用户指南

HP Sure Sense

第一版：2019 年 6 月

文档部件号：L63508-AA1

目录

1 使用入门

HP Sure Sense 使用深度学习模型来检测恶意文件，并防止恶意软件、零日攻击、勒索软件和高级持续性威胁 (APT) 攻击损害您的计算机。

HP Sure Sense 包含以下组件：

- **预测模型：**一种轻量级深度学习预测模型。可自动检测网络威胁并实施零日攻击和 APT 防护。
- **文件信誉云服务：**一种存储已知文件信息的云数据库，添加了第二层分类。启用该选项后，PE (Portable Executable) 文件的哈希会被发送至云中的文件信誉服务。
- **内容传输网络：**一种为 HP Sure Sense 分发最新预测模型和软件更新的系统。

主菜单选项卡

主菜单中包含以下选项卡：

- **状态**：显示防护状态、威胁摘要和其他信息。
- **警报日志**：显示列出安全事件和日志的表格。其中包含有关安全、更新和管理方面的信息。您可从此页查看有关安全警报的更多详细信息，并采取进一步操作。
- **隔离**：显示列出所有隔离文件的表格。每个条目均有一个唯一的哈希值。条目中包含与文件和文件初始位置有关的信息。您可从**操作**列恢复隔离文件。
- **设置**：允许您配置是否显示通知、设置控制台语言和管理其他偏好。要查看或更改**高级设置**，请执行以下操作：选择**编辑**，并输入管理员凭证。

完全扫描

完全扫描可分析计算机本地驱动器上所有的现有文件。任何被识别为恶意的文件会被阻止并隔离。

增强型威胁防护

启用“增强型威胁防护”时，可监控所有正在运行的进程的行为以检测是否存在恶意软件。如果进程被识别为勒索软件，则会被终止。

2 安全进程

恶意软件防护

所有添加至计算机本地驱动器的文件都会进行自动扫描和分析。当文件被识别为恶意文件时，会进行以下操作：

- 阻止并隔离文件。隔离进程将文件复制至隔离文件夹，将其从初始位置删除，并添加至隔离表。
- 将事件添加至**警报日志**页面。显示通知，表明该威胁已被阻止。点击通知时，**隔离**页面将打开，并突出显示相关条目。

注：该功能将阻止和防止外接存储设备上的恶意文件的运行，但不进行隔离。

恢复和删除隔离文件

已被移至隔离文件夹的文件可根据需要进行恢复或删除。恢复的文件将移至其初始位置，并可运行。删除隔离文件会从隔离表中删除相应条目，并将文件从隔离文件夹中删除。该操作不会改变文件的分类，且任何新的文件实例会被阻止并隔离。

要删除或恢复隔离文件，请执行以下操作：

1. 打开**隔离**页面。
2. 选择想要删除的文件。选择**操作**图标。
3. 从选项中选择**恢复文件**、**删除文件**或查看**文件详细信息**。

切记：在恢复隔离文件之前，需核实文件并非恶意文件。

要一次删除所有文件，请执行以下操作：

▲ 在**隔离**页面上，选择搜索框右侧的垃圾桶图标。

添加和删除受信任文件

受信任文件是指曾经被阻止，后来又被用户恢复并允许运行的文件。您可从**隔离**页面或**警报日志**页面将受信任文件添加至“受信任文件”列表。但将进程添加至“受信任文件”列表仅可从**警报日志**页面进行操作。

被添加至“受信任文件”列表的文件将恢复至初始文件夹，并从隔离文件夹中删除。被添加至“受信任文件”列表的进程将被允许运行，且不再受到勒索软件行为监控。添加至“受信任文件”列表的文件和进程将不会被扫描。

要添加受信任文件或进程，请执行以下操作：

1. 打开**警报日志**页面。
2. 在您想要添加的文件或进程条目中选择“操作”图标。
3. 要添加文件，请选择**恢复文件**。

   要添加进程，请选择**添加至受信任文件**。

切记：在将文件或进程添加至“受信任文件”列表之前，需核实其并非恶意文件或进程。

要从“受信任文件”列表中删除受信任文件或流程，请执行以下操作：

1. 从**设置**页面选择**编辑受信任文件**。
2. 选择您想要删除的文件或进程，然后选择**操作**图标。
3. 要删除文件，请选择**隔离文件**。

   要删除进程，请选择**从列表中删除**。

排除项

若使用**排除项**选项，可将文件夹和进程从扫描中排除。

切记：在将文件夹添加至“排除项”列表之前，HP 建议参考以下提示：

- 仅添加只读文件夹，以尽量减少受信任文件夹遭受攻击者滥用的机会。
- 请勿添加临时文件夹。恶意软件常常将模块写入临时文件夹。该建议同样适用于 `Windows` 或 `system32` 等系统文件夹。
- 如果某个特定解决方案持续出现误报，请咨询该解决方案的供应商以寻求相关建议。

要访问“排除项”列表，请执行以下操作：

1. 打开**设置**页面，向下滚动至**高级设置**。
2. 选择**编辑排除项**。

A 卸载 HP Sure Sense

若您的设备已安装 HP Sure Sense，并需安装新版本，则必须先删除现有版本。根据 HP Sure Sense 的安装方式，卸载方式也有所不同。

若 HP Sure Sense 通过安装向导手动安装，请执行以下操作：

▲ 运行安装程序，并选择**卸载**。

若 HP Sure Sense 预安装在您的设备上，请执行以下操作：

1. 在 **Windows 设置**中，转到**应用和功能**。
2. 卸载 HP Sure Sense 安装程序。