

Prisma SASE 應用程式加速

概覽

在現今的雲端優先環境中，Web 應用程式的速度和效能對於混合工作者與數位企業提高生產力及保持競爭力至關重要。效能緩慢的應用程式可能會導致使用者感到困擾、生產力低落，以及失去商機。Palo Alto Networks Prisma SASE 應用程式加速提供最先進的解決方案，可以大幅提升網路和應用程式效能，確保可享受到比直接連線更為快速的體驗，同時提供卓越的 ZTNA 2.0 安全性，無須任何妥協。

影響應用程式效能和使用者體驗的問題

企業應用程式和員工比以往任何時候都更加分散，這讓要在各地提供安全且一致的體驗也變得越來越困難。因此企業在將混合工作者連接到應用程式時，將會面臨效能和體驗方面的挑戰，包括：

1. 目前多雲端環境和內部部署數據中心的應用程式普遍存在著**延遲和效能低下**的問題。由於動態雲端環境的運作方式本身就存在著延遲的問題，不僅造成載入時間較長且回應速度降低，還會導致混合工作者的生產力低下。
2. 住家辦公室或咖啡廳及機場等高密度環境中的 **WiFi 訊號不佳且網路擁塞**。消費級連線缺乏企業級設備的效能和可靠性，隨著越來越多的使用者同時連線，本機網路的速度和穩定性都會受到影響。這可能會導致協作工具出現緩衝、連線中斷，或者是視訊或音訊品質不佳的情況。
3. 當混合工作者透過不安全的網路存取敏感資訊，或是關閉 VPN 連線以享有更快的網際網路存取速度時，將會出現**安全性不一致**的情況。

Prisma SASE 應用程式加速重點

Palo Alto Networks Prisma SASE 應用程式加速可提供同級最佳的安全性，其速度比應用程式直連的效能更加快速，並且提供機器學習式 ZTNA 2.0 安全性，而且不會影響使用者體驗。在克服傳統方法的侷限性之後，唯有 Prisma SASE 應用程式加速才能對所有應用程式達到高效能、低延遲的安全存取，而且速度比直接存取應用程式快上五 (5) 倍。

- **為所有應用程式和數據提供一致的同級最佳安全性，毫不妥協：**具有應用程式加速功能的 Prisma SASE 可以提供 ZTNA 2.0 的絕佳防護，包括 AI/機器學習支援的內嵌保護，以防範最複雜和持續的威脅，同時提供完整的 DLP 支援以保護所有數據不會遭到意外或蓄意洩露，同時提供比應用程式直連更快的效能。
- **提高網路效能：**跟傳統的 WAN 最佳化方法不同，只有 Prisma SASE 應用程式加速器能夠以動態方式適應混合工作者的「第一哩」連線條件以提高連線效能，而且無需變更或更換現有硬體。

- **大幅減少延遲狀況並提高應用程式效能：**Prisma SASE 應用程式加速利用智慧型應用程式感知邊緣平台來了解員工如何與 SaaS 和其他雲端應用程式互動，並且使用該資訊來提高雲端應用程式的回應速度，比網際網路直接連線的速度快上 5 倍。

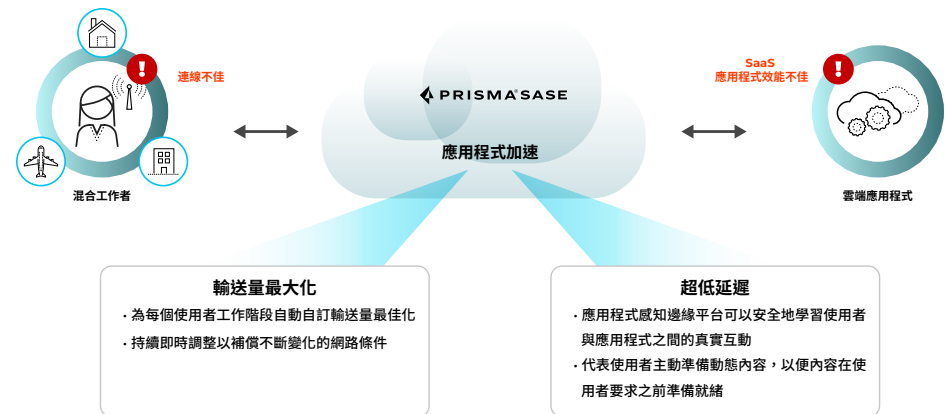


圖 1：Prisma SASE 應用程式加速可以提供「優於直接」的效能，達到毫不妥協的使用者體驗。

Prisma SASE - 業界最完整的 SASE 解決方案

Palo Alto Networks Prisma SASE 會將同類最佳的安全性與新世代 SD-WAN 融合至單一雲端交付平台。其將包含 ZTNA 2.0、雲端 SWG、CASB、FWaaS 與 SD-WAN 在內的多種單點產品進行整合，推出單一整合服務，可以降低網路與安全性複雜度，同時提升企業的敏捷性。

ZTNA 2.0 的絕佳安全性可以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。

Prisma SASE 內建於雲端中，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。真正的雲端原生架構提供獲得業界領先的 SLA 所支援、毫不妥協的效能。業界首個 SASE 原生 ADEM，可以協助確保優異的使用者體驗。

Prisma SASE 應用程式加速概覽

Prisma SASE 使用案例

三個根本性的轉變正在推動企業的網路轉型需求：混合工作、雲端和數位轉型以及分公司轉型：

- 對於受到疫情影響的許多企業來說，**混合工作模式**已變成新的常態和需求。研究顯示，即使在 COVID-19 疫情解封之後，企業仍預期會有 62% 的員工維持遠端或混合工作模式（「2021 SASE 趨勢調查」，ESG，2021 年 7 月）。因此，大部分企業都正在規劃支援這樣一種工作模式，亦即大部分員工都能夠在總部、分公司、住家辦公室和路上流暢地進行工作。
- 雲端和數位計劃**可讓企業增加對於 SaaS 和其他公用雲端服務的投資。雲端採用讓公司更具敏捷性、效率和靈活性，這也是現在有 92% 的企業會採用多雲端策略的原因（Flexera，2021 年）。SASE 能夠更貼近保護使用者，因此流量無需回傳到總部即可到達雲端。
- 由新混合工作模式和數位轉型計劃所帶動的**分公司轉型**目前正順利進行中。企業正在徹底改變分公司的型態，也就是利用分公司作為協作中心而不是主要的工作地點，而且零售商也正在改變在店內與客戶互動的方式。此一趨勢會加劇 WAN 從傳統 MPLS 轉型至 SD-WAN 和 SASE 的需求。

Prisma SASE 功能

自發性數位體驗管理 (ADEM)：透過實際和綜合流量分析，可在整個服務交付路徑上獲得市場區隔見解，進而針對數位體驗問題進行主動補救。

雲端存取安全代理：透過對於 SaaS 應用程式的內嵌和 API 式安全性來套用監管、數據分類並阻止威脅。

CloudBlades：不需更新分公司設備或控制器，就能將分公司服務與 SASE 網狀架構進行緊密整合，因此可完全排除服務中斷和過於複雜的情況。這種雲端型獨特 API 架構可以自動部署第三方服務，因此企業能夠簡化網路作業和多雲端連線，並且加快部署。

雲端安全網路開道：使用靜態分析與機器學習來防範網路威脅，同時簡化從傳統 Proxy 型解決方案移轉到 SASE 的客戶的上線體驗。

明確 Proxy：Prisma SASE 提供具有彈性的連線選項，包括對於明確 Proxy 連線方法的支援。透過 Prisma SASE 明確 Proxy，客戶可以輕鬆地從傳統 Proxy 型解決方案進行移轉而無需進行網路架構變更，達到更加安全的解決方案轉換，並且保護所有的應用程式、連接埠和通訊協定的安全無虞。

數據遺失防護：全面性的數據保護會將敏感數據分類並在遠端使用者和遠端位置之間移動這些數據時提供保護，以確保數據絕對的安全。

DNS Security：使用進階分析和機器學習功能，可以防止 DNS 流量遭受威脅。

防火牆即服務 (FWaaS)：透過從雲端以服務形式交付的 Palo Alto Networks 新世代防火牆安全性，保護每個遠端位置。

IoT Security：結合機器學習、風險評估、內嵌防禦、政策建議和自動執行政策以保護 IoT 裝置，而無需部署昂貴且難以管理的感應器。

機器學習式安全性：運用機器學習以主動提供即時和內嵌的零時差防護，以及自動化政策建議。

SD-WAN：跟 Prisma SD-WAN 進行深度且無縫的整合，這是業界第一個以應用程式定義、自發並透過雲端交付的新世代 SD-WAN。

Threat Prevention：使用整個 Palo Alto Networks 生態系統的已整合威脅情報，封鎖各種入侵、惡意軟體和命令與控制流量。

VPN：IPsec、SSL 和無用戶端 VPN 可以提供將使用者和網路連接至安全存取服務邊緣的選項。

零信任網路存取 (ZTNA) 2.0：結合最為精細的最低權限存取與行為式持續信任驗證，以及深入且持續的安全檢查和企業 DLP，以持續保護任何位置的所有使用者、裝置、應用程式和數據。

應用程式加速：提供比應用程式直連更快速的效能，以獲得最佳的使用者體驗。

深入了解 Prisma SASE，請造訪 paloaltonetworks.com/sase。