



使用指南

HP Sure Sense

© Copyright 2019 HP Development
Company, L.P.

Microsoft 和 Windows 是 Microsoft
Corporation 在美國和/或其他國家/地區
的註冊商標或商標。

此為機密電腦軟體。持有、使用或複製
均需要 HP 的有效授權。在遵守 FAR
12.211 和 12.212 條款的情況下，「商
用電腦軟體」、「電腦軟體說明文件」
和「商用項目技術資料」係按照廠商的
標準商用授權條款授權給美國政府。

本文件包含的資訊可能有所變更，恕不
另行通知。HP 產品與服務的保固僅列
於產品及服務隨附的明確保固聲明中。
本文件的任何部份都不可構成任何額外
的保固。HP 不負責本文件在技術上或
編輯上的錯誤或疏失。

第一版：2019 年 6 月

文件編號：L63508-AB1

目錄

| | |
|--------------------------------------|----------|
| 1 快速入門 | 1 |
| 主功能表標籤 | 1 |
| 完整掃描 | 1 |
| 增強型威脅防護 | 1 |
| 2 安全程序 | 2 |
| 惡意程式防護 | 2 |
| 還原和刪除已隔離檔案 | 2 |
| 新增或移除受信任檔案 | 2 |
| 除外項目 | 3 |
| 附錄 A 解除安裝 HP Sure Sense | 4 |

1 快速入門

HP Sure Sense 使用深度學習模型來偵測惡意檔案，並預防惡意軟體、零日攻擊、勒索軟體和高級持續性威脅 (APT) 傷害您的電腦。

HP Sure Sense 使用以下元件：

- **預測模型**：一個輕量的深度學習預測模型。它可以自動檢測網路威脅並實現零日和 APT 保護。
- **檔案信譽雲端服務**：已知檔案資訊的雲端型資料庫，為系統增添了第二層分類。啟用此選項後，系統會將可移植可執行 (PE) 檔案的雜湊發送到雲端中的檔案信譽服務。
- **內容傳遞網路**：為 HP Sure Sense 分發最新預測模型和軟體更新的系統。

主功能表標籤

主功能表包含以下標籤：

- **狀態**：顯示防護狀態、威脅摘要和其他資訊。
- **警示記錄**：顯示一份列出安全事件和記錄的表格。其中包含有關安全性、更新和管理的資訊。您可以在此頁檢視有關安全警示的其他詳細資訊，並採取進一步動作。
- **隔離**：顯示一份列出所有隔離檔案的表格。每個項目都基於唯一的雜湊值。項目包含與檔案和檔案原始位置相關的資訊。您可以從**動作**欄還原已隔離檔案。
- **設定**：讓您設定是否顯示通知、設定主控台語言，以及管理其他偏好項目。若要檢視或變更**進階設定**：選取**編輯**，並輸入管理員認證。

完整掃描

完整掃描分析所有電腦本機硬碟中的現存檔案。系統會封鎖並隔離任何判定為惡意的檔案。

增強型威脅防護


啟用「增強型威脅防護」時，系統會監控所有運行程序的行為，預防惡意程式。如果某個程序被判定為勒索軟體，則該程序將被終止。

2 安全程序

惡意程式防護

自動掃描和分析所有新增至電腦本機硬碟內的檔案。當系統找到惡意檔案時，會採取以下動作：

- 封鎖並隔離該檔案。隔離程序會將檔案複製到隔離資料夾，從原始位置刪除該檔案，然後將該檔案新增至隔離表格中。
- 系統會在**警示記錄**頁面新增一個事件。系統會顯示通知，指示已防護該威脅。如果您點擊該通知，系統會開啟**隔離**頁面，相關的項目將會反白顯示。


 **附註：**系統會封鎖並阻止外接式儲存裝置上惡意檔案的運行，但無法隔離該檔案。

還原和刪除已隔離檔案

您可以依照需求還原或刪除被移至隔離資料夾的檔案。還原的檔案會被移至原始位置，並且可以繼續運行。刪除已隔離檔案會將該項目從隔離表格中移除，並且從隔離資料夾中刪除。此舉不會改變檔案的分類，而系統會封鎖並隔離該檔案任何新的執行個體。

若要刪除或還原已隔離檔案：

1. 開啟**隔離**頁面。
2. 選取您要刪除的檔案。選取**動作**圖示。
3. 從選項中進行選取以**還原檔案**、**刪除檔案**或是**檢視檔案詳細資訊**。

 **重要：**在您還原已隔離檔案前，請驗證該檔案是否為惡意檔案。

若要一次刪除所有檔案：

- ▲ 在**隔離**頁，選取位於搜尋框右側的垃圾桶圖示。

新增或移除受信任檔案

受信任檔案是原本被封鎖，然後被使用者還原並允許運行的檔案。您可以從**隔離**頁或**警示記錄**頁將受信任檔案新增至受信任檔案清單。您僅能從**警示記錄**頁將程序新增至受信任檔案清單。

新增至受信任檔案清單的檔案會被還原到其原始資料夾，並且從隔離資料夾中刪除。新增至受信任檔案清單的程序將被允許運行，並且不再受到勒索軟體行為監控。系統不會掃描新增至受信任檔案清單的檔案和程序。

若要新增受信任檔案或程序：

1. 開啟**警示記錄**頁：
2. 從您希望新增的檔案或程序的項目中選取**動作**圖示。
3. 若要新增檔案，請選取**還原檔案**。

若要新增程序，請選取**新增至受信任檔案**。


 **重要：**在您將檔案或程序新增至受信任檔案清單之前，請驗證其是否為惡意檔案或程序。

若要從受信任檔案清單中移除受信任檔案或程序：

1. 在**設定頁**，選取**編輯受信任檔案**。
2. 選取您想要移除的檔案或程序，然後選取**動作圖示**。
3. 若要移除檔案，請選取**隔離檔案**。
若要移除程序，請選取**從清單中移除**。

除外項目

您可以使用**除外項目**選項，將資料夾和程序排除在掃描之外。

 **重要：**在您将資料夾新增至除外項目清單之前，HP 有以下建議：

- 僅新增唯讀資料夾，以將受信任資料夾遭到攻擊的風險降到最低。
 - 請勿新增暫時資料夾。惡意軟體傾向於將模組寫入暫時資料夾。這項建議也適用於 Windows 或 system32 等系統資料夾。
 - 如果您持續從特定的解決方案收到誤判，請諮詢解決方案廠商並獲得建議。
-

若要取得除外項目清單：

1. 開啟**設定頁**，向下捲動至**進階設定**。
2. 選取**編輯除外項目**。

A 解除安裝 HP Sure Sense

如果 HP Sure Sense 目前已安裝，而您需要進行新的安裝，您必須先行移除目前版本。解除安裝的方式基於 HP Sure Sense 安裝方式。

如果您使用安裝精靈手動安裝 HP Sure Sense：

▲ 請執行安裝程式，然後選取**解除安裝**。

如果 HP Sure Sense 已預先安裝於您的裝置：

1. 在 **Windows 設定** 中，前往**應用程式和功能**。
2. 解除安裝 HP Sure Sense 安裝程式。