Prisma Access
概覽

混合工作模式和「應用程式直連」架構導致傳統的安全架構變得不合時宜，同時顯著加大我們的攻擊範圍。Palo Alto Networks Prisma Access 能透過優異的 ZTNA 2.0 安全性來保護混合工作者，並且藉由簡單、統一的安全產品提供絕佳的使用者體驗。

Prisma Access 重點

Prisma Access 是在雲端中專為特定目的打造，可解決替代方法的限制並且保護現在的混合工作者，可提供：

- **ZTNA 2.0：**Prisma Access 透過領先全球的網路安全公司提供包括零時差威脅防護在內的卓越安全性，同時結合最為精細的最低權限存取與深入且持續的安全檢查以及企業 DLP，以保護所有的使用者、裝置、應用程式和數據，能夠在任何位置防禦最複雜的威脅。
- **統一的安全產品：**透過單一管理平台的可視性和管理、一致的政策以及與所有使用者和所有應用程式共享的數據，將全面性的防護整合至單一的統合式產品，以大幅降低數據洩露的風險。
- **最佳使用者體驗：**專為保護現在的雲端規模數位企業所量身打造的真實雲端原生架構，可提供由業界領先之 SLA 所支援，毫不妥協的效能並實現絕佳的使用者體驗。

保護混合工作模式的挑戰

數位轉型和混合工作模式已促進企業對於雲端的大規模採用及使用。雖然雲端安全產品和 ZTNA 1.0 方法已一躍成為具有潛力的解決方案，但這些產品也只不過是解決一部分的問題，因此不足以保護現今在任何位置工作的使用者和應用程式直連架構，這是因為其中存在幾個關鍵的限制：

- 提供太多的存取權限，卻又極度缺乏防護機制。
- 應用程式和數據的安全性不一致且不完整。
- 整體效能和使用者滿意度不佳，客戶必須犧牲安全性取得使用體驗。

Prisma Access

Prisma Access 可讓企業將所有使用者安全地連線至他們需要的應用程式，無論他們從何處存取或使用哪些裝置，都可以大幅降低風險。

Prisma Access 能夠透過優異的 ZTNA 2.0 安全性來保護混合工作者，並且藉由簡單且統一的安全產品提供絕佳的使用者體驗。它可透過精細的存取控制連接所有使用者和所有應用程式，在使用者連線後提供行為式持續信任驗證以大幅縮小攻擊範圍。它可在任何時候保護所有應用程式，包括內部部署型、網際網路型、舊型、SaaS 以及現代化/雲端原生應用程式，並提供深入且持續的安全檢查 — 包括針對零時差威脅的進階防護 — 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。除此之外，Prisma Access 還提供一致可視性與單一 DLP 政策以保護整個企業的存取和數據。

Prisma Access 的獨特架構內建於雲端中，能夠提供雲端規模、可實際涵蓋多租戶的保護，同時確保所有客戶都能相互隔離開來。Prisma Access 利用全球最大雲端供應商的彈性規模以及專用的頂級光纖網路存取，可提供業界領先的 SLA 進行安全處理以及確保應用程式效能。此外，原生的自發性數位體驗管理 (ADEM) 甚至能夠在使用者察覺之前就主動識別並解決潛在問題。這些功能將能夠保證最佳效能和使用者體驗。

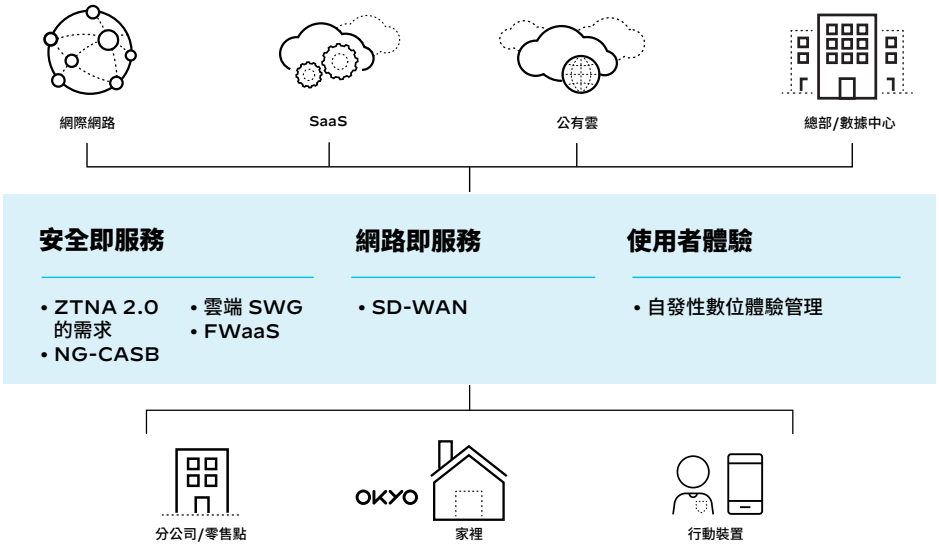

圖 1：Prisma Access 架構

Prisma Access
概覽

Prisma Access 透過單一管理平台簡化所有功能的可視性和設定、持續評估即時安全狀況，並且透過共通的政策架構在任何位置執行一致的安全性，可以快速且輕鬆地消除安全狀況的漏洞。

適用於混合及行動使用者的 Prisma Access

現在的混合及行動使用者需要一致的安全性來存取所有應用程式。傳統遠端存取 VPN 解決方案不足是因為使用者通常連線到閘道以存取數據中心應用程式，然後中斷 VPN 連線，以便在存取雲端和網際網路應用程式時達到更好的效能 (但是較不安全)。

Prisma Access 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。Prisma Access 也包含 ADEM 以提供網路管理員整體服務傳遞路徑中的市場區隔見解，其中包括端點裝置、Wi-Fi、區域網路 (LAN)、VPN、網際網路、應用程式效能和 Prisma Access 本身。解決方案可監控會影響使用者體驗的情況並視需要執行自動補救，包括使用者自助服務補救與 ADEM 自助服務。

不過獨立式 VPN 和 ZTNA 1.0 解決方案仍有不足之處，因為當使用者存取整個 LAN 或應用程式時並無法檢查流量，也無法評估連線裝置的安全狀況。無論應用程式位於何處，Prisma Access 都可透過用戶端或無用戶端形式，提供應用程式和服務使用者需要的身分式 ZTNA 2.0。GlobalProtect 應用程式也可讓您依據主機資訊設定檔 (HIP)，在存取敏感應用程式時擬定與裝置特徵 (像是作業系統、修補程式層級，以及所需的端點軟體存在與否) 有關且更精細的安全存取政策。

面向網路的 Prisma Access

許多分公司和零售商店分佈在不同地點，缺乏全職 IT 人員，因此不容易進行部署、管理、變更控制和硬體更新。

Prisma Access 透過標準 IPsec 連線 (使用任何現有路由器、軟體定義的廣域網路 (SD-WAN) 邊緣裝置或支援 IPsec 的防火牆) 連接遠端網路，藉以保護流量、保護機密資訊，並且滿足數據隱私權需求。Prisma Access 支援使用 Palo Alto Networks Prisma SD-WAN、新世代防火牆 (NGFW) 以及第三方廠商產品的 SD-WAN 選項。透過 Prisma SD-WAN 提供的 Prisma Access ADEM 附加模組可將路徑和效能可視性擴充至所有使用者的所有分公司地點，而且不需要額外部署任何代理程式。解決方案可監控會影響 Prisma SD-WAN 站台體驗的情況，包括分公司應用程式、裝置和使用者流量，並視需要執行自動補救。

Prisma Access 服務

Prisma Access 提供全面的網路和安全服務。

安全

- **防火牆即服務 (FWaaS)：**適用於分公司和零售點的新世代防火牆安全性。
- **雲端安全網路閘道 (SWG)：**使用靜態分析和機器學習阻止惡意網站。
- **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。
- **DNS Security：**進階分析和機器學習功能，可阻止 DNS 流量中的威脅。
- **進階威脅防禦：**使用威脅情報封鎖入侵、惡意軟體和命令與控制 (C2) 流量。人工智慧/機器學習式掃描可防範之前從未見過的威脅。
- **數據遺失防護 (DLP)：**數據洩漏防禦以及數據隱私權和合規性強化功能。
- **新世代雲端存取安全代理 (新世代 CASB)：**監管和數據分類可運用強大的 SaaS 安全狀況管理以及進階內嵌和 API 式安全性來阻止威脅。
- **沙箱：**零時差威脅防禦與業界領先的 WildFire 惡意軟體防禦服務。
- **IoT Security：**保護網路上的每個裝置，透過單一平台提供機器學習式可視性、防禦和執行。

網路

- **SD-WAN：**針對我們的新世代防火牆提供支援並與 Prisma SD-WAN 和第三方產品進行整合。
- **VPN：**用於安全連線使用者和網路的選項，其利用 IPsec、SSL/IPsec 和無用戶端 VPN 封裝流量。
- **明確 Proxy：**行動使用者連線到 Prisma Access 以保護網際網路和應用程式流量 (HTTP/HTTPS) 的另一種方法。
- **服務品質 (QoS)：**關鍵應用程式頻寬的優先順序。
- **數位體驗監控 (DEM)：**對於整個服務鏈在使用者、遠端位置和應用程式之間的可視性。

