SOPHOS

Intercept X

無與倫比的端點保護

Sophos Intercept X 使用深度學習的惡意軟體偵測、漏洞利用防禦、反勒索軟體和其他功能的獨特組合來阻擋最廣泛的攻擊。

重點功能

- 搭載深度學習人工智能，排名第一的惡意軟體偵測引擎
- 漏洞利用防禦可阻止攻擊者用來控制易受攻擊軟體的技術
- 主動攻擊緩解可防禦電腦上的持續性攻擊
- 根本原因分析可讓您掌握惡意軟體的行為以及來源
- 針對勒索軟體的防禦技術
- Intercept X 可補強現有的防毒部署。Intercept X Advanced 結合了現代技術與基礎方法，可取代您現有的端點安全保護。

Sophos Intercept X 採用全方位的縱深防禦方法來實現端點保護，不單只是仰賴一種主要的安全技術。這就是“加成的力量”，領先的基礎技術和現代技術的結合。

現代技術包括深度學習的惡意軟體偵測、漏洞利用防禦和反勒索軟體等專屬功能。基礎技術包括特徵碼型惡意軟體偵測、行為分析、惡意流量偵測、裝置控制、應用程式控制、Web 篩選、資料遺失防禦等。

深度學習的惡意軟體偵測

Intercept X 內建的人工智慧是一種深度學習神經網路，是一種先進的機器學習形式，可以在不使用特徵碼的情況下偵測出已知和未知的惡意軟體。

在深度學習的支援下，Intercept X 擁有業界最佳的惡意軟體偵測引擎，並經第三方測試機構的驗證。藉此 Intercept X 可以偵測到躲過其他端點安全工具的惡意軟體。

阻擋漏洞利用，阻擋攻擊

軟體中的弱點以驚人的速度激增，需要廠商不斷修補。但另一方面，新的漏洞利用技術非常罕見，並且攻擊者會反覆使用它們來攻擊弱點。漏洞利用防禦會阻擋用來散佈惡意軟體、竊取認證和躲避偵測的漏洞利用工具和技術，以防範攻擊者。藉此，Sophos 能避開網路中躲藏的駭客和零時差攻擊。

經過驗證的勒索軟體防護

Intercept X 利用行為分析來阻止前所未見的勒索軟體和開機記錄攻擊，使其成為目前最先進的反勒索軟體技術。即使可信任檔案或處理序被濫用或綁架，CyptoGuard 也能在無須使用者或 IT 支援人員的介入下阻擋並恢復它們。CryptoGuard 將在檔案系統層進行無回應的運作，持續追蹤試圖修改文件或其他檔案的遠端電腦和本機處理序。

端點偵測與回應 (EDR)

端點偵測和回應功能必須超越防禦，以偵測額外威脅、進一步調查，並有信心地回應。現在 Sophos Intercept X Advanced with EDR 將智慧型 EDR 與業界頂級的端點保護整合在單一解決方案中，藉此，組織得以解決和安全事件相關的難題。

簡化管理和部署

由 Sophos Central 管理安全產品，意味著您不再需要安裝或伺服器來保護您的端點。Sophos Central 會提供預設政策和建議的設定，確保您從一開始就能獲得最有效的保護。

Managed Threat Response (MTR)

由 Sophos 專家團隊提供的全天候威脅追捕、偵測與回應，是一項完全託管式服務。利用 Intercept X Advanced with EDR 中的智慧型 EDR，Sophos 分析人員可回應潛在威脅、尋找感染指標，並提供事件的詳細分析，包括發生的狀況、地點、時間、方式和原因。

技術規格

Sophos Intercept X 支援 Windows 7 和以上版本 (32 和 64 位元)。它也可以與第三方端點和防毒產品一起運作，以新增深度學習惡意軟體偵測、防漏洞利用、防勒索軟體、根本原因分析，以及 Sophos Clean 等功能。

	特點	
漏洞利用防禦	執行資料執行防禦	✓
	強制位址空間配置隨機化	✓
	隨機化記憶體配置	✓
	Null 頁面 (Null 解除參照保護)	✓
	堆積噴灑配置	✓
	動態堆積噴灑	✓
	堆疊樞紐	✓
	堆疊執行 (記憶體保護)	✓
	以堆疊為基礎的 ROP 緩解技術 (呼叫者)	✓
	以分支為基礎的 ROP 緩解技術 (以硬體增強)	✓
	結構式異常處理程序覆寫 (SEHOP)	✓
	匯入位址表格篩選 (IAF)	✓
	載入程式庫	✓
	反射型 DLL 插入	✓
	Shellcode (能取得系統控制權的惡意程式碼)	✓
	VBScript 上帝模式 (God Mode)	✓
	WoW64	✓
	系統呼叫	✓
	中空程序	✓
	DLL 劫持	✓
	Squlydoo AppLocker 繞過	✓
	APC 防護 (Double Pulsar/AtomBombing)	✓
	處理序權限提升	✓
主動攻擊減緩	認證竊盜防護	✓
	程式碼洞穴緩解	✓
	瀏覽器中間人防護 (Safe Browsing)	✓
	惡意流量偵測	✓
	Meterpreter 殼層偵測	✓

	特點	
反勒索軟體	勒索軟體檔案防護 (CyperGuard)	✓
	自動檔案復原 (CryptoGuard)	✓
	磁碟和開機區防護 (WipeGuard)	✓
應用程式鎖定	網頁瀏覽器 (包括 HTA)	✓
	網頁瀏覽器外掛程式	✓
	Java	✓
	媒體應用程式	✓
	Office 應用程式	✓
深度學習	深度學習的惡意軟體偵測	✓
	深度學習阻擋可能不需要的應用程式 (PUA)	✓
	減少誤報	✓
	即時保護	✓
回應 調查 移除	根本原因分析	✓
	Sophos Clean	✓
	同步安全活動訊號	✓
部署	可以獨立代理程式運作	✓
	可與現有防毒一起運作	✓
	可作為現有 Sophos Endpoint 代理程式的元件運作	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* 由 CryptoGuard、惡意流量偵測、同步安全活動訊號、根本原因分析等功能支援

已經使用 Sophos Endpoint Protection 的企業主控台進行管理？您可以使用 Sophos Central 管理您的端點，並啟用 Intercept X 進行自動部署。

台灣業務窗口
電話：+886 2 7709 1980
電子郵件：Sales.Taiwan@Sophos.com

立即免費試用

取得 30 天免費試用版本
www.sophos.com/intercept-x

2019-12-13 DSZHTW (PC)

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市前鎮區一心二路128號9樓之1

SOPHOS