SOPHOS
Security made simple.

Intercept X

Deep Learning深度學習惡意軟體偵測、漏洞利用攻擊防禦、防勒索軟體、根本原因分析，以及 Sophos Clean

Sophos Intercept X 可在正確的時間使用正確的技術來阻止未知威脅並拒攻擊者於門外。其可以運作在現有的防毒之上，或是與 Sophos Endpoint Protection 一起運作，以提供完整的新一代防護。

重點功能

- 訓練有素的深度學習模式可以偵測出未能發現的惡意軟體
- Exploit Prevention漏洞利用攻擊防禦可阻止攻擊者用來控制易受攻擊軟體的技術
- 主動攻擊減緩(Active Adversary Mitigation)可防禦攻擊在電腦上存留
- 根本原因分析(Root cause analysis)可讓您掌握惡意軟體的行為以及來源
- Sophos Clean 將刪除惡意軟體及其餘留的蹤跡
- 補強現有的防毒措施

建立新一代端點保護

只用檔案掃描的日子已經一去不復返。現在，您的目標是避免威脅接觸您的裝置、阻止它運作，以及在其躲過防範措施時被偵測出來，而且不只是要能清除惡意軟體，還必須分析和還原它造成的任何影響。

Sophos Intercept X 使用可與現有防毒軟體共存的多層式技術來提供全面的新一代保護。

Deep Learning深度學習惡意軟體偵測

Intercept X 在 SophosLabs 中使用深度學習神經網路進行訓練，無須特徵碼即可以高準確度偵測出新的和未知的惡意軟體檔案。 其他機器學習方法通常會要求資料科學家識別要尋找的屬性， 因此所得到的模型會受限於選擇的屬性和訓練資料的有效性。 而 Intercept X 使用的深度學習會識別出可區分惡意軟體和良性檔案的重要屬性。 將這項能力與 SophosLabs 提供的大型訓練資料集相結合，可確保在良性檔案和惡意檔案之間建立準確且有效的決策分界。 這個訓練模型小於 20MB，而且不需要經常更新。 在雲端中，SophosLabs 會不斷地使用新的和未知的惡意軟體樣本來訓練模型並監控決策分界的有效性。

保護易受攻擊的軟體

弱點以驚人的速度出現，它們是軟體中的缺陷且需要廠商進行修補。另一方面，新的漏洞利用攻擊手法平均每年只會出現兩次，攻擊者會一次又一次地利用它們來攻擊已經被發現的弱點。Exploit Prevention漏洞利用防禦可在弱點被修補之前阻止攻擊者對此發動的攻擊和伎倆。

有效的勒索軟體偵測

CryptoGuard 技術能偵測出自發性的惡意資料加密情形，阻斷勒索軟體的運作。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 將在檔案系統層默默地運作，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。

SiPRO 瑞虹科技股份有限公司 | 電話：(02)2999-0857 | 電郵：siprotech_sales@siprotech.com.tw
www.siprotech.com.tw | 傳真：(02)2999-0852 | 地址：新北市三重區光復路一段83巷1號3樓

根本原因分析

會識別惡意軟體，然後將其隔離並移除，以解決當前的問題。但是，您真的知道惡意軟體在被移除前做過什麼，或是它最初是如何出現在您的環境中？根本原因分析能顯示導致該次偵測的所有事件，您將可以瞭解該惡意軟體接觸過哪些檔案、程序和登錄檔機碼，並且啟動您的進階系統清除來倒回時間。

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部署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。

	Features	
EXPLOIT PREVENTION	Enforce Data Execution Prevention	✓
	Mandatory Address Space Layout Randomization	✓
	Bottom-up ASLR	✓
	Null Page (Null Deference Protection)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Stack-based ROP Mitigations (Caller)	✓
	Branch-based ROP Mitigations (Hardware Assisted)	✓
	Structured Exception Handler Overwrite (SEHOP)	✓
	Import Address Table Filtering (IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	APC Protection (Double Pulsar / AtomBombing)	✓
	Process Privilege Escalation	✓
ACTIVE ADVERSARY MITIGATIONS	Credential Theft Protection	✓
	Code Cave Mitigation	✓
	Man-in-the-Browser Protection (Safe Browsing)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection	✓

已經使用 Sophos Endpoint Protection 的Enterprise Console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。

取得保護的四個步驟

1. 造訪 sophos.com/zh-tw/intercept-x 以開始試用。
2. 建立一個 Sophos Central 系統管理帳戶。
3. 下載並安裝 Intercept X 代理程式。
4. 透過 Sophos Central 管理您的保護。

技術規格

Sophos Intercept X 支援 Windows 7 和以上版本 (32 和 64 位元)。當使用 Sophos Central 管理時，其可以和 Sophos Endpoint Protection Standard 或 Advanced 版本一起運作。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、防入侵攻擊、防勒索軟體、根本原因分析，以及 Sophos Clean 等功能。

	Features	
ANTI-RANSOMWARE	Ransomware File Protection (CryptoGuard)	✓
	Automatic File Recovery (CryptoGuard)	✓
	Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN	Web Browsers (including HTA)	✓
	Web Browser Plugins	✓
	Java	✓
	Media Applications	✓
	Office Applications	✓
DEEP LEARNING	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
	False Positive Suppression	✓
	Live Protection	✓
RESPOND INVESTIGATE REMOVE	Root Cause Analysis	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DEPLOYMENT	Can run as standalone agent	✓
	Can run alongside existing antivirus	
	Can run as component of existing Sophos Endpoint agent	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* Features supported CryptoGuard, Malicious Traffic Detection,Synchronized Security Heartbeat, Root Cause Analysis

17-09-10-DS-ZHTW (DD)

SOPHOS