零信任資安發展趨勢

零信任資安市場將以 17.3%的複合年增長率快速成長。美國政府積極制定相關制度、架構與推動指引，帶動世界各國共襄盛舉。組織導入零信任架構非一次性的技術汰換，會遇到組織文化與資安/IT 跨部門協同不足、人才不足與治理能力缺口等問題，在技術層面會遇到 Legacy 系統整合、多雲/多供應商環境的存取一致性與策略執行等難題，造成使用與管理上的不便，需要靠 AI 來協助。零信任資安資本市場近年持續活躍，大量資金投入，提升相關新創邁向 IPO 之動能。相關應用領域廣泛多元，正持續滲透進各垂直領域。導入零信任的組織須採取分階段實施策略，並同時投資人才與自動化監控平台，以降低轉型風險並加速資安價值的實現。

零信任架構

隨著全球數位化浪潮的擴散，傳統的網路安全防禦方式已越來越難抵擋無孔不入的網路攻擊。2010 年，John Kindervag 提出零信任架構（Zero Trust Architecture，ZTA），以「受信任的網路周邊並不存在」為假設，採取不信任所有連接的原則，整合各種網路安全保護方法，驗證每一個存取，以期有效保護重要資產、資料、應用程式與服務不被惡意方所掌握。

其後， 各種零信任方案陸續被提出， 例如 2014 年 Google Cloud 展開零信任架構實作， 於 2022 年對外說明實踐成果，並繼續努力推出解決方案；雲端安全聯盟（Cloud Security Alliance） 分 別 於 2014、2019 年 推出 Software Defined Perimeter（SDP）1.0 和 2.0 版的架構指南，協助企業實現零信任網路建置。

因應需求上升，美國國家標準暨技術研究所（NIST）也於 2020 年 8 月公佈零信任架構標準化文件 SP 800- 207，指引所有組織將現行的資安防護架構轉換為零信任架構，如圖 1 所示。這促使越來越多的組織推動轉換，眾多資安業者也參考此架構發展解決方案。該文件概述零信任七項原則：

1. 所有資料來源和計算服務均被視為資源。
2. 所有通訊均受到保護，無論其位於哪個網路位置。
3. 對單一企業資源的存取是基於會話進行授予。
4. 資源存取權限由動態策略決定。
5. 企業監控並評估所有自有及相關資產的完整性和安全性。

6. 所有資源的身份驗證和授權都是動態的，並且在允許存取之前會嚴格執行。
7. 企業盡可能收集有關資產、網路基礎設施和通訊當前狀態的信息，並利用這些資訊來提升其安全態勢。

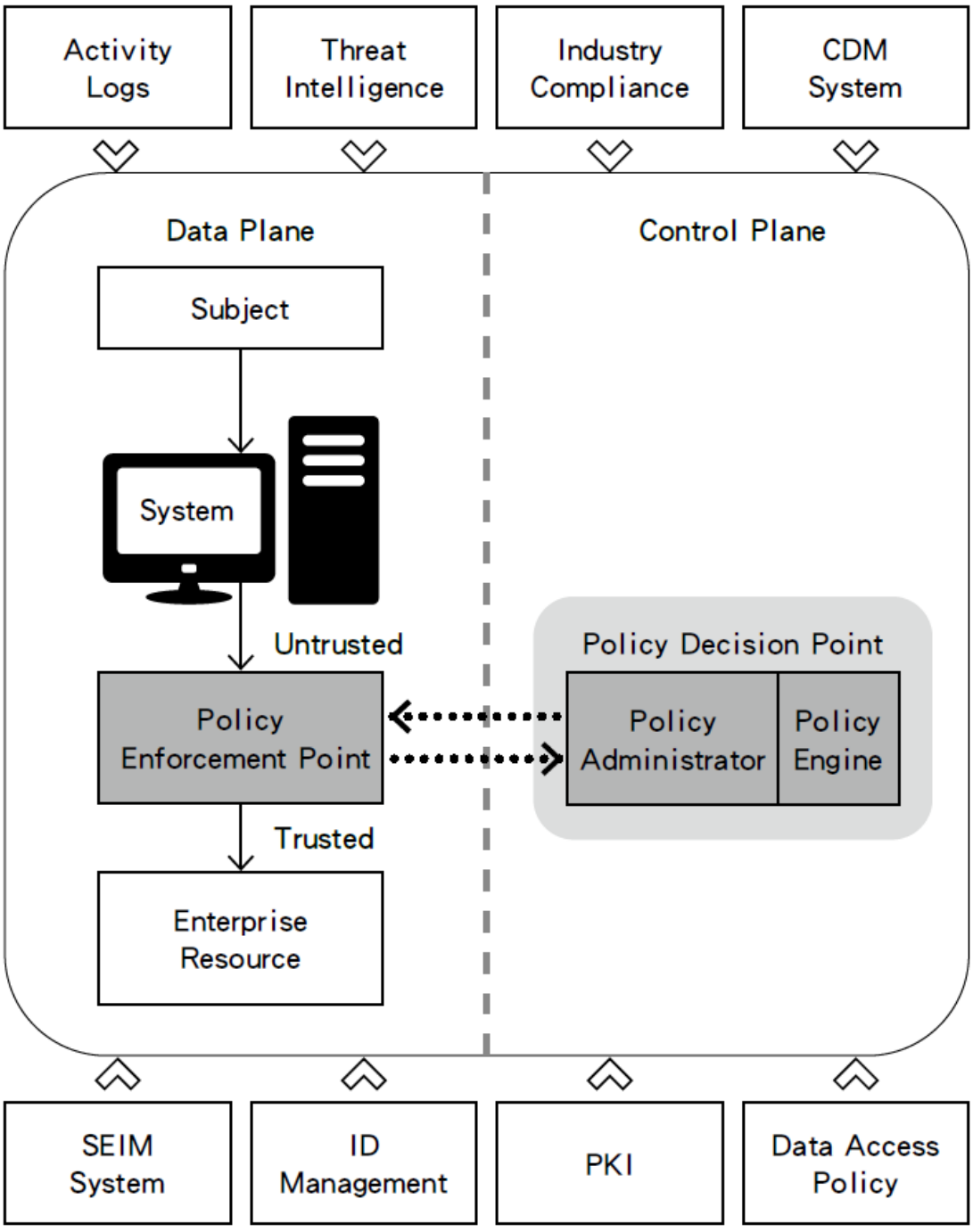

圖 1　Core Zero Trust Logical Components

銳企製圖，參考資料：美國國家標準暨技術研究所

與此同時，伴隨全球地緣政治的緊張與對抗持續上升，在政府政策面向上已可看到美國行政管理和預算局（OMB）於 2022 年 1 月 26 日 正式發佈新網路安全策略與 M-22-09 備忘錄，要求政府機關實施零信任架構（Zero Trust Architecture）。各機關在備忘錄發布後 30 天內應指定零信任戰略實施負責人，在 2024 年前達到 5 項資安標準要求。五角大廈已計畫要在 5 年之內將所有網路轉換成零信任架構。未來可預期零信任架構的轉換需求勢必會躍升為資安領域的主流。

2024 年，John Kindervag 說明零信任的實施可分為五個步驟：Define the protect surface → Map the transaction flows → Architect a Zero Trust Environment → Create Zero Trust policy → Monitor and maintain，以利簡化安全流程，確保組織系統的反脆弱性（Antifragile），增加面對資安挑戰時的韌性。

零信任資安市場現況

依據調研公司 Claight 之報告，2024 年全球零信任資安市場規模約為 316.3 億美元。預估未來十年，市場將以 17.30%的複合年增長率持續成長，至 2034 年，市場規模將達到 1,559.8 億美元左右。美國是此市場的主要推手，使得北美市場在零信任相關產業發展上佔據相當大的份額，主因美國政府與公部門在此領域的支出大幅上升，並且透過制定政策與產業規範，持續推出日益嚴格的資料隱私和安全標準及政策，以及物聯網（IoT）、人工智慧（AI）和數位技術的普及，帶動中小企業和大型企業相關資安需求大增，都顯著促進了該地區市場的成長。其他地區的主要國家也持續跟進，各類組織對於零信任安全實施方案的解決方案之需求不斷增長，有望顯著推動整個市場的成長。

各國推動零信任現況

零信任架構已從早期概念探討進入到實務部署階段，美國、歐盟、英國、日本、韓國、澳大利亞、新加坡等國陸續制定零信任架構推動策略。在推動過程中，零信任架構的導入需要與傳統既存的資安模式混合運作，如同於開車中同步改車。推動時須留意整個流程非一次性的技術汰換，而是要確保整個導入過程中，系統能持續運作，無資安空窗期或衍生出新的漏洞。以下摘要說明各國推動做法之特色。

美國在政策端以 OMB / White House 的 M-22-09 為里程碑，要求聯邦機關採行零信任原則，並有 DoD 及多個聯邦機構制定專屬策略與成熟度模型；

網路安全暨基礎設施安全局（CISA）與 NIST 提供實作與成熟度工具以支持部署。2023 年 4 月，CISA 推出零信任成熟度模型 2.0 版，以五個不同支柱凸顯漸進式實施過程，隨著時間的推移，可以逐步進行最佳化。這五個支柱包括身分（Identity）、設備（Devices）、網路（Networks）、應用程式和工作負載（Applications and Workloads）以及資料（Data）。每個支柱都包含以下跨領域功能的共通細節：可見性和分析（Visibility and Analytics）、自動化和編排（Automation and Orchestration）以及治理（Governance）。CISA 也提供各階段的指導標準如表 1 所示，供各機構識別每個零信任技術支柱的成熟度，以此確保成熟度模型的一致性。

表 1　零信任成熟度發展歷程（Zero Trust Maturity Journey）

階段	**核心特徵**
傳統階段 **Traditional**	● 手動設定生命週期（建立→變更→停用） ● 身份屬性、存取控制、日誌屬性皆需人工設定 ● 安全策略為「靜態」、且多由個別系統獨立管理 ● 最小權限僅在帳號建立時設定一次，缺乏後續調整 ● 資安技術與防護措施「各自為政」，存在大量壁壘 ● 回應事件依賴人工流程 ● 日誌/遙測（telemetry）無法跨系統進行關聯分析 典型狀態 ● 仍以傳統周邊式資安為主、缺乏動態調整能力 ● 階段特色：低自動化、低協作、低可見性
初始階段 **Initial**	● 元件屬性（如身份、裝置健康度）開始「部分自動化設定」 ● 初步建立跨技術領域（pillars）間的整合作法 ● 存取控制會在最小權限原則上「做有限度調整」 ● 能與外部系統進行部分整合（例如 IDaaS、資安監控） ● 可對部分資安事件進行初步回應 ● 內部系統開始具備「整合式的可見性」 典型狀態 ● 開始導入 ZTNA、IAM、自動化政策等，但覆蓋不全面 ● 階段特色：開始自動化、開始整合，但仍有限度

高階階段 **Advanced**	● 生命週期與屬性設定（身份、裝置、風險、策略）高度自動化 ● 跨 Zero Trust 五大支柱能協作：身份、裝置、網路、應用與資料 ● 實現「集中式視覺化管理與身份控制」 ● 策略與存取控制能跨支柱一致執行 ● 已可自動執行預定的緩解措施（例如封鎖帳號、降低權限） ● 最小權限可依照 風險等級、姿態(posture) 動態調整 ● 邁向企業範圍整合，包括外部資源、雲端、多雲環境 典型狀態 ● 已具備成熟姿態管理、XDR、動態政策、跨平台協作 ● 階段特色：高度自動化、集中治理、風險導向
最佳化階段 **Optimal**	● 生命週期全面自動化（Just-in-Time / Just-enough access） ● 所有資產、裝置與身分皆可「自我回報」狀態並自動驅動政策 ● 動態政策依據偵測事件、行為、風險而自動變動 ● 全企業一致（Enterprise-wide）的敏感度與事件偵測能力 ● 依據角色、行為、風險自動提供動態最小權限（JEA/JIT） ● 各支柱全面互通，達成「持續動態的全域監控」 ● 具備「完整情境感知」與跨環境（含雲端/外部與供應鏈）防護能力 典型狀態 ● 零信任已完全滲透企業營運、策略、架構 ● 階段特色：全自動化、全動態、全跨支柱、全範圍可視化

銳企製表，參考資料：美國國土安全部網路安全暨基礎安全局

歐盟在資安與資料保護（GDPR）的大框架下，強調資料最小化與跨境合規；英國與個別成員國亦將零信任納入重要基礎設施防護要求。

亞太國家多以關鍵基礎設施為優先推動對象，日本與新加坡發布專門指導與試點，澳洲亦把零信任與智慧國家防護列為資安重要項目。

韓國政府整理出零信任六大應用情境：分公司遠端存取、第三方協作、組織內部網路/網際網路隔離、內部部署與雲端整合、OT/ICS 工業控制、M2M/物聯網，分別擬訂推動目標、要求與實踐重點，供產業界導入時參考。

臺灣零信任推動狀況

臺灣政府於 2021 年 2 月發佈「第六期國家資通安全發展方案」，啟動政府組織導入零信任架構。2022 年 7 月，確定優先推動資通安全責任等級為 A 級之機關導入零信任架構，並同步推動國內廠商發展零信任資安產業鏈，相關業務由新成立之數位發展部轄下資通安全署進行政策規劃與投入資源。

另外，數位發展部指派轄下國家資通安全研究院，與數位政府司和資通安全署合作定期檢核政府的資安韌性。

政府參考美國 NIST 相關文件，以「使用者身分、使用設備、行為」作為控制資料存取和應用的依據，對應「身分識別、設備鑑別、信任推斷」三項核心機制。2023 年，數位發展部已優先輔導 22 個資安 A 級機關導入身分識別，並接續導入設備鑑別與信任推斷機制。

推動零信任時會遇到之挑戰

零信任機制會造成使用與管理上的不便，像是在組織與營運層面，會遇到組織文化與資安/IT 跨部門協同不足、人才不足與治理能力缺口等；在技術層面，會遇到 Legacy 系統整合（OT/ICS 與醫療系統為典型難題)、多雲 / 多供應商環境的存取一致性與策略執行等難題。

解決方案發展趨勢

未來需要靠 AI 來協助辨識與管理，運用 AI 作為隱形的守門員，才能有效降低機制造成的不便。奧義智慧科技（CyCraft Technology）是臺灣聚焦 AI 資安技術的新創公司，該公司於 2023 臺灣資安大會表示，資安業者除了要遵守政府日益嚴謹的法規，還必須在更短的時間內完成偵測→調查→處置。若繼續依賴過往作法，將會犧牲防護品質而無法達成防護目標，導入 AI 等自動化科技勢在必行，尤其是在事發前的偵測和發生中的調查階段幫助最大，未來將成為資安人員不可或缺的夥伴。

零信任資安募資市場近況

資安資本市場在 2024 至 2025 年持續活躍，SASE / ZTNA / 零信任相關廠商如 Netskope、Zscaler、Palo Alto 之雲端產品均吸引大量資金與 IPO 動能；以下列舉幾家近期有募資的零信任資安新創企業。

表 2　零信任資安新創募資近況

公司	主要業務 / 定位	**募資近況 / 最近事件**
Elisity	身份導向 (identity-centric) 微分段 + 零信任存取控制 (針對 IT + OT / IoT 環境)	2024 年 4 月拿到 US$ 45 million Series B。
TXOne Networks	專注工業 / OT / 關鍵基礎設施 (ICS/SCADA) 的零信任 / OT 安全解決方案	2024 年 5 月完成 US$ 51 million Series B extension。
NetBird	開源 / 社群導向的 Zero-Trust 網路 overlay 解決方案	2024 年 12 月獲得 seed 融資 € 4 million。
Hypori	提供零信任 BYOD / 虛擬移動工作區 (virtual workspace) 平台	2025 年 1 月完成 Series B extension ($12 million)。
Portnox	雲端原生存取管理 / 網路存取控制 (取代傳統 NAC)	2025 年 4 月取得 US$ 37.5 million Series B。
Zero Networks	提供 agentless、自動化 micro-segmentation / 零信任網路存取 (ZTNA) 平台	2025 年 6 月拿到 US$ 55 million Series C 融資。
Noma Security	零信任 + 資料 / AI-模型安全 (針對 AI agent、雲端環境的威脅)	2025 年 7 月宣布 私募 $100 million (Series B)，累計資金達 ~$132 M。

銳企製表，參考資料：Crunchbase

零信任資安商機

目前零信任資安於主要產業的應用機會包括金融業涵蓋身份與交易保護、反詐騙；能源/公用事業涵蓋 OT/ICS 的網路分段與製程保護；電信業涵蓋跨域認證與邊緣安全服務；Managed Zero Trust / MSSP 提供零信任代管服務。

透過分析前述近年獲得募資的零信任資安新創，可觀察出以下發展趨勢，有意投入資安領域之新創團隊可留意相關商機。

1. 多樣化應用場景：從企業 IT / 雲端、混合/多雲環境，到工業 OT / ICS、IoT / 邊緣裝置 (如 TXOne)、BYOD、AI-agent / 雲端服務安全 (如 Noma Security)——顯示零信任不再是單純 VPN 替代，而是貫穿 IT、OT、Cloud / AI / 混合環境的全面防護。

2. 資金流入強勁：多家公司在 2024–2025 年成功取得 B / C 輪資金，金額從數千萬到上億美元不等，代表市場與投資人對零信任安全解決方案需求日益看好。
3. 新技術 / 新模式：不只是傳統 ZTNA / 微分段，有些創業公司聚焦於 identity-first、安全雲端 workspace、AI / 模型保護、agentless micro-segmentation、工業控制系統 (OT) 的零信任整合，展現技術與應用層的創新。
4. 市場涵蓋面擴張：從企業 / 雲端到工業、OT、IoT、AI 等，意味著未來零信任市場將不只是企業 IT，也包含運營技術 (OT)、工業製造、雲端服務供應商、AI 研發機構等多領域 — 對資安廠商、服務提供者都有廣泛機會。

結語

零信任架構正從政策驅動走向商業化落地。建議政府與企業採取分階段（Identity → Device → Network → Applications and Workloads → Data）實施策略，並同時投資人才與自動化監控平台，以降低轉型風險並加速資安價值的實現。

參考資料

•【搞懂零信任，從理解 NIST SP 800-207 著手】打造以零信任原則的企業網路安全環境。iThome。2021

•【臺灣企業應加強對於零信任的認知】迎接零信任時代！從盤點資產與資料流程著手。iThome。2021

•【臺灣資安大會直擊】資安院：政府推動零信任架構，今年完成 A 級機關導入身分鑑別，2 機關將先導入信任推斷機制。iThome。2024

•導入零信任架構的五步驟：從內向外的安全策略。iThome。2024

•Zero Trust Architecture. National Institute of Standards and Technology (2020)

•Zero Trust Maturity Model. Cybersecurity and Infrastructure Security Agency (2023)

•Zero Trust Security Market Size, Share, Growth Analysis Report and

Forecast Trends (2025-2034). Expert market research (2025)