SOPHOS

# Sophos Firewall 功能介紹


## Sophos Firewall

### 產品重點

- Xstream 架構透過以串流為基礎的封包處理，提供超高等級的可見度、保護能力和效能
- Xstream TLS 檢查提供高效能，支援 TLS 1.3 而效能不會降級、不限連接埠、使用含預設例外項目的企業級政策、擁有獨特的儀表板可見度，以及具備相容性故障排除能力
- Xstream DPI 引擎使用一個高效能引擎，為 IPS、AV、Web、應用程式控制和 TLS 檢查提供串流掃描保護
- Xstream Network Flow FastPath 自動提供以政策驅動的智慧型可信任流量加速
- 具有互動式控制中心的專用使用者介面，會利用交通號誌燈號 (紅、黃、綠) 立即標示出需要注意的內容
- 控制中心提供多種即時深入資訊，包括端點健康狀況、未識別的 Mac 和 Windows 應用程式、雲端應用程式和影子 IT、可疑裝載、有風險的使用者、進階型威脅、網路攻擊、令人討厭的網站等
- 最佳化的兩點擊操作
- 政策控制中心桌面工具會監控業務、使用者和網路政策的政策活動，並追蹤未使用、停用、已變更和新的政策
- 統一政策模型可將所有的業務、使用者和網路防火牆規則，整合到一個包含群組、篩選和搜尋選項的單一畫面中
- 使用自訂的自動和手動群組功能，以及一目瞭然的滑鼠操作和執行指標，進行流暢的防火牆規則管理
- 所有防火牆規則都提供所應用的防毒、沙箱、IPS、Web、應用程式、流量塑型 (QoS) 和安全心跳 (Heartbeat) 等安全性和控制的概觀
- 預定義的 IPS、Web、應用程式和流量塑形 (QoS) 政策，可針對一般部署情境 (例如CIPA、典型的工作場所政策等) 進行快速設定和輕鬆地客製化
- IPS、Web、應用程式和流量塑形 (QoS) 政策可以納入防火牆規則，並可以直接編輯，提供一個強大且直覺的模型來設定和管理安全性與控制
- Sophos Security Heartbeat™ 將Sophos 端點與防火牆連接起來，共用健康狀態和遙測功能，以便即時識別出不健康或被入侵的端點
- 動態防火牆規則支援端點健康 (Sophos Security Heartbeat)，可自動隔離或限制被入侵的網路
- 同步應用程式控制功能可以自動識別、分類和控制網路上所有未知的 Mac/Windows 應用程式
- 雲端應用程式可見度可立即啟用影子 IT 探索功能，並提供一鍵流量塑形功能
- 政策測試模擬器工具可根據使用者、IP 和一天中的時間，啟用防火牆規則和 Web 政策模擬與測試
- 使用者威脅商數可根據最近的瀏覽行為和 ATP 觸發器來識別出有風險的使用者
- 適用於 RMM/PSA 所有整合功能的設定 API
- 探索模式 (TAP 模式) 可在試用和 PoC (概念驗證) 時無縫整合，且支援同步安全
- SD-WAN 會連接分散各地的網路的遠端/分公司站台
- 透過一個免費且易於操作的 Windows/Mac 用戶端使用遠端存取 VPN
- 適用於多個防火牆的 Sophos Central 雲端管理和報告功能可進行群組政策管理，以及透過單一主控台管理您的所有 Sophos IT 安全產品
- 輕鬆且經過簡化的設定精靈，可在幾分鐘內快速實現立即可用的部署
- 在 Sophos Central 中零接觸部署和設定新的防火牆

## 基礎防火牆

### 綜合管理

- 針對大型規則集的專屬精簡化使用者介面和防火牆規則管理功能，並使用一目瞭然的規則功能和執行指示器進行分組
- 雙因素驗證 (動態) 可支援系統管理員存取、使用者入口網站、IPSec 和 SSL VPN
- 圖形化使用者介面 (GUI) 中的進階疑難排解工具 (如封包擷取)
- 使用隨插即用的高可用性 (HA) 設定，可支援以主動-主動或主動-被動模式叢集兩部裝置
- 可從 GUI 使用完整的命令列介面 (CLI)

- 以角色為基礎的管理
- 自動韌體更新通知，並具備輕鬆的自動更新程序和回復功能
- 網路、服務、主機、時段、使用者和群組、用戶端和伺服器的可重複使用系統物件定義
- 自助使用者入口網站
- 設定變更追蹤
- 可根據區域對服務進行彈性的裝置存取控制
- 電子郵件或 SNMP Trap 通知選項
- SNMP 和 Netflow 支援
- 透過 Sophos Central 提供中央管理
- 備份與還原設定：可依需要於每日、每週或每月在本機透過 FTP 或電子郵件進行設定
- 第三方整合功能的 API
- 介面重新命名
- Sophos Support 的遠端存取選項
- 透過 MySophos 進行雲端授權管理

## Sophos Central Management

- 適用於多個防火牆的 Sophos Central 雲端管理和報告功能可進行群組政策管理，以及透過單一主控台管理您的所有 Sophos IT 安全產品
- 群組政策管理可一次性修改物件、設定和政策，並自動同步到群組中的所有防火牆
- 工作管理器提供完整的歷史稽核紀錄，以群組政策變更的狀態監視
- Sophos Central 中的備份韌體管理可儲存每個防火牆的最後五個設定備份檔，並可釘選其中一個以便永久保存和易於使用
- 來自 Sophos Central 的韌體更新提供一鍵式韌體更新，可應用於任何裝置
- 零接觸部署可以在 Sophos Central 中執行初始設定，將設定匯出，以便在啟動外部裝置時用快閃磁碟機將設定載入裝置，然後自動將裝置連線回 Sophos Central

## 防火牆、網路和路由

- 狀態式深度封包偵測防火牆
- Xstream 封包處理架構透過以串流為基礎的封包處理，提供超高等級的可見度、保護能力和效能
- Xstream TLS 檢查提供高效能，支援 TLS 1.3 而效能不會降級、不限連接埠、使用企業級政策、擁有獨特的儀表板可見度，以及具備相容性故障排除能力
- Xstream DPI 引擎使用一個高效能引擎，為 IPS、AV、Web、應用程式控制和 TLS 檢查提供串流掃描保護
- Xstream Network Flow FastPath 自動提供以政策驅動的智慧型可信任流量加速
- 以使用者、群組、時間或網路為基礎的政策
- 根據使用者/群組的存取時間政策
- 跨區域、網路或根據服務類型實施政策
- 區域隔離和區域型政策支援。
- 預設區域包含LAN、WAN、DMZ、LOCAL、VPN 及WiFi
- LAN 或 DMZ 上的自訂區域
- 具有 IP 偽裝和全物件支援的可自訂 NAT 政策，可以在單一規則中重新導向或轉發多個服務，只要點擊幾下，即可使用一個方便的 NAT 規則精靈快速且容易地建立複雜的 NAT 規則
- 泛流防護：DoS、DDoS 和連接埠掃描阻擋
- 根據 IP 地理位置阻擋特定國家
- 路由：靜態、多點傳送 (PIM-SM) 和動態 (RIP、BGP、OSPF)
- 上游代理支援
- 採用 IGMP 窺探技術的與通訊協定無關的多點傳送路由
- 橋接 STP 支援和 ARP 廣播轉發
- VLAN DHCP 支援和標記
- VLAN 橋接支援
- 巨大框架 (Jumbo Frame) 支援
- WAN 連結平衡：多重網際網路連線、自動連結健康狀況檢查、自動容錯移轉、自動加權平衡以及精細的多路徑規則
- 無線廣域網路支援 (不含虛擬部署)
- 802.3ad 介面連結彙總
- DNS、DHCP 和 NTP 的完整設定
- 動態 DNS (DDNS)
- IPv6 就緒標誌核可憑證
- IPv6 通道技術支援，包括 6in4、6to4、4in6 和透過 IPSec 的 IPv6 快速部署

## SD-WAN

- 支援多個 WAN 連結選項，包括 VDSL、DSL、纜線，以及具有基本監視、平衡和容錯移轉功能的 3G/4G/LTE 行動數據
- 應用程式路徑選擇和路由，用於確保品質並將 VoIP 等關鍵性應用程式的延遲降至最低
- 同步 SD-WAN 是同步安全的功能之一，可在 Sophos 管理的端點和 Sophos Firewall 之間共用同步應用程式控制資訊時，增加應用程式識別的明確性和可靠性。

- 透過防火牆規則或以政策為基礎的路由，由偏好的連結進行應用程式路由
- 價格合理、彈性，以及零接觸或低接觸的部署
- 健全的 VPN 支援，包括 IPSec 和 SSL VPN
- 集中式 VPN 協調
- 具備路由功能的獨特 RED 第 2 層通道

## 基本流量塑形和配額

- 彈性的網路或使用者型流量塑形 (QoS) (Web Protection 訂閱隨附增強的 Web 和 App 流量塑形選項)
- 針對上傳/下載，或是總流量以及週期性或非週期性，設定以使用者型為基礎的流量配額
- 即時 VoIP 最佳化
- DSCP 標記

## 安全無線

- Sophos 無線存取點 (AP) 採用簡單的即插即用部署 — 自動顯示在防火牆控制中心
- 利用內建的無線控制器集中監控和管理所有存取點 (AP) 和無線用戶端
- 橋接存取點到區域網路、VLAN 或一個具備用戶端隔離選項的單獨區域
- 每個射頻都支援多個 SSID，包括隱藏的 SSID
- 支援多種安全和加密標準，包括 WPA2 個人和 WPA2 企業
- 通道寬度選擇選項
- 透過主要和輔助伺服器支援 IEEE 802.1X (RADIUS 驗證)
- 支援 802.11r (快速轉換)
- 支援無線熱點的 (自訂) 憑單認證、當天密碼認證，或是接受條款和條件的認證
- 具備圍牆花園 (walled garden) 選項的無線訪客網際網路存取
- 以時間為基礎的無線網路存取
- 透過 Sophos 支援的 AP 進行無線中繼和橋接網狀網路模式
- 自動頻道選擇背景最佳化
- 支援 HTTPS 登入

## 驗證

- 同步使用者 ID 利用同步安全功能，在 Sophos 端點和防火牆之間共用目前登入的 Active Directory 使用者 ID，無需使用 AD 伺服器或用戶端上的代理程式
- 透過以下方式進行驗證：Active Directory、e Directory、RADIUS、LDAP 和 TACACS+
- Active Directory 單一登入 (SSO)、STAS、SATC 的伺服器驗證代理程式
- 單一登入：Active directory、eDirectory、RADIUS 帳戶處理
- Windows、Mac OS X、Linux 32/64 的用戶端驗證代理程式
- 瀏覽器 SSO 驗證：透通的代理驗證 (NTLM) 和 Kerberos
- 瀏覽器驗證入口網站
- iOS 和 Android 的驗證憑證
- IPSec、SSL、L2TP、PPTP 的驗證服務
- 對使用 Active Directory 和 Google G Suite 的環境提供 Google Chromebook 驗證支援
- 以 API 為基礎的驗證

## 使用者自助服務入口網站

- 下載 Sophos Authentication Agent (SAA)
- 下載 SSL 遠端存取用戶端 (Windows) 和設定檔 (其他作業系統)
- 熱點存取資訊
- 變更使用者名稱和密碼
- 檢視個人網際網路使用量
- 存取被隔離的郵件和管理使用者的阻止/允許寄件者清單 (需要 Email Protection)

## 基本 VPN 選項

- 站台對站台 VPN：SSL、IPSec、256 位元 AES/3DES、PFS、RSA、X.509 憑證、預共用金鑰
- Sophos RED 站台到站台 VPN 通道 (強大且輕巧)
- L2TP、PPTP
- 以路由為基礎的 VPN
- 遠端存取：SSL、IPsec、iPhone/iPad/Cisco/Android VPN 用戶端支援
- IKEv2 支援
- 透過使用者入口網站下載 Windows SSL 用戶端和設定

## Sophos Connect 用戶端

- 驗證：預共用金鑰 (PSK)、PKI (X.509)、權杖和 XAUTH
- 為遠端連線使用者啟用同步安全和安全心跳
- 智慧型分割通道技術，以最佳化流量路由
- NAT 穿越支援技術
- 用戶端端監視器，以取得連線狀態的圖形化概觀
- 支援 Mac 和 Windows

# Network Protection

## 入侵防禦 (IPS)

- 高效能的新一代 IPS 深度封包偵測引擎，具備可應用在防火牆規則的選擇性 IPS 模式，可實現最佳效能和保護
- 數千種特徵碼
- 精細的類別選擇
- 支援自訂 IPS 特徵碼
- IPS 政策智慧型篩選器可啟用動態政策，可在新模式出現時自動更新

## ATP 和 Security Heartbeat

- 進階型威脅防護 (偵測並阻止嘗試使用多層式 DNS、AFC 和防火牆來聯繫命令控制伺服器的網路流量)
- Sophos Security HeartBeat 會立即識別出受駭的端點，包括主機、使用者、處理序、事件數和被入侵的時間
- Sophos Security Heartbeat 的政策可以限制對網路資源的存取或完全隔離遭駭的系統，直到威脅被清除為止
- 橫向移動防護會讓受 Sophos 管理的健康端點拒絕來自不健康端點的所有流量，進一步隔離被入侵的系統，防止即使是在同一個廣播網域上的威脅移動

## SD-RED 裝置管理

- 集中管理所有 SD-RED 裝置
- 無需設定：自動透過雲端佈建服務進行連線
- 使用數位 X.509 憑證和 AES 256 位元加密的安全加密通道
- 能在不同位置間可靠傳輸所有流量的虛擬乙太網路
- 透過集中定義的 DHCP 和 DNS 伺服器設定進行 IP 位址管理
- 當一段時間沒有活動後，由遠端取消授權 SD-RED 裝置
- 通道流量壓縮
- VLAN 連接埠設定選項

## 無用戶端 VPN

- Sophos 獨特的加密式 HTML5 自助服務入口網站，且支援 RDP、HTTP、HTTPS、SSH、Telnet 和 VNC

# Web 保護

## Web 保護和控制

- 適用於反惡意軟體和 Web 篩選的完全透通代理
- 增強的進階型威脅防護
- URL 篩選器資料庫中有由 SophosLabs 所支援的數百萬個網站，高達 92 種不同的網站類別分類
- 根據使用者/群組的瀏覽配額時間
- 根據使用者/群組的存取時間政策
- 惡意軟體掃描：在 HTTP/S、FTP 和以 Web 為基礎的電子郵件上阻擋所有形式的病毒、Web 惡意軟體、木馬程式和間諜軟體
- 透過 JavaScript 模擬進行進階的 Web 惡意軟體防護
- 可即時從雲端查閱最新的威脅情報以提供即時保護功能
- 透過第二個獨立的惡意軟體偵測引擎 (Avira) 進行雙重掃描
- 即時或批次模式掃描
- 網址嫁接防護
- 可在任何網路或使用者政策中設定 HTTP 和 HTTPS 掃描與強制，並完全可自訂和支援例外情況
- SSL 通訊協定通道偵測和強制
- 憑證驗證
- 高效能網頁內容快取
- 強制快取 Sophos 端點更新
- 透過 MIME 類型、副檔名和主動內容類型 (如 Activex、applet 和 cookies 等) 進行檔案類型篩選
- 根據政策實施 YouTube for Schools (使用者/群組)
- 為主要搜索引擎提供 SafeSearch 功能 (以 DNS 為基礎) (使用者/群組)
- Web 關鍵字的監控和強制功能，可以登錄、報告或阻止符合關鍵字列表的網頁內容，並可選擇上傳自訂清單
- 阻擋可能不需要的應用程式 (PUA)
- 適用於教師或工作人員的 Web 政策複寫選項，允許他們臨時使用特定使用者可完全自訂和管理的被阻止網站或類別
- 在 Google Chromebook 上執行使用者/群組政策

## 雲端應用程式可見度

- 控制中心螢幕工具能顯示上傳和下載到雲端應用程式，並被分類為新的、被核准、未核准或許可的資料量
- 快速找出影子 IT
- 深入取得使用者、流量和資料的詳細資訊
- 一鍵使用流量塑形政策
- 按類別或數量篩選雲端應用程式使用情況
- 詳細且可自訂的雲端應用程式使用情況報告，以用於完整的歷史報告

## 應用程式保護與控制

- 同步應用程式控制功能可以自動識別、分類和控制網路上所有未知的 Windows 和 Mac 應用程式流量，在 Sophos 管理的端點和防火牆中共用資訊
- 利用數千種應用程式的模式，進行以特徵碼為基礎的應用程式控制

- 應用程式可見度和控制以找出影子 IT
- 應用程式控制智慧型篩選器可啟用動態政策，可在新模式出現時自動更新
- 微型應用程式搜尋和控制
- 採用以類別、特徵 (如頻寬和消耗產能)、技術 (如 P2P) 和風險層級為基礎的應用程式控制
- 可根據各使用者或網路規則實施應用程式控制政策

### Web 和應用程式流量塑形

- 增強的流量塑形 (QoS) 選項，可根據網頁類別或應用程式限制或確保上傳/下載的優先性，以及個別或共用的位元速率

## 零時差威脅防護

### 動態的沙箱分析

- 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 (包括 .exe、.com、.dll、.doc、.docx、.docm 和 .rtf 與 PDF)，以及包含上列任何檔案類型的壓縮檔 (包括 ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet)
- 積極的行為、網路和記憶體分析
- 偵測規避沙箱的行為
- 使用深度學習的機器學習技術可掃描所有下載的執行檔
- 包括 Sophos Intercept X 的漏洞利用防禦和 Cryptoguard Protection 技術
- 提供包含螢幕擷取畫面的詳盡惡意檔案報告，並可直接從儀表板釋放分析後的檔案給使用者
- 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

### 靜態威脅情報分析

- 透過 Web 下載或以電子郵件附件進入防火牆，且內含作用程式碼的所有檔案，包括執行檔和有可執行內容的文件 (包括 .exe、.com、.dll、.doc、.docx、.docm 和 .rtf 與 PDF)，以及包含上列任何檔案類型的壓縮檔 (包括 ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet)
- 檔案會對照 SophosLabs 的大量威脅情報資料庫進行檢查，並接受多種機器學習模型的分析，以識別新的和未知的惡意軟體
- 豐富的報告功能，包括用於分析檔案的儀表板桌面工具、分析檔案的詳細列表和分析結果，以及概述每個機器學習模型結果的詳細報告。

## Central 協作

(即將推出)

### SD-WAN 協作

- 透過簡單且自動化的精靈，在網路位置間使用最佳化架構 (星狀、網狀拓撲或部分組合) 建立站台間的 VPN 通道，以進行 SD-WAN 和 VPN 協作。支援 IPSec、SSL 或 RED VPN 通道。與 SD-WAN 功能無縫整合，以便安排應用程式優先性、路由最佳化，並利用多個 WAN 連結來提高彈性和效能。

### Central Firewall Reporting Advanced

- 可用於歷史防火牆報告的 30 天雲端資料儲存，並具備進階功能可保存、排程和匯出自訂報告。

### XDR 和 MTR 連接器

- 已經可以與 Sophos 擴充式威脅偵測和回應 (XDR) 整合，以進行跨產品威脅搜尋和分析
- 支援 Sophos 全天候託管式威脅回應 (MTR) 服務

## 電子郵件保護

### 電子郵件保護和控制

- 使用 SMTP、POP3 和 IMAP 支援進行電子郵件掃描
- 具垃圾郵件疫情監控能力的信譽服務採用專利的循環模式偵測 (Recurrent-Pattern-Detection) 技術
- 在 SMTP 交易期間阻擋垃圾郵件和惡意軟體
- DKIM 和 BATV 反垃圾郵件防護
- 垃圾郵件灰名單和寄件者原則架構 (SPF) 保護
- 進行收件者驗證以防電子郵件地址錯誤
- 透過第二個獨立的惡意軟體偵測引擎 (Avira) 進行雙重掃描
- 可即時從雲端查閱最新的威脅情報以提供即時保護功能
- 自動特徵碼和特徵更新
- 智慧型的主機出站中繼支援
- 檔案類型偵測/阻擋/掃描附件
- 接受、拒絕或丟棄過大的郵件
- 偵測電子郵件中的網路釣魚 URL
- 使用預定義的內容掃描規則，或使用精細的政策選項和例外設定的一組條件建立自訂規則
- 對 SMTP、POP 以及 IMAP 的 TLS 加密支援
- 自動對所有外寄郵件附加簽名檔
- 電子郵件封存
- 透過使用者入口網站，進行以個別使用者為基礎的阻擋，以及維護允許的寄件者清單

### 電子郵件隔離管理

- 垃圾郵件隔離摘要和通知選項
- 可根據日期、寄件者、收件者、主旨當成搜尋與篩選選項，以隔離惡意軟體和垃圾郵件，並可依需要釋放和刪除郵件
- 自助服務使用者入口網站可檢視和釋放被隔離的郵件

### 電子郵件加密與 DLP

- 提供獨家 SPX 加密技術，可用以保護外寄的郵件訊息
- 收件者自我註冊的 SPX 密碼管理
- 將附件新增到 SPX 安全回覆中
- 完全透通，不需要額外安裝用戶端軟體
- DLP 引擎可自動掃描電子郵件和包含敏感資料的附件
- 適用於 PII、PCI、HIPAA 等的預封裝敏感資料類型內容控制清單 (CCL)，該清單由 SophosLabs 所維護

## Web 伺服器保護

### Web 應用程式防火牆保護

- 反向代理
- URL 強化引擎，具備深度連結和目錄跨越防禦功能
- 表單強化引擎
- SQL 插入防護
- 跨站台指令碼保護
- 雙防毒引擎 (Sophos 與 Avira)
- HTTPS (TLS/SSL) 加密卸載
- 使用數位簽章的 Cookies 簽章
- 以路徑為基礎的路由
- Outlook Anywhere 通訊協定支援
- 反向驗證 (卸載)，在存取伺服器時可用於以表單為基礎和基本的驗證
- 虛擬伺服器和實體伺服器抽象
- 整合式負載平衡器可將訪客分配到多台伺服器
- 可根據需要以精細的方式略過個人檢查
- 符合來源網路或指定目標網址的請求
- 支援 AND/OR 邏輯運算式
- 輔助各種設定和非標準部署的兼容性
- 變更 Web 應用程式防火牆效能參數的選項
- 掃描大小限制選項
- 允許/阻止 IP 範圍
- 伺服器路徑和網域支援萬用字元
- 自動附加用於驗證的前置詞/後置詞

## 報告功能

### Central Firewall Reporting

- 具備彈性自訂選項的預定義報告
- Sophos Firewall 報告功能—硬體、軟體、虛擬和雲端
- 直覺的使用者介面提供資料的圖形化表示
- 報告儀表板提供過去 24 小時的事件總覽
- 輕鬆掌握網路活動、趨勢和可疑的攻擊
- 輕鬆備份日誌並提供快速檢索，以供稽核之用
- 簡化的部署，無需技術專業

### Central Firewall Reporting Advanced

- 多防火牆彙整報告
- 保存自訂報告範本
- 排程報告功能
- 以 PDF、CFV 或 HTML 格式匯出報告
- 最多一年的資料儲存 (單一防火牆)
- MTR/XDR 連接器

### 內建的報告功能

**注意：Sophos Firewall 報告功能是免費的，但可用的日誌、報告和桌面工具取決於各自的保護模組授權。**

- 數百個立即可用的報告和自訂報告選項：儀表板 (流量、安全和使用者威脅商數)、應用程式 (應用程式風險、已封鎖應用程式、已同步應用程式、搜尋引擎、Web 伺服器、Web 關鍵字比對、FTP)、網路和威脅 (IPS、ATP、無線、Security Heartbeat、Sandstorm)、VPN、電子郵件、合規性 (HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3 和 CIPA)
- 目前活動監控：系統健康狀態、當前使用者、IPSec 連線、遠端使用者、有效連線、無線用戶端、隔離和 DoS 攻擊
- 報告匿名
- 透過具彈性頻率選項的報告群組，排程發送報告給多個收件者
- 匯出報告成 HTML、PDF、Excel (XLS)
- 報告書籤
- 根據類別自訂日誌的保留功能
- 具有行檢視和詳細檢視的全功能日誌檢視器，提供強大的篩選器和搜尋選項、包含超連結的規則 ID，以及資料檢視自訂功能

# Sophos Firewall 功能摘要 (依訂閱)

| | Xstream Protection 搭售套件 | | | | | 單獨購買 | | |
|---|---|---|---|---|---|---|---|---|
| | Standard Protection 搭售套件： | | | 單獨購買 | | | | |
| | 基礎防火牆 | 網路保護 | Web 保護 | 零時差威脅防護 | Central 協作* | Central Firewall Reporting Advanced | 電子郵件保護 | Web 伺服器保護 |
| 綜合管理 (包括 HA) | ● | | | | | | | |
| Xstream 架構 | ● | | | | | | | |
| 防火牆、網路和路由 | ● | | | | | | | |
| 基本流量塑形和配額 | ● | | | | | | | |
| 安全無線 | ● | | | | | | | |
| 驗證 | ● | | | | | | | |
| 自我服務的使用者入口網站 | ● | | | | | | | |
| 基本 VPN 選項 | ● | | | | | | | |
| RED 站台對站台 VPN | ● | | | | | | | |
| Sophos Connect VPN 用戶端 | ● | | | | | | | |
| 入侵防禦 (IPS) | | ● | | | | | | |
| ATP 和 Security Heartbeat™ | | ● | | | | | | |
| SD-RED 裝置管理 | | ● | | | | | | |
| 無用戶端 VPN | | ● | | | | | | |
| 同步應用程式控制 | | | ● | | | | | |
| Web 保護和控制 | | | ● | | | | | |
| 應用程式保護與控制 | | | ● | | | | | |
| 雲端應用程式可見度 | | | ● | | | | | |
| Web 和應用程式流量塑形 | | | ● | | | | | |
| 動態沙箱分析 | | | | ● | | | | |
| 威脅情報分析 | | | | ● | | | | |
| SD-WAN 協作 | | | | | ● | | | |
| Central Firewall Reporting 資料 | 7 天 | | | | 30 天 | 最多一年 | | |
| Central Firewall Reporting Advanced 功能 | | | | | ● | ● | | |
| XDR 和 MTR 連接器 | | | | | ● | ● | | |
| 電子郵件保護和控制 | | | | | | | ● | |
| 電子郵件隔離管理 | | | | | | | ● | |
| 電子郵件加密與 DLP | | | | | | | ● | |
| Web 應用程式防火牆保護 | | | | | | | | ● |
| 記錄和報告 | ● | ● | ● | ● | ● | ● | ● | ● |
| Sophos Central 管理 | ● | ● | ● | ● | ● | ● | ● | ● |

*即將推出

請注意：

- XGS 87 和 XG 86 型號不支援某些功能，包括立即可用的報告、雙防毒掃描、WAF 防毒掃描和電子郵件傳輸代理(MTA) 功能
- MSP 授權選項與上述內容略有不同
- 如需 XG 系列硬體/虛擬授權的資訊，請參見 www.sophos.com/compare-xg 的手冊。

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com



21-04-09 FL-ZHTW (PC)

SOPHOS