

Sophos Workspace Protection

為遠端及混合辦公員工提供簡易且經濟實惠的防護方案

Sophos Workspace Protection 讓您重新掌控公司工作環境。安全存取您的應用程式、資料、員工與訪客 —— 隨時隨地，輕鬆便捷，經濟實惠。

人們的工作方式已經改變

網路邊界已不復存在，員工、應用程式與數據遍佈任何地方。您擁有自行架設的私有應用程式，或租用的 SaaS 應用程式，而每個人都依賴著網路上每日使用的應用程式、服務與網站。大多數組織都擁有駐點員工、與遠端或行動工作者的混合辦公人力資源，他們可能身處辦公室、家中、在途中，甚至在公共場所工作。這一切加起來，對任何組織而言，要妥善對其監察、管控與保障安全，都構成了極其艱鉅的挑戰。

傳統的雲端交付式 SASE 或 SSE 解決方案的營運成本高昂，因此購置成本相當昂貴。這些方案需要將流量回傳至雲端節點進行檢查，並執行中間人解密操作，這不僅增加不必要的延遲，更導致使用體驗問題。一定有更好的方法 —— 所幸有 Sophos Workspace Protection。

保護您的應用程式、資料、作業及訪客

Sophos Workspace Protection 提供簡易且經濟實惠的解決方案，全面保護您的應用程式、資料、員工及訪客 —— 無論身處何地。它透過單一應用程式反和瀏覽器來整合您所需的所有防護功能，因此無需回傳流量、雲端處理、額外解密 —— 只有透明且安全的體驗。

您可以獲得

Sophos Protected Browser

提供單一應用程式以為保護您的所有其他應用程式。它將 ZTNA、DNS 防護、SaaS 應用程式控制、安全 web 閘道器及本地資料控制整合至強化版 Chromium 瀏覽器中，操作體驗熟悉且完全透明。

Sophos ZTNA

僅向使用者所需應用程式提供安全存取權限，同時使這些應用程式對其他人（包括外部世界）保持隱形，從而保護其免受攻擊。

Sophos DNS Protection for Endpoint

無論員工身處何地，為瀏覽器及支援 web 的應用程式增添額外的安全防護層，以防範惡意與不受歡迎的 web 內容。

Sophos Email Monitoring System

與您現有的電子郵件解決方案協同運作，以強化安全性與可視性，以及補足其他解決方案未能偵測的進階郵件威脅的報告功能。

產品優點

- 保護您的應用程式、資料、員工與訪客。
- 在保護應用程式免受攻擊的同時，提供對其的安全存取權限。
- 消除影子 IT，安全地採用 Generative AI (生成式人工智慧) 等新興技術。
- 保護網路上的員工並執行安全瀏覽政策。
- 輕鬆保障訪客、併購團隊成員或其他需要臨時存取權限的人員。
- 將 Synchronized Security 同步安全能力擴展至遠端及混合辦公員工。
- 防範攻擊與入侵



Sophos Workspace Protection 所能提供



消除影子 IT 行為：
監察與控制未經授權的 web 及 SaaS 應用程式的使用行為。



便於生成式人工智慧的採用：
推廣並監控您核准的 AI 解決方案，控制存取權限，並限制資料移動。



保護網路上的員工：
為 web 應用程式執行一致的政策，並實現何時何地的存取。



防止造成高昂的數據失誤：
禁止複製貼上，或與網站及應用程式交換敏感資料，以防止資料外洩疏失。



保護您的應用程式：
為您自行託管的應用程式提供安全存取管道，同時使其對外界隱形



安全訪客存取：
輕鬆為訪客、承包商或併購人員啟用對應用程式與系統的存取權限



擴展 Synchronized Security 的覆蓋：
運用 Sophos Synchronized Security 解決方案以暫時阻止遭入侵的裝置存取重要應用程式與系統



防範安全漏洞：
保護您的網路免受潛在入侵威脅（可能源自暴露於網際網路的系統、應用程式及員工）



提升您的電子郵件安全性：
透過補強您現有防禦的額外安全防護層，來強化您的電子郵件安全狀態

簡單、經濟實惠、安全可靠

Sophos Workspace Protection 比雲端交付的 SASE 或 SSE 解決方案更簡便且更經濟實惠，無需回傳或中間人解密，部署與擴展皆輕鬆無虞。您將獲得一個您早已需要的簡易應用程式——一個瀏覽器——它能保護您所有的其他應用程式，全都透過單一雲端控制台管理：Sophos Central。Sophos Protected Browser 將原本的安全漏洞轉化為堅固的安全資產。

整合並擴展您的防火牆與端點防護

防火牆保護您的網路，而端點保護您的裝置，Sophos Workspace Protection 則保護所有其他：您的應用程式、資料、員工以及訪客。它整合並擴展您的網路與端點防護方案，以保障工作空間的安全。它還能與 Sophos Firewall 和 Sophos Endpoint 更有效地協同運作，將 Synchronized Security Heartbeat 功能擴展至您的遠端及混合辦公員工。若裝置遭到入侵，Heartbeat 政策可阻止其連接到重要應用程式和資料，直至其完成清理為止。

簡單授權模式 — 物有所值

購買 Sophos Workspace Protection 再簡單不過，採用簡便的用戶授權模式並有極具吸引力的價格：

- **獨立式：**購買 Sophos Workspace Protection 獨立版，您可獲得完整解決方案，包含 Sophos Protected Browser、Sophos ZTNA、Sophos DNS Protection for Endpoints，以及可與任何防火牆或端點解決方案配合使用的 Sophos EMS。
- **與 Sophos Endpoint 搭配購買：**便捷的搭售組合讓您輕鬆地同時採購這兩款產品。兩者透過 Synchronized Security 更高效地協同運作，並皆由 Sophos Central 進行管理。
- **與 Sophos Firewall 搭配購買：**將網路安全延伸至遠端、混合辦公員工及訪客，透過 ZTNA 保護應用程式等等——全透過 Sophos Central 集中管理。

Sophos Workspace Protection 是任何現有或新部署的 Sophos 解決方案的完美強化方案。

技術規格

Sophos Workspace Protection 產品旨在無縫融入至您的現有環境，並與最主流身分識別提供商及平台整合。

身分識別提供商

ZTNA 與 Endpoint DNS Protection :

Microsoft Active Directory (本地部署版)、Microsoft Entra ID (Azure Active Directory)、Okta

受保護的瀏覽器

Microsoft Entra ID (Azure Active Directory)、Okta

作業系統與平台：

ZTNA 閘道 **：

VMware ESXi 7+、Hyper-V 2016+ 及 Sophos Firewall

ZTNA 代理程式：

Windows 10、Windows 11 (Intel 與 ARM 處理器)；macOS Sonoma、Sequoia、Tahoe (Intel 與 Apple 處理器)

Endpoint DNS Protection：

Windows 10、Windows 11 (Intel 與 ARM 處理器)

受保護的瀏覽器：

Windows 10、Windows 11、Windows Server 2022、Windows Server 2025 (僅限 Intel 處理器 — ARM 版本即將推出)；macOS Sonoma、Sequoia、Tahoe (Intel 與 Apple 處理器)

裝置狀態：

ZTNA 代理程式：

Sophos Security Heartbeat (Sophos Endpoint)

受保護的瀏覽器：

作業系統、Endpoint Protection (Sophos 及其他廠商) 與磁碟加密狀態

ZTNA 閘道器規格

推薦的 VM 虛擬機器：

2 核心 /4GB

多節點叢集：

虛擬機器可組成最多 9 個節點的叢集，Sophos Firewall 可部署於 HA 高可用性環境，以提升網關效能、擴充容量並確保業務連續性。

節點容量和擴展：

一個節點 10,000 個用戶端，一個叢集最多可達 90,000 個用戶端 (最多 9 個節點)

了解更多資訊並開始您的免費試用：sophos.com/Workspace Protection