SOPHOS
Cybersecurity made simple.

CLOUD READY

Intercept X for Server

無論在雲端或本地預置，您都需要保護組織核心的關鍵應用程式和資料。Intercept X for Server 使用深度學習惡意軟體偵測、漏洞利用防禦、反勒索軟體技術、應用程式白名單、主動攻擊防護以及深入的根本原因分析，提供全方位的縱深防禦方法。

產品重點

- 探索並保護 Microsoft Azure 和Amazon Web Services 中的工作負載
- 防範伺服器上的勒索軟體，包括來自惡意端點的遠端攻擊
- 伺服器鎖定白名單中的應用程式
- 阻止進階的駭客攻擊手法和漏洞利用
- 根本原因分析可詳細說明攻擊原因和感染途徑
- 同步安全(Synchronized Security) 會在多個 Sophos 產品共享威脅、健康狀態和安全的資訊
- Sophos Central 提供簡化的管理
- 對 Windows 和 Linux 系統的威脅防護

強大的伺服器專屬保護

Intercept X for Server 利用多種保護措施來阻擋零時差攻擊、漏洞利用和駭客。這些保護可以防止攻擊到達伺服器、在攻擊發動之前就偵測出來，或是在攻擊躲避保護時阻止它們並進行徹底的清理。其不斷更新的人工智慧模型經過培訓，可以在伺服器上找出潛在惡意程式碼的可疑屬性。此外，伺服器專屬功能 (如伺服器鎖定和雲端工作負載探索) 可確保伺服器組態安全。

Intercept X for Server 可探索並保護雲端的工作負載，包括 Microsoft Azure 和 Amazon Web Services。透過將 Sophos Central 與 AWS 和 Azure 連線，Intercept X for Server 可以直接確認伺服器受到保護，而且經由在 Sophos Central 中顯示相關資訊，可使管理更加輕鬆。

阻擋以伺服器為基礎的勒索軟體

CryptoGuard 在檔案系統層級運作，可防禦勒索軟體，偵測和攔截未經請求的檔案加密，無論是在伺服器還是連接到伺服器的遠端端點上。WipeGuard 同樣可以避免主開機記錄遭到惡意加密。

Sophos Intercept X for Server 只需單擊即可鎖定伺服器、將應用程式列入白名單，以保護處於安全狀態的伺服器，並防止未經授權的應用程式執行。Sophos 會自動掃瞄系統並建立已知良好應用程式的清單 (白名單)，無需手動建立規則。Sophos 在應用程式和相關檔案 (如 DLL、資料檔案和指令碼) 之間建立了緊密的聯繫。

中斷攻擊：拒絕駭客存取伺服器

漏洞以驚人的速度出現，在不影響使用者的情況下修補伺服器極具挑戰性。漏洞利用攻擊可以引起大破壞，傳統的伺服器保護技術通常偵測不到它們。Intercept X for Server 的目的是阻擋即使是最頑強的駭客使用漏洞利用技術來竊取憑證，無論他們試圖躲藏且持續進行，或是橫向移動，Intercept X 都會阻止它們。

根本原因分析

Intercept X for Server 還具備偵測和回應技術，以提供完整的可見度，因此系統管理員可以知道攻擊是如何進入、軌跡與行為，以及後續應該採取的動作。Intercept X for Server 無需其他代理程式或管理主控台及可提供這項功能。

同步安全 (Synchronized Security)

同步安全(Synchronized Security) 是同級最佳的安全系統，可使各種防禦措施如同所受攻擊一樣進行協作。它結合了直覺的安全平台和屢獲殊榮的產品，這些產品將積極協作以阻止進階的威脅，為您提供無與倫比的保護。

使用 Sophos Central 輕鬆管理

從 Sophos Central 管理安全，意味著您不再需要部署伺服器來保護系統。由 Sophos 託管的 Sophos Central 無需架設主控台伺服器即可進行即時存取。Sophos Central 為伺服器提供立即可用的政策，同時還能管理其他 Sophos 產品，包括 Sophos Intercept X、Mobile、Wireless、Email和 Web - 全都透過一個單一的管理平台。

Intercept X for Server 的主要功能

平台	Windows Server	✓
	Linux[1]	✓
	Public Cloud (Microsoft Azure and Amazon AWS)	✓
防禦 / 減少受攻擊面	應用程式白名單 [伺服器鎖定]	✓
	Web Security	✓
	Windows Firewall Control	✓
	Download Reputation	✓
	Web Control (URL Blocking)	✓
	Peripheral Control (e.g., USB)	✓
	Application Control	✓
防禦 / 避免其在裝置上運作	Deep Learning Malware Detection	✓
	Exploit Prevention	✓
	Anti-Malware File Scanning	✓
	Live Protection	✓
	Pre-execution Behavior Analysis [HIPS]	✓
	Off-board scanning for VMs (ESXi and Hyper-V)[2]	✓
	Detect Potentially Unwanted Applications (PUA)	✓
	Data Loss Prevention	✓
偵測 / 停止運作中的威脅	反駭客/主動攻擊緩解	✓
	勒索軟體檔案防護 [CryptoGuard] 包括偵測遠端連線端點對伺服器的攻擊	✓
	Disk and Boot Record Protection [WipeGuard]	✓
	Malicious Traffic Detection	✓
回應 / 調查與刪除	Sophos Clean Automated Malware Removal	✓
	Root Cause Analysis	✓
管理 / 控制	Server-specific policy management	✓
	Update Cache and Message Relay	✓
	Automatic Scanning Exclusions	✓
	Synchronized Application Control[4]	✓
管理 / 可見度	Azure Workload Discovery and Protection	✓
	AWS Workload Discovery and Protection	✓
	AWS Map, multi-region visualization	✓
	Synchronized Security with Security Heartbeat™ (Enhanced threat protection, positive source identification, and automated isolation)[4]	✓
	Windows Remote Desktop Services (user visibility)	✓
管理 / SOPHOS CENTRAL	Cloud-based management, eliminating the need the install and maintain a separate server on premises, and managing security of servers in a single console with endpoints, mobile, email, wireless	✓
	Multi-factor authentication	✓
	Role-based administration	✓

1 Windows 上提供所有功能；Linux 上提供部分功能
2 請參閱《Sophos 虛擬環境授權指南》中的〈超精簡型代理程式部署〉
3 對由 Sophos Enterprise Console 管理的 Windows 伺服器而言，可透過 Endpoint Exploit Prevention (EXP) 附加授權取得 CryptoGuard
4 與 Sophos XG Firewall 一起使用時

Azure

aws partner network
Advanced Technology Partner
Security Competency
Public Sector Partner
Marketplace Seller

立即免費試用

取得 30 天免費試用版本

sophos.com/server。

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

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

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

亞洲業務窗口
電話：+65 62244168
電子郵件：salesasia@sophos.com

2018/6/28 DS-ZHTW (MP)

SOPHOS