VMware ZTA

零信任是一種 IT 安全性方法，不僅假設受信任的網路周邊並不存在，也會先行驗證每一筆網路交易，再予以放行。

- 會依循「永不信任，一律驗證」的原則，並運用其他多項網路安全性方法，包括網路分段和嚴謹的存取控制
- 定義一個「保護範圍」，以納入重要資料、資產、應用程式和服務
  - 保護範圍僅包含重要資產，因此規模通常遠不及整體攻擊範圍
- 零信任安全性會將信任視為弱點
  - 「受信任」網路中的使用者，皆有能力在網路中四處移動，或造成自身可存取的任何或部分資料發生外洩
- 零信任架構不會嘗試建構受信任的網路，而是完全排除「信任」的概念
- 一旦決定好保護範圍，就會運用多項關鍵依據來建立和強制執行受保護資料的安全存取原則
  - 網路流量如何流經此一範圍
  - 哪些使用者正在存取受保護資料並為所使用的應用程式建立目錄
  - 採用何種連線方法

VMware 如何實現零信任架構？

1. 識別保護範圍(包括敏感資料和應用程式)
   - 簡單的三大類別模式，內容區區分為
     - 公開
     - 內部
     - 機密
2. 比對所有敏感資料的交易流量
   - 資料如何在人員、應用程式，以及連往商業合作夥伴及客戶的外部連線之間移動
   - 公開且保護網路和系統物件的相依性
3. 定義每個微周邊的零信任架構
   - 以資料和交易在企業 (和外部合作夥伴) 流動的方式做為依據
   - 透過軟體定義的網路 (SDN)
   - 使用實體或虛擬新一代防火牆的安全性通訊協定來達成
4. 在網路設計完成後建立零信任原則
   - 只讓已知且經授權的應用程式或使用者存取保護範圍，同時假定所有個人裝置都不安全
5. 進行自動化、監控和維護

零信任的核心原則為何？

> 「永不信任，一律驗證」

- 防範關鍵業務資產遭到窺探，或遭受惡意軟體攻擊
- 無法藉由單一方法或技術達成
- 推動零信任，企業可能需要重新評估每項資產的保護方式
- 零信任不會判斷要求來源及網路安全與否，而是嘗試驗證特定的使用者和裝置，以確保對方確實如所宣稱的一樣

- 零信任要有能力根據所提供的其他驗證機制，對裝置授予信任