VMware Cloud Web Security

vmware
Cloud Web Security™

VMware Cloud Web Security 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
- 使用雲端規模平台交付服務，實現在地服務
- 單一管理介面
- 為任何地點的使用者提供全面的安全保障

常見使用情境

- 提供在任何地點都能安全瀏覽的網頁安全性
- 電子郵件和文件下載防護
- 透過個別應用程式原則，實現軟體即服務應用程式的能見度和控制力
- 確保合規，同時降低複雜性並提供共通的管理檢視方式

VMware Cloud Web Security™ 是雲端代管服務，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免受威脅，提供能見度和控制力，並確保合規。

企業採用軟體即服務和網際網路應用程式的情況正大幅增加。不過，如 Microsoft 365 等 IT 批准的應用程式在整體現狀中僅佔少數。許多業務線和員工使用的軟體即服務和網際網路應用程式，並未得到 IT 的同意或管理。

雖然這些應用程式對業務生產力來說很重要，但也會帶來風險，因為幾乎不受 IT 監督。風險包括進階威脅、惡意軟體，以及意外或故意洩露資料。根據 Verizon 的《2021 年資料漏洞調查報告》(2021 Data Breach Investigations Report)[1]，約 85% 的漏洞都牽涉到人為因素。

隨著用戶自攜裝置 (BYOD) 方案和物聯網裝置的應用逐漸增加，網路上的異質性和數位連結的裝置數量成長十分可觀，也增加了潛在的攻擊範圍。

傳統的企業網路周邊幾乎已經消失。使用者預期隨時隨地在任何裝置上存取企業應用程式時，都能享有安全和順暢的經驗。此外，員工想要在企業和個人應用程式之間切換，特別是在用戶自攜裝置上，而不必擔心安全性威脅或害怕不合規。IT 團隊則想要確保能透過不致阻礙員工生產力的方式，來保護使用者和基礎架構。

傳統安全性機制與現代化應用程式互不相容

傳統網頁安全性解決方案缺少彈性，難以因應應用程式和個人化網站靈活且依情境變化的特性。這些地端部署的解決方案因為採用並非最佳的路由而導致不必要的延遲，增加廣域網路成本，並造成不良的使用者體驗。

[1]《Verizon 資料漏洞調查報告》(Verizon Data Breach Investigations Report)：https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf

多數網際網路和軟體即服務應用程式經過加密，需要更深入的檢查。由於應用程式採用較新的加密方式，或是使用者採用較新的應用程式，因此應用裝置型解決方案缺少檢查加密應用程式流量所需的延展性。缺少對於這些應用程式的能見度和控制力，為 IT 團隊帶來巨大的負擔，因為 IT 團隊必須評估風險、安全性、隱私權、合規及其他因素才能判斷這些應用程式是否能安全使用。

企業的應用程式安全性缺點包括：

- **安全性大打折扣**：根據 CVE Details 資料庫[2]，已知關鍵弱點有 16,000 個以上。採用修補安全性功能的方式，將導致暴露於多種樣態的威脅中且無法即時因應。這種方式缺少一致的能見度和控制力，限縮使安全態勢更為嚴謹的能力，難以因應變化萬千的威脅情勢及日益廣泛的攻擊範圍。將安全服務和網路服務作為各自獨立的堆疊來部署，可能會導致難以將安全性原則轉換成網路原則。如此也可能造成原則的實作依使用者的位置而有所不同，使用者可能在家中、辦公室或任何其他地點工作，進而影響使用者體驗。
- **缺少靈活性**：隨著大多數的網頁應用程式使用 HTTPS 通訊協定，越來越多的流量需要進行解密，擴充的需求也持續增長。傳統的應用裝置型安全性機制面臨擴充的挑戰，並且缺少因應新興業務需求的靈活性。使用虛擬應用裝置的部署項目會定期升級，需要大量規劃和停機時間。
- **複雜性增加與成本提高**：部署在資料中心以及選擇性分散在邊緣的安全性功能，為 IT 帶來管理上的挑戰。一部分原因是大量實體和虛擬應用裝置的生命週期與更新週期管理起來相當複雜，對設計與營運可靠分散式安全性應用裝置系統的需求更是提高了總持有成本。將軟體即服務和網際網路流量先回傳至資料中心，然後才傳送至雲端目的地，會提高頻寬用量並增加不必要的 MPLS 連結成本。
- **隨處辦公使用者體驗不良**：隨處辦公的員工需要能夠順暢安全地存取所有應用程式，不必為了落實資料中心安全性而不得不進入企業網路。這類回傳流量會造成延遲，導致使用者在不同位置產生不一致的使用者體驗，並且大幅降低生產力。

[2] Common Vulnerability and Exposure Details：https://www.cvedetails.com

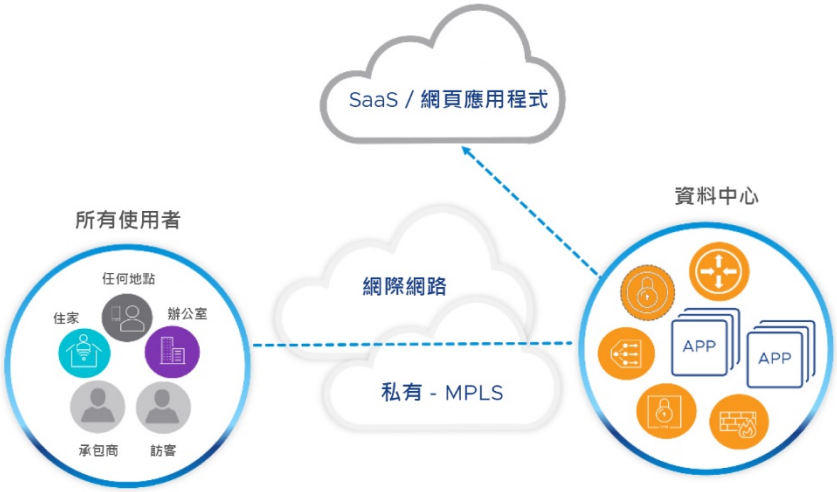

圖 1：回傳軟體即服務流量的地端安全性機制會增加成本並影響生產力

由於缺乏更好的選項，企業安全性團隊為了因應變化萬千的威脅情勢，只能擴展傳統安全性解決方案的修補工作。這些解決方案很難整合與管理，在安全性機制的實作中留下盲點。資安人員需要的解決方案要能在員工使用批准和未批准的軟體即服務應用程式時保護使用者和基礎架構，讓使用者可隨處存取應用程式，並提供能見度和控制力。

VMware Cloud Web Security 簡介

VMware Cloud Web Security 是雲端代管服務，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，免受變化萬千的威脅情勢影響，提供能見度和控制力並確保合規。Cloud Web Security 包含於 VMware SASE (安全存取服務邊緣) 當中，透過 VMware SASE 網路連接點 (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。

Cloud Web Security 可擴展 VMware SD-WAN 和 VMware Secure Access 所提供可靠有效率服務的優勢，為位在各處的使用者連上軟體即服務和網際網路應用程式，並以最佳路徑落實安全性。

VMware Cloud Web Security 提供以下獨特優勢：

- **豐富的使用者體驗、更高的生產力與整合式服務交付**：VMware SASE PoP 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執行。免除網路與安全服務的多躍點處理作業，減少延遲、頻寬用量和成本，最終有助於提高生產力。
- **使用雲端規模平台交付服務，實現在地服務**：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。客戶可更快速地部署安全服務，消除從地端移轉至雲端安全服務的阻礙，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。

- **單一管理介面**：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。IT 不必使用互不相通的管理工具來設定原則。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。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 與合規團隊可針對網路效能和安全態勢，享有共通且一致的能見度。

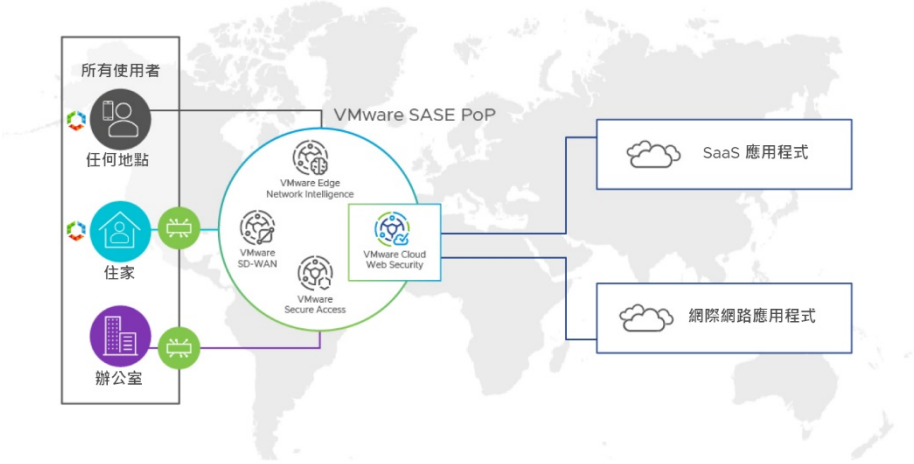

圖 2：為隨處辦公提供全面的安全保障

- **為任何地點的使用者提供全面的安全保障**：VMware Cloud Web Security 為任何類型的使用者提供全方位的安全保障，包括身處任何地點的進階使用者和輕度使用者。由於安全性原則將隨著使用者移動，不論使用者身在何處，Cloud Web Security 都會套用一致的原則，為分散式的隨處辦公提供順暢的經驗。

解決有關靈活性、使用者體驗等問題

Cloud Web Security 可以協助處理企業 IT 團隊每天遇到的問題，包括：

- **靈活的安全態勢**：Cloud Web Security 讓企業資安團隊針對瞬息萬變的威脅情勢和業務需求進行調整，使其安全態勢不會出現落差。雲端代管的解決方案可因應支援新加密方式、新應用程式及流量成長的需求而擴充，隨著日新月異的業務環境進行調整。雲端式解決方案會分析和提供可運用的洞悉見解，使安全態勢更為嚴謹。
- **為隨處辦公提供順暢且安全的存取**：Cloud Web Security 根據身分識別、情境、原則和應用程式目的地，無論使用者是在辦公室或居家辦公，都套用一致的原則，如此可消除依使用者位置管理多組原則的需求。這款解決方案使用 SASE PoP 的全球網路，可提升使用者的安全性，同時確保使用者能夠輕鬆存取自己的應用程式。

- **簡化的作業**：Cloud Web Security 提供設定安全性機制和網路原則的單一管理介面。IT 使用 VMware SD-WAN Orchestrator 確保安全性原則部署於整個網路，提供一致的體驗，而不致有原則實作上的差異。網路與安全性團隊可用共通的檢視方式來查看網路狀態和安全態勢，著重處理業務需求，而非花時間解讀來自多個管理解決方案的資料。
- **降低營運成本**：Cloud Web Security 可針對軟體即服務與網際網路應用程式，減少對地端安全性應用裝置的需求。這項解決方案讓您可在資料中心管理實體或虛擬應用裝置的生命週期和更新，進而節省成本，也可在安全服務受分配於更接近使用者的位置時，選擇在分公司據點進行管理。大多數的網頁應用程式採用 SSL 加密，需要更深入的檢查才能判斷威脅。這個解決方案在以下情形可輕鬆擴充：識別網頁內容、解密和分析流量、落實原則和流量加密。不需將流量回傳資料中心，因此可減少 MPLS 連結的頻寬用量，進一步減少額外成本支出。

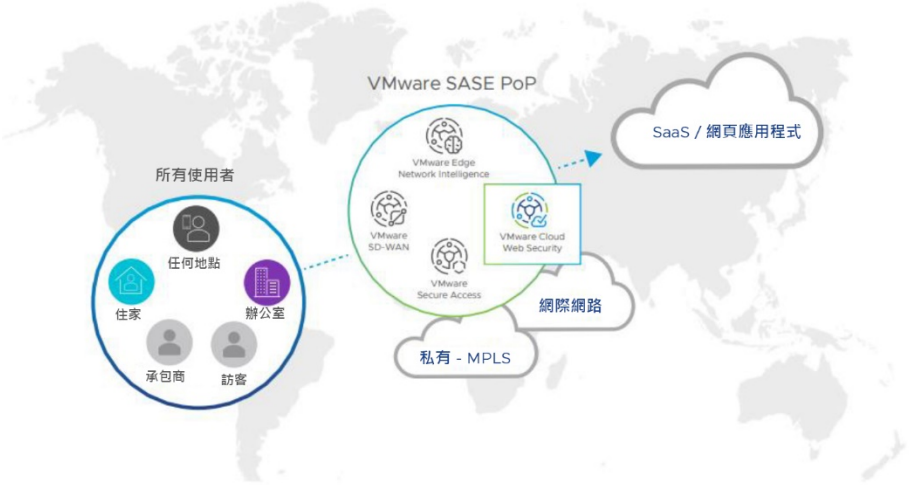

圖 3：在使用者和軟體即服務 / 網際網路應用程式之間的最佳路徑實施安全性機制

使用情境

Cloud Web Security 可處理下列使用情境：

- **網頁安全性**：Cloud Web Security 做為安全性集中控制點，可確保只有獲授權的使用者能存取軟體即服務與網際網路應用程式，以及落實隨處皆能安全瀏覽的原則。安全性管理員可以根據風險、行為、位置、使用者群組等因素，設定網頁存取原則。此解決方案會分析風險以判斷哪些 URL、應用程式或使用者容易受到惡意軟體的攻擊，偵測是否有多形惡意軟體，留意入侵指標，以及判斷縮小暴露範圍所要採取的行動。此解決方案還能保護基礎架構免於受感染裝置的威脅。

- **電子郵件和文件下載防護**：網路釣魚是常見的技倆，用於引誘使用者點按惡意連結，或下載看似可信任來源傳來的惡意文件。Cloud Web Security 確保員工可安全地下載電子郵件附件，而不致成為網路釣魚或勒索軟體攻擊的目標。根據 Verizon 的《2020 年資料漏洞調查報告》(2020 Data Breach Investigations Report)，46% 的組織曾透過電子郵件收到惡意軟體[1]。有了 Cloud Web Security，電子郵件附件和文件會受到檢查，以判定下載內容是無害或受到感染。此解決方案可確保使用者和基礎架構不受已知和零時差惡意軟體攻擊的威脅，結合檔案雜湊檢查、防毒保護，以及不明簽章的沙箱程序。
- **軟體即服務應用程式能見度和控制力**：Cloud Web Security 可協助 IT 在使用者存取軟體即服務應用程式時，獲得對使用者活動的能見度。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。例如，IT 可決定讓全職員工擁有 Box 等檔案類應用程式的登入存取權限、下載存取權限或上傳存取權限，但限制暑期實習生不可下載檔案。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，使用者可從 Dropbox 下載檔案，但是無法在其 LinkedIn 電子郵件中附加任何檔案。

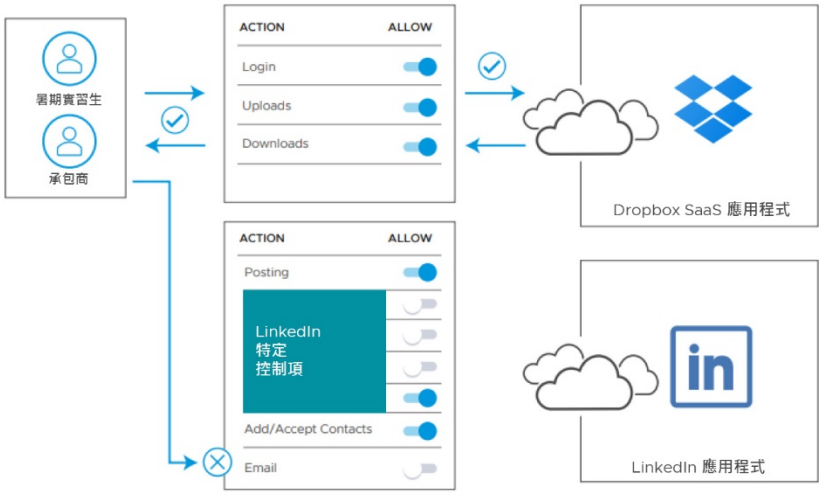

圖 4：適用於企業和社交應用程式的精密控制能力

Cloud Web Security 是透過 VMware SASE PoP 的全球網路提供，可隨 VMware SD-WAN 或 VMware Secure Access 一併交付。如要深入瞭解 VMware Cloud Web Security，請造訪 *https://www.vmware.com/tw/products/cloud-web-security.html*

- **保護敏感資料並確保合規**：VMware Cloud Web Security 可防止敏感資料從企業環境流出。此解決方案會監控、偵測、封鎖和回報資料外洩，並協助因應如 HIPAA、PCI、GDPR 及其他資料隱私權法律的合規需求。單一管理介面有助於大幅降低營運複雜性，並可針對網路、資安與合規等多個營運團隊之間的溝通，提供共通的檢視方式。

Cloud Web Security 是透過 VMware SASE PoP 的全球網路提供，可隨 VMware SD-WAN™ 或 VMware Secure Access™ 一併交付。

文件編號：sdwan-974-Cloud-Web-Security-so-0621