

VMware Cloud Web Security

vmware®

Cloud Web Security™

簡介

VMware Cloud Web Security™ 是一項雲端代管服務，可保護存取軟體即服務與網際網路應用程式的使用者和基礎架構不受到瞬息萬變的威脅態勢影響。使用者存取軟體即服務應用程式時，這款解決方案會為 IT 團隊提供能見度與控制能力，並確保合規。Cloud Web Security 是透過 VMware SASE PoP 的全球網路進行交付，藉此確保能以最佳方式存取應用程式。

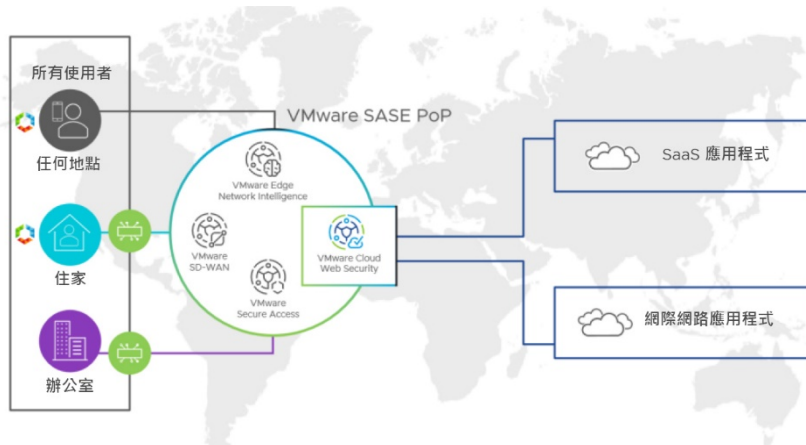


圖 1：VMware Cloud Web Security 可保護存取網頁應用程式的使用者流量。

VMware Cloud Web Security 優勢

敏捷的安全態勢

VMware Cloud Web Security 讓企業資安團隊可針對瞬息萬變的威脅態勢和業務需求進行調整，使其安全態勢不會出現落差。這款雲端式解決方案會利用有關新發現病毒碼的最新威脅情報，或網站分類的更新資訊，協助縮小攻擊範圍。而隨著企業採用的軟體即服務與網際網路應用程式數量漸增，VMware Cloud Web Security 也有助於消弭地端應用裝置所帶來的規模挑戰。這款解決方案能提供可運用的洞悉見解，以實現更嚴謹的安全態勢。

為隨處辦公提供順暢的安全性

使用 VMware Cloud Web Security，讓使用者無論位於分公司、遠端據點、住家或出門在外，都能根據身分識別、情境、原則和應用程式目的地，以最佳方式安全地直接存取網際網路與軟體即服務應用程式。這款解決方案使用安全存取服務邊緣網路連接點 (PoP) 的全球網路，因此可提升使用者的安全性，同時確保使用者能更輕鬆存取其應用程式。

簡化作業

VMware Cloud Web Security 提供單一管理介面與經過整合的後端作業，能在高彈性的雲端基礎架構上為各種規模的客戶提供易於部署且立即可用的解決方案。

降低營運成本

針對軟體即服務與網際網路應用程式，雲端式解決方案可減少其對地端安全性應用裝置的需求。VMware Cloud Web Security 讓您在資料中心管理實體或虛擬應用裝置的生命週期，當安全服務分配到較接近使用者的位置時，也可選擇在分公司據點進行管理，從而節省成本。

VMware Cloud Web Security 獨一無二的優勢

透過整合式服務交付帶來豐富的使用者體驗和更高的生產力

VMware 的安全存取服務邊緣網路連接點全球網路可確保 SSL 解密、安全性檢查和相關施行作業等安全功能，都是在使用者和應用程式之間的最佳路徑上大規模執行。如此一來，就能藉由避免流量回傳至資料中心來減少延遲並降低成本，同時還可免除網路與安全服務的多躍點處理作業，進而提高生產力。

使用雲端規模平台交付服務，實現在地服務

VMware Cloud Web Security 使用經業界實證且支援 VMware SASE™ 的部署架構進行交付，以協助客戶輕鬆靈活地採用安全服務。客戶可更快部署安全服務、加速從地端移轉至雲端安全服務、確保符合地方法規，並獲得對應用程式和員工活動的能見度。VMware SASE PoP 的全球網路可在更靠近使用者的位置，也就是在通向軟體即服務與網際網路應用程式目的地的最佳路徑上管理安全性。

單一管理介面

安全性原則和應用程式原則之間順暢配合，可確保一致的安全性施行。集中化的 Orchestrator 提供單一介面，能以融合式堆疊來管理安全服務和網路服務。Orchestrator 支援角色型存取控制 (RBAC)，可在網路與資安團隊之間提供管理區隔。這有助於資安團隊設定安全性原則，供網路團隊指派給適用於應用程式流量的業務原則。IT 不必使用互不相通的管理工具來設定原則。透過集中化的原則入口網站，IT 就能管理分散式企業中的安全性，而不會出現任何盲點。網路營運、安全營運、CSO、CIO 與合規團隊可對網路效能和安全態勢享有共通且一致的能見度。

使用情境

控制網頁存取

VMware Cloud Web Security 可確保只有獲授權的使用者能存取軟體即服務與國際網路應用程式，並施行原則，讓使用者在任何地點都能安全瀏覽。網站會根據風險進行分類，例如已知的惡意軟體和網路釣魚網站，以及賭博或鼓吹暴力等行為。安全性管理員可限制暴露於攻擊範圍、讓安全態勢更為嚴謹，並確保符合組織的可接受使用原則 (AUP)。

防範來自文件下載與電子郵件附件的攻擊

VMware Cloud Web Security 使用最新的威脅情報，確保使用者與基礎架構皆受到保護，不會遭到已知病毒的惡意軟體攻擊。這款解決方案支援在完備環境中檢查檔案行為的沙箱，藉此抵禦惡意軟體的零時差攻擊。員工可安全地下載文件、存取電子郵件與開啟附件，不會成為網路釣魚或勒索軟體攻擊的目標。

對軟體即服務應用程式的能見度和控制能力

有了 VMware Cloud Web Security，IT 可在使用者存取軟體即服務應用程式時掌握使用者活動。這款解決方案運用內嵌的雲端存取安全性代理程式 (CASB) 功能，根據應用程式類型協助針對使用者可採取的不同動作設定原則。舉例來說，IT 可以決定讓全職員工擁有 Box、Dropbox 等檔案類型應用程式的登入存取權限、下載存取權限或上傳存取權限，但暑期實習生無法下載檔案。此外，這款解決方案也可在員工在企業和社交應用程式之間切換瀏覽時，提供控制能力和安全性。例如，允許使用者從 Dropbox 下載檔案，但不允許他們在 LinkedIn 電子郵件中附加任何檔案。

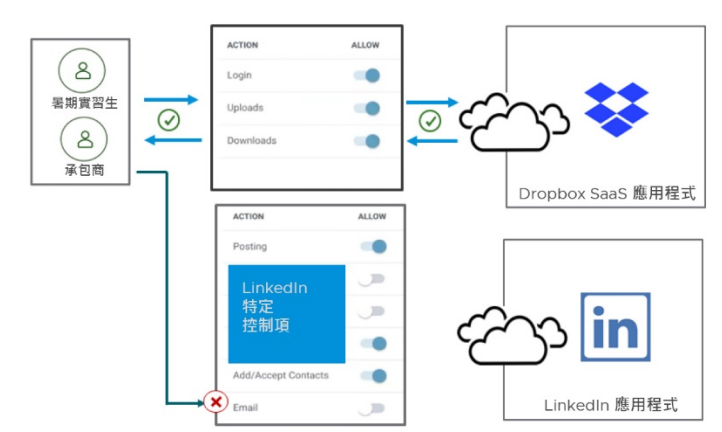


圖 2：適用於企業和社交應用程式的精密控制能力

保護敏感資料，確保合規

VMware Cloud Web Security 可防止敏感資料從企業環境流出。這款解決方案會監控、偵測、封鎖及回報資料暴露狀況，並協助許多產業因應合規需求，包括醫療照護、零售、金融、製造、政府單位、公用事業、交通運輸和服務業等等。擁有單一管理介面可大幅降低複雜性並提供共通的檢視畫面，方便網路、安全性和合規等多個營運團隊之間進行溝通，讓作業更為順暢。

VMware Cloud Web Security 功能

URL 篩選

Cloud Web Security 可限定使用者與特定類別的網站互動，並以精密的原則透過使用者、使用者群組或 IP 來控制員工的網頁瀏覽。這款解決方案能協助使用者防範會散佈惡意軟體、竊取資訊或代管不當內容的網站。

內容篩選

這款解決方案讓資安團隊能夠指定可上傳或下載的內容類型，進而縮小攻擊範圍。內容篩選規則可套用至執行檔、檔案、文件和存檔。比方說，IT 可允許下載 PDF、Word 文件、Zip 檔案和 PowerPoint 文件，但禁止下載 Linux 和 Windows 執行檔。

內容檢查 (反惡意軟體、防毒) 與沙箱

VMware Cloud Web Security 能保護使用者和基礎架構不受使用中網站、文件與電子郵件附件內的惡意軟體內容影響。這款解決方案可防範已知病毒與零時差惡意軟體的攻擊。

雲端存取安全性代理程式 (CASB)

IT 管理員需要能掌握及控制企業正在使用的已批准和未批准應用程式。VMware Cloud Web Security 會針對使用者存取的軟體即服務與網頁應用程式提供能見度和控制能力。這款解決方案協助 IT 管理員決定使用者可存取哪些應用程式，以及他們可透過這些應用程式執行什麼活動。這款解決方案不僅提供適用於所有應用程式的一般控制項，也提供指定應用程式特定控制項的彈性。

資料外洩防護 (DLP)

資料外洩防護協助 IT 確保敏感資料不會從企業周邊流出。DLP 有助於企業遵守合規需求，例如 HIPAA、PCI、GDPR 和其他資料隱私權法律。VMware Cloud Web Security 會檢查內容、偵測敏感資料是否暴露、依據原則進行封鎖或監控，並提供詳細的稽核記錄。這款解決方案具備豐富的字典，收錄被識別為敏感資訊的資料，並提供彈性來建立自訂定義。解決方案會使用這個資料字典，依據檔案類型、規則運算式或設定的資料類型，找出被視為性質敏感的資料類型。稽核記錄包括使用者、外流資料、時間戳記、目的地網域、檔案類型、檔案名稱和已採取的行動等相關資訊。

分析與安全性儀錶板

安全性管理員需要能掌握每個使用者的網頁瀏覽活動。VMware Cloud Web Security 會記錄每個工作階段，以及偵測到的每個威脅。

諸如使用者 ID、使用的瀏覽器、發現的威脅、威脅來源、有弱點的網站和威脅類型等詳細資訊，都有助於資安和鑑識團隊分析並調整安全態勢。安全性儀錶板可針對使用者活動與威脅態勢提供一致的能見度，並協助管理員降低曝險。客戶也可使用 API 將日誌記錄提取至外部 SIEM 工具。

SSL Proxy

有極高比例的網頁應用程式都經過 SSL 加密，因此需要解密流量並檢查內容，以提高安全性。Cloud Web Security 可解決因流量增加、支援新應用程式和引進新加密法所產生的相關需求。Cloud Web Security 運用 VMware SASE PoP 的全球網路來提供可延展的解決方案，解密不斷增加且龐大的網頁應用程式流量。這款解決方案也可在使用者存取個人財務或醫療照護網站時協助企業略過 SSL 解密，或協助企業遵守當地隱私權法律。

使用者與使用者群組原則、驗證

這款解決方案能讓管理員針對特定使用者、使用者群組和內容類型 (所有內容、有風險的內容、未分類的內容) 設定並管理原則。管理員也能對使用者、使用者群組和內容類型建立例外原則。Cloud Web Security 支援 SAML，可與 SSO 和 IAM 解決方案整合來進行使用者驗證。

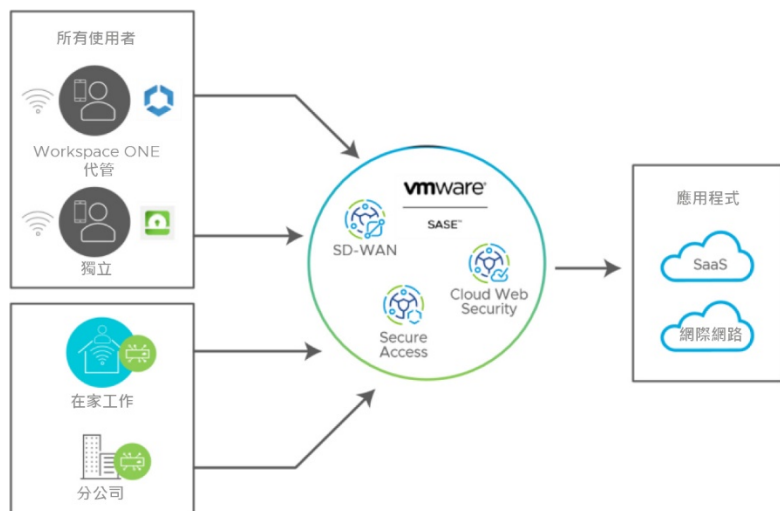


圖 3：VMware Cloud Web Security 可保護在在家、辦公室與任何地點工作的使用者

部署選項

VMware Cloud Web Security 可搭配下列其中一種選項部署：

- **VMware SD-WAN™**：當位於分公司、校園、辦公室或住家的使用者存取軟體即服務與網際網路應用程式時，可針對經由 VMware SD-WAN 層疊網路傳輸的流量管理安全性。
- **VMware Secure Access™**：企業可為其遠端與行動員工部署 VMware Secure Access，並在使用者存取軟體即服務與網際網路應用程式時透過 VMware Cloud Web Security 保護他們。
- **VMware SD-WAN 與 VMware Secure Access**：無論員工位於辦公室或住家，注重員工生產力的企業都能享有彈性，可搭配 VMware SD-WAN 與 VMware Secure Access 來部署 VMware Cloud Web Security。

授權

客戶擁有彈性選項，可根據使用者數量或站點頻寬來購買 Cloud Web Security。解決方案能以 1 年、3 年或 5 年期訂閱方案的形式購買。購買 Cloud Web Security 需要 VMware SD-WAN 或 VMware Secure Access。解決方案備有 Standard 或 Advanced 訂閱版本可購買。

Standard 授權為有意控制網頁存取權限、確保威脅防護和取得軟體即服務應用程式能見度的客戶提供分層式防禦。

Advanced 授權包含 Standard 版本中提供的所有功能，並進一步加強安全態勢。此版本支援進階沙箱功能，可協助 IT 管理員決定使用者可透過軟體即服務應用程式採取什麼動作，並防止敏感資料從企業環境流出。

Standard 授權	Advanced 授權
SSL 檢查	Standard 授權的所有功能
URL 篩選	進階沙箱*
防毒 (惡意軟體) 防護	雲端存取安全性代理程式 (CASB) 控制
基本沙箱*	資料外洩防護 (DLP) 能見度與控制
雲端存取安全性代理程式 (CASB) 能見度	
SIEM 日誌記錄	

*詳情請參閱下表。

其他詳細資訊

VMware Cloud Web Security 支援 SAML 第 2 版，以連接至身分識別供應商，且 SSL Proxy 支援 TLS 1.2。VMware Cloud Web Security 可透過頻寬式授權或使用者式授權進行購買。

深入瞭解

- VMware SASE : sase.vmware.com
- VMware SD-WAN : sase.vmware.com/sd-wan
- VMware Secure Access : sase.vmware.com/products/vmware-secure-access

		基本沙箱	進階沙箱
文件類型	工程應用程式		✓
	生產力應用程式		✓
	文書處理器		✓
	試算表		✓
	簡報工具		✓
檔案類型	指令碼與執行檔	✓	✓
	存檔與壓縮的套件	✓	✓
	多媒體		✓
	行事曆		✓