ZTAG零信任存取閘道

確保應用存取安全

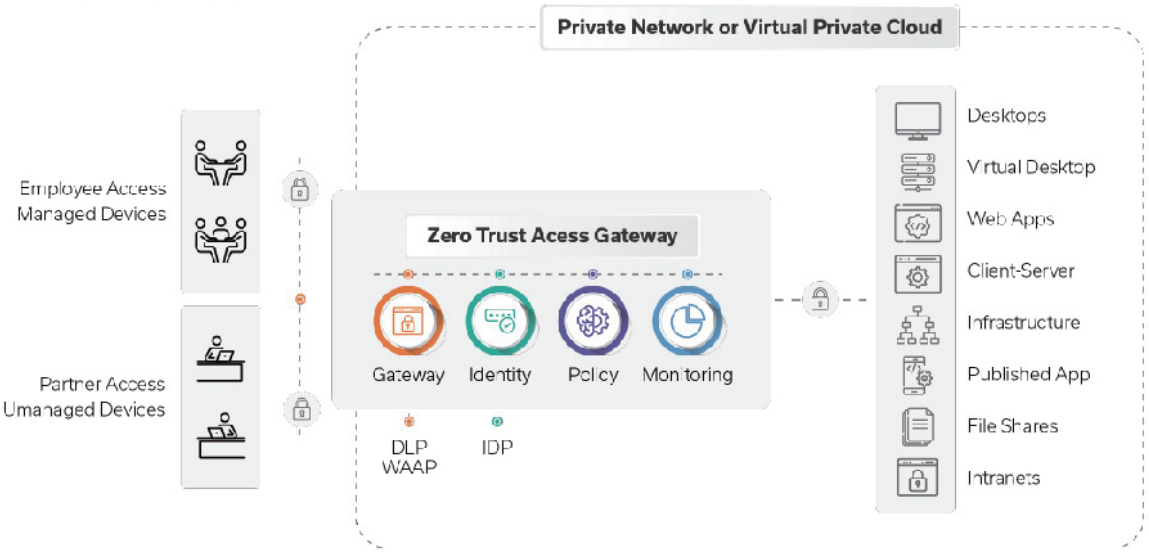
傳統資安防護主要依賴邊界防禦，透過防火牆來阻擋外部未經授權的訪問，而 VPN 則用於內部應用的遠端存取。然而，隨著雲端應用的普及與企業用戶的行動化發展，現代企業需要一種能夠隨時隨地提供安全存取的機制，無論應用或使用者身處何地。

此外，攻擊手法日益複雜，駭客透過釣魚攻擊、暴力破解、惡意軟體等技術滲透傳統防護機制。因此，「零信任」（Zero Trust）架構因應資安威脅與企業需求誕生，不僅能有效對抗攻擊，還能確保業務的持續運行。其核心概念為「永不信任任何人」，即所有存取請求皆須驗證，並搭配最小權限原則授權使用者只能存取特定服務。

ZTAG 提供連續性的應用層級存取保護，確保內外部員工與合作夥伴安全存取企業資源。

ZTAG 零信任安全架構

Array ZTAG 提供最高等級的遠端安全存取解決方案，滿足企業對可擴展性、可靠性、靈活性與資安要求的標準。



ZTAG 功能特色

SPA 單一封包授權

提供 UDP 端口敲門驗證，未授權前封鎖所有端口，阻擋 IP / TCP 連線，確保存取安全與隱蔽性。

動態存取授權

依使用者身份、應用、設備狀態及環境風險調整存取權限，確保最小權限存取原則。

端點安全檢測

檢測作業系統、應用程式與防護狀態，未符合資安標準的設備將無法接入網路。

身份驗證與單一登入 (SSO)

支援 LDAP、SAML、OIDC 與雲端 IDaaS，提供多重身份驗證(MFA)與單一登入(SSO)以簡化存取流程。

角色導向存取政策

依據身份、應用與 URL 制定存取政策，提供詳細的存取紀錄與稽核能力。

客製化虛擬入口

最多可建立256個入口，根據不同使用者群組 客製化存取權限與安全性偏好。

任何裝置皆可安全存取

支援Windows、Mac、Linux、iOS、Android、Chromebook。

混合雲與虛擬部署

支援實體設備、虛擬化應用(VM)及雲端平台(AWS, Google Cloud)部署，滿足不同環境需求。

零信任安全存取
確保遠端存取無漏洞

面臨挑戰

- 遠端存取安全風險：政府機構需確保內部人員與外部合作夥伴的存取安全，避免未授權存取與資料外洩。
- 傳統 VPN 弱點：既有的 VPN 架構無法有效防禦進階持續性攻擊（APT），且存取權限難以動態調整。
- 合規與政策需求：須符合政府資安規範，確保內部機敏資訊的存取安全與合規性。
- 設備端點安全性不足：需提升終端裝置的安全檢測能力，以避免受感染設備存取內部系統。

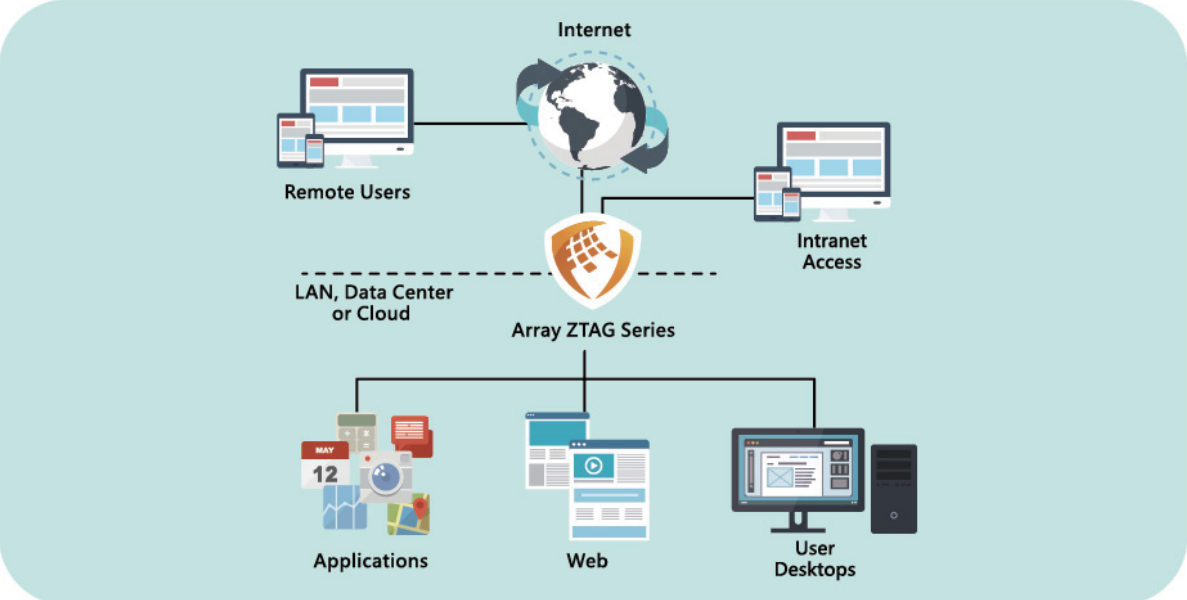
導入方案

ZTAG 透過零信任安全機制，確保每一次存取請求皆經過嚴格驗證，防止未授權存取：

- SPA 單一封包授權：三層驗證機制，內外網隱身，存取閘道更隱密。
- 動態存取授權：根據風險即時調整存取權限，降低資安風險並確保業務不中斷。
- 端點安全全面檢測：自動偵測多重裝置安全，確保僅合規設備可存取機敏資訊。
- 高效能存取架構：提供低延遲、高可擴展性的安全存取解決方案，支援大量遠端工作者。

達成效益

- 存取安全提升：透過零信任架構，確保只有經過驗證的使用者與設備才能存取機敏資訊。
- 動態權限管理：根據風險情境即時調整存取權限，提高安全性與業務連續性。
- 合規與風險降低：符合政府資安規範，確保機敏資料存取安全，避免罰款與法律風險。



台灣代理 定承資訊 股份有限公司
電話：(02)8228-7155 傳真：(02)8227-8508
地址：235603新北市中和區中正路700號15樓之6