零信任架構導入的挑戰與作法

蔡永信

中華民國 112 年 6 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘 要

傳統的網路安全策略是基於邊界防禦的概念，並不斷強調縱深防禦以確保安全，但隨著 2019 年疫情以來，各企業被迫加速數位轉型，邁入雲端並且開放居家辦公，資訊系統使用情境逐漸複雜，企業需要進化防禦思維，朝向「從不信任，總是驗證」的零信任架構邁進，不再預設任何使用者或設備是可信任的，對所有的請求都進行驗證和授權，並進行監控與管理。

隨著零信任架構越來越廣為人知，及其對去邊界化防禦的效益，國際社會已將其納入資訊系統網路安全政策或標準中，設定推動施行期程，有序地逐步推廣，且不少雲端服務廠商早已實行。零信任架構包含零信任原則、零信任網路、及邏輯元件；邏輯元件包括內部邏輯元件及外部資料源元件；內部邏輯元件主要為政策決定點、政策執行點，外部資料源元件則包含企業內各式各樣的作業環境資訊。

應用零信任架構到企業的資訊系統與網路環境，主要有技術面、組織面、業務面與執行面之挑戰，並須從整合性考量零信任解決方案。企業導入時應先盤點資訊系統、使用者與業務流程，挑選合適的候選業務流程，評估該流程風險並發展相應連線存取政策，其後部署、運行，接著修正後，再逐步擴大適用範圍，由淺入深、由點至面，有序地全面實施企業零信任架構。

目　次

壹、資訊安全攻防困境

自從 1986 年第一隻感染個人電腦的病毒—BRAIN 大腦病毒問世以來，隨著攻擊方的技術與工具逐步產業化、自動化，甚至被吸納為國家軍事力量的一部分，期間歷經 30 多年的時光，資訊安全已從選擇性忽視，逐漸轉為必要且成為國安議題，防守方不斷地透過加深防禦縱深，鞏固所謂的安全邊界，建立所謂的網路邊界防禦架構。

傳統的網路安全策略是基於邊界防禦的概念(如圖 1 所示)，即在企業內部和外部之間建立防火牆，將可信任的內部網路與不可信任的外部網路隔離。

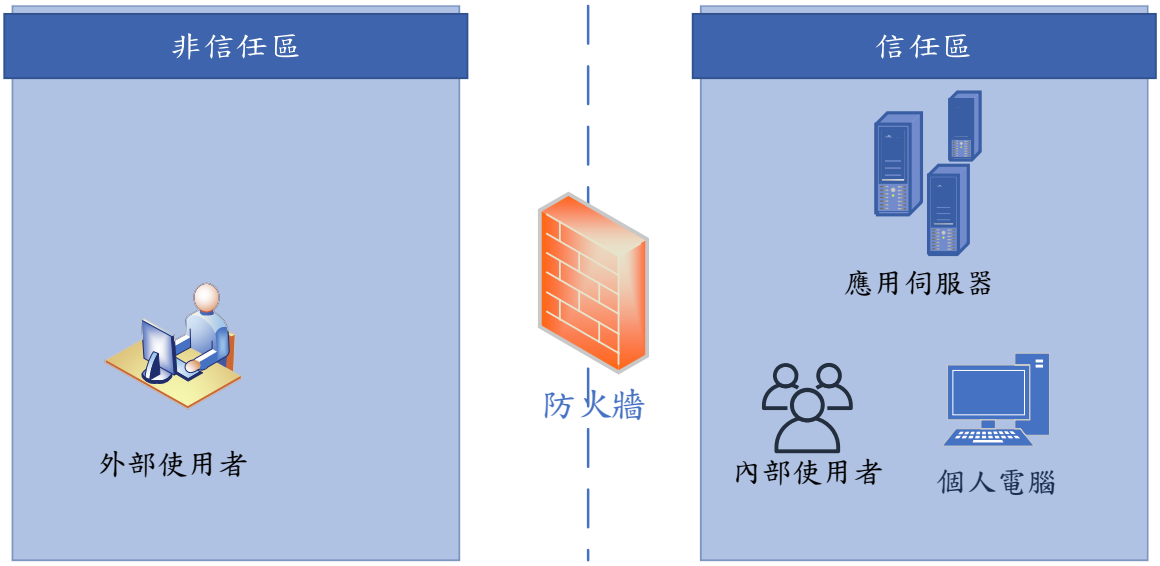

圖 1 傳統網路邊界防禦架構

這種策略假設內部網路是安全的，只要阻止外部惡意流量，就能確保安全。即便是現在不斷強調縱深防禦，透過對外部網路流量層層偵測，如入侵偵測(Intrusion Detection System, IDS)、入侵防禦(Intrusion Prevention System, IPS)，並輔以端點偵測與反應(Endpoint Detection and Response, EDR)，這種策略可能仍有下列 3 點需要強化：

- 不能完全阻止外部攻擊者入侵內部網路

在社交工程、釣魚郵件、惡意軟體等手段日益普遍和精密的情況下，一旦攻擊者成功入侵內部網路，他們就能自由地竊取或破壞內部資源，因為內部網路缺乏足夠的監控和驗證機制。

- 不能有效地管理內部使用者或設備的權限和行為

在遠端工作、雲端服務、物聯網等趨勢下，企業內部網路的邊界變得模糊且不斷變化。這意味著內部使用者或設備可能會因為人為失誤、惡意操作或被感染而成為資安風險的源頭。

- 不能有效地保護企業與合作夥伴或客戶之間的資料交流

在數位化轉型、跨組織協作、開放金融等趨勢下，企業需要與外部實體共享更多的資料和服務。換言之，企業需要在保障資安和提升效率之間取得平衡。

從現實狀況來看，台灣近幾年各行各業受駭事件頻傳(如下圖 2)，例如公共部門的中油公司勒索病毒事件；金融服務業的遠傳銀行、第一銀行受到駭客攻擊，除了蒙受財物損失也影響商譽；科技業的台積電，受到新購機台中毒的影響，即供應鏈攻擊，造成業務中斷，這些案例表示網路邊界防禦策略需要重新檢視。

公共部門	金融服務業	科技業
• 2018.4 高雄果菜公司以比特幣支付贖金，以解鎖交易電腦。 • 2018.12 台灣高鐵票務系統被駭客以手機駭入。 • 2019.1 台北市衛生局 298萬筆個資外流。 • 2019.6 銓敘部 59萬筆資料外流，24萬名公務員個資曝光。 • 2020.5 中油遭到勒索軟體威脅，包括捷利卡以及中油Pay系統遭駭，無法使用。	• 2016.7 第一銀行被東歐駭客集團駭入，從ATM盜領新臺幣8327萬元。 • 2017.2 13家證券公司集體受到駭客勒索，並且對多家券商發動攻擊。 • 2017.5 中國駭客入侵雄獅旅遊，36萬名消費者個資外洩。 • 2017.10 遠東銀行 SWIFT系統受駭，被盜轉6010萬美元。	• 2016.11 華義遊戲伺服器受到駭客攻擊，勒贖比特幣，價值台幣近百萬元。 • 2018.8 台積電生產線嚴重停擺。 • 2019.3 東歐駭客在紐約認罪，坦承竊取廣達身分，向臉書和谷歌。詐取貨款約38億元台幣。華碩軟體更新檔被入侵，導致上萬台電腦受影響。 • 2019.4 友訊和TOTOLINK共近2萬台家用路由器被駭客入侵，讓用戶進入假網站，騙取密碼。

圖 2 近年台灣重大資安事件列表(參考來源：林宏達(2020))

除此之外，隨著資訊系統使用情境逐漸複雜，尤其是 2019 年至 2022 年疫情期間，各國限制人員移動或甚至封城，各企業被迫加速數位轉型，邁入雲端並且開放居家辦公、自攜電子設備(Bring Your Own Device, BYOD)等，打造新的工作型態，使得傳統的網路邊界防護架構漸露短絀，無法有效地抵抗攻擊者無處不在的滲透。這些事件都暴露了傳統的資安防禦策略存在的缺陷，也提醒了企業需要轉變策略，採用更先進的資安架構來保護自己的資產和客戶的隱私。

因此，企業需要進化邊界防禦的思維，朝向零信任架構(Zero Trust Architecture)。零信任架構是一種新型的資安架構，它不再預設任何使用者或設備是可信任的，而是對所有的請求都進行驗證和授權，並進行監控與管理。

貳、零信任概念

零信任一詞的具體概念形成，可追溯至時任 Forrester Research 副總裁的 John KindervagJohn Kindervag 於 2010 年發表的一篇文章—《Build Security Into Your Network's DNA: The Zero Trust Network Architecture》，其中提出「零信任模型(Zero Trust Model)」(Kindervag, J. (2010))，將相關概念刻畫出骨架，從而豐富其內涵。現在零信任成為描述網絡安全解決方案的術語，這些解決方案將安全從基於網路位置的預設信任，轉移到基於每次交易評估信任。

在學術研究上，早在 1994 年 Stephen Paul Marsh 的資訊安全博士論文就有零信任的雛型概念出現。此外，2003 年的 Jericho 論壇，已開始有關於去邊界化(de-perimeterization)的議題討論，包括不根據網路位置預設性地信任及單一靜態防禦在大型網段上的局限性，去邊界化的概念後來進化為更廣泛的零信任概念。在實作面上，2009 年 Google 實施了一種名為 BeyondCorp 的零信任架構。2019 年，美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)發布了 SP 800-207 標準文件，詳細說明了零信任架構的定義、邏輯元件、部署場景和威脅分析(羅正漢(2022 年 8 月 2 日)、Alper Kerman. (2020, October 28))。

所以，零信任概念是一個持續地演變，並經過眾人去蕪存菁後的觀念，起源是為了解決傳統的網路邊界防禦安全模型的不足，特別是在現代的複雜和多變的環境中，依賴固定的網路邊界或預設的信任等級，已無法滿足網路安全需求。零信任概念的核心思想是「從不信任，總是驗證」，即對所有的連線、使用者和資產進行持續和動態地驗證和授權(John Turner and Justin McCarthy. (2023, March 14))。

目前零信任並無統一的認證規範，相同概念但不同名詞的狀況很多，但大多情況下，零信任網路安全，或是簡稱的零信任、零信任模型、零信任架構，其實要描述的概念，可以視為一種企業網路安全的方法、或一套關於工作流程與系統設計及維運的指導原則，且奠基於零信任原則的企業網路安全架構，以改善任何機密或敏感資料的安全。

參、各國零信任架構政策

近年隨著零信任架構(或策略)越來越廣為人知，及其對去邊界化防禦的效益，國際社會已將其納入資訊系統網路安全政策或標準中，其中不少國家已設定推動施行期程，有序地逐步推廣，甚至部分國際大型企業，早已採行零信任架構多年，尤其是雲端服務廠商，如微軟、Google、Amazon、Netflix等。

新加坡為了應對數位技術轉型帶來的挑戰，並確保其在數位時代的安全，於 2021 年 10 月發布新加坡 2021 網路安全戰略(Singapore Cybersecurity Strategy 2021)，其中一個戰略支柱—建設韌性基礎設施，便要求新加坡政府實施政府信任基礎架構(Government Trust-based Architecture, GTbA)，該架構將零信任原則轉化為政府理念，從而加強應用程式和系統的安全性(Singapore, C. S. a. O. (2021))。此外，新加坡政府提出一個網路安全框架—政府零信任架構(Government Zero Trust Architecture, GovZTA)，以實施零信任；基於「永不信任，始終驗證」的核心原則，該框架提出 4 個關鍵原則(應用最小權限並執行存取控制、限制橫向移動、安全自動化和協調流程、及強化偵測和回應)、5 個技術支柱(身分、設備、網路、應用程式和資料)、2 個啟動器(可視化和自動化、與治理)及 1 個零信任引擎，作為建構的基本元件，以打造

出協調、融合並有序的零信任架構(Government Zero Trust Architecture (GovZTA). (2023, May 16))。

日本內閣網路安全中心(内閣サイバーセキュリティセンター)於 2021 年 9 月 28 日發表「網路安全戰略」(サイバーセキュリティ戦略)，旨在數位轉型時代及確保網路安全的背景下，實現一個全民參與的數位社會，並強化國際間網路安全合作，達到整體網路公共空間的自由、公平和安全。為推展前述戰略計畫，建立政府資訊系統的網路安全措施統一標準，日本數位廳(デジタル庁)參考美國 NIST 多項安全標準，於 2022 年 6 月 30 日發布 4 項有關技術文件，分別為政府資訊系統安全設計指引、零信任架構應用策略、持續風險監控與回應(Continuous Risk Scoring and Action, CRSA)系統架構，以及政府信息系統漏洞診斷指引，做為日本政府資訊系統安全控制措施實施的統一標準(妹脊敦子(2022 年 8 月 12 日))。

英國國家網路安全中心（National Cyber Security Centre, NCSC）於 2021 年 7 月 23 日，發布了零信任架構設計原則 1.0，以做為實施零信任網路架構的指引，內含 8 項設計原則，旨在幫助組織安全地構建這種進階的網路架構。零信任架構從網路中移除固有的信任，並透過嚴格的身分驗證(如多因子驗證)、授權、設備健康度和被存取的資料價值，來判斷連線的可信賴程度。每個連線都經嚴格身分驗證，且根據對其授權的原則進行檢查，如果未明確允許，則會中斷連接(Zero trust architecture design principles. (n.d.))。此外，NCSC 並提供相關配套指引，例如，如何由傳統邊界防禦架構移轉至零信任架構的指引、當有老舊系統無法適用零信任架構時，要如何建置混合型的零信任架構指引、以及如何確保設備安全與健康的指引等，這些都有益於組織實際進行零信任架構的實作與應用。

美國政府為應付日趨嚴峻的網路威脅，改善其資安現況，倡議採用零信任原則與方法，保護資訊系統與網路；同時，在聯邦政府 CIO 聯席會(CIO Council)授權下，美國 NIST 及旗下國家網路安全卓越中心(National Cybersecurity Center of Excellence, NCCoE)於 2019 年 2 月正式啟動零信任架構計畫，NIST 負責零信任網路架構的標準，NCCoE 則要發展零信任網路架構的實踐指引，並推動商用產品符合 NIST 零信任架構。隨後，美國總統拜登在 2021 年 5 月發布行政命令，要推動美國聯邦政府網路安全現代化，要求導入零信任架構的網路安全策略，其中特別指出聯邦政府需做出大膽的改變與重大的投資，以保護關鍵基礎設施。

歐盟為保護整個歐盟地區的網路和資訊系統，加強整個歐盟網路安全和彈性，歐洲議會 2022 年 11 月 10 日批准 NIS2 指令(the Revision of the Network and Information Security Directive)，其中要求基礎和重要實體(如銀行、金融、醫療保健、運輸和其他部門)採取若干安全措施，包含零信任作為基本的網路安全衛生措施(Ticlea, A. (2023))。除此之外，有超過三分之二的歐洲企業或機構已經開始制定零信任戰略，高於 2020 年時的四分之一左右 (Muncaster, P. (2023, March 7))。

我國政府於 2021 年 2 月發布的第六期「國家資通安全發展方案（2021 年至 2024 年）」，其 4 大推動策略之一的「善用智慧前瞻科技、主動抵禦潛在威脅」，為完善政府網際服務網防禦深廣度，推動政府機關導入零信任網路，並以 A 級公務機關優先逐步導入，且逐年導入零信任網路的 3 大核心機制：身分鑑別、設備鑑別和信任推斷(行政院國家資通安全研究院 (2022))。我國的零信任網路架構規劃主要參考美國 NIST 發布的零信任架構文件 NIST SP 800-207。

綜上，各國的零信任政策，大多提供相關實施零信任原則標準或指引，即便具體的實施細節可能會略有差異，但是其目標和原則都存在相似之處。

肆、零信任架構

從前一節可知，目前各國推行的零信任架構，若不是參考美國 NIST SP 800-207 所描述的零信任架構內涵，就是可與之相參照。此外，零信任架構並不是一個單獨存在就能完美運行的架構，它需要很多配套的安全控制措施，其中很多措施在邊界防禦模型中，已推行多年。而美國聯邦政府推行的許多資訊安全政策與標準，如聯邦資訊安全管理法案(Federal Information Security Management Act, FISMA)、風險管理框架(Risk Management Framework, RMF)、可信任網路連接(Trusted Internet Connection, TIC)、還有持續診斷和緩解計畫(Continuous Diagnostics and Mitigation Program)，都與 NIST 的零信任架構息息相關，可說是一整套的零信任標準，因此，本節敘述將以美國 NIST 公布的相關標準為主。

一、零信任與零信任架構的定義

NIST 針對零信任與零信任架構的意涵，提供了操作型定義如下：

- 零信任係指一系列概念與想法，使資訊系統與服務運作於假定已被入侵的網路環境時，准駁每個精確與且是最小授權存取請求時，能將其不確定性(允許存取連線的風險)降到最低。
- 零信任架構係指一種企業網路安全計畫，當中利用了零信任概念，並涵蓋架構中的元件(Component)關係、工作流程規劃與存取政策。

從其定義可知，零信任架構假設環境中存在攻擊者，企業不能再有預設性的信任，對於內部資產和業務功能的風險，必須經過不斷地分析與評估，並且制定防護措施來緩解這些風險，其聚焦在 3 個方面，其一為資料保護；其二是企業資產，包括實體資安設備、基礎架構元件、應用程式、虛擬及雲端元件；最後則是主體，也就是來自終端使用者、應用程式及非使用者操作的資源請求資訊。而該架構目的則是盡可能去防止資料外洩與限制內部橫向移動。

二、零信任架構的內容

具體而言，NIST 的零信任架構包含零信任原則、零信任網路、及邏輯元件，其內容如下：

(一)零信任原則

- 所有的資料來源與運算服務，都要被當作是資源。
- 不管與哪個網路位置的裝置通訊，都需確保安全。
- 對於個別企業資源的存取要求，應以連線為基礎去判斷是否許可。
- 對於資源的存取需要由動態政策來決定，包括要基於客戶端識別、應用服務，以及要求存取資產可觀察到的狀態，如其他行為或環境屬性。
- 企業對於所有自有與相關的資產，需監控與衡量其完整性與安全狀況。
- 在允許存取之前，所有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。
- 企業應該要盡可能收集有關資產、網路基礎架構與通訊的資訊現況，並用這些資訊來增進安全狀態。

(二)零信任網路特點

- 企業私有網路不能預設為信任的區域。
- 網路中的裝置可能不是企業所有，也不一定能被企業設定。
- 沒有一個資源是原本就可信賴。
- 並非所有企業資源都位於企業擁有的基礎設施上。
- 遠端使用者存取企業主體與資產時，不能完全信賴本身的網路。
- 在企業與非企業基礎建設之間移動的資產與工作流程，應具有一致的安全政策與安全狀況。

(三)零信任架構邏輯元件

NIST 將零信任架構所需的邏輯元件，大致區分 2 大類—內部邏輯元件與外部資料源元件(如圖 3 所示)，其中內部邏輯元件包含政策決定點(Policy decision Point, PDP)、政策執行點(Policy Enforcement Point, PEP)、設備、連線主體(如使用者或應用系統)、企業資源；另一方面，外部資料源元件則包含企業內各式各樣的作業環境資訊，例如，持續診斷和緩解系統(Continuous Diagnostics and Mitigation System, CDM)、產業合規(Industry Compliance)系統、威脅情資(Threat Intelligence)、網路與系統活動日誌(Activity Logs)、資料

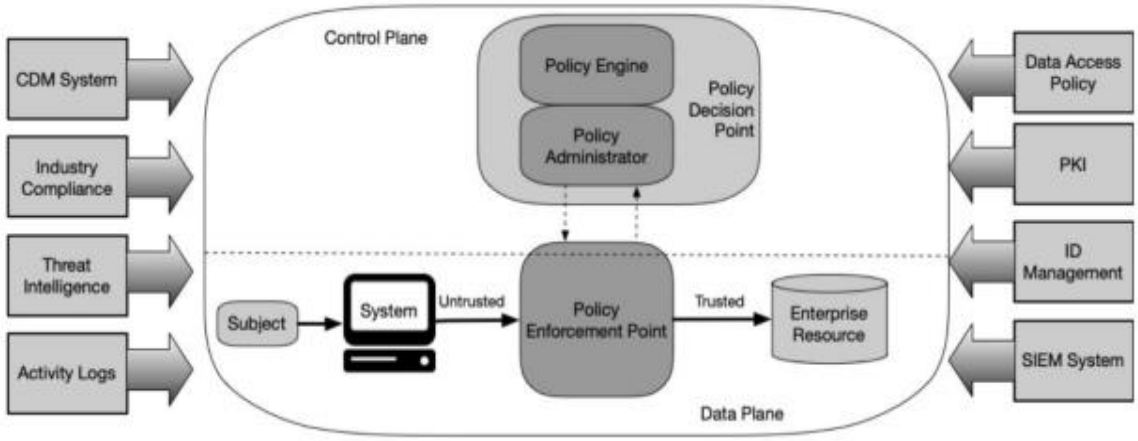

圖 3 零信任邏輯元件(資料來源：NIST)

存取規則(Data Access Policy)、公開金鑰加密系統(PKI)、帳號管理系統(ID Management)、資安資訊與事件管理系統(SIEM System)。

政策決定點(PDP)由政策引擎(Policy Engine, PE)與政策管理器(Policy Administrator, PA)所組成，政策引擎(PE)負責決定是否授予連線主體對企業資源連線存取權限，政策管理器(PA)藉由向政策執行點(PEP)發出指令，以建立或關閉連線主體與企業資源之間的連線。政策執行點(PEP)負責連線主體與企業資源間連線的建立、監控與終止。

前述的內部邏輯元件不需要是唯一系統，可以是單個資產執行多個邏輯元件的角色，或是多個資產執行單個邏輯元件的角色。此外，在 NIST 零信任架構中，將政策決定點(PDP)、政策執行點(PEP)區隔開來，分別置於控制網段(Control Plane)和資料存取網段(Data Plane)，以強化政策決定點的資訊安全。

伍、導入零信任的挑戰及解決方案的選擇

一、導入零信任的挑戰

目前各科技大廠都宣稱其產品或解決方案，支援或符合零信任原則或概念，但要應用到企業的資訊系統與網路環境，仍有不小的難度與挑戰，主要有以下幾個方面：

(一)技術面

需部署多種設備或管理工具，如身分和存取管理(Identity and Access Management, IAM)、端點安全、網路分割、加密、監控等，防止橫向移動和惡意攻擊，還需與既有的安全架構及系統進行整合和協調。此外，考慮不同

的網路環境和設備類型也是必要的，如雲端環境或地端環境、邊緣運算、物聯網等，並適應不斷變化的威脅情資和規範要求。

(二)組織面

需改變組織的安全文化和觀念，從以前的「預設信任」轉變為「永遠驗證」，將帶給使用者衝擊，從而產生抗拒心理。這需要獲得高層領導的支持和資源投入，並推動各部門和角色之間的協作和溝通。同時，也需要培訓和教育使用者和組織內部員工，讓他們理解及遵守零信任的原則和規定，並提高他們的安全意識和配合度。

(三)業務面

需平衡安全性和便利性之間的關係，避免過度限制或干擾業務流程和用戶體驗。因此，需根據不同的業務場景和需求，制定合適的安全政策和控制措施，並持續監測及調整其效果和性能。此外，也需與合作夥伴及供應商協調一致的安全標準和要求，並確保資料在跨組織和跨域時的安全性。

(四)執行面

需要對所有的資源和服務進行識別和分類，建立清晰的存取政策和規則，並對所有的使用者和裝置進行身分鑑別和驗證，根據風險和情境動態調整存取權限，這對人力與物力將是一大考驗。

二、零信任解決方案的選擇

市場上宣稱與零信任相關的產品種類繁多，且功能各異，這主要是因為在零信任架構下，需要做到對設備、連線、識別碼的細緻化管控，此外還要不斷地監控目前的作業環境與網路連線風險，這便需要許多工具來蒐集環境裡各式各樣紀錄，而且企業很有可能已經導入相關的解決方案或工具，因

此，應該先盤點企業內部有哪些已存在的工具，能提供實作零信任架構所需的功能或資訊，針對缺乏或不足的地方，再進行相關產品導入。

舉例來說，一個重視資訊安全的企業，其內部已導入的 IT 與資安工具可能如圖 4 所示，可大致分類如下：

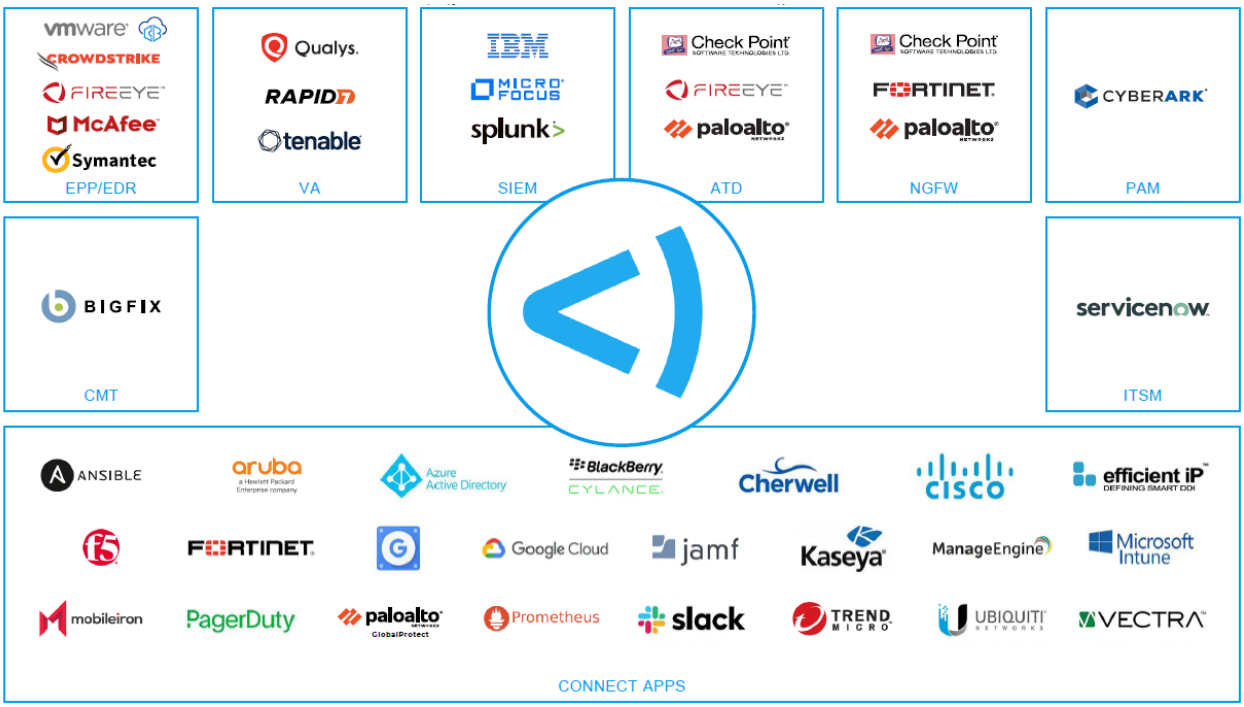

圖 4 企業內部常見 IT 與資安產品與廠商(資料來源：Forescout)

- 端點防護類，如端點偵測與回應(Endpoint Detection and Response/ Endpoint Protection Platform, EDR/EPP)、進階威脅偵測(Advanced Threat Detection, ATD)、防毒軟體等。
- 端點組態與資產管理類，如組態管理工具(Configuration Management Tool, CMT)。
- 弱點管理類，如弱點掃描工具(Vulnerability Assessment, VA)、弱點修補工具等。
- 特權帳號管理(Privileged Access Management, PAM)類。

- 網路防護類，如次世代防火牆(Next Generation Firewall, NGFW)、網頁應用防火牆(Web Application Firewall, WAF)等。
- 事件紀錄與資訊整合平台類，如安全訊息事件管理系統(Security Information and Event Management, SIEM)、IT 服務管理系統(IT Service Management, ITSM) 等。
- 應用系統連線類，如雲端運算服務提供商提供的連線管理工具(如 Google Cloud、Microsoft Intune)、VPN 連線工具(如 PaloAlto GlobalProtect、Fortinet)、IP 與域名管理工具(如 EfficientIP DDI)等。

從前述的舉例，不難發現許多企業其實已經將設備、帳號、工作流程納入管理與監控，只差沒有完善的政策引擎點與政策執行點，此時，可尋找市面上相關的解決方案，以能具備最大整合性的方案為佳，透過整合與整併的做法，將企業目前的網路架構轉向零信任架構。

陸、零信任架構的導入

任何新科技的導入都有一定的風險，零信任架構做為一個進階的資安解決方案，同樣也有導入的風險，如前面提到的有可能會產生新的攻擊弱點，或是初期人員不熟悉相關設定或運作，導致錯誤的組態設定，讓整個企業陷入不安全的狀態，因此，需要有嚴謹的導入規劃與好的零信任解決方案。

為幫助企業能由淺入深、由點擴展至面有序地導入零信任架構，NIST SP 800-207 建議遵循下列 7 大實作流程步驟，這也是 NIST SP 800-37 風險管理框架(RMF)所規範的做法(如圖 5)：

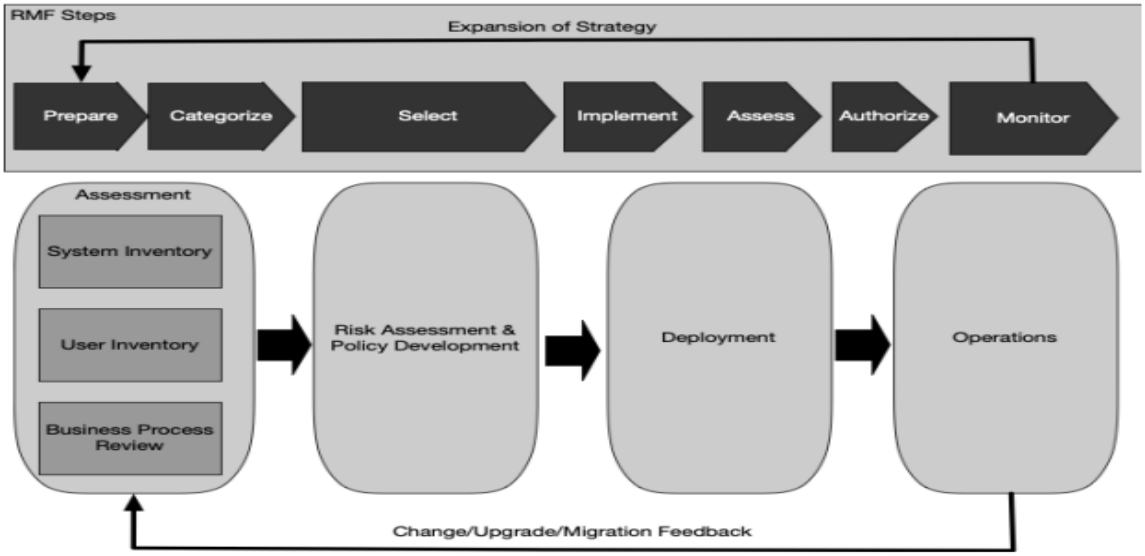

圖 5 零信任架構導入步驟流程圖(資料來源：NIST)

一、識別企業中的角色

為了使零信任得以施行，由政策引擎（PE）的角度來看，必須對於企業內的主體(Subject)先有所認識。這裡指的主體，包含了人員、非人員實體(Non-person Entities, NPE)，如可與資源互動的服務帳號。並可要求管理者依 NIST SP 800-63A 數位身分識別指引，執行註冊和身份驗證，符合更嚴格的驗證標準。

二、識別企業中的資產

企業資產包括硬體及軟體。硬體部分，如筆記型電腦、手機與物聯網裝置等，軟體部分，如使用者帳號、應用程式與數位憑證等數位物件(digital artifacts)，因此，建議考慮建立一套機制，便於將新發現的企業資產，做到快速識別、分類與評估。此外，不僅是對企業資產進行簡單的歸類與維護資料庫，還須包括配置管理與監控。

評估存取請求過程中，需要資產當前狀態資訊，這代表企業須能夠配置、調查與更新企業資產，如虛擬資產與容器，以及實體與網路位置等，以便進行資源存取決策時，將這些資訊輸入至政策引擎(PE)。

此外，非企業擁有的資產，或是企業擁有的 Shadow IT (企業內未經批准使用軟體、硬體或其他系統和服務，而資訊部門往往並不知情)，也應該盡可能的納入盤點，可能包括企業內可見的任何東西，如 MAC 地址、網路位置，並透過管理者的資料輸入加以補充，不僅可用於存取決策，也可用於企業的監控與日誌分析。

三、識別關鍵流程，評估與流程執行相關的風險

將業務流程、資訊流，及其與企業使命(mission)的關係，分別識別出來且排序，並由業務流程，提取出資源存取請求被批准或拒絕的對應情境。在初次規劃的零信任架構移轉，會建議從低風險的業務流程開始，避免失敗衝擊，累績足夠的經驗後，再選擇其他重要的業務流程進行後續移轉。通常會優先從利用雲端資源，或遠端工作者使用的業務流程開始，並驗證其可用性與安全性是否得到改善。

此外，企業用戶可以直接請求雲端服務，而非投射企業邊界到雲端或透過 VPN 連入企業網路，因透過企業的政策執行點(PEP)，可確保向用戶授予資源存取權之前已遵循企業存取政策。最後，還須考慮當實施零信任架構時可能會出現的問題，包括效能、使用者體驗，及可能增加工作流程脆弱性等，這些都需要做出某些程度的權衡與取捨。

四、針對零信任架構候選者制定政策

在識別候選服務或業務工作流程的時候，應考慮該流程對組織的重要性、受影響的主體(Subjects)，以及該工作流程所使用資源目前的狀態，而 NIST 風險管理框架(RMF)可用以評估資產的價值。在識別資產與工作流程之後，接著便是確認所使用或影響的上游資源(如 ID 管理系統、資料庫、微服務)、下游資源(如日誌、資安監控)與實體(如主體(Subject)、服務帳號)。最後，確認要使用的信任演算法(Trust Algorithm)，以動態計算信任程度來監控存取連線，並調整權重標準，確定存取管控政策是有效的。

五、識別候選的解決方案

當確定了業務流程的候選清單後，便是決定部署模型與供應商解決方案，決定時應考量下列因素：

- 解決方案是否要求在客戶資產安裝安全元件

在非企業資產使用或需求上，這因素可能會限制業務流程，像是 BYOD 或跨機構合作的情境。

- 解決方案是否同時支援地端與雲端

有些解決方案預設請求的資源是存放雲端，而不是在企業內部(即地端)。

- 解決方案是否提供即時 Log 紀錄以供分析

零信任的關鍵就是要蒐集工作流程活動相關的紀錄，以提供給政策引擎(PE)，做出存取決策。

- 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的通訊協議(如 Http/Https、SSH 等)與傳輸協議(Pv4 和 IPv6)，但有些解決方案可能只適用於特定協定，如電子郵件。

- 解決方案是否需要改變主體(Subject)原來的行為

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，這將改變執行工作流程的方式。此時的解決方案僅是將現有業務流程建立模型，作為試點計畫，除可確認該解決方案是否具通用性，也可驗證零信任架構效用，驗證完成後後再脫離原本的流程基礎架構。

六、初期部署與監控

在選擇工作流程與零信任架構元件後，便可開始進入初期部署階段。先以觀察或監控模式來進行，在「僅通報模式」(Reporting-only)下，執行一段時間，以確保政策是有效且可行，並讓企業可以理解其運行。此時，大多允許存取請求，並依據運作經驗修改存取政策。

七、擴展零信任架構

經過初期實際部署運作，完善工作流程的所有政策之後，企業便進入穩定運行階段。此時可以規劃下一循環的部署，即回到前述第四步驟，選定下一個工作流程與解決方案，並進行部署。

柒、結語

現今的企業資訊系統運用情境較以往更加複雜，運作的環境有可能在雲端，也有可能在地端，連線設備越來越多元，駭客攻擊無所不在，供應鏈安全屢屢登上新聞媒體版面，這些威脅無時無刻考驗著企業資訊安全管理能力，而零信任架構對於網路安全威脅，有以下幾項優點：

- 防止網路內的威脅橫向移動，減少內部攻擊的風險。
- 解決傳統的「內部等於預設可信」的安全模型在現代環境中的不足，例如遠端工作、雲端服務、移動裝置等。
- 降低未經授權的存取和使用的風險，提高資料和資源的保護。
- 提高安全性的可見度和監控能力，利用分析和情報來偵測及回應異常行為。
- 改善使用者的安全體驗和工作效率，提供一致和便利的存取流程。

簡而言之，在資安防護模型(Cyber Defense Matrix—識別、保護、偵測、回應與回復)裡，零信任架構有助於識別面與保護面的強化。

企業導入零信架構要面對的挑戰包含技術面、組織面、業務面與執行面，克服這些議題將有助推展零信任架構。另一方面，企業挑選零信任解決方案時，應先盤點目前符合零信任架構要求的資安設備或系統，以及對於零信任解決方案的整合性，避免購買重複功能的設備或系統，從整合與整併的角度，將目前的網路安全架構轉向零信任架構，如此便能在經濟效益下，強化企業資訊安全。最後，利用 NIST SP 800-207 的導入作法，盤點資訊系統、使用者與業務流程，挑選合適的候選業務流程，其後評估該流程風險並發展相應連線存取政策、部署、運行，接著修正後，再逐步擴大適用範圍，由點而線，再到面，全面實施企業零信任架構。

參考文獻

趨勢科技 TrendMicro (2018 年 9 月 6 日)。《電腦病毒 30 演變史》首部曲－從 1986 年的大腦病毒到 1996 年的 Taiwan No.1 文件巨集病毒。資安趨勢部落格。https://blog.trendmicro.com.tw/?p=56820

AWS 部落格。數位轉型定義為何？5 分鐘快速掌握數位轉型趨勢和成功案。https://aws.amazon.com/tw/events/taiwan/techblogs/digital-transformation/

林宏達 (2020 年 5 月 19 日)。【總統府遭駭】從政府到企業都受「駭」！3 個關鍵數字暴露台灣資安危機。財訊。 https://www.wealth.com.tw/articles/2f23c254-c3e6-4c6b-b3a4-66ad05201c2c

Kindervag, J. (2010). Build security into your network's dna: The zero trust network architecture. Forrester Research Inc, 27.

Alper Kerman. (2020, October 28). Zero Trust Cybersecurity: 'Never Trust, Always Verify. TAKING MEASURE. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.

羅正漢(2022 年 8 月 2 日)。【ZTA 101】NIST SP 800-207 第一章：簡介。IThome。https://www.ithome.com.tw/tech/152241

John Turner and Justin McCarthy. (2023, March 14). *Zero Trust Architecture: 2023 Complete Guide*. StrongDM. https://www.strongdm.com/what-is/zero-trust

Singapore, C. S. a. O. (2021). The Singapore Cybersecurity Strategy 2021.

Government *Zero* Trust Architecture (GovZTA). (2023, May 16). Singapore Government Developer Portal. https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture.html

妹脊敦子(2022 年 8 月 12 日)。「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」を読んでみた。NEC セキュリティブログ。https://jpn.nec.com/cybersecurity/blog/220812/index.html

Zero trust architecture design principles. (n.d.). https://www.ncsc.gov.uk/collection/zero-trust-architecture

Rose, S et al. (2020), Zero trust architecture (No. NIST Special Publication (SP) 800-207), National Institute of Standards and Technology.

National Institute of Standards and Technology, NIST. (2020). SP 1800-35 (Draft), Implementing a Zero Trust Architecture. https://csrc.nist.gov/publications/detail/sp/1800-35/draft

行政院國家資通安全研究院 (2022)。政府零信任網路說明 [PDF]。Retrieved from https://download.nics.nat.gov.tw/UploadFile/zerotrustnetworks/%e6%94%bf%e5%ba%9c%e9%9b%b6%e4%bf%a1%e4%bb%bb%e7%b6%b2%e8%b7%af%e8%aa%aa%e6%98%8e_V1.9_1110712.pdf

Ticlea, A. (2023). Directive (EU) 2022/2041 of the European Parliament and of the Council of 19 October 2022 on Adequate Minimum Wages in the European Union. Rev. Romana Drept. Muncii, 29.

Muncaster, P. (2023, March 7). Two-Thirds of European Firms Have Started Zero Trust. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/twothirds-of-european-started-zero/#:~:text=Over%20two-thirds%20of%20European%20organizations%20have%20begun%20developing,15%25%20were%20planning%20to%20adopt%20zero%20trust%20tech.