

Zero Trust Architecture

Zero Trust and Zero Trust Architecture

- Zero Trust (ZT, 零架構) 是面對資訊系統與服務在被視為已被入侵的網路環境中運作時，為了讓每個存取請求決定的不確定性最小化，並是在執行準確且最小權限下去執行，所提供的一系列概念與想法
- 就 Zero Trust Architecture (ZTA, 零信任架構) 言，這是一種企業網路安全計畫，當中利用了零信任概念，包含元件關係、工作流程規畫與存取政策。

就整個網路安全策略而言，當企業決定採用零信任作為網路安全核心戰略，就需要根據零信任原則來制定計畫，以產生零信任架構，之後，將需要部署與打造零信任環境，讓企業來使用。

零信任所要解決的問題

1. 防止未經授權存取資料與服務
2. 使存取控制盡可能做到更精細

目的：讓未經授權存取的風險降到最低

- 只讓經過授權與允許的主體可以存取資料，而不讓攻擊者等其他主體能存取，而這裡的主體，包括使用者、應用程式或服務，以及裝置
- 在零信任 (ZT) 與零信任架構 (ZTA) 所指的資源存取，不僅僅包含資料存取，也包含像是印表機、運算資源與物聯網設備等

如何存取 ??

- 由於存取控制有其不確定性，因此存取決策的重點將放在 身分驗證、授權與限縮默示信任區域，同時，需要盡可能減少身分驗證機制的時間延遲，以保持可用性，並盡可能讓存取規則更精細，讓每次資源存取請求的操作，只提供所需的最小權限。