SecuTex ZTA 零信任織網解決方案

為何企業需要注重 ZTA？傳統防禦已不足抵禦持續變化的威脅

在現今數位時代事實證明，基於邊界保護的遠端連線方法已過時，無法應對網路釣魚、勒索病毒及 APT 攻擊(Advanced Persistent Threats)。相對的，ZTA 提供企業安全連線，且不會影響可及性及易用性。

在臺灣最近的網路事件中，安全的存取控制的重要性變得顯而易見。回顧國內知名租車公司個資外洩事件，皆有驗證及存取控制不足的狀況，導致數十萬筆顧客個資外洩。此外，利用竊取的憑證和身分驗證漏洞也是常見的入侵手段。根據中華資安國際 2021 年之事件調查統計數據，「利用公開漏洞」在駭客的初始入侵方法中排名第一，其次是「帳密外洩」。此外，10%的公開漏洞利用是基於身分驗證的漏洞。這凸顯了 ZTA 的必要性，該技術提供更安全的存取控制，以保護重要資產和資源。

ZTA 是什麼？ ZTA 是一種安全模型，其核心是驗證試圖存取網路的每個使用者和每個設備，並根據該身分提供嚴密的存取控制。與基於網路位置的信任假設不同，ZTA 通過持續驗證和動態策略實施信任。透過實施中華資安國際的解決方案，每個企業資源都將根據組織的中央存取策略擁有有條件的、每次請求的存取權限。

該解決方案可從任何地點安全、無縫地存取企業資源。此解決方案有許多關鍵優勢，包含：

- 身份和情境感知存取：在憑證被盜用和存取權杖(token)被竊的情況下，存取控制應超越身份本身。此解決方案驗證每個使用者和設備的身份，然後利用外部情資做出更好的決策，限制惡意內部人員與帳戶入侵所造成的損害。
- 提高可及性和易用性：此解決方案可從任何地點安全存取企業資源，而無需 VPN 或傳統的周邊安全模型。在邊界部署此解決方案，使終端用戶不會遇到連接或延遲問題，使組織擁有運作靈活性和敏捷性。
- 簡化管理：通過簡化存取控制、策略和使用者身份的管理，我們使組織能夠維護安全且易於存取的環境。IT 團隊可以避免將網路分段，而是選擇與此解決方案進行相互驗證，確保內部服務運行更順暢，同時限制橫向移動。
- 稽核日誌：誰存取了什麼、何時、在哪裡以及他們做了什麼？此解決方案提供細粒度的基於請求的稽核日誌，確保組織可以了解網路內發生的所有事情。