Zero Trust Architecture, ZTA

零信任架構

零信任架構是一種建立 IT 安全性的概念，其假設前提為：確認可以信任之前，沒有任何連線、使用者或資產可以信任。目前尚無任何認證或實際的標準可供遵循。

以往連線通過了認證就會視為可以信任，能夠存取企業網路內的所有資源，導致企業成為網路犯罪的目標。在零信任架構中，排除「信任」概念，將信任視為弱點。畢竟，網路中「受信任」的使用者，皆有可能在網路中四處存取，或造成自身可存取的任何或部分資料發生外洩。

零信任會依循「永不信任，一律驗證」的原則，搭配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。零信任架構會定義「保護範圍」，將重要資料、設備、程式和服務納入。

所有的資料來源與運算服務都被視為資源

不管無論網路位置何在的裝置通訊，都需要確保安全

對於個別企業資源的存取要求，應該要以每次連線為基礎去許可

資源的存取應該要基於客戶端識別、應用服務，以及要求存取資安可觀察到的狀態，以及可能包括的行為或環境屬性，去動態決定

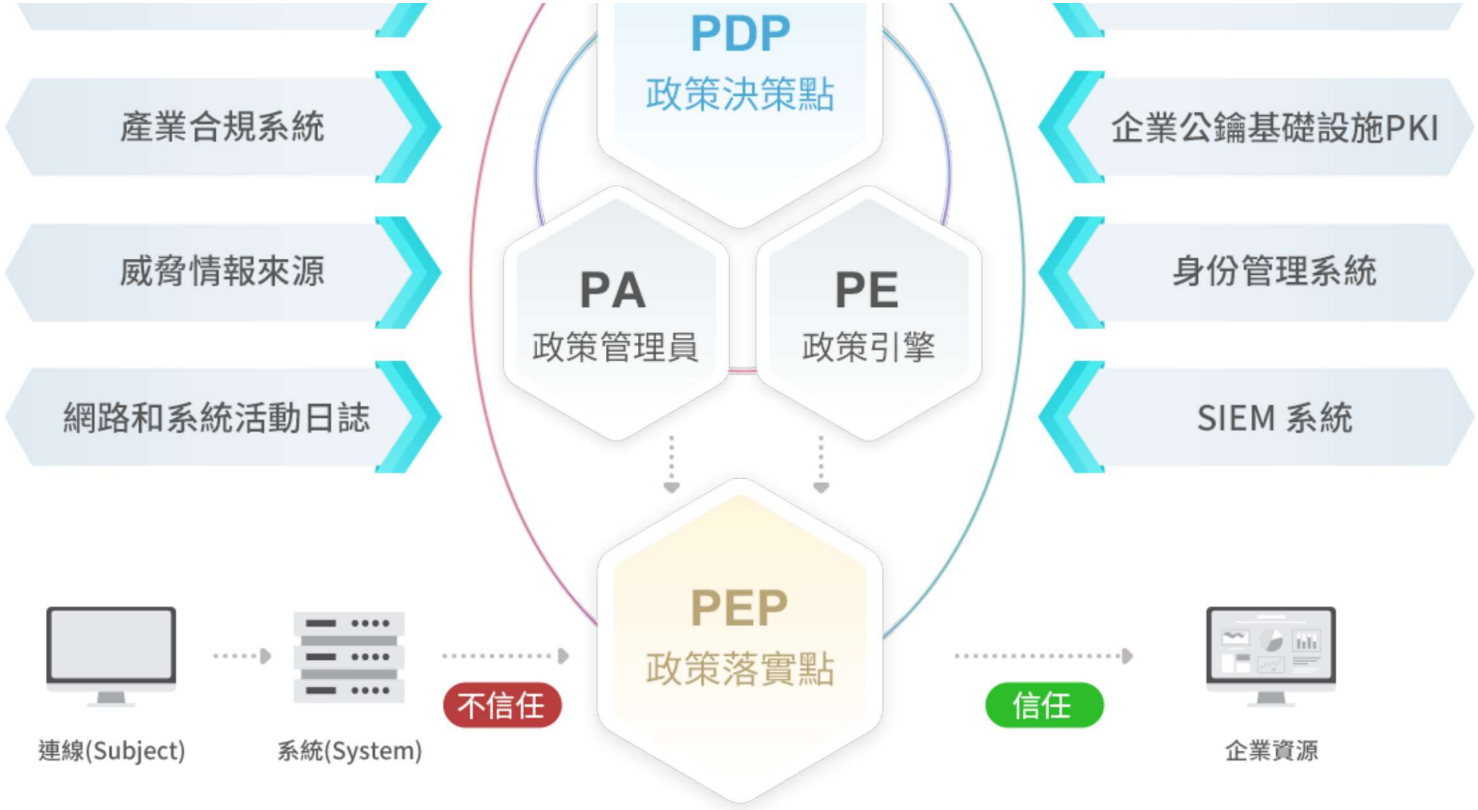
企業監控與衡量所有擁有與相關資訊資產的正確性與安全狀態

在允許存取之前，所有的資源的身分鑑別與授權機制，都要是依監控結果動態決定，並且嚴格落實

企業應該要盡可能收集有關資訊資產、網路架構、骨幹，以及通訊的現況，並用這些資訊來增進安全狀態。

零信任架構模型

上面提到零信任架構是一種概念，是虛擬的，如果把概念具體圖像化，會類似於下方的架構圖。左側來自外部的連線經由系統想要存取企業內部資源，都要預設視為不信任(untrusted)狀態，必須要通過零信任的政策落實點(PEP)的檢核，成為可信任(trusted)狀態後，才可以存取企業內部資源。 判斷來自外部的連線是否可信任，則是交給政策決策點(PDP)來決定。政策決策點由兩部分組成，政策引擎(PE)及政策管理員(PA)。政策引擎(PE)，簡單來說就是一種檢核機制，收集來自外部情報來源，彙整之後交給政策管理員(PA)作出是否放行連線。然後最後由政策落實點(PEP)負責執行。



PE

政策引擎

根據政策和外部情報系統判斷是否該授予存取權限

PA

政策管理員

根據 PE 的決策來放行或關閉存取權限

PDP

政策決策點

由PE & PA 組成，作出是否給予存取權限

PEP

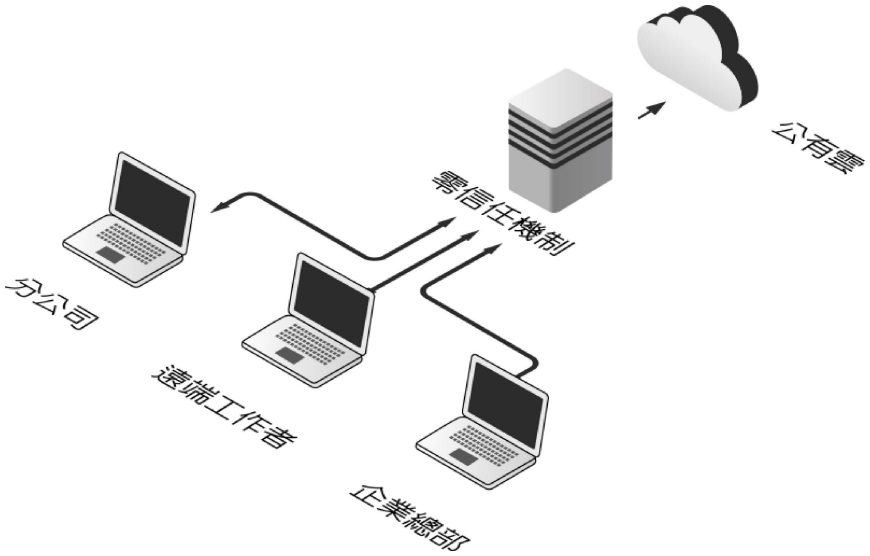
政策落實點

負責准許、監控和終止存取

零信任適用場景

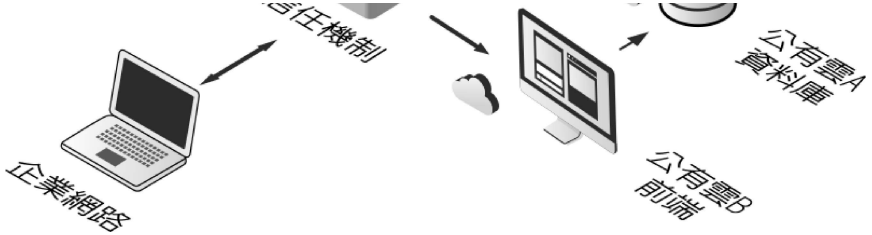
有多處辦公地點或遠距辦公的企業

企業擁有多個辦公地點或是允許遠距辦公，是很常見的情況。如何控管可以存取企業網路資源的設備及設備的權限，對企業來說很重要。遠距辦公的員工有可能會使用自己的筆電或行動裝置，存取企業網路完成工作。面對這種情況，企業要做好對於資源分類及存取控管。例如，內部行事曆、電子郵件可以給大多數的員工存取；資料庫等機敏資料就要加強限制。



使用跨公有雲服務的企業

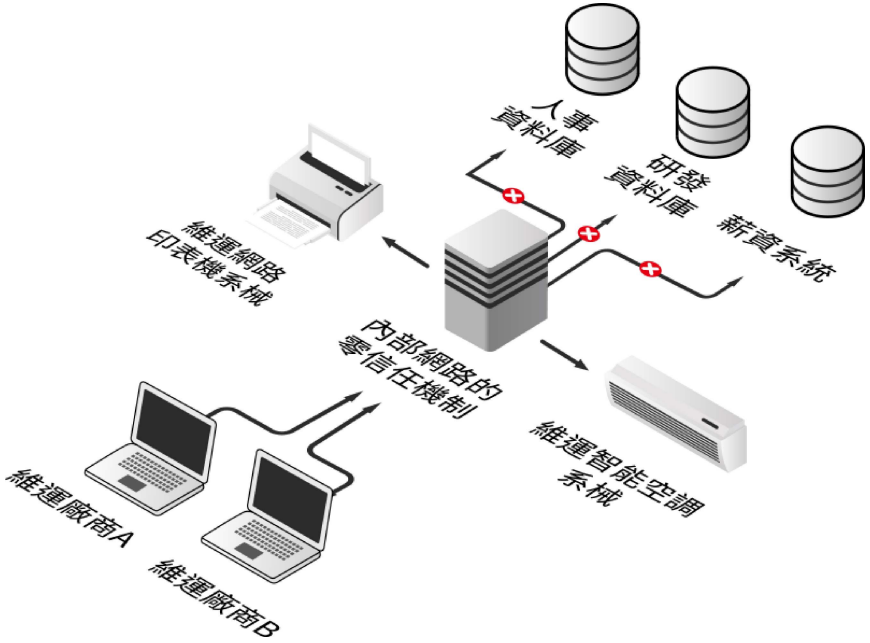
越來越多企業使用公有雲來託管程式或服務，甚至把程式及資料庫分別放在不同的公有雲上。基於效能表現及管理來說，應該由位在B公有雲的程式應該直接連線A公有雲的資料庫，而非強制透過企業網路才連到資料庫。

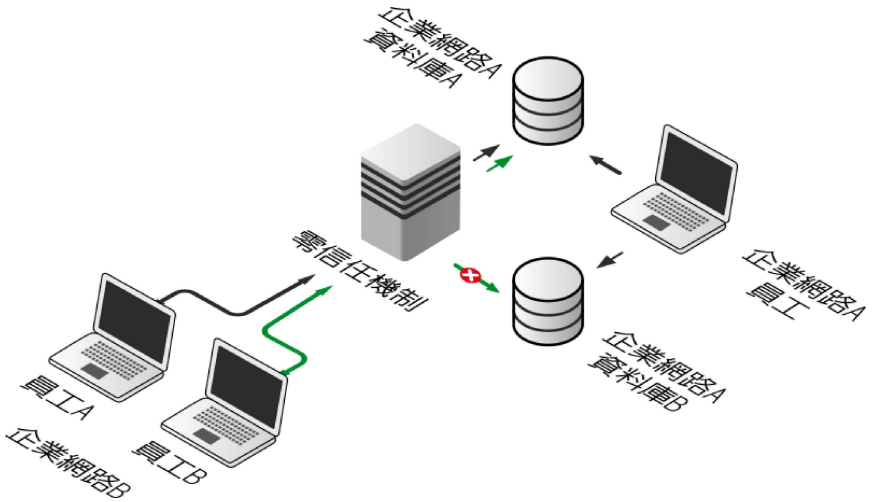


師協助企業執行。

有外包廠商或非員工存取的企業

現行企業或多或少都有部分設備或服務是由外包的維運廠商負責，例如網路印表機、智能空調系統等。外包的維運廠商員工來到現場時，需要連到企業內部網路才能進行工作，例如連回去自家系統下載更新。以往連到企業網路內部就可以看到並存取企業資源，可能造成資料外洩。在零信任架構下，通過身份驗證之後，可以允許外包的維運廠商員工連線使用企業網路，但是無法取得授權使用企業內部資源或程式，例如人事系統、研發系統、薪資資料等。





有跨企業協作的企業

某專案關連到A和B兩個企業的員工。A企業負責管理/操作專案資料庫，需要允許企業B部分成員存取資料庫A。類似之前提到的「有多處辦公地點或遠距辦公的企業」，因為雙方沒有同屬一個企業網路，需要存取的資源位在另外一個企業網路中或公有雲上。表示不需要設置複雜的防火牆規則或企業存取控制列表(ACL)，即可允許企業B某些IP存取企業A的資源，而且合乎企業A的存取策略。如何達成這種存取決策取決企業所使用的技術。

零信任成熟模型





傳統方式	1. 密碼/多階段身份驗證 2. 有限的風險評估	1. 提供有限的合規性 2. 只有簡易盤點	1. 大型微分段架構 2. 最小程度的內外部流量加密	1. 依據本地授權存取 2. 低度與工作流程整合 3. 部分雲端可存取性	1. 未良好進行盤點 2. 靜態控管 3. 未加密
進階方式	1. 多階段身份驗證 2. 結合雲端及本地系統進行身份驗證	1. 強制執行合規性 2. 依據首次存取的設備狀態決定資料存取	1. 由出入口微邊界定義 2. 基礎的分析	1. 依據集中式授權存取 2. 與工作流程有基本的整合度	1. 最低限度權限控管 2. 儲存在雲端或遠端環境的資料採靜態加密
理想方式	1. 持續驗證 2. 即時性機器學習分析	1. 持續設備安全性監控及驗證 2. 依據即時風險性分析進行資料存取	1. 完全分佈式的出入口微邊界 2. 以機器學習為基礎的威脅分析 3. 所有流量皆有加密	1. 持續性授權存取 2. 高度與工作流程整合	1. 支援動態加密 2. 所有資料皆有加密

零信任潛在風險

沒有企業可以完全避免網路安全風險。當與現有的網路安全策略和指南、身份和存取管理、持續監控和一般網路衛生(cyber hygiene)相輔相成時，正確執行和維護零信任架構(ZTA)，才可能降低整體風險並防止常見威脅。不可否認的是，一部分風險是在執行零信任架構(ZTA)時才會凸顯出來。

往來是不被允許的。企業必須正確配置和維護，資源才能交互往來。任何對PE規則具有設置存取權限的管理者都可以執行未經允許的更改或犯下錯誤，進而破壞企業營運。同樣，無法嚴守標準的PA可能允許那些本來不被允許存取資源的設備進行存取(例如已被入侵的個人設備)。為了降低相關風險意就代表著必須正確設定及監控PE和PA，必須記錄任何設置變動並接受稽核。

營運產生不良影響。在安全的雲端環境執行零信任策略，可以降低網路風險。請注意，這樣做可以減輕風險，但不能無法完全消除風險。大規模的DoS攻擊或是雲端服務商不小心讓企業服務離線。以上的情況都會造成無法存取企業的網路資源。

憑證遭竊/內部威脅

存取企業重要資源的帳號，是駭客感興趣的。駭客會利用網路釣魚、社交工程或混合攻擊，取得帳號認證。根據動機不同，「價值」有不同定義。有些針對系統管理者，有些針對存取金融資源的帳號追求經濟利益。啟用多重要素驗證(MFA)可以降低資料外洩的風險。對於取得有效認證的駭客(或惡意內部人員)仍然可以存取帳戶可以存取的企業資源。零信任架構(ZTA)可以降低風險並防止任何遭入侵帳戶或資產在企業網路中進行橫向移動。

網路可見性

網路大部分流量對於layer 3網路分析工具來說是不透明的。流量可能來自非企業的資產或抵抗被動監控(passive monitoring)的服務。無法檢測封包或加密流量的企業必須找尋方法評估網路風險。企業可收集加密流量的元資料(Metadata)(例如來源和目的地位址等)，檢測網路的活躍攻擊者或潛在的惡意軟體。機器學習可用於分析無法解密和檢查的流量，幫助企業將流量分類為有效或可能是惡意的，並進行補救。

系統及網路訊息的儲存

監控掃描、網路流量及元資料(Metadata)儲存是用於建構上下文策略(contextual policies)、鑑識(forensics)或後續分析，這些資料會成為駭客的目標。像是網路圖(network diagrams)、設定檔(configuration files)或其他網路架構文件，也該受到保護。對於所有具有價值的企業資料，都應該採取適當的保護措施，以防止未經授權的存取，具備最嚴格的訪問策略，只能透過指定的管理帳戶進行存取。

使用專有資料格式或解決方案

儲存及處理資訊的資產，對於如何處理或交換資訊，沒有共同的開放標準。可能導致企業缺乏互用性(interoperability)，被侷限於採用某些特定供應商。如果供應商出現危機或中斷供應，會付出極高代價(更換資產)，才能更換新供應商。或者歷經很長的轉換程序(從現存策略移轉)。為了降低風險，應該在效能表現、穩定性之外，根據安全控管、轉換成本和風險管理等，對供應商進行評估。

在架構中使用的非個人實體(AI和代理程式)

零信任導入流程

企業導入零信任架構並不是馬上就能導入，成功實施。應該採取階段式導入，由部分單位或系統率先嘗試，一邊導入一邊掌握零信任實施狀況，隨時調整。等到企業習慣零信任機制後，再逐步擴展至其他單位或系統，以降低企業在導入時的風險及不確定性。

01

識別主題

由哪個單位那些人主導負責零信任導入專案，才不會沒有人作出決策並負責。

02

識別資產

企業要確認本身的資產及相關會用到的資源，才能確認零信任架構實施範圍。

03

識別企業程序與風險

企業整體要理解導入零信任的程序以及相關風險，藉以決定是否導入零信任。

04

發展政策

企業的零信任政策是規劃基礎，需要確認資源標準或加權比重作為依據。

05

識別可行方案

當零信任政策確認後，可由架構師規劃數個可行方案，讓企業內部討論選擇。

06

初步部屬與監控

決定好要實施的零信任方案後，可以進行初步部屬，並隨時監控動態調整。

07

拓展

當企業及員工越來越熟悉零信任架構，可以開始規劃下一階段的零信任部署。

捕夢網數位科技有限公司
Service@pumo.com.tw 客服信箱 02-8226-9123

統一編號 80472760