icono de la papelera que se encuentra a la derecha de la casilla de búsqueda.

Adición y eliminación de archivos de confianza

Los archivos de confianza son archivos que se bloquearon y luego se restauraron para permitir que el usuario los ejecutara. Puede agregar archivos a la lista de archivos de confianza en la página **Cuarentena** o en la página de **Registro de alertas**. Puede agregar procesos a la lista de archivos de confianza solamente en la página **Registro de alertas**.

Los archivos agregados a la lista de archivos de confianza se restauran en sus carpetas originales y se eliminan de la carpeta de cuarentena. Los procesos agregados a la lista de archivos de confianza pueden ejecutarse y ya no se supervisan para detectar comportamiento de ransomware. Los archivos y los procesos agregados a la lista de archivos de confianza no se analizan.

Para agregar un archivo o proceso de confianza:

1. Abra la página **Registro de alertas**.
2. Seleccione el icono de Acciones en la entrada del archivo o proceso que desea agregar.
3. Para agregar un archivo, seleccione **Restaurar archivo**.

   Para agregar un proceso, seleccione **Agregar a archivos de confianza**.

IMPORTANTE: Antes de agregar un archivo o proceso a la lista de archivos de confianza, compruebe que no sea malware.

Para eliminar un archivo o proceso de la lista de archivos de confianza:

1. En la página **Configuración**, seleccione **Editar archivos de confianza**.
2. Seleccione el archivo o proceso que desea eliminar y, a continuación, seleccione el icono de **Acciones**.
3. Para eliminar un archivo, seleccione **Archivo en cuarentena**.

   Para eliminar un proceso, seleccione **Eliminar de la lista**.

Exclusiones

Las carpetas y los procesos pueden excluirse de la exploración mediante la opción **Exclusiones**.

IMPORTANTE: Antes de agregar una carpeta a la lista de exclusiones, HP recomienda lo siguiente:

- Agregue apenas carpetas de solo lectura para minimizar la oportunidad de que los atacantes se aprovechen de las carpetas de confianza.
- No agregue carpetas temporales. El malware tiende a escribir módulos en carpetas temporales. Este consejo también es relevante para las carpetas del sistema, como `Windows` o `system32`.
- Si una solución específica continúa devolviendo falsos positivos, busque recomendaciones del proveedor de la solución.

Para acceder a la lista de exclusiones:

1. Abra la página **Configuración** y desplácese hacia abajo hasta **Configuración avanzada**.
2. Seleccione **Editar exclusiones**.

A Desinstalación de HP Sure Sense

Si HP Sure Sense está instalado actualmente y se requiere una nueva instalación, primero debe eliminar la versión actual. El método para desinstalar se basa en la forma en que HP Sure Sense se instaló.

Si HP Sure Sense se instaló de forma manual utilizando el Asistente de instalación:

- Ejecute el instalador y seleccione **Desinstalar**.

Si HP Sure Sense venía preinstalado en su dispositivo:

1. En **Configuración de Windows**, vaya a **Aplicaciones y características**.
2. Desinstale el instalador de HP Sure Sense.