Trend ZTA

> 零信任架構的假設前提是：在確認可信之前，沒有任何連線、使用者或資產可以信任。反觀傳統以邊界為基礎的資安架構則認為，一旦連線通過了認證就值得信任，因此可存取整個網路，這使得企業資產經常成為網路犯罪集團的目標。能改造企業但卻耗時的零信任專案，通常建立在現有的架構之上，然後加以改造。

零信任架構

零信任架構是一種持續演進的概念，目前尚無任何認證或實際的標準可供遵循。許多企業都仰賴一些產業認證，如 International Organization for Standardization (ISO) 認證來讓他們有所遵循，而零信任目前並無明確的定義，因此也造成了一些觀念上的混淆。

在這樣的混淆下，有些廠商會宣稱某項產品或服務是一套完整的零信任解決方案，但這完全忽略了零信任只是一套方法，它可以使用現有或新開發的產品或服務，但並不等於某種產品或服務。

零信任框架

目前市面上有各種零信任框架和方法。雖然零信任是一種概念，但美國國家標準與技術局 (National Institute of Standards and Technology，簡稱 NIST) 和 Forrester、IDC、ESG 等研究機構，都對零信任框架的基本元素提出了他們的定義。 - Gartner 使用「安全存取服務邊際」(Secure Access Service Edge，簡稱 SASE) 一詞來統稱「雲端存取安全代理」(Cloud Access Security Broker，簡稱 CASB)、安全網站閘道 (SWG) 及進階虛擬私人網路 (VPN) 的組合 - Forrester 則稱之為「零信任邊緣」(Zero Trust Edge，簡稱 ZTE)

零信任基本原則

- **將所有資料和服務都視為資源**
  - 軟體服務 (SaaS)、雲端服務等各類服務，以及存取企業資源的個人裝置，都可納入零信任的範疇之下
- **絕不信任網路位置或身分**
  - 傳統的邊界防護僅靠一道門來把關想要存取企業資源的使用者。使用者只要通過認證，就能存取各式各樣的企業資產。但這樣的作法也為駭客開了一道方便之門。一旦駭客進入了企業，他們就能在內部網路四處遊走，順便安裝各種惡意程式和勒索病毒
- **授予的資源存取權限只限用於當下的連線階段**
  - 先建立信任，然後再授予存取權限，並且只提供執行工作所需的最低必要權限
- **根據動態的政策來決定存取權限**
  - 持續監控的使用者、裝置和行為 (例如觀察到的使用模式) 等條件的風險等級。也可包含環境周邊條件，例如：網路位置、時間、進行中的攻擊。
- **沒有任何資產天生值得信任**
  - 藉由一套持續監控系統在某項資源請求期間評估資產的資安情況。將個人裝置也納入考量，選擇這些裝置該有的存取等級
- **不斷重複驗證是否繼續信任**
  - 一旦使用者或裝置的風險升高，就必須斷然採取行動，立即將連線終止，或者將帳號重設
- **嚴格執行認證與授權**
  - 使用動態原則在通訊過程當中持續掃描、評估威脅、做出調整，然後再重新評估是否繼續信任

- **盡可能蒐集越多資訊**
    - 好好利用這些資料來了解該如何改善資安政策以及政策的落實