NIST 800-207 零信任架構（Zero Trust Architecture）

1 簡介

傳統典型企業的基礎架構日益複雜，企業內部可能擁有多個內部網路、分公司員工使用當地基礎設施的工作、行動裝置應用程式以及使用雲端服務。現在企業的網路架構幾乎沒有單一的、易於識別的邊界，因此傳統基於網路邊界安全的防護方法也被證明是不夠的，一旦攻擊者突破了邊界防護，進入內網就可暢行無阻的橫向移動。

如此複雜的企業環境導致發展出一種被稱為「零信任」（Zero Trust，ZT）的新網路安全架構。零信任著重於保護企業資料、服務，和所有企業的資產（包含實體設備、基礎架構元件、應用程式、虛擬平台和雲端服務元件）和主體（終端使用者、應用程式、自動化執行的資源存取請求）。本文件中當終端使用者為人類，則採用「使用者」這個名詞，其他則使用通用的「主體」一詞。

零信任安全模型假設環境中隨時存在攻擊者，企業內部或任何非企業的環境都不值得信賴。換言之，零信任，是將原本的信任視為弱點，企業不再存有任何預設的隱性的信任，對於內部資產和業務流程必須不斷分析和評估風險，並制定保護措施來緩解風險。在零信任中，這些防護措施要求主體盡可能對資源的存取降至最低，只允許那些被確定為需要存取的使用者對資產進行存取，並持續對每一個存取請求的身分及安全狀態進行驗證、授權和檢查。

零信任架構（Zero Trust Architecture，ZTA）是基於零信任原則的企業網路安全架構，目的在盡可能防止資訊外洩並限制內部的橫向移動。本文件討論零信任架構的定義、組成零信任架構的邏輯元件、可能的佈署方案和威脅、零信任網路架構設計方法、遷移到零信任架構過程的路線圖，同時討論影響零信任架構的相關美國聯邦政策，透過 7 章節介紹實現零信任架構的指引。

零信任是一套關於工作流程、系統設計和維運操作的指導原則，其用途為改善任何機密分類或敏感資料的安全狀況。朝著 ZTA 網路安全邁進之際，企業與組織要先有過渡是一段漫長過程的心理準備，因為遷移到 ZTA 是持續的技術革新也是組織持續評估其業務風險的過程，並不只是全面技術替換。事實上，現在企業的 IT 基礎架構就已經有 ZTA 元素，組織對於零信任原則與流程上的變動，應該要逐步實施，並採用保護資料資產與業務功能的技術解決方案。因此，邁向零信任網路安全架構的過程，大多數企業都是同時以零信任與以傳統邊界防護的模式的方式並行，透過持續投資轉向 ZTA 並改善業務流程。

由於零信任一詞在字面上容易造成誤解，因此應釐清其含義：關於零信任一詞，網路安全是一大前提，在大部分情境下的可能只直接聯想到「預設都不信任」，此假設不只是在網路安全領域，在許多不同資安構面中，常常也隱含這樣的概念。以白名單機制為例，就是除了名單上列出的標的外，預設都不允許存取，這部分道理是相通的，還有許多情境也都是如此。但網路安全零信任的內涵不僅於此，也因此，普遍大眾首次聽到零信任一詞，每個人想像到的輪廓可能不同，就容易搞混。

網路安全零信任發展至今，對應的是傳統邊界防護策略，概念是不因內網或外網而有信任或不信任的區別，零信任架構當中具有相當多的內涵，包括從預設都不信任出發，進行持續驗證、動態評估等，在架構面還包含具備零信任的原則、核心元件與必要技術等。

美國聯邦機構致力於零信任的歷史

在「零信任」一詞被創造出來之前，零信任的概念就已經存在於網路安全中。美國國防部轄下的國防資訊系統局（Defense Information Systems Agency，DISA）曾公布更加安全的企業戰略改善作法，稱之為「黑核」（BlackCore，BCORE）。「黑核」的理念是由傳統基於邊界的防禦模式，改進為每次存取請求都要檢查的模式。

在 2004 年，傑里科論壇（JerichoForum）宣揚了去邊界化的想法：限制存取的網路的預設隱性信任，以及限制採用依賴於單一大型網段的靜態防禦。

去邊界化的概念逐漸演變，到了 2010 年由 Forrester Reseacher 公司副總裁 John Kindervag 創造了更大的零信任概念，並成為描述各種網路安全解決方案的術語，零信任概念將安全性從基於網路位置的預設隱性信任轉移到專注於評估每筆交易是否可信任的模式。

這十多年來，美國聯邦機構積極轉向基於零信任原則所建立的安全管理和政策，例如，聯邦資訊安全管理法案（FISMA）、風險管理框架（RMF）、聯邦身分憑證和存取管理（FICAM）、可信任網際網路連接（TIC），以及持續診斷和緩解（CDM）計劃等，所有這些計劃目的都在限制被授權方對資料和資源存取的範圍。起初啟動這些制度時，因受到傳統資訊系統技術能力的限制，導致只能執行靜態的安全策略，並僅在企業可以控制的“瓶頸點”上實施，以獲得最大的工作效益。隨著技術日益成熟，已經可以做到更細緻地動態持續分析和評估存取請求，以“需要存取”為基礎授權，降低因使用者洩露帳戶密碼、受攻擊者監聽網路封包和其他威脅而導致的資安風險。

零信任網路架構，逐漸進化成形的歷史：

◆ 2003、2004 年，網路邊界消弭（De-perimeterisation）

Jericho 論壇上開始探討網路邊界消弭（De-perimeterisation）的議題，從企業間共享網路資源，探討消除企業與企業間的網路邊界，再到無邊界趨勢下的網路安全問題。雖然此時零信任的概念仍然抽象，但此年代被認為是網路安全零信任議題最早的起源。

◆ 2010 年 11 月，Forrester 提出「Zero Trust」

在 Forrester 發表的 Build Security Into Your Network's DNA: The Zero Trust Network Architecture 文件中，第一次出現零信任網路架構一詞，相關概念開始變得具體。時任 Forrester Research 副總裁的 John Kindervag 並提出了零信任模型（Zero Trust Model），從網路架構開始探討預設不信任任何事物。同年，網路巨擘 Google 因為自身面臨「極光行動（Operation Aurora）」APT 攻擊，於是在內部推動全新的安全架構發展計畫。

◆ 2014 年 12 月，Google 釋出 BeyondCorp 文件

Google 釋出《BeyondCorp》文件，說明自家規劃的零信任網路架構與資源存取流程，並指出其建立了可信任並持續的驗證請求的架構，讓公司員工、連網設備存取內部應用系統時，不論其位於內部網路或公共網際網路，都能夠透過這樣的機制與流程來確實驗證人與裝置的身分，這也意味著打造零信任網路安全環境不再是空談，已有具體的實踐。

◆ 2018 年 12 月，Gartner 提出「Lean Trust」

零信任概念持續演化與普及，並且影響 IT 市場研究機構的資安議題設定。在 2017 年底、2018 年初，

Forrester 首席分析師 Chase Cunningham 提出了擴充概念，稱為零信任延伸(Zero Trust eXtended，ZTX) 生態系統。2017 年 6 月，Gartner 基於他們先前提倡的自我調整安全架構（Adaptive Security Architecture），推出一套新的防護策略，稱之為「持續適應風險和信任評估（Continuous Adaptive Risk and Trust Assessment，CARTA）」，當中也包含了與零信任相似的概念。2018 年 Gartner 發表的 Zero Trust Is an Initial Step on the Roadmap to CARTA 文件提出精實信任（Lean Trust），強調以信任與風險為中心，持續動態調整資源請求的信任評估，ZTX 和 CARTA 兩者經常被相提並論。

◆ 2020 年 8 月，NIST 發布 SP 800-207

2019 年 9 月，美國國家標準暨技術研究院（NIST）針對零信任架構（Zero Trust Architecture），公布他們所制定的草案標準，廣邀各界評論，隔年 2 月推出第二版草案，8 月拍板定案、正式頒布 SP 800-207 標準，也讓各界面對零信任架構時，有了共同討論與發展的基礎。

而這項國家等級的資安標準，將聚焦在保護資源，而不只是網路分段。之所以如此，是因為現今的企業人員運作型態已趨向遠端使用者的配置，而且基於雲端服務而成的各種 IT 資產，也未必都設置在企業的網路邊界之內。NIST 表示，美國聯邦政府在當前的網路安全政策，以及相關防護計畫的實施作為上，也已經將零信任資安策略體現在其中，而他們所發布的這份標準文件內容，將會呈現零信任的抽象定義，以及通用的部署模式、應用案例，協助企業改善整體 IT 資安態勢，並提供實作這項策略的高階發展藍圖。這份文件不只成為美國政府新一代網路安全策略指南，在國際上也被認定為企業組織實踐零信任的重要參考標準。

◆ 2021 年 5 月，美國總統拜登發布的行政命令要求聯邦政府導入零信任架構的網路安全策略

該行政命令除了公布多項國家網路安全策略，當中提及要推動美國聯邦政府網路安全現代化，並要求導入零信任架構的網路安全策略。也特別指出聯邦政府需做出大膽的改變與重大的投資，以保護支撐美國生活必需的重要機構。在這樣的趨勢之下，零信任網路安全策略，儼然已經發展成為國家級別的安全策略。

文件的結構

本文件包含 7 個章節，各章節的內容簡述如下：

第 2 章，定義零信任架構，介紹企業設計零信任架構的一些假設，同時說明零信任架構設計的原則。

第 3 章，說明標準化零信任邏輯元件，並介紹不同零信任邏輯元件的組合及提供各種實踐的方式。

第 4 章，介紹透過零信任架構使擁有遠距辦公、雲端服務和訪客網路等情境的企業網路更加安全、更不容易被利用的實際案例。

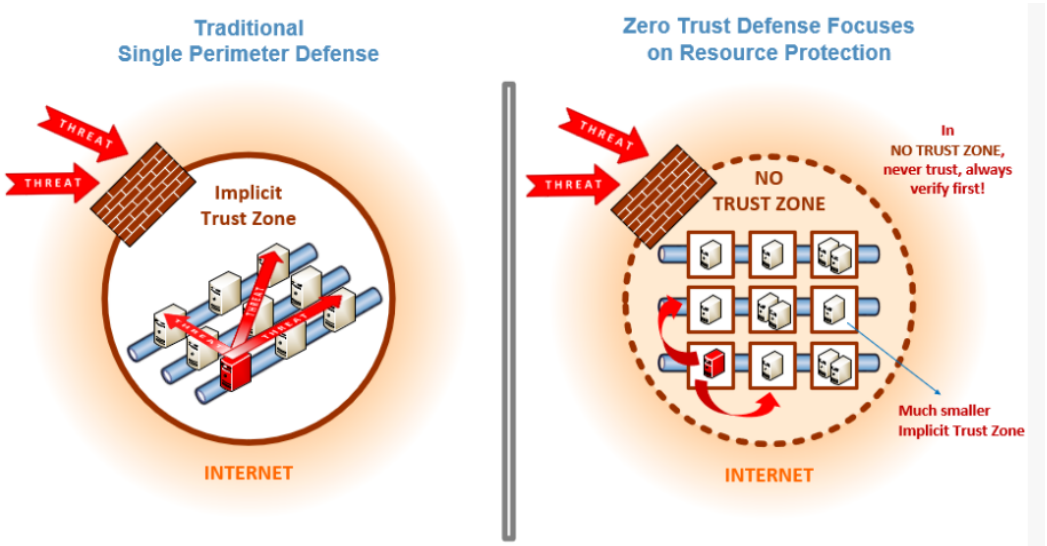
第 5 章，討論使用零信任架構的企業可能面臨的威脅及解決方法。

第 6 章，討論零信任原則如何與美國聯邦機構的相關規範互相結合呼應。

第 7 章，說明企業如何從傳統架構逐步過渡到零信任架構。

2 零信任基礎認知

信任的前提在於持續評估而不是預設隱性授予權限。傳統上組織專注於邊界防禦，一旦經過身分驗證的主體進入內部網路後，就有權限存取廣泛的資源集合，導致環境中未經授權的橫向移動一直是企業面臨的最大挑戰。零信任是一種資源保護的安全典範，零信任架構實現端點到端點存取企業資源和資料安全方法，其內容涵蓋了身分認證、帳號密碼與憑證管理、資源存取管理、操作介面、裝置端點、託管網路環境和相互連接的基礎設施等。而最基本的重點應放在限制資源存取，也就是只讓有需要存取的人才能存取該資源，並且僅授予執行任務所需的最低權限。



受信任的網際網路連接（Trusted Internet Connections、TIC）和代理邊境防火牆提供強大的網際網路閘道功能，這有助於阻止來自 Internet 的攻擊者，但 TIC 和邊境防火牆對於檢測和阻止來自內部網路的攻擊不太管用，並且無法保護企業邊境之外的遠距辦公人員、雲端服務、邊緣裝置等資源。

零信任和零信任架構的操作型定義如下：

零信任（Zero Trust）- 假設網路環境並不安全，隨時都有潛伏的破壞者，資訊系統和服務在運作時，為了讓每一個決定存取請求是否放行的不確定性最小化，於是以最小權限下去執行任務的一系列概念與想法。
零信任架構（Zero Trust Architecture）- 是一種企業網路安全規劃，其中引用了零信任概念，在實作面則包含邏輯元件關聯性、業務流程規劃與資源存取政策。
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，然後部署與打造零信任環境，讓企業來使用。

此定義說明了要解決的問題癥結，即在於防止未經授權存取資源和服務，同時使存取控制盡可能做到更精細。也就是說，經過授權和被核准的使用者、應用程式、服務和裝置等主體可以存取資料，但其他主體（例如，攻擊者）則會被排除在外。

為了減少無法消除的不確定性，是否信任的決策的重點是將身分驗證、是否授權存取限縮在預設信任的區域，同時需保持決策系統高可用性並盡可能減少身分驗證機制的時間延遲，而存取規則盡可能更精細分割，只提供每次資源請求的操作所需的最小權限。

關於存取模型的概念，如下圖 1 所示，當主體(使用者或設備)需要存取企業資源時，需要經過策略決策點（Policy Decision Point，PDP）並經由相對應的策略實施點（Policy Enforcement Point，PEP）來決定是否授予存取權。

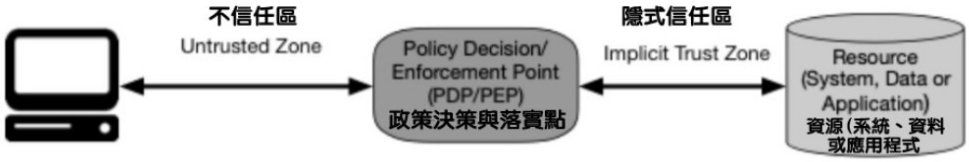


Figure 1: Zero Trust Access

中間的 PDP 和 PEP 提供適當的判斷確保左邊的主體是真實的，以及請求是有效的，從而判斷是否允許主體存取資源。在此也需同時考慮主體身分的信任程度，例如，請求來源設備的安全現況(設備的位址、請求的時間、設備是否更新修補程式等種種因素)。

在 PDP/PEP 與資源之間會形成默認信任區（Implicit Trust Zone），實體通過 PDP/PEP 閘道的信任檢查後就取得信任，如同機場航站安檢區的概念，通過機場安全檢查站 (PDP/PEP) 進入候機室的旅客、機場員工、機組員，都被視為是可信的。如何讓如此重要的 PDP/PEP 做到嚴謹的決策，就需要透過即時且基於風險評估的結果，給出適當的判斷，以決定是否能夠存取資源。

企業需要制定和維護基於風險的動態資源存取策略，並建立一個系統以確保每次資源存取請求都能透過這個動態政策來正確執行。企業不應依賴於主體已通過基本身份驗證級別（例如，透過帳號密碼登入系統），就假定此主體後續所有資源請求均同樣有效的這種默認的信任假設，默認信任區必須盡可能越小越好。

整體而言，零信任提供了概念和原則，其作法是讓 PDP/PEP 更接近資源，對企業的所有主體、資產和業務流程都做到明確地身份驗證和授權。

2.1 零信任原則

零信任的許多定義和討論雖然都在於強調消除廣域的邊界防禦（企業邊境防火牆）概念，然而，這些定義大多數仍持續以某種邊界防禦方式（微分段或微邊界）定義零信任架構功能。以下舉出零信任架構設計與部署所需遵循的 7 項基本原則：

1. 所有資料來源和運算服務都被要被視為資源。
2. 無論與哪一個網路位置的裝置通訊，都必需是安全的。不應以設備位於企業網路內部就自動給予信任，所有通訊都應以加密的方式進行，保護資料的機密性和完整性，並能夠對請求來源身份進行驗證。
3. 對企業資源的存取應以連線為基礎去判斷是否許可。在授予存取許可權之前，需評估對請求者的信任程度，且盡可能只授予完成任務所需的最低許可權。
4. 對資源存取的許可權由動態策略決定，透過用戶端身份識別、應用程式及服務和請求的當下資產的狀態、其他行為和環境屬性作整體綜合評估。識別用戶端包括使用者帳戶以及企業分配給該帳戶或專案的屬性，以自動化方式進行身份驗證。請求資產狀態包括設備安裝的軟體版本、網路位置、請求的時間日期、歷史紀錄的行為模式和已安裝的授權憑據。行為屬性則包括主體分析、設備分析以及與歷史紀錄的使用模式。環境屬性包括請求者的網路位置、時間、正處於活躍狀態的攻擊方法等因素。

5. 企業需監控和衡量所有自有與相關資產的完整性和安全狀況。沒有任何資產是天生可信任的，企業必須透過資源請求時當下資產的安全狀況評估對資源存取的信賴度。實施零信任架構的企業應建立持續診斷和緩解（CDM）系統或類似的系統來監視設備和應用程式的狀態，並適時根據需要進行修補或修正。
6. 在決定是否允許存取之前，所有資源的身分鑑別與授權機制，都要依監控結果動態決定，並且嚴格落實。獲取存取授權、掃描和評估威脅，調整與不斷對資料通訊進行信任評估是一個持續的循環。實施零信任架構的企業應建置身分憑證和存取管理（ICAM）及資產管理系統，包括採用多重身份驗證（MFA）。在整個使用者存取資料的活動中持續監控（例如，存取的時間、是否要求新的資源存取、修改資源、偵測到的主體有異常活動）並參考政策定義強制進行重新身份驗證和重新授權，在安全性、可用性和成本效益取得平衡。
7. 企業應盡可能地收集有關資產狀態、網路基礎設施和通訊的資訊狀況，並使用這些資訊來增進安全狀況資料。利用分析這些數據獲得的資訊來改進政策制定和實施授權。

上述原則與技術無關，因此這些原則適用於企業內或共同合作的組織，但須注意，在企業導入零信任架構的過程中不能將這些內部的零信任原則強加給客戶或一般網際網路使用者。

2.2 零信任觀點下的網路架構

任何使用 零信任架構規劃和佈署的網路架構必須建立在 6 項假設前提之下，包括:

1. 企業私有網路不能預設為信任區域，零信任原則始終假設攻擊者存在企業網路中，因此要以最安全的可行的方式進行溝通（參考上面的零信任原則 2），這代表所有的連線都需進行身份驗證並加密網路封包。
2. 網路上的設備可能不是企業所擁有，也無法被企業限制，例如，企業需允許個人擁有的自帶設備（Bring-Your-Own-Device，BYOD）能夠存取企業資源。
3. 沒有資源是天生可信賴的，因此在存取企業的資源之前，所有資產都必須經過 PEP 評估其安全狀況，確保所有設備存取的資源是在安全的狀態。
4. 並非所有企業資源都位於企業擁有的基礎架構上，例如託管於公有雲的資產需要透過雲端服務商的網路才能進行連接和使用網路服務。
5. 遠端使用者存取企業主體與資產時，不能完全信賴使用者本身的網路。企業應假設非企業內部網路的所有私人網路的流量都攻擊者受到監視，並且可能被竄改封包，因此，所有連線請求都應經過身份驗證和授權，通訊應該加密。
6. 在企業和非企業網路之間移動資產和業務流程，應保有一致的安全策略與安全狀態。包括資產從企業內網移動到非企業網路的設備或者資料從企業數據中心遷移到雲端服務，都要保持資料和資產的完整性、一致性和可用性。

3 零信任架構邏輯元件

企業的零信任架構是由許多邏輯元件組成，這些元件可能是企業內部運行的服務或是託管於雲端的服務。圖 2 的概念框架顯示了零信任組件的核心架構，當任何主體 (Subject) 透過應用系統要存取企業資源前，需經過存取控制的政策落實點（PEP）決定是否給予權限，這個授權的動作發生在網路環境的資料層（Data Plane）。而在 PEP 的背後，將會藉由控制層所相應的政策決策點（PDP）來判斷， PDP 由兩個邏輯元件配對構成，包括政策引擎（Policy Engine，PE）與政策管理者（Policy Administrator，PA）。零信任架構邏輯元件在控制層進行通訊，而應用程式與資源在資料層進行通訊。

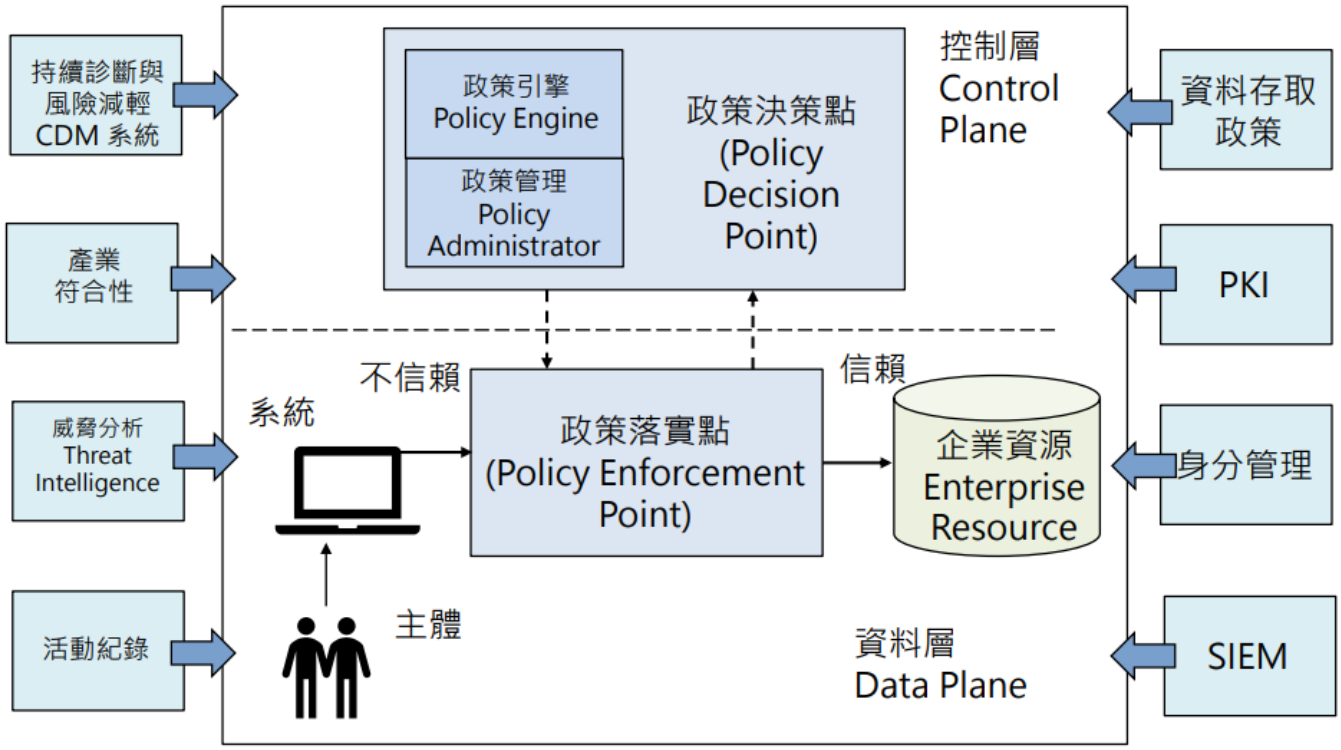


圖 2，零信任架構的邏輯元件

- 策略引擎（PE）：此組件負責運算以決定是否授予特定主體存取資源的權限。 PE 使用企業政策和外部 CDM、威脅情報等資訊作為信任演算法的輸入進行風險評分及決策運算以決定是否授予、拒絕或撤銷主體存取資源之權限。 策略引擎與策略管理員互相合作，當策略引擎做出決策並留下記錄後，則交由策略管理員執行決策。PE 運用 8 種資料來源以提高存取控制動態決策的精確度：
  1. 持續診斷與風險緩解（CDM）系統：此系統持續收集企業資源當前狀態，例如資源否運行在已更新修補程式的作業系統 (OS)、是否安裝企業認可的軟體元件或是否存在未經批准的組件以及該資產是否具有任何已知的漏洞。
  2. 產業合規系統：確保企業遵守所屬產業的監管制度及產業政策規則。
  3. 威脅分析情報：來自企業內部或外部來源的威脅情報可幫助策略引擎做出存取決策，包括新發現的軟體漏洞、新識別的惡意軟體以及來自其他資產的被攻擊報告。
  4. 網路和系統日誌：包括企業系統日誌、網路流量、資源存取操作以及其他提供即時或接近即時的企業事件回饋資料與系統安全狀態等紀錄。

5. 資料存取政策：有關存取企業資源的屬性、規則和策略，這些規則可以透過管理介面設定或由策略引擎動態產生。資料存取策略是授權存取資源的起點，它們是基於組織定義的任務角色和需求為企業中的帳戶和應用程式及服務提供基本存取權限。
6. 企業公開金鑰基礎設施（PKI）：該系統負責產生並記錄企業向資源、主體、服務和應用程式頒發的憑證。
7. 身分管理系統：負責建立、儲存和管理企業使用者帳戶和身分記錄之系統，如 AD 伺服器。該系統包含必要的主體資訊（姓名、電子郵件地址、個人憑證等）和其他的企業特徵(角色、存取屬性和被配置的資產等)。
8. 安全資訊和事件管理（SIEM）系統：此系統集中收集供日後分析安全事件的資料，並可設定規則為企業資產偵測可能遭受攻擊發出警報。

- 政策管理員 (PA)：此組件負責建立或關閉主體與資源之間的通訊路徑、產生客戶端存取企業資源時連線階段 (Session) 所需的身分驗證，以及驗證 Token 或憑證之正確性。它與 PE 密切相關，用來執行 PE 的決策，當 PE 同意授權時，表示請求資源已通過驗證， PA 會向 PEP 發出信號允許連線階段啟動；反之若 PE 拒絕授權時，表示連線請求被拒絕或先前雖批准但新的請求拒絕，PA 就會向 PEP 發出信號以關閉連線。PA 與 PEP 的溝通是透過控制層完成的。
- 策略執行點 (PEP)：該組件負責啟用、監控以及終止主體和企業資源之間的連線階段。 PEP 與 PA 彼此通訊以轉送資源請求或從 PA 接收策略更新。PEP 是零信任架構中擔任主體與資源之間通訊路徑看門人的邏輯元件，可以是單一元件，但架構上也可以分為兩個不同的元件：例如，安裝在執行應用程式電腦的代理程式用戶端元件、放在企業資源前面的存取控制閘道資源端元件。

3.1 各種零信任架構方法

只要實作方法符合零信任原則，企業可以透過各種方式設計零信任架構，不同方法採用的組件組合和政策規則來源各不相同，基本上，零信任架構有三種解決方案: 增強的身分治理(Enhanced Identity Governance，EIG)、網路微分割(Micro-Segmentation)、軟體定義邊界(Software Defined Perimeters，SDP)，各有不同適用情境，若企業在設計零信任架構時會發現其選擇的方法比其他方法適合，這不代表其他方法不管用，只是企業流程使用其他方法更難執行，或者需要針對企業的業務流程進行根本上的改變。

3.1.1 使用增強的身分治理

增強的身分治理方法藉由使用者的身分作為政策執行的關鍵，如果該主體的身分不是用於請求存取企業資源的，則無需為其制定存取策略。這種方法的企業資源存取策略是基於身分認證和身分的屬性。是否能夠存取資源主要是基於授予主體的存取權限，至於其他因素，例如使用的設備、資產狀態和環境因素也會改變信任等級計算及最終的是否授權存取的結果（例如，可以根據使用者的網路位置僅授予對給定資料來源的部分存取權限）。

增強型身分治理的方法通常用於企業開放大眾存取的網路、企業中具有訪客存取權的網路或放在雲端透過非企業設備存取企業資源的環境。此架構通常預設開放所有網路連線，但限制具有適當存取權限的身份才能存取企業資源。然而預設授予網路連線有一個缺點：惡意攻擊者可以掃描網路弱點或發動阻斷式攻擊，因此企業仍需要持續進行監控並在惡意行為影響到業務流程之前做出回應。

增強的身分治理方法特別適合搭配資源入口網站模型(透過入口網站提供外部存取內部資源)，其次，有些雲端應用程式或服務不允許企業採用零信任安全組件，也可以透過增強身分治理方法的設計架構達成零信任。

3.1.2 使用網路微分割

此架構是透過將資源放在受網路安全閘道保護的網段上實現零信任架構。企業可透過智慧交換機、路由器、次世代防火牆 (NGFW) 或特定用途的網路閘道器作為 PEP，以保護資源。這些設備動態地授予對來自用戶端資產每一次請求的存取權。根據模型的不同，閘道器可以是唯一的 PEP 元件，也可以是由閘道和用戶端代理程式組成的多組件 PEP。

此方法將負責保護資產的閘道設備充當 PEP，而這些設備的管理工具充當 PE 和 PA 元件。這種方法的關鍵要點在於，PEP 元件必需可配合身份治理計畫 (Identity Governance Plan，IGP)設定授權規則，並且能夠根據需要作出反應和動態重新配置，以回應外部威脅或工作流程的快速變更。雖然使用不太先進的閘道設備甚至無狀態防火牆也可以實現微分割的某些特性，但難以快速應變反而會提高管理成本。

3.1.3 使用軟體定義邊界

最後一種方法是使用網路基礎架構來實現零信任，透過使用覆蓋網路（即建立在另一網路之上的電腦網路，可由 OSI 第 7 層實現，但也可以設定在較低的網路堆疊層）實作，這方法也被稱為軟體定義邊界 (Software Defined Perimeters，SDP) ，包含了軟體定義網路 (SDN) 和基於意圖的網路 (IBN) 中的概念。在此方法中 PA 充當為網路控制器，並根據 PE 做的決策建立或重新配置網路連線，使用者端則透過由 PA 元件管理的 PEP 請求存取資源。

透過應用層（即第 7 層）實作時，最常見的設計是代理人/閘道器架構，此方法亦適用於雲端虛擬網路或非基於 IP 的網路架構。

3.2 各種佈署方式的抽象架構

由於各企業的環境不同，根據其網路建立方式，以及不同業務流程，有各種不同的佈署模型。

3.2.1 代理人及閘道器的部署方式

如圖 3 所示，此模式將 PEP 拆分為代理人、閘道器兩個元件，企業系統中擺放代理程式(做法是將 Agent 程式安裝在使用者電腦或伺服器上)，資源前端有一個閘道器(擔任類似 Proxy 的功能)，閘道器跟 PA 溝通並接收 PA 的指令來執行 PE 做的決策(例如，是否放行)。

當安裝了 Agent 的設備(例如，公司配發的筆記型電腦) 要求存取某一個企業資源時(例如，人力資源資料庫)，此 Agent 會攜帶這項設備的一些基本資料(如 OS、IP Address 、Port、Session key 等)跟控制層的 PA 和 PE 溝通，當驗證成功並同意存取後 Agent 與 Gateway 會建立一個加密的通道進行資料傳輸，完成任務後這個連線即被終止，連線終止的原因也有可能是發生一些不正常的因素，例如 Session Timeout 或者於連線過程的驗證失敗。

此模型最適合擁有強大數位資產管控能力的企業，如果企業連數位資產或設備在做些什麼都不清楚，這種方式也不適合單位來佈署，另外這方法也不適合有未將 BYOD 納入資產管控的企業。

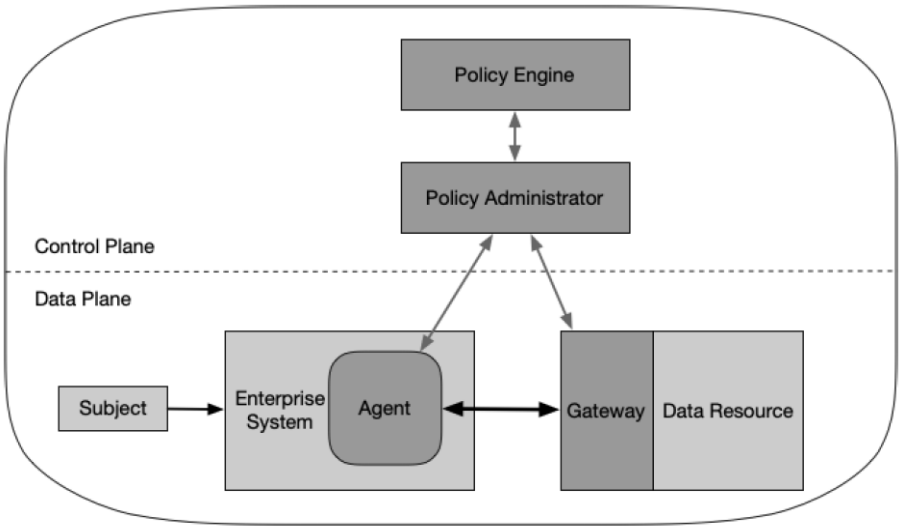


Figure 3: Device Agent/Gateway Model

3.2.2 安全區 (Enclave) 架構的部署方式

此架構是上述裝置代理人及閘道器模型的變形，此架構的閘道器不會駐留在單一資源前面，而是駐留在資源群體（例如，擁有多台伺服器的資料中心）的邊界處，如圖 4 所示。此模型適用於使用雲端微服務進行業務流程（例如，使用者通知、搜尋資料等）的企業，整個私有雲位於閘道器後面。

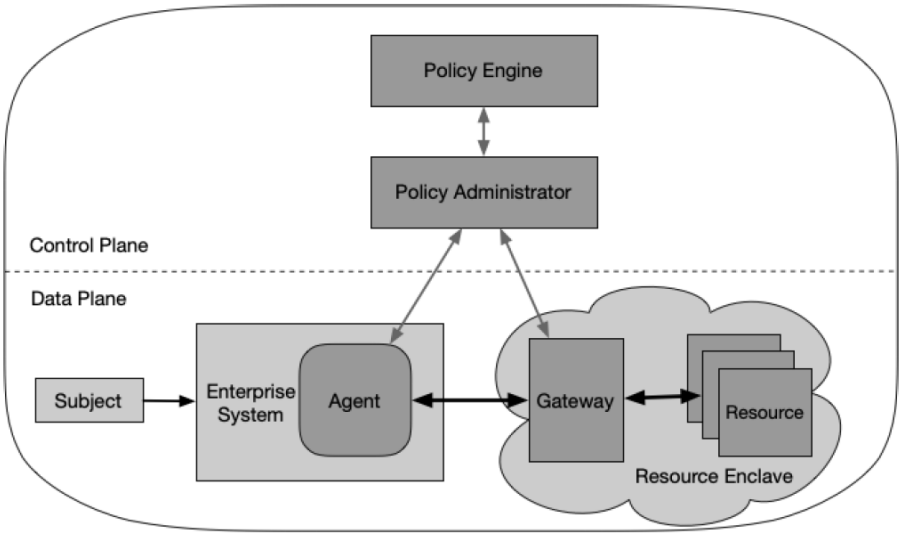


Figure 4: Enclave Gateway Model

這種模式類似一般傳統防火牆，在 Gateway 後面有好幾個 Resources，這些 Resources 通常是一組 Business Function 的組合，例如，由 Web Server、AP Server 和 DB Server 組成的電子表單簽核系統。此架構適用於企業的 Resource 無法在前面放置 Gateway 的狀況(例如，老舊系統沒有提供 API 跟 Gateway 溝通)，其缺點就是無法個別保護每一個資產，存取政策和規則是對這一群 Resources 做保護。

3.2.3 資源入口的部署方式

在此部署模型中，PEP 元件負責客戶端要求資源存取的入口閘道，入口閘道可以針對單一資源，或多個業務功能資源集合做存取限制，如圖 5 所示。

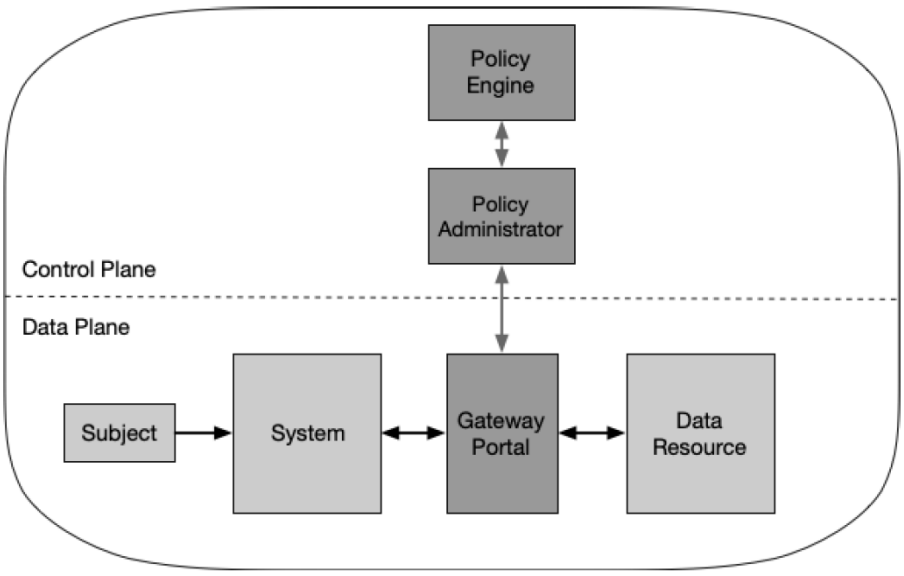


Figure 5: Resource Portal Model

這種方式的好處是不用為公司的設備主體安裝 Agent(適用 BYOD 無法安裝 Agent 的公司)，只要能能夠通過入口閘道的驗證就好，其缺點是驗證時只有一次性掃描來源端的狀況，之後就無法持續監控來源端的狀況。由於有這種缺點存在，企業必須要有其他的補償措施(例如，縮短 Session Timeout 時間)，而且這個單一入口把 PE、PA、PEP 變成單一元件，容易成為駭客發動阻斷式攻擊目標。

3.2.4 裝置應用程式沙箱

基本上就是把 OS 和 Apllication 分開，也就是只信任在 Sandbox 執行的 Application，這類的 Sandbox 可能是 VM、Contianer 或 Chef Habitat。此架構 PEP 與沙箱內的 Application 直接溝通，其目標是保護應用程式免於被受損的主機或主機運行的其他應用程式所影響，同一台主機的其他服務無法共享同樣的存取請求。

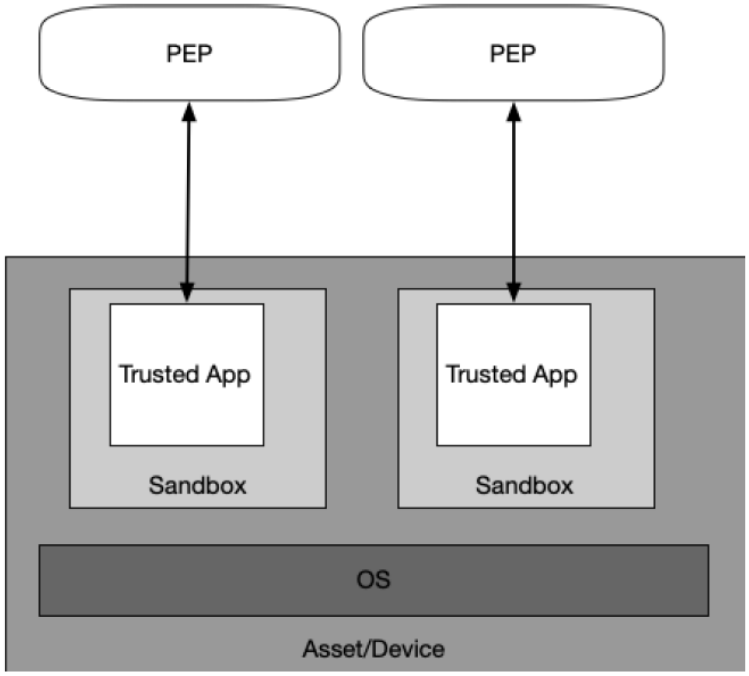


Figure 6: Application Sandboxes

這個模式的好處是，我們已經把信任的範圍縮小到 Application，即使所在 OS 發生資安事件，只要 Sandbox 可以運作正常就不太會受這些異常事件的影響。但缺點是由於這些 Application 運行在 Sandbox 環境，即使導入數位資產管理也有可能無法掌握這些 Sandbox 及確認它的環境是安全的，所以在 Sandbox 整體監控也必須有對應的做法，這可能比監控一般的裝置需要投入更多的努力。

3.3 信任評估演算法

零信任架構的策略引擎可視為企業的大腦，其思維的核心就是信任評估演算法。策略引擎經過信任評估演算法（TA）最終決定授予或拒絕對資源的存取，這如同人腦一般，會藉由很多資訊綜合判斷並做出決定，如圖 7 所示，PE 需要接收多方資訊來做出決策。

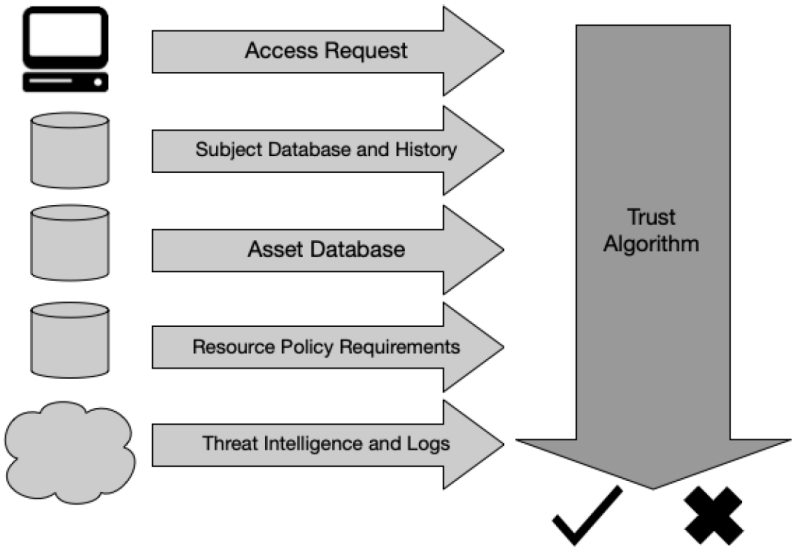


Figure 7: Trust Algorithm Input

輸入資訊分為 5 大類別：

1. **存取請求 (Access Request)**：這是來源端自帶的要求內容，這些要求內容是信任演算法主要的參考資料。來源端的本身資訊也會被使用，例如來源端的 OS 版本，使用甚麼樣的應用程式提出要求，應用程式的版本是否正確乃至於其他關於這些來源端的安全狀態相關資訊都會被用到。
2. **主體資料庫及存取歷史 (Subject Database and History)**：主體指的是請求資源的來源端，主體的屬性和存取歷史紀錄構成存取資源策略的基礎。基本上就是甚麼樣的人或應用程式有甚麼樣的權限做甚麼樣的事，提供信任演算法根據不一樣的人、事、時、地、物條件給出不一樣的權限。
3. **資產資料庫 (Assest Database)**：該資料庫包含企業擁有的資產與資產的狀態，數位資產資料庫會跟現行的資料狀態做比對，包括作業系統版本、安裝的軟體及其完整性，網路或地理位置和修補程式等級等資料，若比對不符就會拒絕該項要求。
4. **存取資源的政策與規範**：這是一個預先定義好的政策集合，主要是每一個使用者 ID 與其相對應的最小權限動作、要求身分驗證需要有 MFA、正常的網路 IP 位置（例如，拒絕來自海外 IP 位址的存取）、限制存取資料的敏感度。這些政策要求應由負責資料管理的資料保管人和負責使用資料的執行業務流程人員共同制定。
5. **威脅情報與日誌紀錄**：這些資訊來源主要是很多業者提供的威脅情資平台，或者包括從網際網路搜尋到的漏洞和已知活躍中的惡意攻擊。

基本上，PE 所仰賴的就是信任演算法，這些提供信賴演算法的資料來源重要性或權重可以由企業自行設定，也可以使用專有的演算法計算。

3.3.1 信任演算法規則

信任演算法的方法可以有很多種，零信任架構設計者考量各因素的重要性，會希望有不同的權衡，基本上，信任演算法規則可區分兩種型態：一種是依據條件與分數（Criteria versus Score-based）的方法；另一種是單獨或參考上下文情境（Singular versus Contextual）的方法，單獨是指每次都會獨立評估，而後者則是會評估歷史記錄，比單一信任規則更靈敏偵測到異常存取行為。

依據條件與分數的評估的方法：Criteria-based 就是企業為每一個資源對不同請求來源的要求事先定義好能執行的動作(例如，讀取或寫入)，演算法評估時依據條件計算信任度。Score-based 則要求為來源的各項資訊打分數並綜合企業已經定義好對這一項來源的分數，只要計算後分數高於設定好的值，來源請求就會被通過，若如果分數沒有達到的話，原來預先定義好的允許動作還可能會被取消(例如，原本能夠對某一個檔案讀取與寫入，分數沒有達標會被降級為只能讀取)。

單獨或參考上下文情境的方法：單獨指的是每次的存取請求都會被獨立評估，也就是 PE 系統不在乎這個來源上一次的評估要求是不是屬於惡意的要求或者通過評估，每次請求都重新計算，其好處是系統很快就可以評估要不要通過信任，然而缺點是它無法參考之前的歷史紀錄一起評估。參考上下文就與單獨評估相反了，它會參考該來源端請求評估的歷史紀錄，優點是能精確地偵測到異常存取行為，但缺點是 PE 評估的歷史紀錄越多，存取請求評估的反應就會愈慢。

上述所提及到的這些演算法是可以搭配使用的，例如 Contextual + Score-based 的方式可提供更動態與更精細的存取控制能力。

在定義與實現信任演算法時，最重要的是必須從安全性、易用性與成本效益來考量，再逐步朝目標邁進。理想情況下，我們應該盡量使用參考上下文情境的演算法，但現實中受限於 IT 基礎建設，有些企業有可能沒辦法一下子就實行這種做法，基於參考上下文情境能夠將潛伏在公司內部的攻擊者的風險減到最低，規劃信任演算法時應該朝著這個方向前進。

安全性和具成本效益相信大家都很明瞭，什麼是具易用性呢? 就是過去的歷史紀錄可以很容易拿來作為演算法的參考資料。舉例來說，零信任架構中持續驗證使用者與分析使用者的行為就會有易用性的情況發生：在過去的使用紀錄中 HR 部門有 10 位同仁在周一到週五的上班時間平均有 50 次使用紀錄，當有加班情況時大概會多出 10 次左右，若有一天發生假日使用次數超過 15 次系統就要發出相關的告警給 HR 部門主管或是自動採取下一個動作，這就是歷史紀錄提供易用性的資料給系統參考的實例。

要為每一個資源開發一套存取標準或權重值，需要經過審慎規劃與不斷測試。在實際部署過程中，企業流程可能遇到問題，例如，配置不當導致原本可允許的存取被拒絕。因此在部署初期會經過不斷優化的階段，持續調整標準或權重值以確保政策被執行並兼顧不影響業務流程正常運作，優化階段經歷的時間取決於企業對影響或衝擊業務流程的容忍度。

3.4 網路和環境元件

在零信任架構環境中，用於控制和配置網路通訊流的控制層和用於執行組織的實際工作的應用或服務通訊流的資料層應該是分離的，這方面與軟體定義式網路（SDN）的概念相同。控制層由企業擁有或來自服務提供者的各種基礎設施元件組成，用來維護和配置資產、判斷授予或拒絕對資源的存取、在資源之間建

立通訊路徑以執行必要的操作。數據層用於軟體元件之間的實際資料通訊。零信任架構中，PA 和 PEP 在控制層建立主體與企業資源之間的通訊，而應用程式或服務使用建立的資料層通訊路徑提供服務，

3.4.1 支援零信任架構的網路基本要求

1. 企業需具備基本的網路建設，包含區域網路 (LAN)、 DNS 等，讓企業的資產有網路連線能力。
2. 企業必須要能夠區別本身所擁有與管理的資產，並且能夠由企業核發的憑證，而非使用無法辨識的資訊 (例如，可以欺騙的網路 MAC 位址) 掌握資產的安全狀態。
3. 有相關的產品或解決方案能夠監控企業內的網路流量，提供給 PE 作為決策的資料來源。
4. 未存取 PEP 前，不能夠接觸到企業資源，PEP 在 Resource 之前，因此相關的網路掃描或攻擊都無法直接接觸到 Resource。然而有些網路基礎服務是不經過 PEP 而是公開的，例如 DNS 服務，這一類基礎服務就必須用其他的方式來防禦。
5. 零信任架構中的資料層與控制層是邏輯上分開的，而且不會讓來源端”直接”存取企業的資源或數位資產，這些服務只是像 Gateway 決定要不要放行而已。
6. 主體必須透過 PEP 元件才能存取資源，這可以透過採取 Web 入口網站、網路設備設定或企業資產上的軟體代理程式實現。
7. PEP 是唯一在業務流程中可以存取策略管理員 (PA) 的元件。企業網路上運行的每一個 PEP 都與策略管理員連接，以建立從客戶端到資源端的通訊路徑。
8. 遠端企業資產可以不需要經過企業骨幹就進行存取，不應要求遠距主體透過 VPN 存取企業採用的公有雲服務。
9. 提供存取決策流程所需要的基礎架構，應具有可擴展性，以因應流程負載的變化。在零信任架構中使用的 PE、PA、PEP 是任何業務流程中都需要的關鍵元件，因此延遲性、問題處理，或具備擴充彈性都需有所考量。
10. 企業資產可能會因為某些原因，無法被 PEP 所連線。例如，佈署在雲端的資料庫資產位於企業之外 PEP 無法直接存取到該資源。

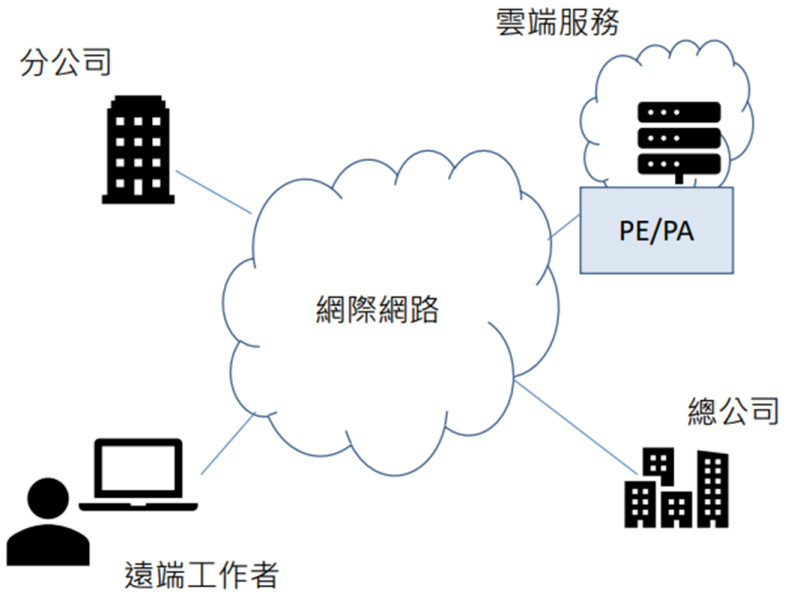
4 零信任架構佈署場景與案例

任何企業網路環境都可採取基於零信任原則設計，事實上大多數企業組織的網路基礎架構已具備零信任原則的某些要素，或是已經透過各種資訊安全實踐做法來達到零信任。接下來，將透過五個章節，說明不同的佈署情境與使用案例。請注意，在企業實際邁向零信任架構的過程中，應該是傳統邊界防護與零信任架構並行持續運行一段時間後再全部過渡到零信任架構。

4.1 擁有衛星設施的企業 (企業總部與分公司的架構)

這是大多數企業的場景。企業擁有一個總部以及多個分散不同地理位置的據點，這些據點的網路不與企業實體網路相連，為了讓員工在工作上能夠存取企業資源，通常會仰賴電信服務供應商提供的專線，透過 MPLS（Multiprotocol Label Switching）來連接這些據點，以建立安全連線。

實際上，企業可能受網路頻寬限制，因此不希望雲端服務的流量都經過公司總部網路，同時，員工也希望可以透過個人擁有的裝置做到遠端存取。在此情形下，企業可以設定規則提供某些資源的存取權限，包括員工行事曆、郵件等，但拒絕存取機敏的資料，例如研發資料庫或人力資源的資料庫。

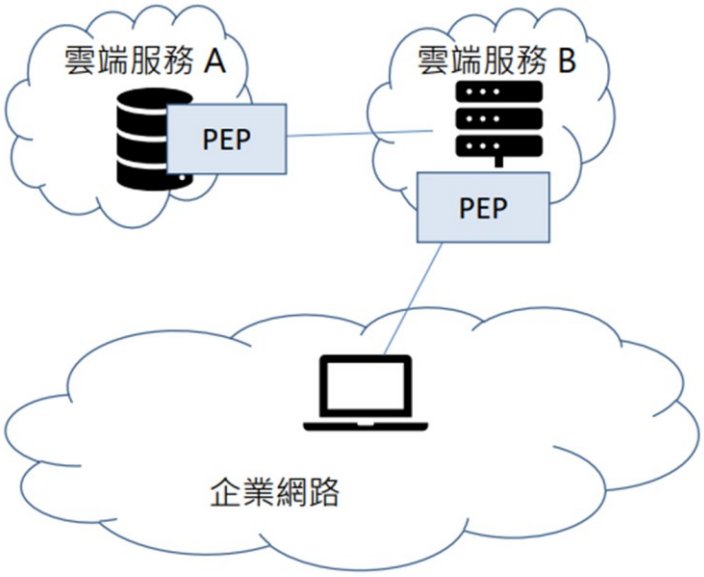


在這樣的場景下，策略引擎 (PE) 和策略管理器 (PA) 通常託管於雲端服務，使其具有更高的可用性，遠端工作者也不用經過企業內部網路存取雲端資訊，但用戶端需要安裝代理程式，或是經過網頁入口存取資源。基本上，企業不用將策略引擎（PE）和策略管理器（PA）設置於企業內部網路，否則遠端辦公室的人員還要經由企業網路才能存取雲端服務上的應用，影響使用系統時的回應速度。

4.2 使用多種雲端服務的企業

為了不讓單一雲端業者綁住同時也擔心該雲端業者服務有問題時造成企業無法營運，多雲策略也應運而生，這是要談的第二種類型，使用多種雲端服務或雲端對雲端。此種情境導入零信任網路架構時，企業本身擁有自己的本地端網路，同時使用多個雲端服務商託管應用程式、服務與資料，而且應用服務與資料是託管在不同的雲端服務上。

實務上為了效能與便於管理，雲端平台 A 應能夠直接與雲端平台 B 溝通，而不是強制經由企業網路存取，在多雲環境使用的零信任方法的場景，是在每個應用程式、服務與資料來源都設置策略實施點（PEP）。

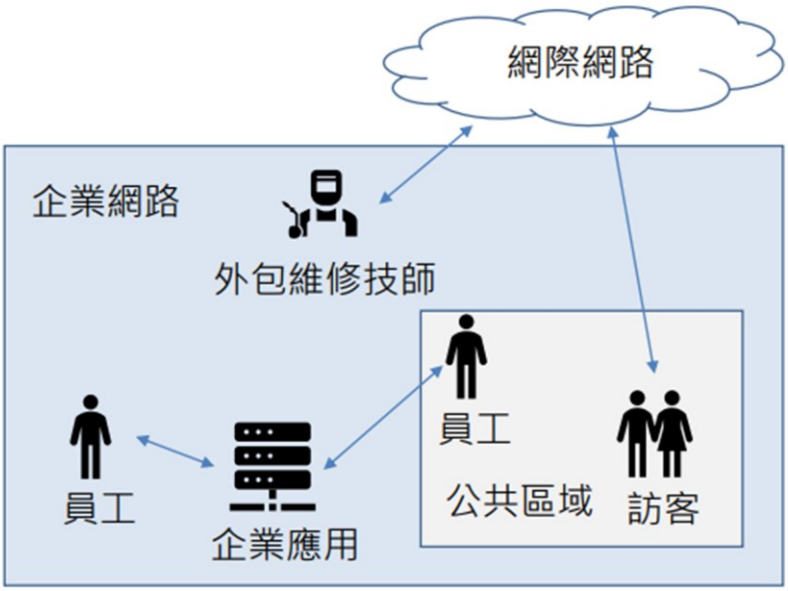


如上圖，我們將服務佈署在不同的雲端平台上，兩個平台之間使用 SDP (Software Defined Perimeter) 作為安全的連線。在此可以看到若企業還是使用傳統防火牆來管理企業與雲端的連結就會有很多不足的地方。

基於不信任公司內外部的網路環境的零信任精神，PE 及 PA 元件可能會選擇放在公司內部也可能放在雲端業者 A 或 B，也有可能是另一個雲端業者 C ，取決於對於內外部網路的信任程度。基本上安裝代理程式或經由網頁入口的用戶端，透過存取策略實施點（PEP）存取資源，所有企業內外部的資源存取都會在企業的管理掌控之下。這裡的挑戰是，不同雲端平台提供者也會有各自獨特的方式來實踐類似功能，因此，企業架構師必需懂得利用各業者的機制才能整合企業零信任的架構。

4.3 提供外包商與非員工存取資料

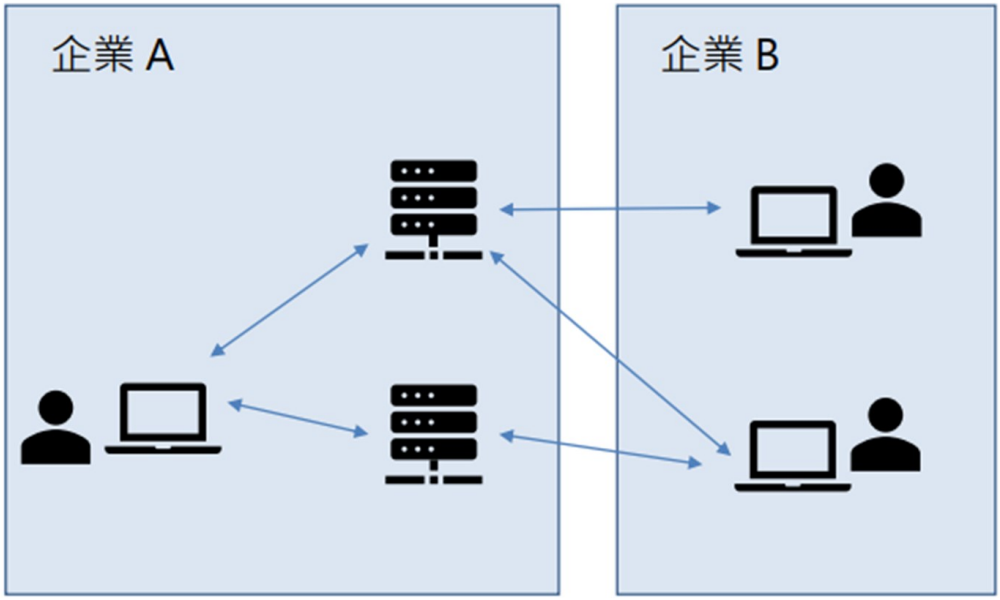
這種狀況是也是普遍常見的情境，企業合作的駐點工作者或外包商需要有存取企業資源的權限，例如，由將智慧空調、照明系統外包給承包商管理，而這些承包商人員需要遠端連接企業內部網路以進行他們的工作。傳統做法是切 VLAN 外加一些防火牆的隔離規則，進階一點的可能再把允許存取的電腦 IP 和 MAC Address 加到可存取的資料庫管理。然而現今的網路是動態的，可能遇到惡意的外來者拿著電腦接上公司網路，即使有 MAC Address 作為來源，也有可能惡意使用者偷用員工的電腦或不小心的員工提供電腦給外包商使用等等不確定的情事。此種情境可使用 SDP (Software Defined Perimeter) 的方式來遮蔽企業資源，並允許外包人員透過網際網路存取企業資源。



此範例的企業有一個供訪客與員工互動的公共區域，透過軟體定義邊界方法，讓不同主體以適當方式存取企業資源，例如，進入公司的訪客可以存取網際網路，但不能存取企業資源，甚至無法透過網路掃描發現企業服務，防止網路探查行為和任意橫向移動。

4.4 跨企業合作

這種類型屬於跨企業的協同合作，例如，有一項涉及 A 公司與 B 公司的合作計畫，其中 A 公司的專案資料庫，必須讓 B 公司的員工存取。實務上，企業 A 可以設置專用帳戶供企業 B 員工存取需要的資料，並拒絕其他帳戶存取資源，但是，這種做法若帳戶和權限組合多就會變得難以管理。如果企業雙方建立聯合身分識別管理系統，提供雙方組織可使用的政策落實點（PEP）進行認證，就可以更快速的建立起關係。



這樣的場景有點類似第一節提到的案例一，雙方員工可能不在本地組織網路架構中，但需要存取一個企業網路或託管於雲端的資源。因此，策略引擎（PE）和策略管理器（PA）可託管於雲端服務，而無需建立 VPN 或類似的服務。企業 B 員工則需要在其系統上安裝代理程式，或透過網頁入口存取企業 A 的必要資源。

4.5 提供大眾或特定客戶服務的企業

這種類型是許多企業的一個共同特點：企業對外提供的公眾服務，可能是針對廣泛大眾企業公開網站，或是針對業務往來關係的客戶，甚至是針對特殊的非企業客戶，像是員工家屬之類。

在上述情境請求的資源可能不是企業所擁有，因此企業內部網路的安全政策套用到非企業擁有的資源時會就受到限制，基本上，不需要登入就能存取的對外服務像公開網站等，零信任原則並不適用。若是針對註冊的會員用戶，或商業往來客戶與特殊用戶，企業可以要求限制政策，包含要求密碼長度、變更密碼週期，以及提供多因子驗證。特別要注意的是，需限制那些來自未知類型的瀏覽器與程式版本過時的存取請求，這些很可能是偽裝合法用戶的攻擊行為，但實作時這些限制時應遵守蒐集使用者請求與其資產資訊紀錄方面的法規(例如，個人資料保護法)。

5 零信任架構相關威脅

任何企業都不可能做到完全防範網路安全風險，不存在百分百的安全環境。實施零信任的主要目標是在參考網路安全政策與指南，加上身分識別與存取管控與持續監控、普及化網路衛生相輔相成，達成降低總體風險，防範共同威脅。然而在導入零信任架構時，也會面臨一些特定的風險，這將成為企業與業者在設計或導入零信任架構時必須考量或注意的面向。

5.1 零信任元件設定不當或版本不一致 (Subversion of ZTA Decision Process)

零信任架構的策略引擎 (PE) 與策略管理器 (PA) 就是第一個風險。因為它們是整個系統的關鍵元件，企業資源的請求都經由此機制來控制是否授權，如果這部分的設定及其相關的參數沒有做好，那麼馬上就衝擊到公司的服務與業務流程，因此這些元件必須要正確的設置與維護。

可存取 PE 政策的企業的系統管理者，若執行了未經授權的變更或是犯了錯，就會擾亂企業的運行。遭受入侵的 PA 可能被破壞，任意放行未經核准主體進行資源存取。要防範 PE 與 PA 的相關風險，就必須具有適當的設定變更流程與監控機制，對於任何變更設定，都要做到紀錄與稽核。這項議題的挑戰是如何平衡管理與效率，設定不好有「被攻擊的風險」，太過嚴苛可能遭遇「營運的風險」。

5.2 遭遇 DoS 阻斷服務或網路中斷 (Denial of Service or Network Disruption)

網路被癱瘓全部的服務都無法運作，所以需要考量網路的高可用性。如上所述，PE 與 PA 是整個系統的關鍵，而零信任架構的第二個風險就是若攻擊者透過 DoS 攻擊、路由劫持等方式造成與 PEP、PE、PA 連線中斷或拒絕存取，就會影響相關系統並衝擊企業業務流程。

企業可以遵照 NIST SP800-160 v2 網路彈性架構指南的作法，將 PEP 放在安全可靠的雲端環境或是設於多個位置互相備援以降低此種威脅的風險。不過這可能無法完全消除風險，畢竟過去曾發生如 Mirai 等僵屍網路發起大規模的服務阻斷攻擊，或者攻擊者可能針對性地攔截或中斷部分流量使部分用戶受影響，此外雲端服務提供者也可能發生意外，導致設於雲端的 PE 或 PA 離線。

5.3 憑證資訊被竊或內部竊賊 (Stolen Credentials/Insider Threat)

由於零信任架構不再有預設隱性的信任，因此攻擊者只能靠入侵既有的帳戶或裝置才能在企業中獲得立足點，這表示具備資源存取權限的有價值帳戶，將成為攻擊者的主要目標。也就是說，對於企業而言，正確開發與實施零信任架構，應能夠防止遭入侵的帳戶或資產以超出其正常權限或存取模式的行動。

一般而言攻擊者慣用網路釣魚、社交工程，以及兩者合併使用的手法獲取這類具有價值的帳戶。從攻擊角度來看，企業系統管理員的帳號通常被認為很有價值，但若是對於公司機敏資料有興趣的攻擊者，就會對可以存取這些資料的高層主管發起攻擊。

採用多因子身份驗證 (MFA) 可降低資料被入侵帳戶存取的風險。但若是攻擊者或是惡意的內部員工連 MFA 都騙到並取得了有效憑證，仍然無法防止此類資安事件。

5.4 網路可見性 (Visibility on the Network)

網路上所有封包都需經過檢查、記錄與分析，其目的是要識別與應對潛在的攻擊活動。但隨著企業網路中越來越多的服務流量都被加密(例如 HTTPS)，對於第三層的網路分析工具而言這些封包並不透明，再加上這些流量可能並非來自企業或是應用程式與服務本身可抵抗這類監控，因此企業無法容易地執行深度封包檢測（DPI）或檢查加密流量。但這並不代表企業無法分析這些加密流量，企業還是可以蒐集加密流量的資料（Metadata）檢測網路上的攻擊者活動，或是使用 Machine Learning 方式分析是否存在的惡意軟體通訊行為。

5.5 系統與網路資訊儲存 (Storage of System and Network Information)

收集網路流量資料所存放的地點需要被嚴格保護及管控，否則這些歷史資料一旦被修改或刪除，整個零信任架構也就沒有意義了。

5.6 依賴特殊的資料格式或解決方案 (Reliance on Proprietary Data Formats or Solutions)

由於零信任架構需要很多數據來源做為決策參考，在整合或交換這些資料時所用的資料格式必須是可以通用的，否則很容易被某個廠商或特定解決方案綁架，當現有的設備或服務在資產更換時也會受到很多限制或增加轉換成本。

5.7 非人類來當 ZTA 的管理者 (Use of Non-person Entities (NPE) in ZTA Administration)

用 AI 或其他軟體解決方案替代人類當零信任架構的管理員，進行 PE 或 PA 調整可避免人為錯誤，但這些非人類的管理者怎麼樣在零信任架構中驗證自己仍是一個未解決的問題，最大的風險是這些自動化的管理方案會帶來兩個問題：

1. false positives(假警報)，正常的存取請求卻被判斷有問題。
2. false negatives(未警報)，真正有問題的存取請求卻被放行。

相關風險就是攻擊者駭入 NPE，讓 NPE 執行攻擊者無權執行的動作。與人類用戶相比較，軟體代理程式在執行管理或安全相關任務上，會因為自動化無人為介入而刻意設計採用較低的身分驗證標準，若攻擊者攻陷代理程式，就能夠欺騙代理程式，讓攻擊者暢行無阻獲得更大存取權限或是任意執行功能。

6 零信任架構與美國現有聯邦指引的相關性

美國國家標準暨技術研究院(NIST)主要任務是制定國家標準，提供美國聯邦政府可依循的技術指南。在 NIST SP 800-207 說明了零信任架構的運作以及與美國聯邦指引的關連，也包括美國政府在各方面提出的資訊安全框架及相關法規要求等。這些政策雖然會影響零信任戰略的制定，但不是要禁止企業朝向零信任導向的架構規劃，相反地，在與現有的網路安全政策與指南、ICAM、持續監控以及一般網路衛生互相結合的情況下，零信任架構可以更加強化組織的安全狀況以防範常見威脅。

6.1 零信任架構（ZTA）與風險管理框架（RMF）

零信任架構的焦點圍繞在指定任務或業務流程的可接受風險程度，並據以制定存取政策，因此有可能發生允許連結的終端設備存取資源，但拒絕該設備對外的所有網路存取。NIST 已發佈 NIST SP 800-37 風險管理框架（RMF），要求美國聯邦機構執行任務必須識別、評估與緩解執行任務的相關風險，並規劃可接受風險層級。在零信任架構的導入與實施中，風險程度會改變企業對於認證邊界的定義。

6.2 零信任與 NIST 隱私框架

對於用戶個人資訊的隱私保護，一直是企業與組織關注重點，聯邦資訊安全管理法（FISMA）以及美國醫療資訊保護法規（HIPAA）就是規範個人資訊的法規。NIST 亦制定提供組織參考的隱私框架「NISTPRIV」，這份文件提供描述隱私風險與緩解策略的框架，內容包含企業組織對於用戶隱私的識別、評估與緩解風險，隱私資訊的儲存與處理的過程。

零信任核心要求之一是企業應在其網路環境中檢查並記錄所有流量，這些流量可能包含了個人隱私資訊，因此，企業在開發零信任架構時，透過 NIST 隱私框架將有助於開發一個正式的流程，可用以識別與緩解任何與隱私相關的風險。

6.3 零信任架構與聯邦身分識別、認證與存取管理（FICAM）

請求主體是零信任架構的關鍵元素之一，若政策引擎（PE）沒有足夠資訊來識別使用者與資源，則 PE 將無法確定是否授權連接到資源。在佈署零信任架構之前，需要針對主體制定嚴格的身分驗證策略，因此企業需要具備明確的使用者管理政策才能讓 PE 準確評估存取請求。

針對聯邦政府的身分識別管理，美國行政管理和預算局（OMB）發布 M-19-17 的備忘錄，該備忘錄呼籲所有聯邦機構成立一個 ICAM 辦公室，目的是治理與身份管理相關的工作，其中許多的管理策略及作法是依循 NIST SP 800-63-3 Digital Identity Guidelines 指引。由於零信任架構需要精確的身分識別管理，在零信任架構上所進行各項努力，都需要與組織的 ICAM 政策相結合。

6.4 零信任架構與可信賴網際網路連線第三版（TIC 3.0）

TIC 是一項由 OMB、DHS 與 GSA 聯合管理的網路安全計畫，其目的是期望建立聯邦政府網路安全的最低基準。TIC 是一種基於邊界防護的網路安全策略，要求機構整合與監控其外部網路連接。早期的 TIC 1.0

與 2.0 中，主要假設內部連接都是可信任的，其中 TIC 2.0 提供一系列基於網路的安全功能，包括內容過濾、流量監控與身分驗證等，並佈署於機構周邊的 TIC 接入點，其中已經有許多功能符合零信任原則。

到了 TIC 3.0，新版擴展到雲端服務與行動裝置，不僅如此，人們也開始意識到「信任」的定義可能隨著運算環境條件而有差異，而且每一個機構對不同的風險承受能力也不同。簡單地說，TIC 3.0 聚焦在網路的安全保護，而零信任則是更廣泛的架構，不僅針對網路，還強調應用程式、使用者與資料的保護。

6.5 零信任架構與國家網路安全保護系統（NCPS）

關於國家網路安全保護系統（National Cybersecurity Protection System，NCPS），也就是愛因斯坦計畫（EINSTEIN），這是一個多系統的整合，主要提供入侵偵測、進階分析、資訊共享與入侵防禦功能，目的是幫助美國聯邦政府防禦網路威脅。基本上，NCPS 的總體目標與零信任一致，都是要管理網路風險、改善網路保護能力。透過系統感測器，可供 CISA 旗下的國家網路安全與通訊整合中心（NCCIC）幫助聯邦機構應對重大資安事件。

美國國土安全部（DHS）同樣運用這些感測器，主要應用於防護國家邊境網路，相對地，零信任架構也是運用感測器資料，其防護更貼近資產、資料與其他資源的所在位置。隨著 NCPS 計畫的發展，將可幫助零信任架構擴展感知與遙測的能力。

6.6 零信任架構與國土安全部持續診斷與緩解計畫（CDM）

國土安全部（DHS）的持續診斷與緩解計畫（Continuous Diagnostics and Mitigations，CDM），目的是要改進聯邦機構的 IT 技術，關注的重點在於強化機構對自身資產、設定配置與主體的洞察力包括：主體連接了什麼？誰在使用網路？網路發生什麼情形？以及資料如何保護？

強大的 CDM 是零信任架構是否成功的關鍵。企業將現有架構遷移到零信任架構前必須擁有一個系統來發現和記錄實體及虛擬資產，以建立可用資產清單。 DHS 的 CDM 計劃經過多項努力，已經建立起聯邦機構轉向零信任架構所需的能力，例如，國土安全部硬體資產管理(HWAM)計畫協助機構識別其網路架構上的裝置並佈署安全性配置，這是於邁向零信任路線的第一步，換句話說，機構必須掌握其擁有的資產及活動，才能為資產進行分類、設定安全配置與監控活動。

6.7 零信任架構與雲端智慧策略、聯邦資料策略

聯邦雲端智慧運算策略、資料中心優化政策更新（備忘錄 M-19-19），以及聯邦資料存取策略，都會影響機構在零信任架構規劃上的考量。這些政策均要求機構必須對資料蒐集、儲存，經由本地或雲端的存取進行盤點與評估後整理成清單，這樣的清單可確定商業流程與資源，對零信任架構導入非常重要。對於主要功能是基於雲端或遠端的使用者而言，零信任架構方案是不錯的選擇，因為資源、應用程式與服務都在企業網路邊界之外，這些企業最能體會零信任的擴展性與安全性帶來的好處。

7 邁向零信任架構

邁向零信任架構並不是一次性全面的技術更換，更像是一段漫長的旅程。既有的企業 IT 基礎架構中，多少都存在零信任的元素，因此對於實施零信任原則、業務流程的變化，以及保護高價值資料資產所採用的技術解決方案，企業需要採用漸進的改變方式。

多數企業的網路安全策略，會以零信任與傳統邊界防護混合的模式進行，並持續很長一段間，在這期間內企業將會持續投資於 IT 基礎架構的現代化。評估企業現行的資安狀態以建立安全水平基準(Baseline)，盤點並分類企業資產、使用者、業務流程，區分那些需要有零信任，那些不需要零信任方案管理，有了這些基本資料才能夠開始往零信任架構前進。以下介紹幾種遷移到零信任架構的過程。

7.1 純粹的零信任架構

若是一個全新的環境，企業便可以從頭開始建構零信任架構。企業會知道需要那些應用程式、服務與工作流程，因此可以為這些資源建立一個基於零信任原則的架構。一旦確定工作流程，企業就可以縮小所需元件的範圍，開始描繪每一個元件的互動關係。從這一刻開始，建立架構與配置元件之設定是企業的大工程活動，配合企業運作與零信任架構配置的狀況，同時也要關注改動企業的組織。

這種架構比較適合一開始公司要重新建立 IT 服務或相關人員正要開始接受零信任的相關概念。好處是一次到位受限制的因素就會很少，但缺點是舊有的設備或服務就無法使用，對於已經投資 IT 運作的企業組織來說，畢竟已經擁有既有網路環境，因此全部重建很少是可行的選項。然而若有機會配合專案要建立新的應用程式、服務或資料庫時，是可以考慮引入全新零信任架構。

7.2 混合零信任架構與傳統邊界防護的架構

這應該是已經擁有 IT 服務的企業會考慮使用的方式，實作這種方式不能只從技術角度來考量，而應該是從每一個企業的業務流程來評估，業務流程關連到那些 IT 設備、使用那些應用程式或服務，一次只針對一個流程去進行。但由於設備、應用程式和服務對應好幾個業務流程，所以也須評估需相關的設備、應用程式、服務是否能夠同時在零信任模式與一般傳統的 DMZ 防禦模式下共存。同時，企業需要確認是否有足夠且靈活的通用共同元件，例如，身分識別管理、裝置管理與事件日誌記錄等以支撐混合式安全架構的運行。沿用既有設備同時限制了我們可以選擇的零信任解決方案，純粹的零信任架構就不會有這樣的問題，優點是原有的設備投資不會浪費可以繼續使用。

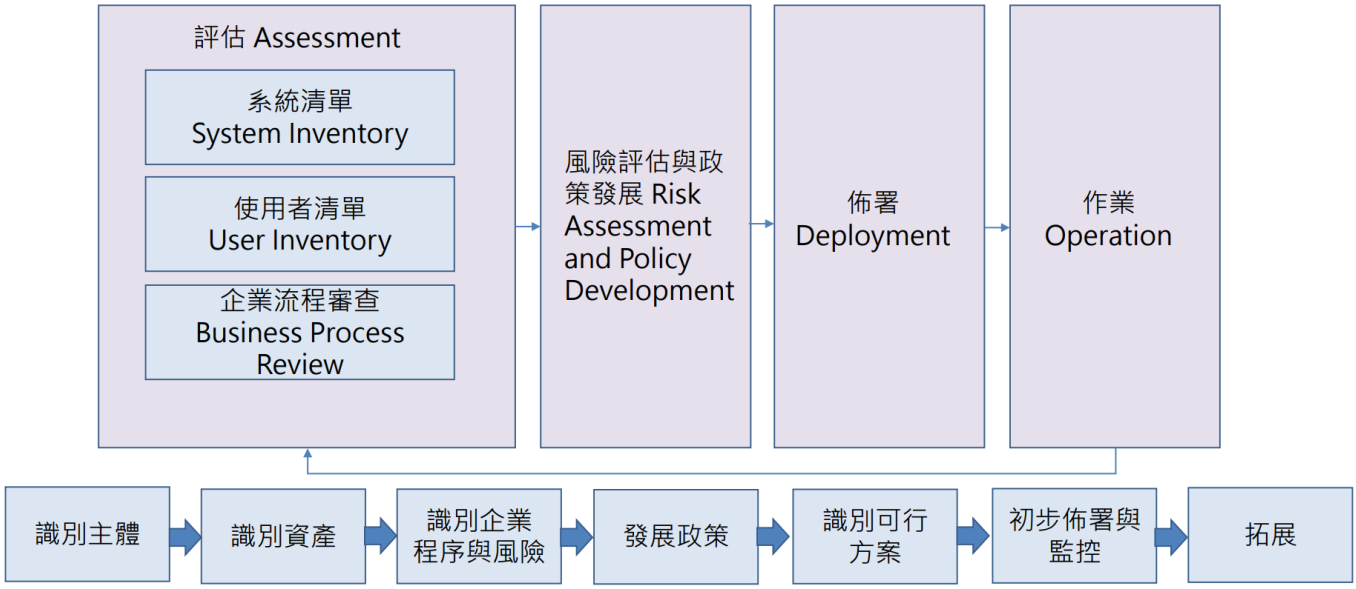
要讓既有業務流程邁向零信任架構，有些部分功能或業務流程需要重新設計，企業也可趁著這樣的機會重構系統或重新檢視業務流程，可參考 SP 800-160 系統安全工程的指引實踐。

7.3 從邊界網路架構邁向零信任架構的步驟

邁向 ZTA 的過程中，企業組織需要詳細掌握自身擁有的實體與虛擬的資產、用戶的帳號權限，還有企業業務流程。這些將是策略引擎 (PE) 在評估資源請求存取時所需的知識內容，一旦這些知識內容不完整，將會導致 PE 因為資訊不足的原因，而拒絕存取請求，影響業務流程失效。因此，企業在零信任架構導入企業之前，對於資產、主體、資料流與工作流程應進行完整調查，這些相關的調查，與組織業務流程的稽查或盤點有關，其實是可以同時進行的。

因為採用零信任架構的任何過程就是降低組織業務功能風險的過程，所以這些步驟是可以和 NIST SP 800-37 的風險管理框架（Risk Management Framework，RMF）相對應的。要注意的是，在初始的盤點清單建立後，需要定期維護與更新，並要注意更新之際，無論會不會更改或影響業務流程，都應該要對業務流程進行評估。

邁向零信任架構有七大建議步驟：（一）識別企業中的角色，（二）識別企業中的資產，（三）識別關鍵業務流程並評估與流程執行相關的風險，（四）針對零信任架構候選者制定政策，（五）選定零信任解決方案，（六）展開初期部署與監控，（七）持續擴展零信任架構。



7.3.1 識別企業中的角色

從策略引擎（PE）的角度來看，為了使企業得以運行零信任架構必須對於企業主體先有所認識。這裡指的主體，包含了人類，或可與資源互動的服務帳號的非人類實體（Non-person Entities，NPE）。我們必須有能力辨識這些主體並以給予正確的權限才能有足夠的信心運作零信任。

特權帳號使用者，例如開發人員或系統管理者，在分配屬性與角色時，需要額外的審查其合理性。在傳統安全架構中，這些特權帳號擁有存取所有企業資源的能力，而在零信任架構之下，除了開放開發人員與管理者有足夠的靈活性以滿足他們的業務需求，同時也要使用日誌紀錄和審核機制來標識特權帳號的存取行為模式。關於系統管理者權限控管的準則或要求可以參考 NIST SP 800-63A 評估是否滿足基本分數或已經符合更嚴格的標準。

7.3.2 識別企業中的資產

零信任架構要求企業要有能力識別與管理自有的設備，同時還要求針對非企業擁有的設備也要有能力去識別與監控，因為這些設備可能存在於企業擁有的網路基礎設施上，或是具有存取企業資源的能力。簡而言之，成功佈署零信任架構的關鍵就是要有能力管理企業資產。

企業資產包括硬體元件(例如，個人電腦、手機與 IoT 裝置等)、數位資產(例如，使用者帳號、應用程式與數位憑證等)。也許我們無法短時間對所有企業擁有的資產進行完整的普查與盤點，所以企業應建立一套機制，將企業基礎設施新發現的設備資產做到快速識別、分類與評估，且不僅僅對企業資產進行簡單的歸類與維護資料，還必須包括持續管理配置與監控活動。畢竟資產當前狀態是評估存取請求過程的一部分，

企業必須能夠配置、調查與更新企業資產資訊，例如資產屬於實體、虛擬機或容器，網路位置等，當 PE 進行資源存取決策需要參考這些資訊。

非企業擁有的資產或企業內部的影子 IT(在組織內未經批准使用的軟體、硬體或其他系統和服務)也應該盡可能的納入分類與控管。這方面可透過企業內可掃描的資訊，例如 MAC 地址、網路位置，或透過管理者的手動資料輸入加以補充。還要注意的是，影子 IT 會帶來一個特殊的問題，因為這些資源是企業所擁有但卻不像其他資源那樣被管理。因此有些零信任方法可能會導致影子 IT 變得不可用。

7.3.3 識別關鍵流程，並要評估與流程執行相關的風險

對於業務流程、資訊流程，以及機構任務中的關係，必須做到識別及優先度排序。建議邁向零信任架構可選擇從低風險的業務流程開始，因為一旦發生錯誤導致業務中斷，還不致於讓對整個組織帶來大幅度的衝擊，當累積足夠的經驗後，就可以選擇其他重要的業務流程繼續進行。或者利用雲端的資源，由遠端工作人員使用的業務流程開始導入零信任架構也是相當不錯的方式，過程中還可能改善可用性與安全性。

導入零信任架構還要考慮一些潛在的不確定因素，當實施零信任架構發生系統效能降低、使用者體驗不佳或增加工作流程複雜度影響效率時，負責推動及規劃的人員需要依據風險做出權衡取捨。

7.3.4 識別導入零信任架構候選程序的政策

在選擇服務或業務工作流程以實施零信任架構的過程中，有幾個重要因素必須注意：業務對組織的重要性，受影響的人數，這個業務流程現行相關的資源狀態、評估資產的價值，或是資產與工作流程的相關風險，相關資訊可參考 NIST SP 800-37。

當某個業務流程被確認作為導入對象後，我們需要開始識別業務流程中所使用或影響的所有上下游資源與實體。

- ◆ 上游資源：如 ID 管理系統、資料庫、微服務
- ◆ 下游資源：如日誌、資安監控
- ◆ 實體：如主體、服務帳號

所有相關都會影響我們第一個選擇實行零信任架構的業務流程，初期導入一部分企業使用者使用的應用程式或服務（如採購系統），可能比選擇整個企業群體至關重要的應用程式或服務（如電子郵件）更適合。

接下來我們就要決定要選擇合適的信任演算法來實現業務流程的零信任架構，過程中管理者需要不斷調整權重以確認有效且不會影響使用者的日常業務活動。

7.3.5 識別可行的解決方案

確定了業務流程清單後，架構師將選定解決方案清單，識別可行性可從五個因素去考量：

1. 解決方案是否要求在客戶資產上安全元件?
   在非企業資產使用或需求上，這可能會限制業務流程，像是 BYOD 或跨機構合作的情境。
2. 解決方案在業務流程完全存在於企業場所的情況下是否有效?
   因為有一些解決方案預設請求的資源是存放雲端(所謂的南北向資料流)，而不是在企業的周邊(東西向資料流)，因此業務流程資源的位置，將影響解決方案與零信任流程的選擇。

3. 解決方案是否提供日誌記錄供分析？
   畢竟零信任的關鍵元件，就是要蒐集與使用流程相關的資料，提供給政策引擎以做出存取決策，因此解決方案是否能夠提供日誌紀錄將影響解決方案的選擇。
4. 解決方案是否針對不同應用程式、服務與協議提供廣泛支援？
   有些解決方案可能支援廣泛使用協議（如 Web、SSH 等）、網路協議（IPv4、IPv6），但一些解決方案可能只適用於特定範圍，像是電子郵件。
5. 解決方案是否需要改變主體的行為？
   有些解決方案可能在執行特定工作流程時需要額外的步驟，這可能會改變企業主體執行工作流程的方式。

總體而言，解決方案是先將現有業務流程建立模型，作為試點計畫，而不是一個替代方案。而這樣的試點方案可以具備通用性，也就是能適用與多個業務流程，也可以僅是當成特定的使用案例，在過渡到真正佈署零信任架構之前，試點計畫可視為零信任架構的驗證場域，待試行成熟之後再脫離傳統的流程基礎架構。

7.3.6 初期部署與監控

在選擇了工作流程與零信任元件後，就可以開始進入初期佈署階段。一開始很少有企業可以在第一次就能充分準備，導致重要的帳戶可能在存取資源時被拒絕，或是錯誤給予不需要的存取權限，在經驗不足的情況下，大部分企業都希望先以觀察或監控模式來進行。因此，新的零信任業務流程，可在「僅報告」（Reporting-only）模式下試行一段時間，以確保政策有效且可行，並讓企業可以理解其運行方式。所謂 Reporting-only 模式是指對於大多數存取請求給予存取許可，利用日誌紀錄與存取蹤跡連結，進而比對並驗證制定的管理政策。

在初始部署時，存取政策可以更寬鬆一點，以便收集零信任工作流在實際交互過程下的相關資料，一旦建立工作流程活動範例的基準，就可以更容易識別異常行為。若無法以更寬鬆的方式運作，企業網路維運人員必需密切監控日誌，並隨時準備依據運作狀況調整存取政策。

7.3.7 擴展零信任架構

實際佈署業務流程上線後，企業就進入穩定運行階段。此時網路與資產仍然被監控，流量也都被記錄，但從各方反映的問題做改進及政策調整的節奏已經可以放慢。接下來企業管理者就可以規劃零信任佈署的下一個循環，也就是回到上述第四步驟，選定下一個工作流程與解決方案，並持續進行部署。

此時需注意如果企業資源環境發生變化，就要重新評估運行中的零信任架構。資源變化包括設備、軟體(特別是與零信任邏輯元件有關)的重大更新、組織架構的調整，都會導致工作流程與政策產生變化。

什麼是影子 IT?

「影子 IT」是指在組織內未經批准使用軟體、硬體或其他系統和服務，而該組織的資訊技術部門往往並不知情。與標準的 IT 基礎結構不同，影子 IT 並非由組織內部進行管理。影子 IT 可能以不同的方式進入組織，但通常是透過下面兩個動作而發生：

- 使用未經核准的工具存取、儲存或共用公司資料。例如，組織僅核准了 Google Workspace 用於檔案共用，那麼員工可能會因選擇透過 Microsoft 365 共用檔案而將影子 IT 引入公司。
- 以未經授權的方式存取核准的工具。繼續上述範例，如果 IT 部門已核准透過公司管理的帳戶使用 Google Workspace，那麼員工可能因選擇透過未受管理的個人帳戶存取 Google Workspace 而將影子 IT 引入公司。

無論影子 IT 的採用是有意還是無意，它都會造成嚴重的安全問題和成本。它增加了資料外洩、竊取和其他網路攻擊的風險，同時阻止了 IT 團隊採取關鍵措施來減少這些可能造成的損害。

使用者為什麼要採用影子 IT？

員工在採用新工具時選擇繞過 IT 部門核准的做法似乎很令人驚訝，他們這樣做的原因可能包括以下幾點：

- 員工沒有意識到影子 IT 固有的安全風險。員工可能不是故意要繞過其 IT 部門所實施的控制，而只是不知道他們的行為會損害敏感的企業資料，增加資料外洩和攻擊的風險。
- 員工更注重使用未經批准的工具所帶來的好處。最適合工作的工具可能不是組織的 IT 部門明確核准的工具。這往往促使員工採用其他服務，從而幫助他們滿足特定的業務需求，在市場上獲得競爭優勢，或更有效地進行工作。
- 員工使用未經核准的工具進行惡意活動。大多數影子 IT 不是為了惡意目的而採用的，然而，一些員工可能會選擇採用未經批准的應用程式和工具，以竊取資料、存取機密資訊或給組織帶來其他風險。

影子 IT 有哪些風險？

雖然影子 IT 可能會讓部分員工更易於完成工作，但它的弊端遠遠超過了它的好處。如果 IT 團隊無法追蹤工具和服務在整個組織中的使用情況，他們可能不知道影子 IT 的滲透程度，也不知道企業資料的存取、儲存和傳輸情況。

影子 IT 的使用還導致 IT 團隊失去對資料管理和移動的控制。當員工使用未經核准的服務或透過未經核准的方法在核准的服務中工作時，他們可能會在沒有 IT 部門適當監督的情況下檢視和移動敏感性資料。由於缺乏可見度和控制，影子 IT 會帶來以下的額外風險：

- 敏感性資料被洩漏或竊取。攻擊者可以利用雲端託管服務中的設定錯誤和漏洞，為資料外洩和其他網路攻擊打開大門。IT 部門可能對此類攻擊並不知情，當攻擊針對未經批准 (且可能不安全) 的應用程

式和工具時則尤為如此。而補救這些攻擊則可能代價昂貴：在 2020 年的一項研究中，IBM 估計，由雲端錯誤設定造成的資料外洩會帶來平均 441 萬美元的損失。

- 組織可能在無意識情況下違反資料合規性法律。對於需要遵守資料保護法規的組織來說，他們必須有能力追蹤和控制資料的處理和共用方式。當員工使用未經授權的工具來處理敏感性資料時，他們可能會無意中使其組織面臨違反這些法律的風險，這可能會導致嚴重的處罰和罰款。