解決方案手冊

Sophos Endpoint

由 Intercept X 驅動

業界最先進的 AI 驅動端點安全解決方案

Sophos Endpoint 由 Intercept X 技術驅動，提供無與倫比的防護，在進階攻擊影響您的系統之前即能加以攔截。強大的端點及擴展式偵測與回應 (EDR/XDR) 工具讓您的組織能夠主動捕獵、調查並應對可疑活動與攻擊跡象。

以預防為先的安全策略

Sophos Endpoint 採用全面且以預防為主的方法來保障安全，可在不依賴單一技術的情況下阻擋威脅。多重深度學習 AI 模型可防禦已知及前所未見的攻擊。Web、應用程式及周邊設備控制可縮小威脅面，並阻擋常見的攻擊媒介。行為分析、反勒索軟體、反漏洞攻擊等先進技術可在威脅升級前就加以迅速攔截，減少資源緊張的 IT 團隊需調查與處理的安全事件負擔。

滴水不漏的勒索軟體防護

Sophos Endpoint 是業界最強大的針對進階型勒索軟體的零接觸端點防禦。CryptoGuard 技術可實時阻止惡意加密，並自動將受影響的檔案還原至原始狀態，將對業務的影響降至最低。

自適應防禦

業界首創的動態防禦技術，能適應以應對主動威脅敵手及手動鍵盤攻擊。此舉可剝奪攻擊者的行動能力，中斷並遏制攻擊，同時爭取寶貴的額外時間來做出回應。

易於設定和管理

Sophos Central 是強大的雲端 AI 原生網路安全管理平台，統一管理所有 Sophos 新一代安全解決方案。推薦的技術和功能預設為啟用狀態，能確保您立即獲得最強保護，無需進行任何調整。

端點安全領域中值得信賴的業界領導者

Sophos Endpoint 持續獲得客戶、分析師以及獨立測試機構的高度認可。Sophos 已 15 次榮獲 Gartner® Magic Quadrant ™ 端點防護平台的領導者殊榮，並在 2025 年冬季 G2 Grid® 報告中名列端點防護套件第一名。

產品重點

- 多重深度學習 AI 模型可防禦已知及前所未見的攻擊。
- 以 Web、應用程式及周邊設備控制，減少威脅面並阻擋常見的攻擊媒介。
- 透過行為分析、反勒索軟體、反漏洞攻擊及其他先進技術，在威脅升級前就加以迅速攔截。
- 憑藉業界領先的防護，保護資料防禦本地及遠端勒索軟體攻擊。
- 透過業界首創的動態防禦，自動適應並回應主動攻擊敵手及人工操作的攻擊。
- 利用強大的 EDR 和 XDR 工具，主動捕獵、調查並回應可疑活動。

以預防為先的策略，有效縮小您的受攻擊面

在攻擊鏈的早期階段阻止攻擊，可減少後期監控和補救所需的資源。Sophos Endpoint 包含先進的防護技術，能夠阻擋最廣泛的攻擊類型。Web、應用程式及周邊設備控制能縮小受攻擊面並阻擋常見的攻擊媒介，進而減少攻擊者滲透到您的環境的機會。

Web 防護

阻擋流向惡意網站的出站瀏覽器流量，在威脅的傳遞階段就加以攔截，並防止來自釣魚網站或惡意軟體網站的攻擊。

Web 控制

阻擋對不良和不當內容的存取。在整個組織內執行可接受的網路使用規範，並防止資料外洩。

下載信譽

利用 SophosLabs 的全球威脅情報來分析下載的檔案，根據普及程度、存在時間及來源提供判定結果，並提示使用者封鎖信譽低或未知的檔案。

應用程式控制

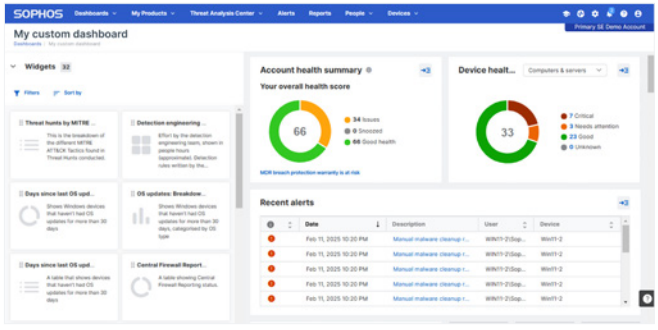
透過預定義的類別，阻擋易受攻擊或不適合的應用程式，無需逐一以雜湊值封鎖應用程式。

周邊設備 (裝置) 控制

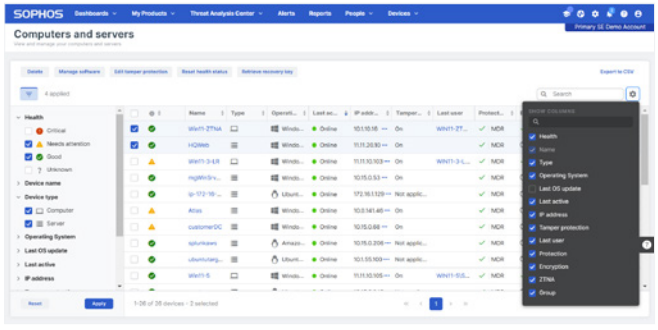
監控並阻擋對抽取式媒體、藍牙及行動裝置的存取，防止特定硬體連線到您的網路。

資料遺失防護

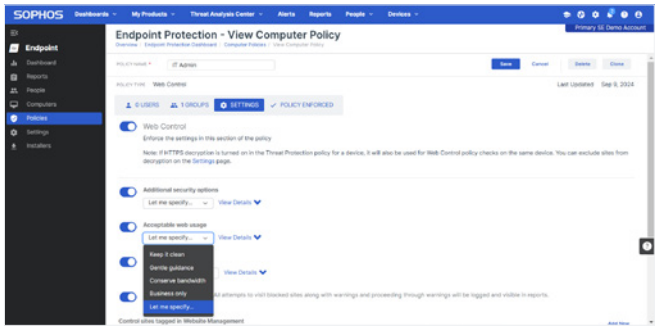
監控或限制含有敏感資料的檔案傳輸。例如，防止使用者透過網頁版電子郵件發送機密檔案。



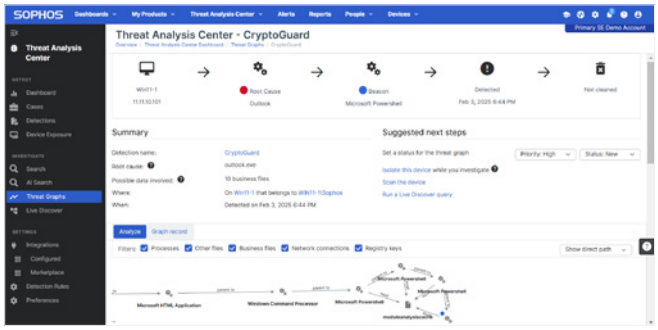
建立自訂儀表板以滿足您的需求。



易於設定與管理的端點安全防護。



可自訂的政策，預設啟用建議的設定。



分析威脅以確定其根本原因。

以預防為先的方式能迅速阻止威脅

盡早偵測並修復威脅，可降低風險。Sophos Endpoint 能在威脅升級前迅速阻止，讓資源有限的 IT 團隊減少需要調查和解決的事件。Sophos 提供強大的威脅防禦能力，其在獨立安全測試中持續獲得頂尖評分得以驗證。

滴水不漏的勒索軟體防護

根據 Microsoft 2024 年《數位防禦報告》，在 70% 的成功攻擊中都發現有遠端加密，而其中 92% 源自網路中未受管理的裝置。Sophos Endpoint 提供最強大的零接觸端點防禦，能夠對抗本地和遠端的勒索軟體。其採用先進的 CryptoGuard 技術來偵測試圖加密的行為，無論攻擊來源為何。

- 阻擋新的和新型的勒索軟體變種
- 實時檢查檔案變更，以偵測惡意加密行為。
- 阻止遠端勒索軟體透過網路遠端加密檔案。
- 自動將任何遭加密的檔案還原至未加密的原始狀態——採用不依賴 Windows Shadow Copy Service 的專有技術。
- 保護所有類型和大小的檔案，並將對效能的影響降至最低。
- 保護主開機記錄 (MBR)，防止針對硬碟的進階型攻擊。

人工智慧驅動的深度學習惡意軟體防禦

透過分析檔案屬性並運用預測性推理來識別威脅，以偵測並阻擋已知和未知的惡意軟體。

反漏洞利用

透過記憶體加固及超過 60 種反漏洞利用技術來保護處理程序的完整性，無需調整，且超越 Windows 原生功能及其他安全解決方案的能力。

行為防護

監控處理程序、檔案和登錄檔事件，以偵測並阻止惡意活動。它會掃描記憶體，檢查執行中的處理程序以發現隱藏威脅，並偵測出攻擊者植入惡意程式碼以逃避偵測的行為。

同步安全 (Synchronized Security)

Sophos Endpoint 與 Sophos Firewall、Sophos 零信任網路存取 (ZTNA) 及其他 Sophos 產品共享狀態和健康資訊，以對威脅和應用程式使用提供的額外可見性，並能自動隔離受感染的裝置。

實時防護

透過實時查詢 SophosLabs 的全球威脅情報，以查找額外的檔案環境內容、決策驗證、誤報減量及檔案信譽，來擴展強大的裝置端防護。

應用程式鎖定

阻止與瀏覽器和應用程式處理程序不常相關的異常行為，防止其被濫用。

反惡意軟體掃描介面 (AMSI)

Windows 反惡意軟體掃描介面 (AMSI) 可阻擋從記憶體直接載入惡意軟體的無檔案型攻擊。Sophos Endpoint 還包含專有的針對規避 AMSI 偵測的緩解措施。

惡意流量偵測

透過攔截並分析非瀏覽器流量中的惡意目的地，來偵測出和命令與控制 (C2) 伺服器通訊的裝置。

自適應防禦

Sophos Endpoint 採用業界首創的動態防禦技術，可實時適應來對抗主動攻擊敵手及手動鍵盤攻擊，來實現自動化保護。Sophos Endpoint 會阻擋在日常環境下可能並非帶有惡意，但在攻擊情境下卻具有危險性的行為。此功能可動態回應並中斷正在進行的攻擊，即使攻擊者已取得立足點而未觸發警示或使用惡意程式碼。

自適應攻擊防護

當偵測到手動鍵盤攻擊時，動態啟用端點上的強化防禦，阻斷攻擊者並為您爭取更多回應時間。

嚴重攻擊警告

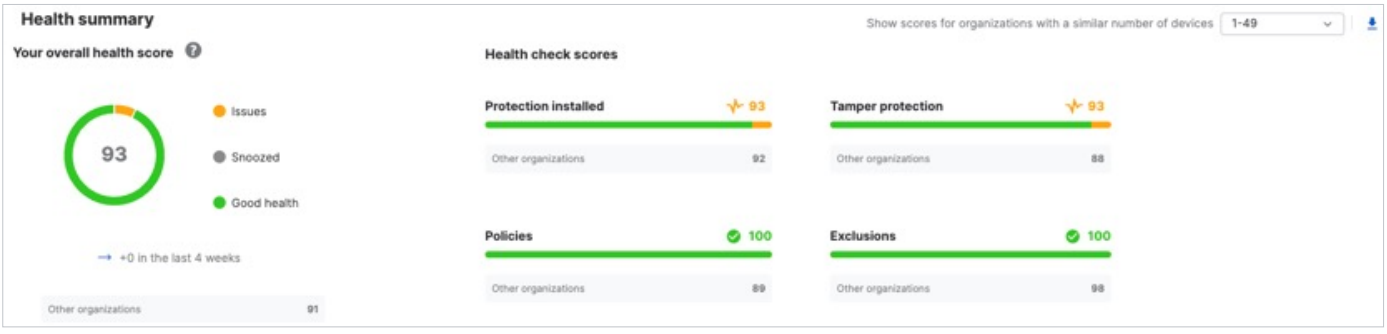
根據對全組織的威脅偵測，通知系統管理員多個端點上正在發生的嚴重攻擊活動。

	行為防護	自適應攻擊防護	嚴重攻擊警告
範圍	**單一裝置**	**單一裝置**	**整體資產**
優點	行為引擎可攔截主動攻擊敵手攻擊的初期階段	提高防護敏感度以防止攻擊	即時提醒您需要立即處理的攻擊事件
觸發	行為規則	偵測到駭客工具組	高影響力的主動攻擊敵手指標，包括組織層級的關聯和閾值
類比	「架起防禦！」	「架起防禦！」	「紅色警戒！」

Sophos Endpoint 中的自適應防禦

識別安全狀態的偏移

配置不當的政策設定、排除項目以及其他因素均可能會減弱您的安全狀態。帳戶健康檢查功能可識別安全狀態偏移和高風險的錯誤設定，並讓您一鍵修復問題。



帳戶健康情況檢查

其他防護層（附加功能）

Sophos ZTNA

使用終極 VPN 替代方案，安全地將您的使用者連線到應用程式。Sophos ZTNA 是唯一與新一代端點防護緊密整合的零信任網路存取解決方案。

裝置加密

由於裝置每天都可能遺失或被竊 因此全磁碟加密至關重要 與 Sophos Endpoint 整合的裝置加密可有效管理 BitLocker (Windows) 和 FileVault (macOS)。

加快偵測、調查和回應

Sophos Endpoint 可自動預先攔截大多數威脅，減少需要調查的事件數量。對於需要人工分析的可疑活動和威脅，Sophos 提供強大的解決方案，能夠快速偵測、調查並回應所有關鍵攻擊媒介。

Sophos XDR

Sophos Extended Detection and Response (XDR) 擴展式偵測與回應讓您能夠在您的整個安全環境中捕獵、調查並回應可疑活動和多階段的攻擊。我們的強大 GenAI 驅動工具由安全分析師設計，適用於不同技能水平的使用者 —— 讓從 IT 普通人員到頂尖 SOC 分析師都能迅速調查威脅並消除攻擊敵手威脅。

Sophos XDR 提供與廣泛的端點、防火牆、網路、電子郵件、身分識別、生產力、雲端及備份解決方案的現成整合，能讓您從現有安全工具獲得更多的投資回報。

如需更多資訊，請瀏覽 www.sophos.com/XDR

Sophos MDR

對於沒有資源在內部管理威脅偵測和回應的組織而言，Sophos Managed Detection and Response (MDR) 託管式偵測與回應是由一組安全分析師、威脅獵人和事件回應專員組成的菁英團隊所提供的全天候服務。Sophos MDR 利用來自 Sophos 及第三方安全技術的遙測數據 來偵測並消除即使是最複雜的威脅。

Sophos MDR 根據您的需求提供多種服務層級和回應模式，可適應您的組織需求，並與您現有的工具和技術相容。

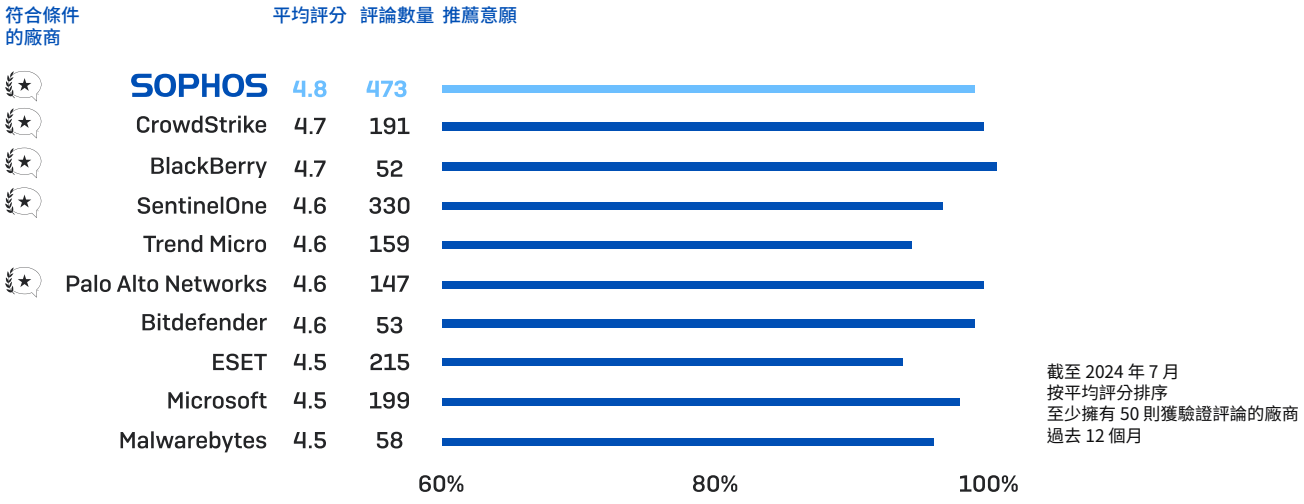
如需更多資訊，請瀏覽 www.sophos.com/MDR

	Sophos Endpoint	Sophos XDR	Sophos MDR
新一代端點防護 AI 驅動的深度學習反惡意軟體與 Web 防護	✓	✓	✓
阻擋惡意活動 反勒索軟體、反漏洞攻擊、自適應防禦	✓	✓	✓
減少威脅暴露 DLP、Web、周邊設備和應用程式控制功能	✓	✓	✓
偵測與回應 強大的威脅調查與回應工具		✓	✓
跨關鍵受攻擊面的可視度 Sophos 與第三方技術的整合		✓	✓
託管式偵測與回應 24/7 全天候由專家主導的威脅監控和事件回應			✓

評價最高且獲最多評論的端點防護解決方案

在 Gartner 2024 年《端點防護平台的客戶之聲》中，Sophos 在所有廠商中收到最多評論並獲得了 4.8/5.0 的評分。Sophos 還被評為 2024 年的「客戶首選」廠商之一，涵蓋報告中所有 11 個產業領域。

端點防護平台



客戶為何選擇 Sophos Endpoint

Sophos 是端點安全領域的知名領導者，並擁有業界認可作為背書。

Gartner

Sophos 在 2024 年 Gartner ® 魔力象限™端點保護平台報告中，已連續在 15 次獲評為領導者之一。

SE Labs

Sophos 持續在獨立端點安全測試中取得業界領先的保護成績。

G2 Leader

Sophos 在 2025 年冬季 G2 Grid® 報告中獲評為端點防護套件、EDR、XDR、防火牆軟體和 MDR 的領導者之一。

IDC

Sophos 獲評為 2024 年 IDC MarketScape 中小型企業全球現代端點安全的領導者之一。

立即免費試用

註冊取得免費 30 天試用，請瀏覽 sophos.com/endpoint

台灣業務窗口
電話：1-866-866-2802
電子郵件：Sales.Taiwan@Sophos.com

2025-03-04 SB-ZHTW (MP)

SOPHOS