Prisma Access

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。雖然雲端安全產品已經出現，不過只能提供不一致和不完整的保護，並提供不盡理想的效能和使用者體驗。

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，並且藉由簡單且統一的安全產品提供絕佳的使用者體驗。Prisma Access ZTNA 2.0 是專為雲端環境所打造來提供雲端規模的保護，其提供了業界唯一的 ZTNA 2.0 解決方案，能透過同級最佳功能保護所有的應用程式流量，同時保護存取和數據以有效地縮小攻擊範圍。Prisma Access 具備共通的政策架構和單一管理平台，因此能夠保護現今的混合工作者而絲毫不影響效能，並由業界領先的 SLA 提供支援以確保絕佳的使用者體驗。

Prisma Access 獨特之處

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。它可提供雲端原生單一產品以保護混合企業和工作模式，並由同級最佳安全功能所組成，可透過動態可擴充性最佳化使用者體驗，並保證最終使用者效能。Prisma Access 可提供以下功能以簡化現今混合工作模式和雲端優先企業的安全維護：

- **卓越的 ZTNA 2.0 防護**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。
- **統合式安全產品**將全面性的防護整合至單一的統合式產品、單一管理平台的可視性、一致的政策以及與所有使用者和應用程式共享的數據。
- **實現絕佳的使用者體驗**，專為保護雲端規模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。

Prisma Access 結合同級最佳安全性與業界領先的雲端原生安全服務邊緣 (SSE) 平台。搭配 Prisma SD-WAN 使用時，企業能夠透過業界最完整的安全存取服務邊緣 (SASE) 解決方案進行網路和安全性的轉型。

安全即服務層

Prisma Access 包含全面的安全功能並整合至單一 SSE 平台，能夠在單一的統合式平台上提供絕佳的 ZTNA 2.0 使用者體驗。

防火牆即服務

Prisma Access 提供防火牆即服務 (FWaaS) 功能以及 Palo Alto Networks 新世代防火牆 (NGFW) 的全部功能。這包括傳入和傳出保護、原生使用者驗證和存取控制，以及第 3-7 層單一通道檢查，藉以保護分公司免於遭受威脅。

雲端安全網路閘道

Prisma Access 提供雲端安全網路閘道 (SWG) 功能，無論遠端使用者位於何處，都能保護他們在存取網路和非網路應用程式時不受到威脅。彈性連線選項包含代理程式、無代理程式、IPsec VPN 和明確 Proxy 連線方法，可簡化從傳統基於 Proxy 的 SWG 解決方案移轉而來的使用者上線體驗。雲端 SWG 已與新世代 CASB 進行原生整合，可支援 Prisma Access 提供的所有網路安全保護，包括 Threat Prevention、WildFire®、進階 URL Filtering、DNS Security 和 DLP。此外，也可透過與 Prisma Access CloudBlades 架構的整合支援遠端瀏覽器隔離 (RBI)。

零信任網路存取 2.0

Prisma Access ZTNA 2.0 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，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 ZNTA 2.0 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。

新世代雲端存取安全代理

Prisma Access 以原生方式提供業界唯一的新世代 CASB，結合強大的 SaaS 安全狀況管理 (SSPM) 功能、主動可視性、即時數據保護，包括在協作應用程式中交換且難以偵測的密碼，以及同級最佳安全性，可自動追蹤 SaaS 激增狀況。它可針對獲批准及未獲批准的 SaaS 應用程式，透過內嵌和 API 式安全性提供多模式功能以協助現今雲端優先的企業：

- 偵測及阻止遭入侵的帳戶和惡意內部人員的活動以避免造成任何損害。
- 偵測帳戶可能遭入侵或顯露出惡意內部人員跡象的可疑使用者活動。

- 透過業界第一個安全狀況政策引擎超越標準合規性檢查並取得全面性的防護。
- 消除因使用者錯誤設定造成的入侵和數據遺失風險。
- 只需按一下即可解決重大錯誤設定問題，大幅減少補救時間。

網路即服務層

對於雲端、數據中心或網際網路中的所有應用程式，Prisma Access 提供一致且安全的存取。

適用於混合及行動使用者的網路連線

將混合及行動使用者連線到 GlobalProtect 應用程式，可支援基於使用者 (始終開啟)、預先登入 (始終開啟) 以及視需要進行的連線。Prisma Access 支援基於存取路由和應用程式類型 (包括相關的風險和頻寬使用) 的分離通道。

遠端網路的網路連線

使用常見的 IPsec 相容裝置，例如現有的分公司路由器或軟體定義的廣域網路 (SD-WAN) 設備，透過標準 IPsec VPN 通道將分公司連線到 Prisma Access。您可以使用分公司的邊界閘道通訊協定 (BGP) 或靜態路由，也可以使用等價多路徑 (ECMP) 路由提高效能，並在多個連結之間達到更好的備援。

數位體驗監控

Prisma Access 的自發性數位體驗管理 (ADEM) 附加模組為 SASE 提供原生點對點可視性。藉由 ADEM，您可以透過實際和綜合流量分析在整個服務交付路徑上獲得市場區隔見解，因此可以在出現數位體驗問題時進行自發性補救 (目前包含使用者自助式服務補救與 ADEM 自助式服務)。互補的 Prisma Access 分析可讓您監控和取得 Prisma Access 部署健全狀況的隨需可視性。

集中管理

Prisma Access 支援靈活的管理選項：

- **Prisma Access 雲端管理**，透過緊密的上線流程，包括建立在最佳實務基礎上的安全預設設定、對安全狀況的持續評估、數位體驗監控以及透過從雲端提供的統一體驗進行的報告來簡化 Prisma Access 設定管理。
- **Panorama 網路安全管理**，可以跨越所有 Palo Alto Networks 新世代防火牆和 Prisma Access 進行集中政策管理。Panorama 透過單一管理平台管理網路安全，因此節省時間並降低複雜度。

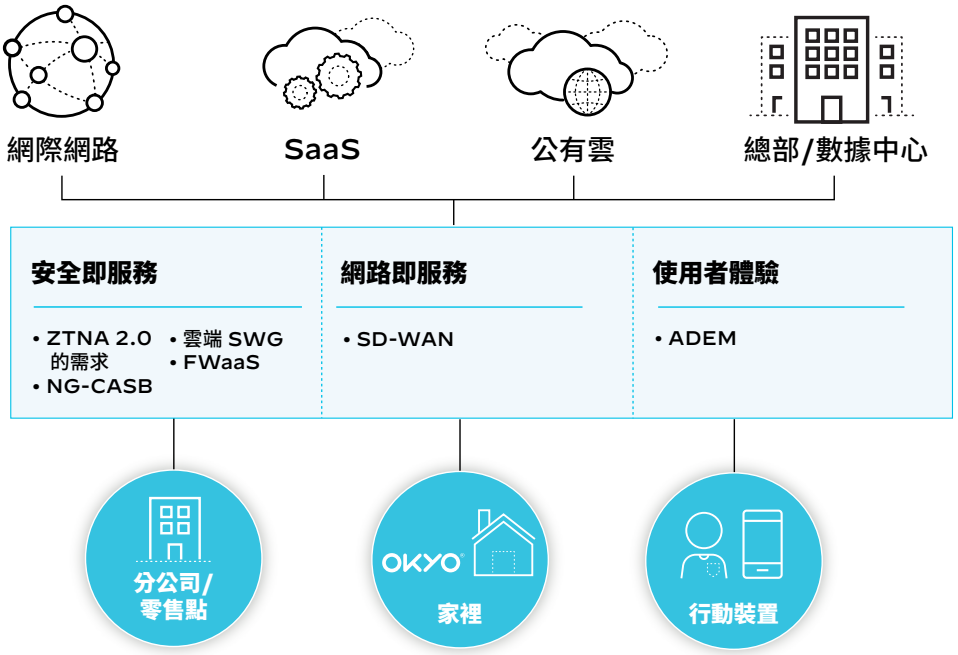

圖 1：Prisma Access 架構

表 1：Prisma Access 詳細資料、功能和規格

	面向網路的 Prisma Access	面向使用者的 Prisma Access	面向清理管道的 Prisma Access
地點	77 個國家/地區的超過 100 個地點	• 在 77 個國家/地區的超過 100 個地點 (GlobalProtect) • 25 個地點 (明確 proxy)	17 個地點
連線類型	IPsec 通道	• GlobalProtect 應用程式 IPsec/SSL • GlobalProtect 無用戶端 VPN • 明確 Proxy	透過合作夥伴互連進行的對等互連 (對於每個租用戶附加 VLAN)
GlobalProtect 應用程式平台支援	無	• Apple iOS • Apple macOS • Google Android • Chromebook 適用的 Android 應用程式 • CentOS Linux • Red Hat Enterprise Linux • Ubuntu • Windows 10 和 UWP **IoT 平台** • Raspberry Pi 作業系統 • Windows IoT Enterprise • Ubuntu • Google Android	無
網路服務層級協定			
執行時間可用性	每個月 99.999%		
連線	99.99% (1 小時內 10 毫秒)		

表 2：Prisma Access 功能	
功能	**說明**
App-ID	不論使用的連接埠、TLS/SSL 加密或攻擊者用來逃避偵測的技術為何，皆會持續對所有應用程式進行分類。不同於在運用應用程式分類之前使用第 3 層和第 4 層做為第一層控制的傳統解決方案，Prisma Access 一起運用 App-ID 與其他第 7 層控制 (如 User-ID)。
User-ID	與各種使用者身分儲存庫整合，因此您的政策可以遵循任何位置的使用者和群組。使用者儲存庫包括無線 LAN 控制器、VPN、目錄伺服器，基於瀏覽器的認證登入控制的入口網站、Proxy 等等。
Device-ID*	無論裝置連接在網路的何處，都可以建立遵循裝置的政策。基於裝置屬性 (例如作業系統版本) 的執行有助於安全團隊更嚴格控制攻擊範圍。Device-ID 記錄提供更多可視性和脈絡，而且搭配 App-ID 和 User-ID 使用，可以深入了解網路上的行為。
SSL 解密	檢查政策並套用於 TLS/SSL 加密的傳入和傳出流量，包括使用 HTTP/2 的流量。為了保護隱私權和合規性，您可以根據 URL、來源、目的地、使用者、使用者群組和連接埠彈性啟用或停用解密。
動態使用者群組 (DUG) 監控	根據使用者行為提供動態安全動作，藉以限制可疑使用者或惡意使用者。可讓您在 Prisma Access 中界定 DUG，藉以採取有時限的安全動作，完全不需要等待變更套用於使用者目錄。
以 AI/ML 為基礎的偵測	提供內嵌、無特徵碼的攻擊偵測和零時差入侵防禦。Prisma Access 可以適應和提供即時保護，而不是計劃的更新。這可以在不到 10 秒的特徵碼傳遞時間內立即阻止多達 95% 的未知威脅，因此受感染的系統減少 99.5%。
IoT Security*	將機器學習與我們領先的 App-ID 技術和群眾外包的遙測相結合，可對所有裝置進行剖析，藉以進行探索、風險評估、弱點分析、異常偵測和以信任為基礎的政策建議。這可以防禦已知和未知的 IoT、IoMT 和 OT 威脅，並且可以使用 Palo Alto Networks 機器學習式新世代防火牆或是與第三方的協調來實施原生執行。
明確 Proxy 上線	可讓客戶選擇設定用戶端 (瀏覽器) 使用 Proxy 伺服器的 Proxy 模式。這個明確 Proxy 選項是行動使用者連線到 Prisma Access 並保護網際網路和 SaaS 應用程式流量 (HTTP/HTTPS) 的另一種方法。對於瀏覽器設定支援 PAC 檔案。
PAN-OS Policy Optimizer	提供簡單的工作流程，藉以將基於連接埠的傳統規則庫轉移到 App-ID 規則庫。如此可以縮小攻擊範圍並提高安全政策的效率。
遠端瀏覽器隔離支援	運用現有的新世代防火牆 URL 分類和 URL 重寫功能，透過 CloudBlades 與第三方 RBI 雲端整合，藉以將選定/所有網際網路的流量轉送到 RBI 雲端。這項功能可提供順暢的使用者體驗，同時將某些流量 (未知或高風險類別) 轉送到 RBI 進行其他檢查，同時其餘的流量可以透過 Prisma Access 進行檢查，然後直接傳送到網際網路。
報告	作為標準的詳細、可自訂 SaaS 應用程式使用狀況報告，可以掌握網路上所有獲批准和未獲批准的所有 SaaS 流量。您也可以視需要建立自訂報告，並可輕鬆排程報告、下載報告並與企業內的其他人共享報告。
使用者驗證	支援所有現有的 PAN-OS 驗證方法，包括 Kerberos、RADIUS、SAML、LDAP、用戶端證書和本機使用者數據庫。GlobalProtect 驗證使用者後，會立即為 Prisma Access 提供使用者與 IP 位址的對應關係，以供 User-ID 技術使用。
進階 DNS Security	套用即時防護和內嵌機器學習以中止 C2 回傳和其他使用 DNS 的攻擊。進階 DNS Security 以原生方式整合至 Prisma Access，可提供自動化防護，防止攻擊者繞過安全措施，並減少對於獨立工具或變更 DNS 路由的需求。
進階 URL Filtering	可以針對如網路釣魚、惡意軟體和 C2 等網路威脅提供卓越的防護，並將強大的數據庫防護與機器學習式網路安全引擎相結合，可即時分類及封鎖新型的惡意 URL。業界領先的網路釣魚防護能夠因應最常見的入侵原因，讓您透過精細的控制和政策設定，並根據使用者、風險評等和內容類別來自動化各種安全動作，以重新掌控您的流量。
數據遺失防護 (DLP)*	包括一組工具和程序，可讓您保護敏感資訊免遭未經授權的存取、濫用、擷取或共享。Prisma Access 上的 DLP 可讓您實施數據安全性政策，並防止行動使用者和遠端網路遺失敏感數據。
數位體驗監控 (DEM)*	透過適用於 SASE 的 ADEM 附加模組，企業可取得對於行動使用者和遠端網路應用程式以及網路效能的可視性。ADEM 透過實際和綜合流量分析在整個服務交付路徑上獲得市場區隔見解，因此可以在出現數位體驗問題時進行自發性補救，包括新遠端使用者自助式服務補救與 ADEM 自助式服務。
主機資訊設定檔 (HIP)	檢查端點以取得有關設定和建立 HIP 的目錄。Prisma Access 使用 HIP 實施應用程式政策，僅允許在端點得到妥善設定和保護時進行存取。

表 2：Prisma Access 功能 (續)	
功能	**說明**
裝置隔離	阻止遭入侵的裝置存取權限數據。您可以手動或自動將遭入侵的裝置新增到隔離清單，並且阻止使用者使用 GlobalProtect 從這些裝置登入網路。您也可以限制從這些遭入侵的裝置存取應用程式。
服務品質 (QoS)	可讓您在有限的網路容量下妥善執行高優先順序的應用程式和流量。QoS 會優先處理關鍵業務流量或要求低延遲的流量，例如 VoIP 或視訊會議。您也可以為企業關鍵應用程式保留最低程度的頻寬。
IPv6 內部流量	保護端點與私人應用程式之間的所有內部 IPv6 流量。目前已針對行動使用者、GlobalProtect、遠端網路和服務連線提供支援。
站台對站台 IPSec VPN	支援透過 IPv4 和 IKEv1/IKEv2 的站台對站台通道，藉以確保相容性。對於多個連線站台，ECMP 路由可以透過平衡可用網際網路連線的工作階段來達到額外的備援和成本效益。
記錄	顯示整體流量、應用程式、使用者、威脅、URL 和數據篩選器記錄，藉以透過雲端式 Cortex Data Lake 整理數據。
政策自動化	可讓您使用來自第三方來源的資訊，透過動態位址群組 (DAG) 和 XML API 的組合動態進行安全性政策更新。
入侵防禦系統 (IPS)	阻止弱點入侵、緩衝區溢位和連接埠掃描。其他功能 (例如阻擋無效或格式錯誤的封包、反 IP 分散以及 TCP 重組等等) 可防範攻擊者的規避和模糊化手段。從 WildFire 惡意軟體防禦服務持續更新基於弱點的特徵碼。自訂特徵碼也可以手動匯入，包括從 Snort 和 Suricata 之類的常用格式匯入。
反惡意軟體	使用基於串流而且能夠快速內嵌阻止的引擎，偵測已知的惡意軟體以及已知惡意軟體系列的未知變體。IPS 和反惡意軟體使用一個授權即可解決多種威脅途徑，因此完全不需要向傳統安全廠商購買和維護基於 IPS 和 Proxy 的個別產品。
C2 防護	阻止源自惡意軟體感染的惡意傳出通訊、被動分析 DNS 查詢，並識別殭屍網路的獨特模式。這可以揭示受感染的使用者，並阻止二次下載和數據離開企業。
使用進階分析進行的未知威脅偵測	使用來自業界最大企業惡意軟體分析社群的共享數據識別未知威脅，包括從網路、端點、雲端和第三方合作夥伴提交的威脅。運用我們的自訂超級管理器和裸機分析功能，WildFire 使用各種互補的分析引擎，可以偵測到規避沙箱的攻擊。
防範未知威脅	初次發現新威脅 (封鎖惡意檔案、對於惡意 URL 和 C2 流量進行的存取) 後，會自動在整個攻擊生命週期中產生保護，然後針對大多數新威脅在數秒鐘內對所有 WildFire 使用者提供這些保護措施。
檔案行為分析	使用詳細的行為分析來協助您了解新發現的惡意軟體所呈現的運作方式。整合式日誌可讓您快速識別受感染的使用者，並且透過對未知威脅事件的仔細分析和可視性來調查潛在的洩漏。
雲端防禦	採用獨特的雲端模組化架構，可根據全球威脅情報提供自動防禦，完全不需要在網路的每個入口/出口點實施和管理網路和電子郵件的個別裝置。
多重途徑分析和可視性	將 WildFire 的雲端規模與進階檔案分析和 URL 抓取相結合，多重途徑遞迴分析提供全面的獨特解決方案，可防止多階段、多重躍點攻擊。不同於其他解決方案，即使在指定階段執行失敗，WildFire 也會經歷多個攻擊階段。WildFire 造訪內嵌連結或電子郵件中的連結進行電子郵件連結分析時，如果任何對應的網頁涉及入侵或顯示網路釣魚活動，則會更新 URL 篩選。
全面的檔案執行	同時執行多個作業系統和應用程式版本中的未知檔案，藉以完全了解威脅的範圍。多版本分析可確保徹底進行 WildFire 分析，這不同於需要黃金映像的沙箱，沙箱可能會認為惡意檔案是良性的，只是因為並未在黃金映像中指定目標作業系統或應用程式版本。

注意：可能存在地區差異。如需詳細資訊，請參閱 Prisma Access 服務層級協定。

* 需要附加模組授權。

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