



安全存取服務邊緣 (SASE)

在現今以身分為中心的世界提供
統一的安全連線體驗



現代化工作環境需要 流暢且安全的連線體驗。

過往數據中心一直是每個公司網路安全的重點，隨著越來越多業務需求透過數位化轉型，使用者和裝置的資料存取不再集中在數據中心。而工作已經從實體位置演變為執行的活動。這些活動正在辦公室以外的任何地方發生，使用者、分公司或物聯網 (IoT) 裝置需要存取網際網路、位在公司資料中心應用、SaaS雲端應用或分公司內的資料來執行日常業務。各種連線會導致大量的安全存取問題，因此需要實施統一的管理策略。

不同於單點式安全解決方案，SASE 是一種全新的架構：將SD-WAN、防火牆即服務 (FWaaS)、安全網路閘道 (SWG)、雲端存取安全代理 (CASB) 和零信任網路存取 (ZTNA) 等網路和安全服務整合到雲端來統一交付服務。無論使用者、應用程式或數據位於何處，SASE 都可以提供一致的高安全網路存取。

SASE 有助於企業實現網路和安全現代化，藉以提升成本效益層級、業務靈活度和成熟性。這種基於平台的做法相當彈性，適用於任何數量的潛在使用案例。SASE 特別適合解決向數萬名遠端使用者提供存取權限、分公司直接存取 internet 的安看管裡，以及支援多雲移轉等挑戰。由於這些工具現在可以協助因應最複雜的 IT 挑戰，因此實施 SASE 已成為國外許多企業的首要選擇。

Gartner® 也指出：「相較於 2021 年時只有 20% 左右，在 2025 年時將有 80% 的企業都會採用新的策略以使用 SASE/SSE 架構來統一管理 Web、雲端服務和私有應用程式存取。」



傳統網路和安全方法的挑戰



採用多個單點解決方案增加營運負擔和成本

單點網路解決方案和安全功能之間缺乏互通性，因此網路和安全團隊難以實施統一的網路安全策略，CAPEX 和 OPEX 也因此增加。



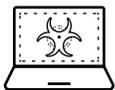
遠端和分公司使用者面臨的延遲

流量透過傳統廣域網路架構從多個分公司或遠端位置集中到總部後，存取網際網路或雲端應用程式時出現額外的延遲，導致使用者體驗不佳。



存取雲端企業應用程式時的漏洞

目前企業使用的遠端存取 VPN 解決方案在現代雲端世界中面臨許多限制，因為企業將整個網路暴露給獲得授權的使用者，因此內部威脅出現的機會大為增加。此外單點 VPN 裝置的部署成本相當高而且不容易管理。



對第 5 代網路威脅的保護不足

大型攻擊 (第5代攻擊) 本質上是多途徑的攻擊，可以快速、隱蔽地傳播到企業基礎結構的任何區域或從企業基礎結構的任何區域傳播，包括網路、使用者裝置、雲端工作負載、IoT 裝置和第三方等等，此類攻擊包括 WannaCry 和 NotPetya 等攻擊。



缺乏可視性和控制導致違反合規性

使用者經常從新的地點、有潛在風險的網路以及違反合規性的裝置來存取數據和應用程式，欠缺對關鍵數據流量以及員工存取和使用數據的地點的可視性和控制能力將企業容易受到入侵。



Palo Alto Networks 推出的 Prisma® SASE 是業界最完整的 SASE 解決方案,能將SSE網路安全、SD-WAN 軟體定義網路與ADEM 自發性數位體驗管理等方案整合由雲端統一交付服務。這個統一的安全產品不但設計為易於使用,克服了舊型方法的缺陷還能提供最佳使用者體驗,也只有它才能夠將 ZTNA 2.0、SWG、NG-CASB、FWaaS、DLP 等各種同類最佳功能整合以實現:

- 透過精細的存取控制,安全地連接所有使用者和所有應用程式,以大幅縮小攻擊範圍
- 在使用者連線後對行為持續進行信任驗證
- 提供深入且持續的安全檢查,確保所有流量都會受到保護且不會妨礙效能或使用者體驗
- 透過統一DLP政策提供一致可視性以同時保護存取權限和數據
- 透過單一產品可在任何時候保護所有應用程式,包括內部部署的、網際網路、SaaS 以及現代化/雲端原生應用程式

我們的解決方案協助全球企業實現對於使用者和裝置的零信任應用程式存取,並確保安全傳輸使用者流量到網際網路或 SaaS 應用程式。這會提供跨越所有實體和虛擬站點、雲端和網路的安全連結。Okta、Azure AD、Ping Identity 等身分服務供應商都可以與我們的解決方案整合。

採用 SASE 的效益

- 藉由提供多種功能的單一解決方案降低管理複雜度和成本
- 改善效能並消除延遲
- 啟用新的數位業務情境
- 為行動工作者、分公司使用者提供安全存取,並且防止不受管理的裝置和 IoT 裝置所造成的影響
- 為使用者提供易用性和可視性,以增強使用體驗
- 降低營運開支
- 啟用零信任網路存取
- 提供以政策為基礎的安全服務
- 透過提供整合的單一的管理介面來簡化操作

Prisma SASE 是靈活且運用雲端的企業安全基礎



優異的 ZTNA 2.0 安全性

Prisma SASE 可持續保護混合工作者使用的所有應用程式，無論使用者是在家工作、以行動方式辦公還是在辦公室工作。ZTNA 2.0 安全是透過同級最佳功能來保護所有的應用程式流量，同時保護存取和數據以大幅降低數據洩露的風險。



簡化的操作

Prisma SASE 將同類最佳的網路和安全性整合到單一雲端服務來簡化操作。統一管理和共享的維運數據可改善團隊協作並簡化作業。



絕佳的使用者體驗

Prisma SASE 運作於雲架構上，能夠以雲端規模提供安全防護，同時提供絕佳的使用者體驗。透過真正的雲原生架構以提供業界領先的 SLA 支援與毫不妥協的效能。業界首個 SASE 原生整合自發性數位體驗管理 (ADEM)，可協助確保優異的最終使用者體驗。



Palo Alto Networks 台灣代表處

11073 台北市信義區松仁路
100號 6F-1

諮詢熱線: 0800666326

網址: www.paloaltonetworks.tw

郵箱: contact_salesAPAC@paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.