SaaS 安全性

可以因應 SaaS 激增的首個整合式 CASB

近幾年來，許多的公司都嘗試將他們所有的應用程式、數據和裝置侷限在他們能夠充分掌握及控制風險的受管理環境中。

現今有許多企業都因為便利性而逐漸採用雲端，並將應用程式和數據從其內部數據中心移轉至軟體即服務 (SaaS) 應用程式，例如 Microsoft 365®、Google Workspace™、Slack® 和 Salesforce®。企業平均會在其業務上使用 288 種不同的 SaaS 應用程式，與上一年同期相比成長 30%。[1] 同時，Gartner 也預測全球性的公有雲服務市場在 2022 年將會成長 19%，且 SaaS 仍佔據最大的細分市場，其營業額預測會在同年成長至 1400 億美元。[2]

商業優勢

- 自動探索及控制新的應用程式以因應 SaaS 激增。
- 透過業界首個雲端交付的企業 DLP 確保所有 SaaS 應用程式的數據保護和合規性。
- 透過整合式、基於機器學習的攻擊防禦來即時防範零時差威脅，不需要使用第三方安全工具。
- 憑藉與傳統 CASB 解決方案相較最低的整體擁有成本，充分利用易於部署的企業 SaaS 安全性。

1. 「Blissfully's 2020 SaaS Trends」，Blissfully，2019 年 10 月 23 日，https://www.blissfully.com/saas-trends/2020-annual-report。
2. 「Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020」，Gartner，2020 年 7 月 23 日，https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020。

由於敏感數據會透過越來越多的獲批准應用程式上傳、建立、共用，並暴露在其中，因此變得更容易遭受損害及竊取。若這些數據未受到適當保護，即使是獲批准的 SaaS 應用程式也會因為產生新的風險而造成損害。此外，雲端式威脅無論是數量和複雜度皆已不斷增加，並且會使用進階技術規避標準防禦方法，進而入侵敏感數據和使用者。

除了獲公司批准的應用程式以外，目前還有無數的公有 SaaS 應用程式可供不具 IT 部門相關知識的員工存取。缺乏對於 SaaS 使用情況的可視性將使得 IT 部門無法管控員工對於未獲批准 SaaS 應用程式的使用甚至濫用，因此將會為企業帶來如數據洩露和違反法規等嚴重的風險。

在現今隨時隨地都可工作的世界中，一旦員工選擇規避 VPN 回傳系統，就能持續存取所有獲批准及未獲批准的 SaaS 應用程式，IT 部門也會因為缺乏必要的可視性和控制而無法有效掌控員工對於這些應用程式的使用情況。

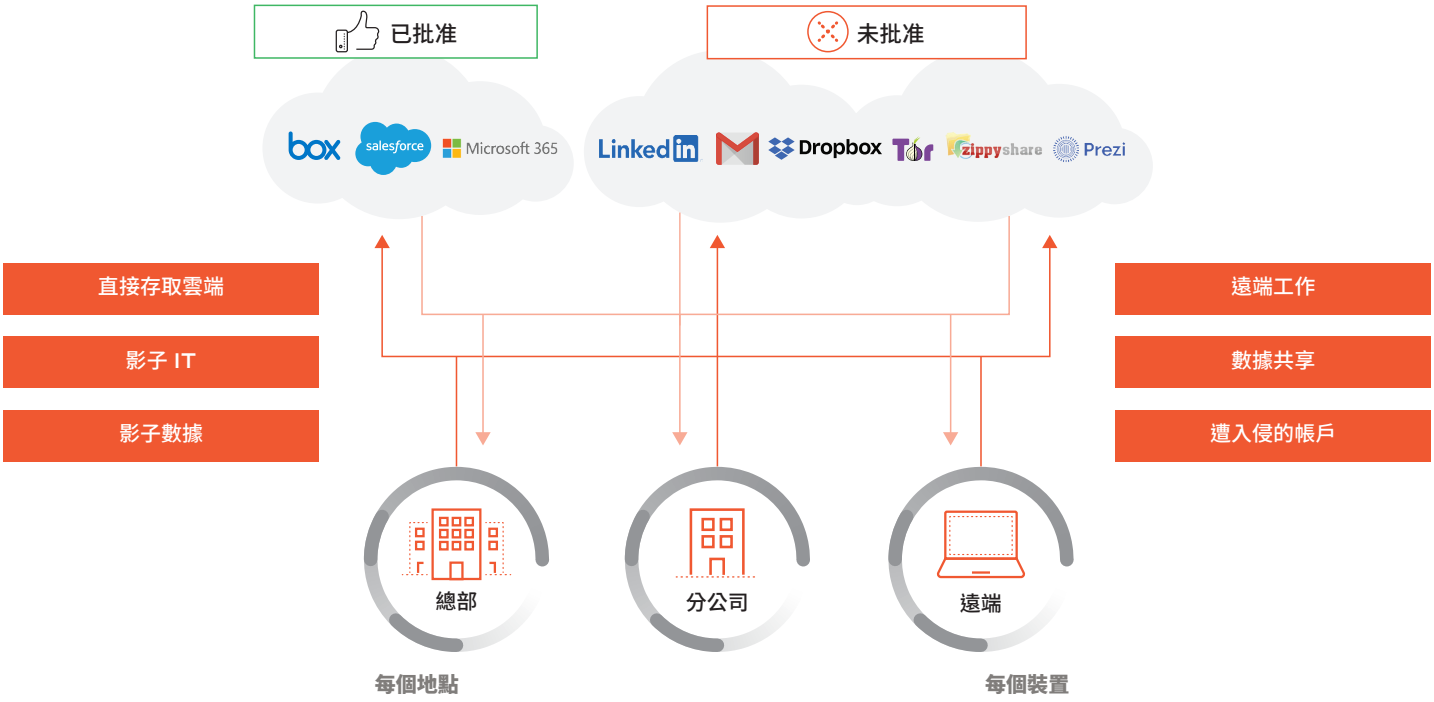

圖 1：雲端採用和 SaaS 應用程式的快速成長

現今 IT 安全團隊需要的是什麼

IT 安全團隊目前所面對的挑戰包括需要保護越來越多獲批准及未獲批准的 SaaS 應用程式、保護雲端中的敏感數據，以及透過一致的方式在不同雲端環境中維護合規性。同時，他們還必須封鎖不斷進化的威脅以防止其敏感資訊、使用者和資源遭到入侵。如今，他們需要的 SaaS 安全解決方案必須：

- 提供對於所有影子 IT 風險的可視性和控制，並以智慧方式跟上勢不可擋的 SaaS 成長速度。
- 保護公司 SaaS 應用程式不會受到所有已知和未知的雲端威脅。
- 以更為可靠的方式保護敏感數據並確保所有 SaaS 應用程式的合規性。
- 僅允許合法使用者存取公司 SaaS 應用程式。
- 易於部署且不會增加不必要的複雜度和成本。
- 與現有的整體網路安全部署緊密連結以構成全面的企業平台。

若要安全地採用雲端，公司將需要透過單一、一致的方式來保護其使用者、應用程式和數據。

圖 2：您的 SaaS 安全產品所必須保護的對象

現今傳統方式的限制

現今的傳統式單點控制，例如傳統雲端存取安全代理 (CASB)、安全 Web 閘道 (SWG) 和內建 SaaS 安全功能，都因為受到無數的架構性及操作性限制而崩解。由於這些解決方案只能解決部分問題，因此企業經常需要部署數種工具來嘗試取得整體防禦。

安全團隊還必須一同修補這些工具，因此會增加作業複雜度並降低安全效率。此外，要從並非以原生方式共用數據的各種個別工具拼湊出所有資訊，也會使得整體效益大打折扣。此一模型最後不僅耗費更多時間，也會削弱安全團隊的能力，使其無法有效保護過度暴露的數據及防禦外來的攻擊。

被動式影子 IT 探索

傳統的解決方案會仰賴以特徵碼為基礎的方式，讓 SaaS 透過經常脫離脈絡的應用程式庫進行探索。事實上，它們需要安全分析師以手動方式趕上追溯中的 SaaS 應用程式特徵碼，而非利用全球社群獲知主動機制來找出新出現的應用程式風險，以防止其變成真正的問題。

不完整的安全性

CASB 和幾家 SaaS 供應商都只能提供一些無論廣度和深度都相當受限的基本安全功能。例如，他們的數據保護機制並非企業等級，並僅限於雲端環境。這些解決方案的設計也無法偵測出攻擊者不斷產生、會規避安全系統，且永無止境的威脅變體。SaaS 和雲端服務供應商所提供的嵌入式安全功能無法保護多個雲端環境。

營運複雜度和高整體擁有成本

如傳統 CASB 等傳統 SaaS 解決方案皆各自獨立，並且與安全基礎結構互不相關。此外，它們也難以進行部署及管理，因為這些解決方案都是以 Proxy 為基礎，且需要從網路防火牆和 Proxy 自動設定 (PAC) 代理程式進行複雜的流量重新導向。最重要的是這些解決方案都無法提供統一的數據保護政策方法與內部部署的管道。

解決方案：Palo Alto Networks SaaS 安全性

Palo Alto Networks SaaS 安全性是首個可以因應 SaaS 激增的整合式 CASB。它會以原生方式整合 Palo Alto Networks 新世代防火牆平台 (雲端式、虛擬和硬體形式)，可提供主動可視性、同級最佳保護以及最快的速度來實現所有 SaaS 應用程式的價值，並具備簡易的部署方式及較低的整體擁有成本 (TCO)。

關鍵元件和功能

影子 IT 可視性和控制

自動探索及防範數千個新增 SaaS 應用程式的風險，以防止其變成真正的問題。App-ID™ 技術可充分利用廣大的全球社群，針對已知及之前未知的 SaaS 應用程式持續進行識別、分類和精細的風險控制，確保在新的應用程式廣泛使用之前能夠自動將其發現。SaaS 安全性目錄可提供精細的可視性以充分掌握各種應用程式、其在企業內的使用情況以及風險。

除了使用者的資訊與其活動 (例如上傳、下載和工作階段) 以外，還有超過 10 種描述屬性和超過 30 種合規性相關的屬性。目錄中的應用程式已分類為超過 400 種不同的類別。您也可以根據會對企業造成最大影響的風險屬性來自訂預設風險評分。此外，您也可以針對現有及未來的應用程式進行風險降低控制和政策建議的自動化，免除耗時的手動政策定義。

全面的內嵌安全性

保護所有 SaaS 應用程式及保全所有 Web 流量和非 Web 流量。SaaS 安全性可透過內嵌方式和 API 將新世代防火牆安全服務延伸至 SaaS 應用程式，並具備深入的應用程式可視性、區隔、安全存取和威脅防禦。業界首個機器學習 (ML) 模型是在機器學習式新世代防火牆上執行，並透過最大的數據庫進行訓練，可在 10 秒內提供特徵碼以減少 99.5% 系統遭感染的機率。這些全面的功能橫跨內部部署和行動工作者，可阻止威脅入侵所有應用程式，在過去三年間將入侵事件降低 45%。[3]

企業數據保護

透過業界首個雲端交付的企業 DLP，可按照一致的方式在所有 SaaS 應用程式中提供數據保護和合規性控制，保護範圍遍及企業內的雲端、內部部署網路和使用者。Palo Alto Networks 企業 DLP 是以單一雲端引擎為基礎，可針對靜態及傳輸中的敏感數據進行精確的偵測並提供一致的政策。它會掃描、分類及保護儲存在 SaaS 應用程式中的所有數據，以確保在執行時任何違反政策、曝露和合規性等情況都能獲得適當解決。

企業 DLP 會使用規則運算式或關鍵字 (例如信用卡或 ID 號碼、財務記錄、GDPR、其他數據隱私和合規性相關資訊) 並透過基於機器學習的數據分類和數百種數據模式來自動偵測敏感內容，然後套用可自訂的數據設定檔和布林邏輯以掃描集體數據類型。曝光類型 (例如公有或內部)、信心層級和精確的脈絡準則 (例如發生次數和模式邏輯) 可減少意外事件和錯誤偵測。進階式機器學習可簡化數據分類。對於如第三方數據標記等具彈性的文件屬性進行偵測，則可強化對於敏感數據的識別。

3.「The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN」，Forrester，2021 年 2 月，https://start.paloaltonetworks.com/2021-forester-tei-report-network-security.html。

SaaS 安全性也包含檔案封鎖設定檔，可用來防止檔案遭到下載，這也是雲端數據保護策略中相當重要的一環。

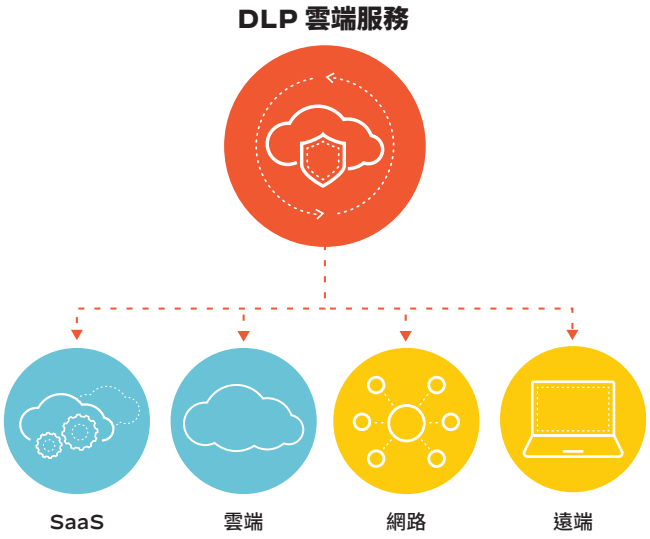

圖 3：Palo Alto Networks 企業 DLP

API 式防護

使用頻外 API 式方法直接連接至獲批准的 SaaS 應用程式。SaaS 安全性會套用企業 DLP、機器學習式威脅防禦以及持續監控使用者活動和管理設定，藉此以一致的方式保護所有 SaaS 應用程式。無論使用者所在的地點或所用的裝置為何，此部署模式都可在任何存取點上運作。它會承襲公司 SaaS 應用程式的使用者體驗，因為它不具侵入性且不會干擾標準業務程序。企業 DLP 和機器學習式威脅防禦可在所有 SaaS 應用程式和您的整個企業中保持一致。這些功能有助於正確地保護儲存在雲端應用程式中的所有敏感數據、維護如 PCI DSS 和 GDPR 等法規的合規性，並可即時阻止所有已知和未知的威脅，且不需要使用第三方安全工具。

調適型存取控制可讓您更精細地管理對於 SaaS 應用程式的存取，以及定義可接受的使用政策。此外也支援無用戶端功能，以保護未受管理裝置對於 SaaS 應用程式的存取。最後，該解決方案可偵測及舉報與失竊憑證或惡意內部人員行為相關聯的異常使用者活動，例如大量數據下載或大規模的數據共享。

透過整合式架構以低整體擁有成本最快實現價值

SaaS 安全性能與多種形式的 Palo Alto Networks 新世代防火牆 (雲端交付、實體和虛擬) 進行整合，以一致的方式保護所有應用程式、裝置、數據和工作負載類型，以及在任何地點工作的所有使用者。此一全面的方法可大幅簡化 CASB 部署與其持續進行的作業。

與傳統以 Proxy 為基礎的 CASB 相較，SaaS 安全性可確保最快實現價值以及最容易部署的企業 SaaS 安全解決方案，因為它能夠避免不必要的人為介入並可在幾分鐘內快速啟動與運作。一般的企業在使用我們的防火牆平台時可獲得 247% 的投資報酬率 (ROI)[4]，與傳統的 CASB 相較，它還可將 CASB 部署速度提高五倍，整體擁有成本降低 50%，這是因為它是以大幅精簡的架構為基礎。

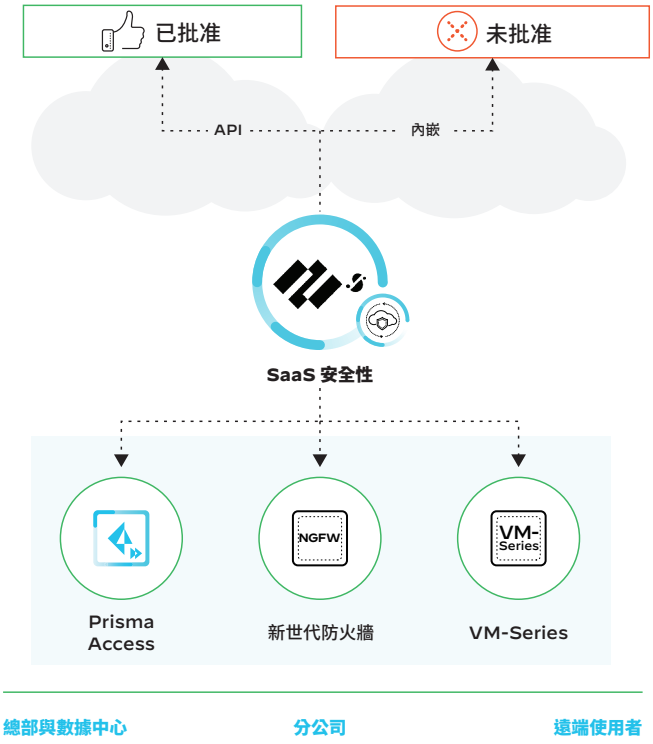

圖 4：SaaS 安全性部署範例

4.「Total Economic Impact」，Forrester。

CASB 和企業 DLP：SASE 的關鍵要素

作為 Palo Alto Networks 安全存取服務邊緣 (SASE) 解決方案的關鍵要素，SaaS 安全性和企業 DLP 有助於企業跨網路和雲端以一致的方式保護數據、應用程式和使用者，同時避免採用多個單點產品的複雜度，因此可大幅簡化採用過程，並節省技術、人力和財務資源。

全面的 SASE 解決方案透過單一雲端平台結合網路與網路安全服務，避免為數據、應用程式和使用者帶來風險，並可協助您完成雲端和網路轉型以及安全地採用 SaaS 應用程式。

建立在零信任與 SaaS 安全性的基礎上

為啟用雲端的企業實施有效率的零信任安全模型時，必須將 SaaS 應用程式與其敏感數據的最低權限存取策略列入考量。

Palo Alto Networks SaaS 安全性是構成 Palo Alto Networks 零信任架構的基礎，可讓企業在高度分散式環境中以一致的方式保護對於 SaaS 應用程式與其數據的存取，其中包括從遠端地點工作的員工及其自備裝置。

表 1：功用和功能重點

- 內嵌、API 和 DLP 的統一管理
- 與新世代防火牆直接進行整合，不需要使用 Proxy
- 與業界領先的雲端式惡意軟體解決方案 WildFire 進行整合
- 對於數千個 SaaS 應用程式的可視性和風險控制
- 可自訂的風險評分，涉及 40 種以上的屬性
- 使用者活動和數據曝露監控
- 多模式：內嵌和 API 控制
- 未受管理裝置存取控制
- 立即可用的合規性報告 (例如 GDPR)
- 自訂標記

表 2：隱私權和授權

信任與隱私權	授權和支援要求
Palo Alto Networks 擁有嚴格的隱私權與安全性控制措施，以防止在未獲授權情況下存取機密或個人身分識別資訊。我們會套用業界標準的最佳實務提供安全性和機密性。您可在我們的隱私權型錄中找到進一步的資訊。	• SaaS 安全性包含 SaaS 內嵌安全性、SaaS API 安全性和 DLP，並已各自獲得授權 • 新世代防火牆 (硬體/虛擬) 或 Prisma Access • Cortex Data Lake • PAN-OS 8.1.x+ (10.1 適用於 ACE 和政策建議)

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓