SOPHOS
Security made simple.

Sophos Sandstorm

可輕鬆實現的新一代進階型威脅防禦

Sophos 使用高度有效的技術（如即時 JavaScript 模擬和行為分析）來帶領安全產業對抗進階的惡意軟體。雖然將傳統反惡意軟體防護作為第一道防線仍然很重要，但企業需要額外的工具來對抗當今的惡意軟體和目標式惡意軟體。

Sophos Sandstorm 是一個對抗勒索軟體和進階型持續威脅（APT）的防禦解決方案，可用於增強 Sophos 安全產品。其使用強大的新一代雲端沙箱技術，可以快速、準確地偵測、阻止和回應其他解決方案無法找到的入侵攻擊威脅。

重點功能

- 可與您的 Sophos 安全解決方案無縫整合
- 可以在幾分鐘內就架設完成並開始運作
- 可防範勒索軟體類型 APT、未知惡意軟體和目標式攻擊
- 可以啟用威脅情報
- 精細且以事件為中心的報告

針對目標式攻擊的進階防護

讓勒索軟體和未知的資料竊取惡意軟體遠離您的網路強大的新一代雲端沙箱技術意味著您可以快速、準確地偵測、阻止和回應 APT 和零時差威脅。

我們讓它保持簡單易用

Sophos Sandstorm 可完全整合到 Sophos 安全解決方案中。只需更新訂閱授權、套用 Sandstorm 政策，您就能夠立即受到保護並阻擋目標式攻擊。您可以在幾分鐘內就開始運作這項保護。

阻止其他產品看不到的躲避式威脅

偵測出專為躲避第一代沙箱設備而設計的勒索軟體和未知威脅。我們的全系統模擬可對未知惡意軟體的行為進行最深的了解，以及可偵測出其他解決方案容易錯過的惡意攻擊。

深入的鑑識報告

以簡單且以事件為中心的入侵分析來加速對進階型威脅的反應。我們會關聯起相關證據以最優先的 APT 情報。這種方法既可以減少雜訊，也可以節省時間。

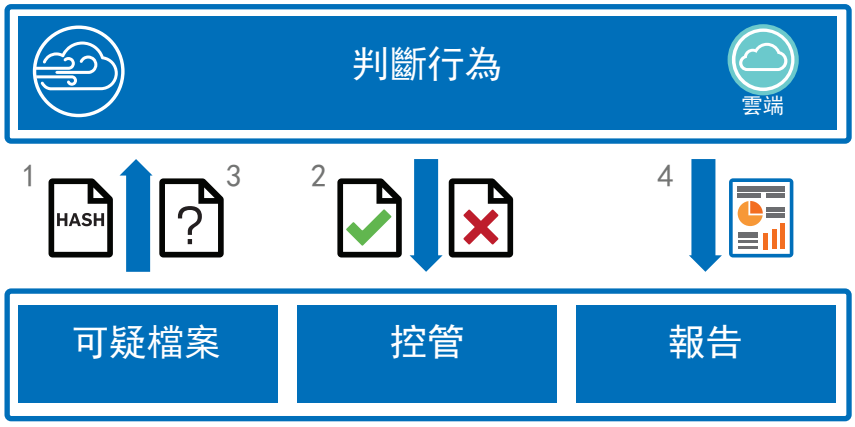
快如閃電的效能

您的 Sophos 安全解決方案可以準確地預先篩選流量，只有可疑的檔案才會提交給 Sandstorm，以確保延遲和對使用者的影響都降到最低。

Sophos Sandstorm 功能

- 完全整合到您的 Sophos 安全解決方案
- 檢查包含可執行內容的可執行檔和文件
  - Windows 執行檔（包括 .exe、.com 和 .dll）
  - Word 文件（包括 .doc、.docx、docm 和 .rtf）
  - PDF 文件
  - 可於壓縮檔內偵測到上述任何檔案（ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet）
  - 支援超過 20 種檔案類型
- 可在真實環境中執行檔案分析動態惡意軟體行為
- 提供詳盡的惡意檔案報告，並可直接從儀表板釋放分析後的檔案給使用者
  - 分析時間平均不到 120 秒
  - 對檔案類型、例外狀況和分析後動作可提供彈性的使用者和群組政策
  - 支援單次下載連結

運作方式



1. Sophos 安全解決方案會掃描所有檔案，進行所有的一般安全檢查（例如反惡意軟體特徵碼、錯誤 URL 等）。如果該檔案是可執行檔案或具有可執行內容並且不是透過安全網站下載，則該檔案會被視為可疑檔案。Sophos 安全解決方案會將可疑檔案進行雜湊演算並傳送到 Sophos Sandstorm，判斷它是否曾經被分析過。
2. 如果過去該檔案雜湊已經分析過，Sophos Sandstorm 就將威脅情報回傳給 Sophos 安全解決方案。此時，根據 Sophos Sandstorm 提供的資訊，檔案會送達使用者裝置或被阻擋。
3. 如果該檔案雜湊之前沒有被分析過，則可疑檔案的副本就會傳送到 Sophos Sandstorm，然後嘗試執行檔案運作並監控其行為。經過充分分析後，Sophos Sandstorm 會將威脅情報回傳給 Sophos 安全解決方案。此時同樣會根據 Sophos Sandstorm 提供的資訊，檔案會送達使用者裝置或被阻擋。
4. Sophos 安全解決方案會使用來自 Sophos Sandstorm 的詳細情報為每個威脅事件建立深入的鑑識報告。