資安產業

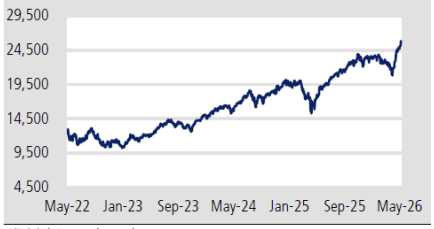
Cybersec 2026：Agent 世代數倍生產力也帶來數倍風險

焦點內容

1. Agent 世代需要用 AI 對決 AI，立體化防禦策略成為必須。
2. SASE/Network security：集中化管理平台與零信任架構趨勢更加明確。
3. XDR/CNAPP：龐大的私有化&即時資料是 AI 無法取代的護城河。
4. Data security/IAM/Governance：從 DLP 被動防禦到 DSPM 主動情報蒐集，數位員工的權限管理與可視化挑戰即將到來。

Nasdaq 指數

Nasdaq 指數，點



資料來源：Bloomberg

ESG 分數評等

Company		Overall	E	S	G
Amazon	AMZN US	83	90	80	79
Alphabet	GOOGL US	80	77	84	78
Microsoft	MSFT US	91	78	94	92
Cloudflare Inc	NET US	62	26	72	64
CrowdStrike Holdings	CRWD US	25	20	29	23

資料來源：Refinitiv、凱基

重要訊息

Cybersec 2026 台灣資安大會(5/5-5/7)追蹤最新資安產業趨勢。

評論及分析

Agent 世代需要用 AI 對決 AI，立體化防禦策略成為必須。相較於雲地混和及 AI 賦能趨勢，2026 隨著 AI 能力提升及 Agentic workflow 逐漸落地，雖然帶來數倍生產力的提升，但同時也伴隨著數倍的風險與管理挑戰：(1)OpenAI GPT-5.5 與 Anthropic Mythos 在第三方 AISI 機構測試網路攻擊能力較過往大幅提升，Zero day clock 顯示從發現漏洞到實際利用時間差正在大幅縮短，自 2025 年的 23 天預計降低至 2026 年的僅 1 小時與 2028 年的僅 1 分鐘，OpenAI 與 Anthropic 分別發起 Trusted Access for Cyber(TAC)與 Project Glasswing，以 AI 對決 AI；(2)Agentic AI 相較過往增加工具調用、記憶系統等能力，企業 Agent 數量也將大幅增加，需要更立體化的防禦策略以同時管理風險與進行可視化。

SASE/Network security：集中化管理平台與零信任架構趨勢更加明確。NET 與 FTNT 提及傳統資安架構工具過多且彼此割裂，VPN 與 Legacy Access 已難應對混合辦公與 AI Agent 流量，企業開始轉向 Unified Platform 與 Zero Trust 架構降低管理複雜度，CSCO 指出企業 Network Infrastructure 長期面臨技術債問題，近半數網路設備已進入 EOL/EOS 階段，超過 10 年的 Router、Switch 與 Firewall 仍大量存在，相關投資仍明顯落後。

XDR/CNAPP：龐大的私有化&即時資料是 AI 無法取代的護城河。GOOGL 觀察到 APT 組織已開始將自主 Agent 直接整合進漏洞利用、防火牆探測、SQL Injection、橫向移動與惡意程式生成流程，可 24/7 持續執行攻擊，使傳統 Signature-based 偵測有效性持續弱化，Cloud Security 架構開始朝向 Code-to-Cloud 整合平台演進，結合 Attack Path Visualization、Remediation Agent 與 AI-driven True Positive 判斷，推動 SecOps 從被動告警進一步邁向 Self-healing 與自動化修復。

Data security/IAM/Governance：從 DLP 被動防禦到 DSPM 主動情報蒐集，數位員工的權限管理與可視化挑戰即將到來。MSFT 認為 AI 從 Chatbot 走向 Agent 後，風險從回答錯升級成執行錯，數位員工(AI Agent)治理與防禦框架強調多層次結構，而非單一產品解法，Azure AI Content Safety 負責偵測 Prompt Injection 與語意攻擊，PyRIT 用於模型紅隊測試，Entra ID 與 Purview 管控 Agent 身分與資料邊界，而 Agent 365 的定位是 AI Agent 治理底座，先看見再進一步做到存取控管、風險偵測與生命週期管理。

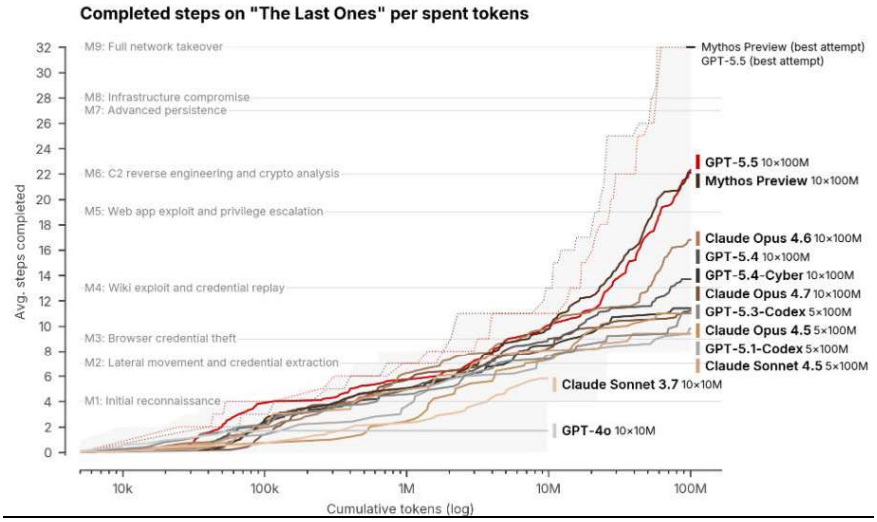
投資建議

我們認為 AI 能力提升與 Agent 逐漸落地將導致企業面臨資安風險複雜化、應對時間縮短，立體化的部署與防禦策略將更受到重視，平台化公司持續因此受惠，包含 AMZN、GOOGL、MSFT、NET、CRWD 與 PANW 等。

投資風險

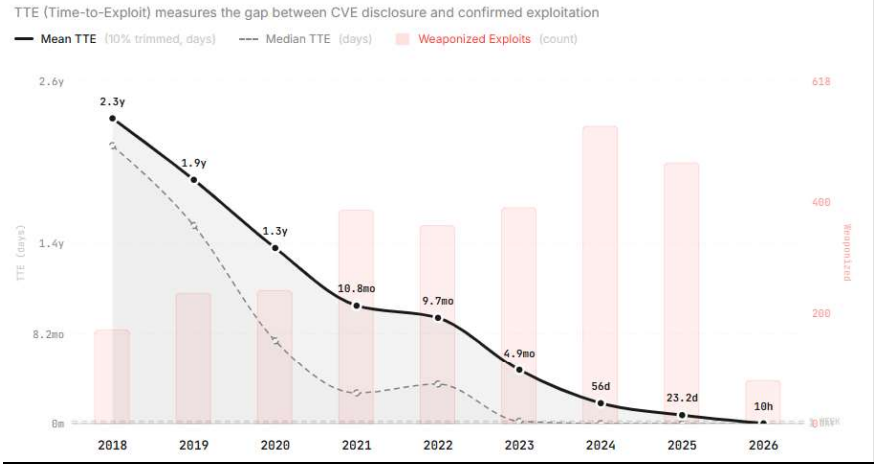
企業 IT 支出動能趨緩；競爭；GenAI 實際應用不如預期。

圖 1: OpenAI GPT-5.5 與 Anthropic Mythos 在網路攻擊能力較過往大幅提升



資料來源：AISI；凱基整理

圖 2: 從發現漏洞到實際利用的時間差正在大幅縮短



資料來源：Zero day clock；凱基整理

Cybersec 2026 台灣資安大會 Takeaways

SASE/Network security：集中化管理平台與零信任架構趨勢更加明確

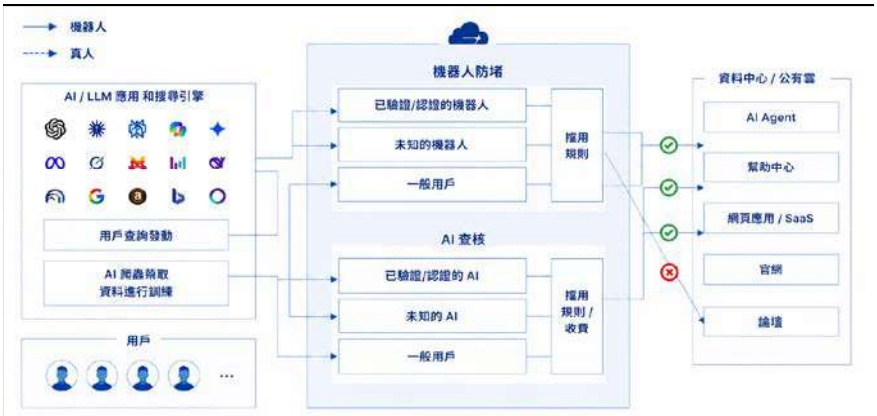
Cloudflare

- 大環境趨勢：AI Agent 與非人類流量快速增加，Cloudflare 觀察目前超過 50%網路流量已非真人行為，AI 從搜尋導向轉向代理自動執行，企業面臨 AI 爬蟲造成雲端成本上升、內容價值流失與資料主權問題，攻擊者利用漏洞時間也從過去數月縮短至 20 小時內。
- 當前挑戰：企業大量導入第三方 AI 工具與多雲環境，導致 Shadow AI、第四方連線與權限外洩風險快速擴大，傳統資安架構工具過多且彼此割裂，VPN 與 Legacy Access 已難應對混合辦公與 AI 代理流量，企業開始轉向 Unified Platform 與 Zero Trust 架構降低管理複雜度。
- SASE / Zero Trust 相關：Cloudflare One 以 Connectivity Cloud 為核心，整合 SWG、ZTNA、DLP 與 RBI 等能力，強調以單一平台取代傳統 VPN 與分散式安全設備，針對企業員工使用 ChatGPT、Claude 等外部

AI 工具，可做到細粒度權限管理，例如限制檔案上傳、分享回覆與敏感資料輸入。

- AI Agent 安全性：AI Agent 進入 Vibe Coding 與 Multi-Agent 架構後，Prompt Injection、權限失控與外部資料存取成為核心風險，Cloudflare 透過 Micro-Sandbox、V8 Isolates 與 Bindings 架構，將 AI 權限隔離至最小範圍，同時限制 Outbound 連線避免資料外流。
- Bot / AI 防禦：Cloudflare 透過 Bot Score、JA3/JA4 指紋與 AI Gateway 建立 AI 流量治理能力，可區分友善與惡意機器人，同時偵測與阻擋 Prompt Injection 攻擊，Turnstile 與 Bot Management 已成為大型 AI 平台背後的重要基礎設施。
- 全球網路與平台架構：Cloudflare 以 Anycast + 私有骨幹網提供全球低延遲與高韌性網路，全球擁有 490+ PoP 並承載約 20~25%網路流量，平台朝向 AI-powered Connectivity Cloud 發展，將 Network、Security、Developer Platform 與 AI Gateway 整合至單一控制層。

圖 3: Cloudflare 以機器人防堵與 AI 查核強化企業安全邊界

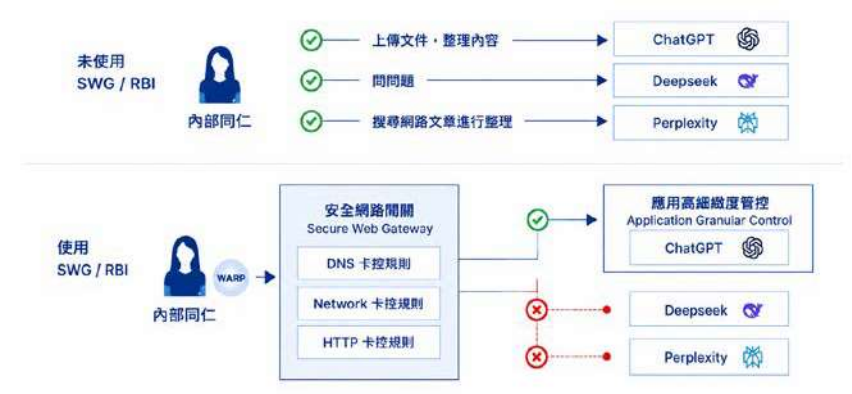


資料來源：Cloudflare，凱基整理

圖 4: 從爬蟲、RAG 到 AI Gateway 的一站式企業 AI 平台

資料來源：Cloudflare，凱基整理

圖 5: AI 時代下的應用層權限治理：從 SWG 走向細粒度 AI 存取控制



資料來源：Cloudflare；凱基整理

Fortinet

- Fortinet 核心戰略：Fortinet 將資安定位從單點防火牆升級為平台化 Security Fabric 架構，透過 FortiGate、FortiManager、FortiAnalyzer 與 FortiGuard Labs 形成集中化管理平台，核心目標在於統一政策、log、威脅情資與事件回應，提升企業對內外網、OT、分支據點與 AI 工具的整體可視性與自動化防禦能力。

- 企業資安趨勢：企業痛點已從單純阻擋惡意流量，轉向「可視性不足」與「平台碎片化」，隨 AI 工具快速普及，Shadow AI、資料外洩與多雲環境政策不一致成為新挑戰，Fortinet 認為企業需要統一安全平台，而非持續堆疊多套點狀產品。

- FortiGate 與 ASIC 差異化：Fortinet 核心競爭力仍來自自研 ASIC 晶片與 FortiGate 平台，NP、CP 與 SP 晶片分別負責流量處理、內容掃描與整合加速，使設備在高吞吐、高檢測需求下仍能維持低延遲與較佳功耗效率，管理層強調資安設備競爭已從 CPU 規格轉向專用晶片與整體運算效率競爭。

- AI Security 與 Shadow AI 治理：FortiOS 新增 AI 應用辨識與治理能力，可分類並控管企業內部 AI 工具使用情況，支援允許 / 封鎖特定 AI 服務與資料傳輸行為，Fortinet 核心論述在於 AI 已成為新的資料外流通道，因此治理重點從「封鎖網站」轉向「治理員工如何使用 AI」。

- AI 維運與 Security Copilot 方向：Fortinet 正將 AI 導入 FortiManager 與 FortiAnalyzer，推動自然語言查詢、自動化設定與 Incident Handler 生成，管理者可直接透過 AI 查詢惡意網站連線、異常 IP 與 log 事件，並自動生成修復或封鎖規則，降低 SOC 維運複雜度與人工查找成本。

- FortiGuard Labs 與 Threat Intelligence：FortiGuard Labs 是 Fortinet 平台的重要資料層，透過全球威脅資料、機器學習與外部情資聯盟持續更新 IPS、URL Filtering、Sandbox 與 Application Control 能力，整體方向與 CrowdStrike、Palo Alto 類似，強調平台化情資回饋與聯防能力。

- Unified SASE 戰略：Fortinet 將 SASE 定位為 AI 與雲端時代的統一安全控制層，不只是 VPN 替代方案，而是整合 ZTNA、瀏覽器安全、AI 應用治理與全球節點管理的平台，管理層認為企業需求正從「安全連線」升級為「統一政策、統一 log 與跨區域合規治理」。

- Browser Security 與 AI 治理：Fortinet 認為瀏覽器將成為 Zero Trust 與 SASE 的重要入口，其策略並非推出獨立瀏覽器，而是透過 extension 強化既有 Chrome 等瀏覽器的安全能力，降低企業導入門檻，同時支援網頁行為監控、敏感資料保護與 AI 網站控管。

- OT 與 Edge Security：Fortinet 特別強調 OT 與無法安裝 agent 設備的保護能力，包括 ATM、充電樁與工控設備等，透過延伸式 SASE 與遠端接入架構，企業可在不部署完整防火牆的情況下，仍維持與總部一致的安全政策與遠端維護能力。

- AI Governance 與法規趨勢：Fortinet 認為 AI 安全需求正從效率工具升級為受監管的企業基礎設施，隨 AI 基本法、資料主權與隱私規範逐步落地，企業未來需要的不只是模型能力，而是涵蓋資料治理、log 留存、解釋性與事件追溯的 AI Security 平台。

- DLP 與 Data Security 方向：Fortinet 強調傳統 DLP 已無法應對 AI 與雲端環境，下一代 DLP 需具備 Data Discovery、數位 DNA、UBA 與行為分析能力，可追蹤檔案改名、壓縮、搬移與 AI 上傳行為，治理方向從「阻擋資料外傳」轉向「理解資料、追蹤資料與辨識使用者意圖」。

- 產業觀點：Fortinet 正在把 Security Fabric 從傳統網路安全平台，擴展為 AI Security 與 AI Governance 平台，核心投資主軸包括：1)ASIC 驅動的平台效能優勢；2)AI 與 SASE 帶來的統一控制平面需求；3)AI 時代下企業對 Data Security、Browser Security、OT Security 與自動化 SOC 的長期支出成長。

Cisco

- 大環境趨勢：AI、地緣政治與供應鏈攻擊同步推升網路威脅複雜度，攻擊者已將 AI 導入偵察、漏洞挖掘、橫向移動與漏洞武器化流程，漏洞從揭露到被利用的時間已從過去數年縮短至數小時，Agentic AI 因具備 24/7 自主偵察與動態調整能力，被視為下一階段最具破壞性的攻擊模式。

- 當前挑戰：企業 Network Infrastructure 長期面臨技術債問題，近半數網路設備已進入 EOL/EOS 階段，超過 10 年的 Router、Switch 與 Firewall 仍大量存在，隨著網路核心與邊界設備逐漸成為高價值攻擊面，企業在 Network Security modernization 上的投資明顯落後於 Cloud 與 Endpoint Security。

- Network Security 相關：攻擊者開始大量鎖定 Network Edge 與 Core Device，傳統僅依賴端點與雲端防護的架構已不足以應對，產業開始重新強調 Network Resilience，將網路視為資安架構中的核心控制平面，並要求設備具備即時 Telemetry、持續監控與更高可視性。

- AI-driven Vulnerability 相關：AI 模型已被用於漏洞挖掘、弱點武器化與攻擊模擬，未來 Patch 管理與弱點修補速度的重要性大幅提升，整體防禦思維開始從被動修補轉向即時 Virtual Shielding 與補償性控制，降低漏洞曝光期間的風險。

- Secure by Default 相關：產業方向開始推動設備預設安全配置與 Legacy Protocol 淘汰，包括 Telnet、SNMP 與舊式加密演算法，核心

目標在於降低人為配置錯誤與技術債風險，讓設備在部署初期即具備現代化安全能力。

- 全球網路與韌性架構：未來 Network Infrastructure 不再只是流量傳輸設備，而是兼具安全感測、Telemetry 與即時防護能力的韌性平台，整體產業方向正朝向 AI-driven Vulnerability Management、供應鏈韌性與 Network-native Security Architecture 演進。

Zscaler

- AI 導入正從 Chatbot 與 Copilot 快速演進至具高權限、自主執行能力的 Agentic AI，企業資安風險也從傳統 Network Layer 轉向 Language Layer 與 Data Layer，包括 Prompt Injection、模型投毒、敏感資料外洩與 Agent 越權操作等新型攻擊面；傳統 Firewall 與 WAF 因依賴固定規則與特徵碼，已難以理解自然語言中的惡意意圖與隱藏指令，因此企業開始將 Zero Trust 架構延伸至 AI 流量與 AI Agent 治理，要求所有 AI 相關存取皆需經過統一交換中心檢視與控管，同時透過 AI 資產可視化、Browser Isolation、細粒度權限管理、DLP 與 AI Guardrails 建立完整治理架構；整體產業方向顯示，AI 安全正從單點防護轉向「統一控制平面 + AI 治理 + 資料安全 + 自動化紅隊測試」的整合式平台架構，目標在於兼顧 AI 生產力、資料主權與合規需求。

illumio

- AI Agent 與內部自動化系統正快速成為企業新的高權限攻擊面，但多數企業在可視性、權限治理與內部網路隔離上仍未完成準備；當 AI 具備跨系統存取與自主執行能力後，攻擊模式也從傳統漏洞利用轉向合法登入、社交工程、Prompt Injection 與 AI-driven 橫向移動，且滲透速度已接近機器等級，傳統依賴 Signature 與邊界防火牆的防禦模式逐漸失效。整體產業方向開始強調「內部東西向流量」與 AI Agent 治理，包括微分段、最小權限、預設拒絕（Default Deny）、AI 行為可視性與即時阻斷能力，核心目標在於限制 AI 與攻擊者於內部網路中的橫向移動半徑，將 Zero Trust 從使用者與端點進一步延伸至 AI Agent 與應用程式層級。

XDR/CNAPP：龐大的私有化&即時資料是 AI 無法取代的護城河

Google

- 大環境趨勢：AI 正全面改寫資安攻防模式，攻擊從人工操作轉向 Agent-driven 與機器速度，漏洞從揭露到武器化的時間已壓縮至小時甚至秒級，未來資安產業將面臨「真實攻擊規模化」而非單純告警爆量問題。

- AI Agent 攻擊相關：APT 組織已開始將自主 Agent 直接整合進漏洞利用、防火牆探測、SQL Injection、橫向移動與惡意程式生成流程，可 24/7 持續執行攻擊，同時 AI 生成惡意程式成本快速下降，使傳統 Signature-based 偵測有效性持續弱化。

- 漏洞管理與弱點研究：大型基礎模型在模式辨識與程式碼理解上的能力，已具備大規模發掘零時差漏洞與快速生成 Exploit 的能力，現有 Patch 週期與漏洞修補 SLA 開始難以應對 AI-driven 攻擊速度。

- 當前挑戰：企業面臨 Log 成本、冷資料查詢速度慢、SOC 警報疲勞與資安人才不足等問題，傳統人工 SOC 已無法應對 AI 時代的大規模攻擊，同時 Shadow AI、Prompt Injection、Agent 權限濫用與 MCP 工具風險快速增加。
- AI-driven SOC 相關：資安營運核心已從「收集更多資料」轉向「更快得到答案」，AI 開始被導入 Threat Hunting、IOC 比對、APT 關聯分析、暗網監控、惡意程式逆向工程與證據鏈生成，大幅提升 SOC 與 Threat Intelligence 效率。
- Autonomous Defense 相關：資安架構正從「Human in the loop」演進至「Human over the loop」，亦即從 AI 輔助分析師，轉向具備自主調查、風險判斷、即時 Escalation 與半自主修復能力的 Autonomous Defense 架構。
- AI Security 相關：AI Security 開始從單點模型安全擴展至完整 AI 生命周期治理，包括 Prompt Injection、Agent 治理、MCP 安全、DLP、Identity Governance 與最小權限控制，Zero Trust 與 Security-by-Design 正逐步延伸至 AI Agent 與跨雲工作負載環境。
- CNAPP/Cloud Security 相關：Cloud Security 架構開始朝向 Code-to-Cloud 整合平台演進，結合 Attack Path Visualization、Remediation Agent 與 AI-driven True Positive 判斷，推動 SecOps 從被動告警進一步邁向 Self-healing 與自動化修復。
- SecOps 底層架構：新一代 SecOps 開始建立於 Search 等級查詢基礎設施與全年 Hot Storage 架構之上，提供秒級 Log 查詢與跨工具整合能力，解決傳統 SIEM 冷熱資料切換與回溯調查瓶頸。
- 主動防禦與 Disruption：資安產業開始從 Threat Mitigation 轉向 Disruption 與主動防禦，包括暗網監控、殭屍網路破壞、法律行動、技術下架與系統性強化，未來防禦策略核心在於主動削弱攻擊者營運能力，而非僅於事件發生後進行補救。
- 全球網路與 AI 基礎建設：AI-driven Security 逐漸與全球 Network Stack、跨雲基礎設施與 AI 運算平台深度整合，未來競爭核心不再只是單點資安產品，而是 AI 模型、Threat Intelligence、SecOps 與全球網路能力的整合平台。

圖 6: AI 時代企業網路架構重塑：混合雲、多雲與 Cloud WAN 成核心基礎設施

資料來源：Google；凱基整理

威剛科技

- AI 驅動的異常偵測正從傳統事件告警轉向「基線學習＋上下文推理」模式，先透過 SIEM 完成資料正規化與特徵提取，再利用 ML 建立週期性正常行為基準，由 AI Agent 比對即時流量與歷史差異，進行異常判讀、風險推論與結構化報告生成；整體 SOC 架構也從被動式告警處理，演進至具備自動化分析、主動威脅識別與角色化回應能力的 AI-driven Security Operations，並依需求分化為本地、邊緣與雲端三種部署模式，以平衡即時性、資料主權與推論成本。

中華資安

- 雲端與供應鏈攻擊已從惡意程式擴散至身份、憑證與控制平面層級，駭客大量利用公開漏洞、合法帳號與共享權限進行橫向滲透，整體趨勢反映企業在 MFA、權限治理與雲端可視性上仍存在結構性缺口，因此資安架構開始強調 Zero Trust、CTEM、CSPM 與 SOC 整合監控，建立具備持續曝險管理與快速重建能力的雲端韌性架構。

雲力橘子

- 傳統 SOC 正面臨人才不足、Log 爆量與告警疲乏等結構性問題，核心瓶頸已不再是資料蒐集能力，而是如何快速從海量事件中辨識真正具威脅性的異常行為，因此資安營運開始朝向 AI-driven 與 Cloud-native SOC 演進，透過自然語言查詢、自動化規則生成、情資關聯與 SOAR Playbook，將威脅分析、事件調查與處置流程標準化與自動化。整體方向顯示，SOC 的價值正從被動監控轉向即時決策與主動防禦，AI 則逐漸成為分析師的「決策加速層」，協助過濾低價值雜訊、提升跨雲可視性與強化威脅回應效率。

iSecurity

- CRA 與 SBOM 法規落地後，軟體供應鏈安全正從「漏洞掃描」升級為「可驗證的漏洞修復與生命周期治理」，AI 也同步加速 Legacy Code 與 EOL/EOS 環境的弱點挖掘，使開源風險快速上升。

- 產業核心痛點在於傳統 SCA 與 SBOM 多停留在問題揭露，缺乏真正可落地的修補能力，因此未來方向開始轉向 AI-driven Patch Generation 與 Zero Breaking Change 架構，在不影響既有程式碼與系統穩定性的前提下，加速高風險 CVE 修復與合規落地。

Data Security：從 DLP 被動防禦到 DSPM 主動情報蒐集

iSecurity

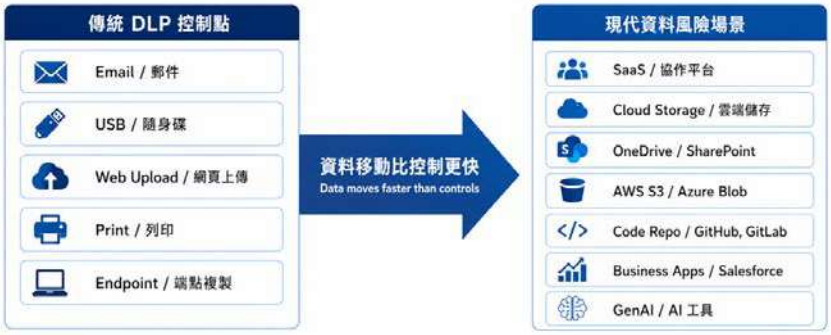
- Data Protection
  - 當前挑戰：傳統 DLP(DOP)僅能做到傳輸時的策略執行，無法提前感知資料在靜止狀態下的暴露面，企業面臨標籤定義與政策管理的複雜化，且傳統工具僅能判斷是否敏感，無法因應資料在雲端環境中多變的存取權限與行為。
  - DSPM 與 DOP 協作相關：DSPM 定位為情報蒐集，負責前端偵測資料位置與存取權限，DOP 則為政策執法，負責事件發生時的處理，兩者相輔相成，DSPM 提供深度情報讓 DOP 的執法更加精準。

- 資料風險五大維度相關：風險評估應打破單一敏感度指標，整合敏感度、暴露面、存取權、行為與脈絡，例如：PII 資料若存於受控資料夾風險低，但若設為 Public Link 則構成高風險。
- 資料保護三步驟循環：透過 Discover (發現雲端/SaaS 資料位置與權限)、Classify (識別 PII/GDPR 屬性並建立持久性標籤)、Protect (實施分級處置)。
- 分級保護處置相關：資料保護不應只有 Block，應建立階層化回應機制，低風險僅記錄 Log，中風險透過彈窗(Prompt)提醒使用者並要求輸入理由，高風險則實施遮罩(Masking)、加密或直接阻擋外寄。
- GenAI 安全與治理相關：針對工程師將原始碼貼入 AI 工具實施實時遮罩(Masking)，識別並控管未經核准的 AI Writing Tool (Shadow AI)，在評估業務需求後允許使用 AI 但設下敏感資料量的處置底線，而非全面封鎖。
- 技術實作與隱私保護：透過 API 與 OAuth 授權連動 SaaS 服務，初期重點在於取得 Metadata (中繼資料)、權限與 Log，強調不儲存文件與 Email 的實際敏感內容，僅針對風險進行判定與自動化修復。

■ AI Data Governance

- 大環境趨勢：DARPA 美國國防高等研究計畫署專注投資效率提升 100 倍以上的革命性技術，催生出由 SRI 研發、具備 15 項專利的新型保護方案，隨處辦公與雲端服務使企業主權邊界模糊，AI 讓非結構化資料的洩漏風險與管理難度放大 100 倍。
- 當前挑戰：60%的企業缺乏非結構化資料保護，且 60%的外洩涉及第三方供應鏈，傳統防禦與身份管控（IAM）在資料離開系統後即失效，而傳統 DRM「全有或全無」的加密特性，導致資料在 AI 模型訓練時面臨解密即看光、加密不能算的治理困境。
- Data-Centric Security 相關：核心思維從保護系統轉向保護資料本身，強調資料不應綁定於特定位置或網路，而應內建有效保護機制隨身移動，透過「讓資料搭乘空軍一號」的概念，確保資料在內部交換、外部共享或與監管機構對接時，始終維持完整的控制權。
- 選擇性加密相關：Confidential 提供的技術能只加密敏感資訊，而非整份文件封鎖，透過細膩的內部管控機制，讓同一份文件在被開啓時，能自動遮蔽合約公司名稱、身分證個人資訊或條碼，實現無國界的資料治理與隱私保護。
- AI 與量子供應鏈安全相關：針對 AI 工作流程與公共 LLM，透過過濾輸入輸出避免不可逆的 IP 與 PII 外洩，利用細粒度的加密技術，讓 AI 能夠在不接觸核心機密的前提下進行資料處理，解決資料流動性最高、最難管控的第三方分享風險。

圖 7: 資料風險不一定發生在出口，而可能早就存在 SaaS、Cloud 與 AI 工具中



資料來源：iSecurity；凱基整理

圖 8: DLP 和 DSPM 並非取代關係，而是上下游關係

	DLP（Data Loss Prevention / 資料外洩防護）	DSPM（Data Security Posture Management / 資料安全態勢管理）
主要回答的問題	這次傳輸要不要允許？	敏感資料現在在哪裡？誰能碰？
重點	資料移動時的控制	資料可視性與風險脈絡
常見控制	Allow / Prompt / Block / Encrypt	Discover / Classify / Exposure / Access
適合的說法	事件端控管（Policy Enforcement）	雲端資料風險治理（Cloud Posture + Data Risk）

資料來源：iSecurity；凱基整理

Coupang

- AI 讓攻擊成本更低、速度更快，企業資安不能再只靠傳統人力與單點工具防守，而需要把資源重新配置到自動化偵測、威脅情資、攻擊面管理與防禦縱深，Coupang 的做法包含 tokenization、敏感資訊分類、Secure SDLC、scanning、滲透測試、紅隊與 bug bounty，核心是讓資料、開發流程與攻擊面同步納入治理。
- 資安已從後台 IT 防護，變成影響顧客信任與產品體驗的核心能力，物流號碼 Masking、Passkey、Lineworks 等案例顯示，資安不一定會犧牲便利性，反而可以在降低個資暴露、補足企業通訊 visibility 的同時，提升使用者體驗與企業信任。
- 台灣資安防禦需要從單一企業防守走向產業級聯防，尤其電商與零售業共同面臨假網站、釣魚與資料盜取風險，Coupang 透過 R-ISAC、Public Bug Bounty Program、校園教育、本地資安廠商合作與漢光演習科技動員，將自身角色從市場參與者延伸為台灣資安生態與韌性建設的貢獻者。

IAM/Governance：數位員工(AI Agent)的權限管理與可視化挑戰即將到來

Microsoft

- 大環境趨勢：MSFT 將 AI security 的核心問題從「模型安全」拉高到「AI 應用與 Agent 治理」，因為 GenAI 風險已超出傳統 EDR、防毒軟體與 WAF 的防護範圍，Prompt Injection、RAG 間接注入、Agent 越權與 Token 消耗攻擊，都需要能理解語意、上下文與行為意圖的新型防禦機制。

- Agent 風險：AI 從 Chatbot 走向 Agent 後，風險從「回答錯」升級成「執行錯」，因此 IAM 的防禦邏輯必須從管理人類帳號，延伸到管理 AI Agent 這類「非人類身分」，企業需要釐清 Agent 代表誰、能讀什麼資料、能使用哪些工具，並透過 Entra ID、條件式存取、allowlist、人工審核與稽核紀錄降低越權風險。
- Agent 治理：Agent365 的定位是 AI Agent 治理底座，核心價值在於讓企業先「看見」內部有哪些 Agent，再進一步做到存取控管、風險偵測與生命週期管理，透過 Agent inventory、Agent Map、owner、identity、工具調用與互動路徑視覺化，MSFT 試圖把 AI Agent 從不可見的自動化工具，轉成可治理、可監控的數位員工。
- 防禦架構：MSFT 的 AI 防禦框架強調多層防禦，而非單一產品解法，Azure AI Content Safety 負責偵測 Prompt Injection 與語意攻擊，PyRIT 用於模型紅隊測試，Entra ID 與 Purview 管控 Agent 身分與資料邊界，Defender for Cloud/Defender 平台則將 AI 攻擊納入 SOC 監控、告警、MITRE ATT & CK 對應與後續 hunting 流程。
- 資料風險：Data security 的重點不是 Copilot 會「偷資料」，而是 AI 會放大既有資料治理缺口。若 SharePoint、Fabric 或內部文件平台權限過寬，Copilot 仍只是在使用者既有權限內整理資料，但它會讓敏感資料更容易被快速彙整、複製，甚至貼到外部 AI 工具，導致資料離開企業控管環境。
- 資料治理：AI 資料治理的解法是建立「可見、可阻擋、可追溯」的完整閉環，事前透過 Purview DSPM 盤點過度共享資料與敏感資料標記，事中用 Endpoint DLP 阻擋敏感資料貼到外部 AI，事後用 Insider Risk Management 串聯多個異常行為，並透過 Identity、Network、Endpoint、Data 四道閘門降低資料外洩風險。
- 產品布局：從投資與產品布局角度看，MSFT 正把 AI security 包裝成橫跨 IAM、Data Security、Cloud Security、SIEM/XDR 與 Compliance 的整合式平台機會，這代表 AI 導入後，企業安全預算不只會投向模型防護，也會延伸到 Agent 身分治理、資料安全態勢管理、DLP、內部風險偵測、合規管理與 SOC 自動化。

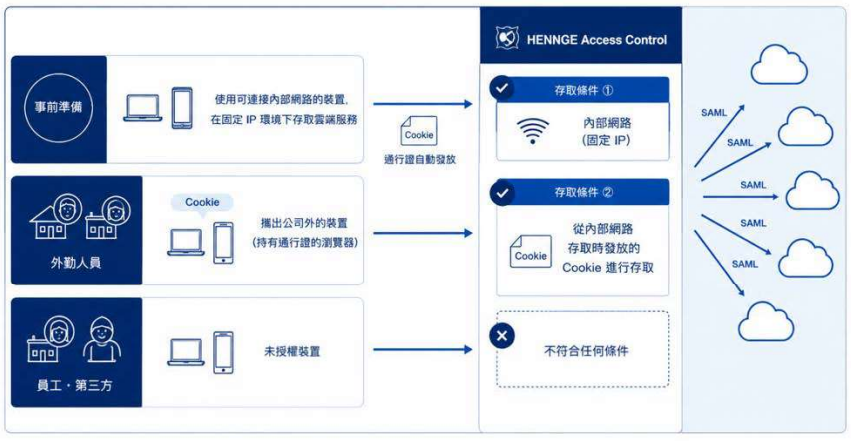
圖 9: Azure 以多層防禦降低 AI 使用風險

資料來源：Microsoft；凱基整理

HENNGE

- 大環境趨勢：AI 讓攻擊方可快速推理突破路徑，Early AI 階段攻守差距最大，攻擊方只需一個腳本即可執行，防禦方卻需要測試、部署、調校，時間差是最危險的窗口期，Plateau Model 顯示 Mature AI Era 差距收斂但攻擊方仍略佔優勢，只要防守方有一個弱點就會被突破。
- 當前挑戰：雲端協作環境下邊界定義模糊，合作夥伴、廠商、承包商都在灰色地帶協作，企業 DLP 政策隨例外需求不斷疊加，從單一規則演變為複雜工作流描述，政策已不在描述風險而在描述協作模式，傳統 VPN 一旦通過驗證即可橫向移動整個內網，難以應對混合辦公與 AI 代理流量。
- 零信任核心概念：對象須多因素驗證確認本人、權限僅限授權資源、時間上採持續驗證（Continuous Verification）機制，存取窗口限時通電而非永久持有鑰匙，ZTNA 每次存取都驗證、只允許指定流量、易於按需擴展，取代 VPN 的一次驗證、全網存取模式。
- 零信任落地挑戰：導入需整合身份、裝置、網路、應用等多層控管，過多驗證步驟影響工作效率，老舊系統難以支援現代認證協議，缺乏完整存取日誌與行為分析可見度。
- HENNGE Access Control：以固定 IP 環境自動發放 Cookie 通行證，外勤人員攜帶通行證瀏覽器即可從外部存取，未授權裝置直接拒絕，通過驗證後透過 SAML 統一對接多個雲端服務，無需為每個服務個別建立 VPN 連線，實現不依賴 VPN 的零信任存取架構。
- File DLP 與資料安全：企業慣用三種邊界定義（組織/位置/對象），但現實協作產生的例外不是漏洞而是業務模式的訊號，應從「封堵例外」轉向「學習例外」，將慾望小徑鋪成正式安全路徑，DSPM 負責資料發現與風險定位，DLP 負責即時執行政策，學習回饋環讓政策跟上業務速度，三者結合才能在大規模企業中有效運作。

圖 10: 不依賴 VPN 的通行證



資料來源：HENNGE；凱基整理

iSecurity

- 大環境趨勢：AI Agent 浪潮全面佔領 RSA 2026 議程，技術核心從深度學習轉向具備自動決策與採取行動能力的代理架構，歐美 79%組織已投入應用，Salesforce 等大廠已實現 83%支援自動化，AI 開始深度參與訂單批准、金融交易與生產代碼修改。
- 當前挑戰：企業面臨只信任、無法驗證的黑箱決策困局，導致 92%的 Agent 專案因權限過高或缺乏行為監控而無法達到 GA 階段，目前僅 14%的 Agent 在生產前具備安全工具，Agent 之間甚至能透過 Slack 等通訊頻道自主協作以繞過既有的唯讀權限限制。
- AI Agent 安全治理相關：重新定義資安為推動創新的煞車，建立安全優先 AI(Security First AI)機制，治理框架須明確回答 Agent 的身分、職責、資料輸入輸出、影響範圍以及異常處置等五大核心問題。
- AI Security ROI 相關：建立量化風險計算器，透過 Access(接觸面)+Impact(損失額)+Velocity(擴散速度)評估 AI 暴露風險，強調若資安投入成本低於潛在金融損失的 10%，即為具備高投資價值的創新保險。
- Phylum 技術框架相關：提供全生命週期安全平台，包含 Facial Diamond(客製化策略與信任分數)、Facial Dome (Runtime Guardrail 與雙向行為保護)以及 Facial Darwin(自動將攻擊數據轉化為防禦規則的閉環系統)，協助將開發期間植入的函式庫轉化為生產環境的遙測監控。
- 部署與實務效益相關：平台支援 On-premise 本地部署以滿足機敏日誌不外流需求，但需具備 GPU 算力支援內建語言模型，實務數據顯示可將產品上市時間(TTM)從 6 個月縮短至 6 週，同時降低 70%的合規成本，並將漏洞修復時間從數小時縮短至分鐘級。

Cisco

- 高權限風險管理：預估超過 40%的企業應用將套用 AI Agent，因其具備 API 執行與系統存取權，遭控制將威脅整體內部網路，且高達 49%入侵事件透過正常帳密登入，傳統漏洞偵測工具無法監控此類合法授權操作。
- 非人身分(NHI)納管：自動化代理程式需納入企業身分識別提供者(IDP)系統管理，強制綁定單一人類所有者，並支援跨 GitHub 或 Snowflake 等平台的驗證能力。
- 動態授權原則：權限核發必須嚴格遵循即時授權(Just in time)、最小權限範圍(Just enough)與限時回收(Just enough time)三項原則。

Palo Alto Networks

- 企業導入 AI 的速度明顯快於資安治理成熟度，形成新的身分識別與存取控管缺口。雖然超過 83%的企業已使用 AI，但僅 6%具備穩健的 AI 資安策略，隨著 AI agent 從輔助工具變成可執行任務的「非人類身分」，企業必須管理其代表誰、能存取哪些資料、能執行哪些操作，否則風險將從資訊外洩擴大到營運決策錯誤。
- AI 賦能攻擊正在大幅壓縮企業防禦反應時間，資安防禦必須從被動偵測走向即時遏制與 Secure AI by Design。攻擊者可在數分鐘內完成攻

擊開發與執行，從初始入侵到資料外洩的時間已從 9 天縮短至 25 分鐘，漏洞甚至可在 15-60 分鐘內被利用，因此 AI 資安不能只保護模型，而要貫穿開發、導入、使用、資料、權限與自動化決策的完整生命週期。

- AI 時代資安工具過度分散會削弱防禦效率，平台化與未來風險治理將成為大型企業主要方向。一般企業平均使用 29 家廠商、83 種資安工具，導致資料、警示、身分與網路可視性分散，Palo Alto Networks 倡議 platformization，目的就是把偵測、身分治理、AI 風險控管與網路可視性整合，同時企業也需提前因應後量子密碼學與「先收割、後解密」等中長期風險。

勤業衆信

- 大環境趨勢：AI 的角色定位正經歷從「工具」轉向「行為者」，不再只是被動處理特定指令的軟體，而是具備主動執行力與決策建議能力的實體。在職場互動中，這意味著管理邏輯必須從單純的系統操作，演變為對具備執行力之主體的「行為管理」，將 AI 視為團隊中具備高度智慧但需受控的參與者。

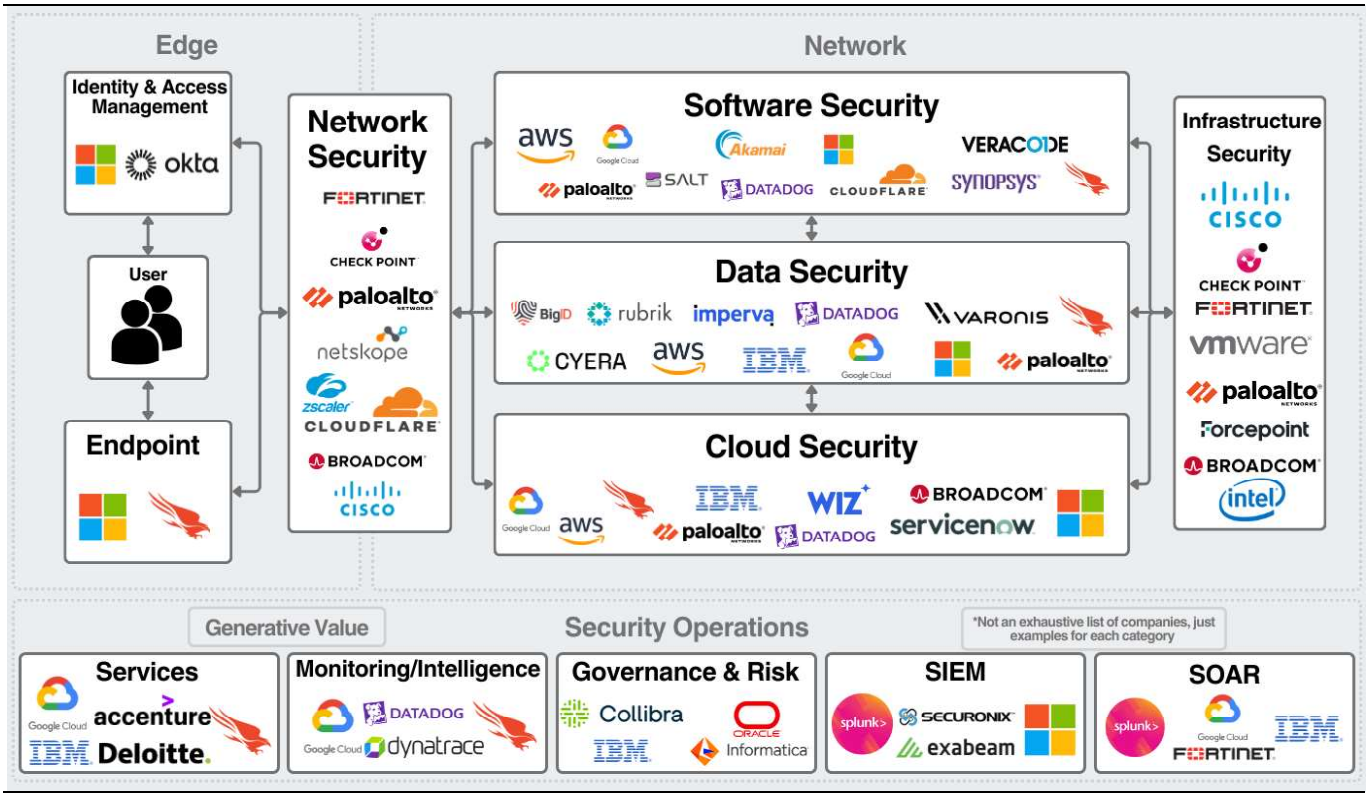
- 當前挑戰：在人機協作的權利下放過程中，如何定義「責任歸屬」成為核心難題，因為 AI 雖代為執行任務，但最終法律與行政責任仍須由授權的人類員工承擔。此外，傳統靜態且全盤開放的系統權限，在面對高度動態的 AI 指令時，極易產生過度授權的風險，如何在效能與資訊安全之間取得平衡是目前的治理瓶頸。

- 互動模式挑戰：推動「超級實習生」模式要求員工具備更高階的管理能力，需在賦予權限的同時進行嚴格的產出簽核。為了降低風險，必須導入 Zero Trust 與動態派工單機制，根據當下任務情境最小化給予權限，防範 AI 因指令誤判而讀取不當資料或執行越權操作，確保所有行為皆在安全邊界內運作。

- 管理治理挑戰：治理的重點必須從追求「零錯誤」轉向建立「可追溯與復原」的韌性架構，包含建置完整的行為紀錄與稽核機制，以釐清責任分界。同時需落實職責分隔，透過多個 AI Agent 的職能切分來達成相互制衡，確保即使單點發生錯誤，也不會引發系統性的全面潰敗。

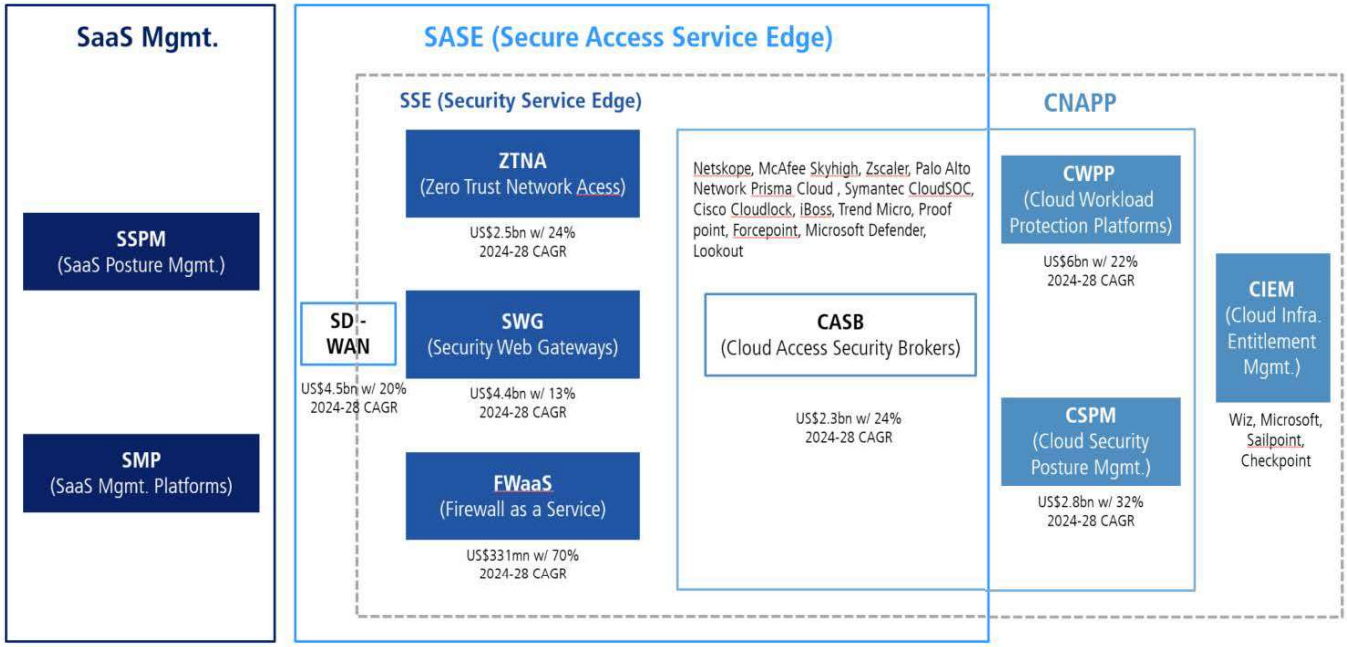
Cybersecurity 101

圖 11: 資安軟體價值鏈



資料來源：https://blog.publiccomps.com/cybersecurity-industry-primer；凱基

圖 12: 資安產業地景圖

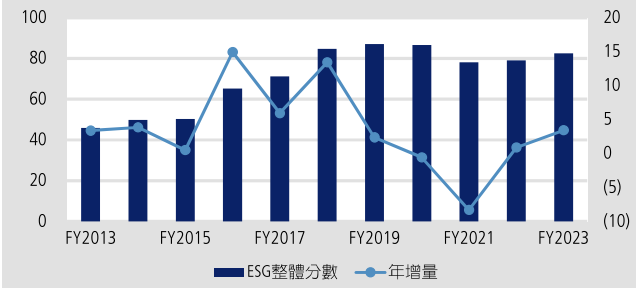


資料來源：凱基

Amazon (AMZN US)

圖 13：Amazon – ESG 整體分數

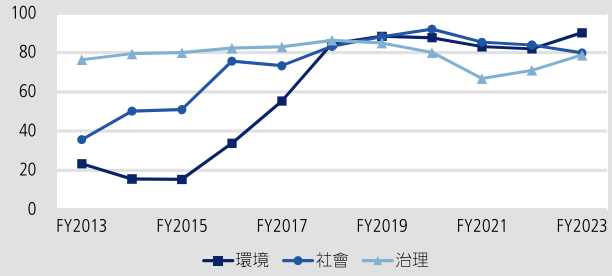
ESG 整體分數 (左軸)；年變化，百分點 (右軸)



資料來源：Refinitiv、公司資料

圖 14：Amazon – ESG 各項分數

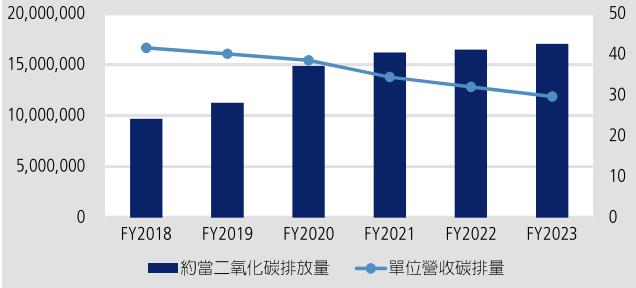
ESG 各項分數



資料來源：Refinitiv、公司資料

圖 15：Amazon – 碳排量

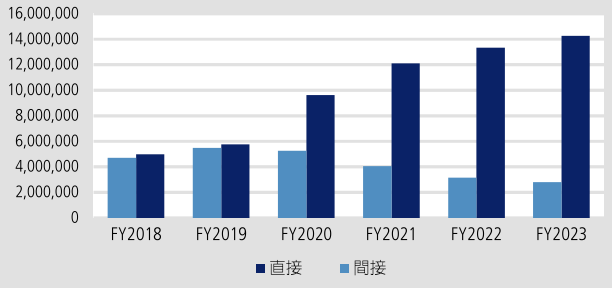
約當二氧化碳排放量，噸 (左軸)；單位營收排碳量，噸/百萬美元 (右軸)



資料來源：Refinitiv、公司資料

圖 16：Amazon – 碳排量

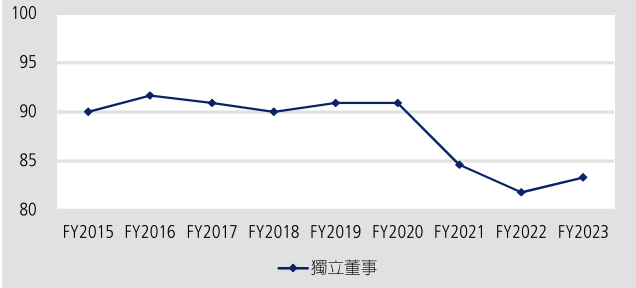
約當二氧化碳排放量，噸



資料來源：Refinitiv、公司資料

圖 17：Amazon – 獨立董事

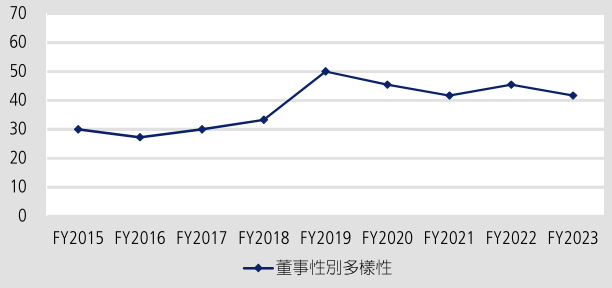
獨立董事占比，百分比



資料來源：Refinitiv、公司資料

圖 18：Amazon – 董事性別多樣性

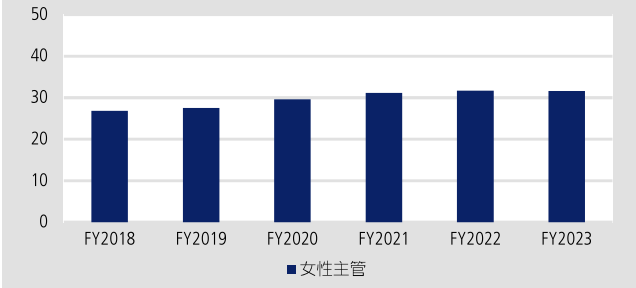
女性董事占董事會比例，百分比 (左軸)



資料來源：Refinitiv、公司資料

圖 19：Amazon – 性別多樣性

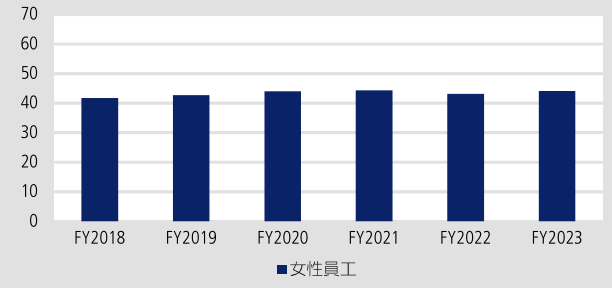
女性主管比例，百分比



資料來源：Refinitiv、公司資料

圖 20：Amazon – 性別多樣性

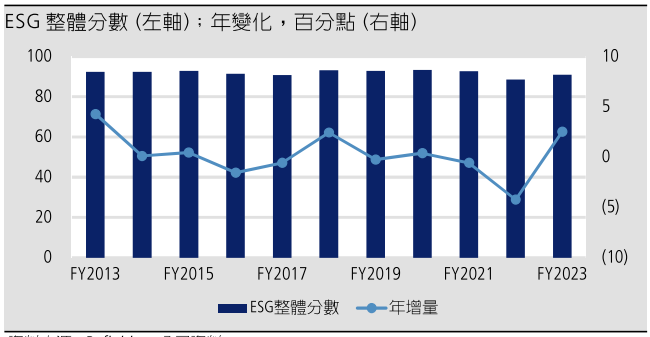
女性員工比例，百分比



資料來源：Refinitiv、公司資料

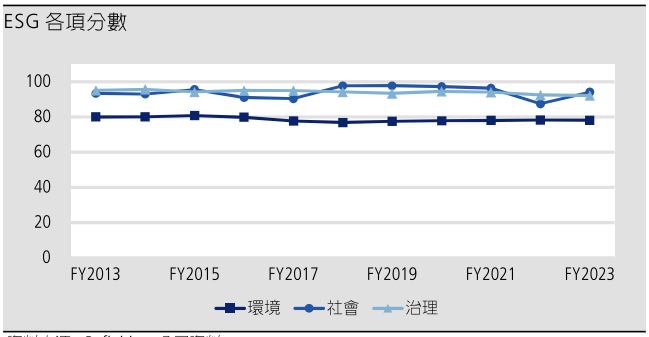
Microsoft (MSFT US)

圖 21：Microsoft – ESG 整體分數



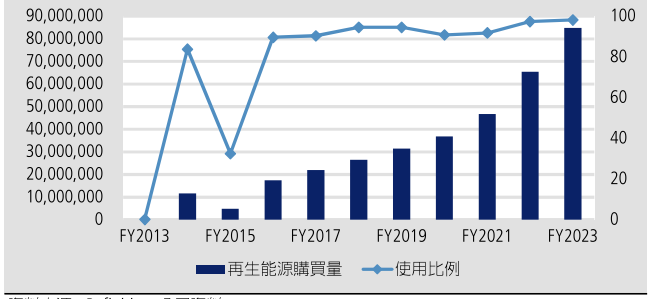
資料來源：Refinitiv、公司資料

圖 22：Microsoft – ESG 各項分數



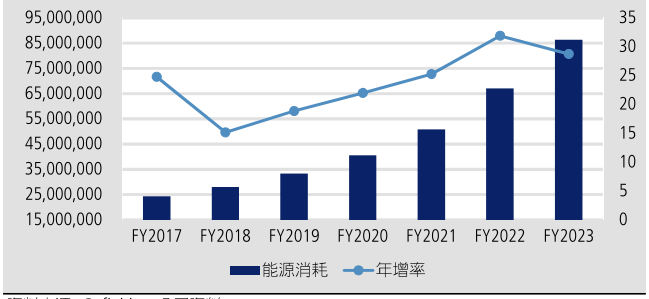
資料來源：Refinitiv、公司資料

圖 23：Microsoft – 再生能源使用



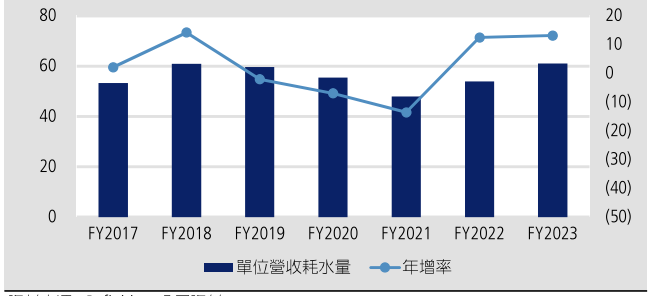
資料來源：Refinitiv、公司資料

圖 24：Microsoft – 能源消耗



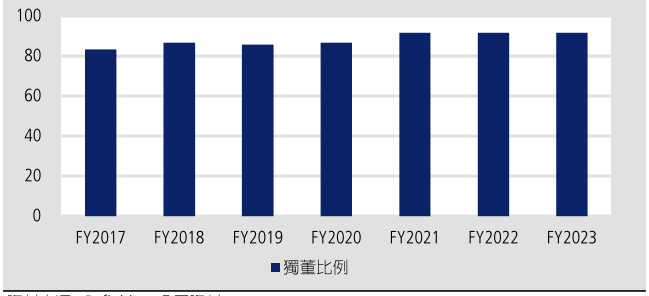
資料來源：Refinitiv、公司資料

圖 25：Microsoft – 耗水量



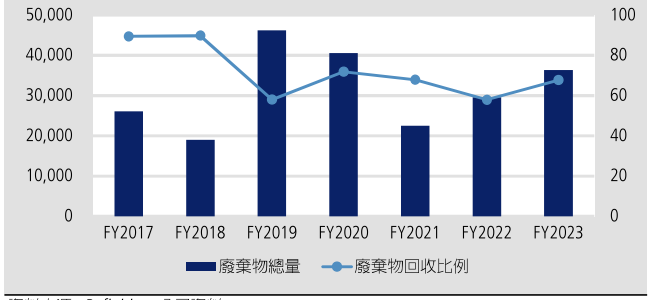
資料來源：Refinitiv、公司資料

圖 26：Microsoft – 獨立董事



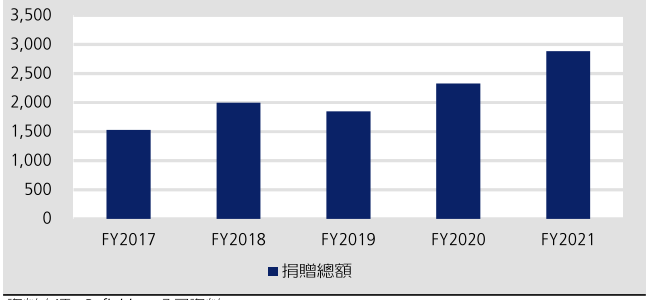
資料來源：Refinitiv、公司資料

圖 27：Microsoft – 廢棄物回收總量



資料來源：Refinitiv、公司資料

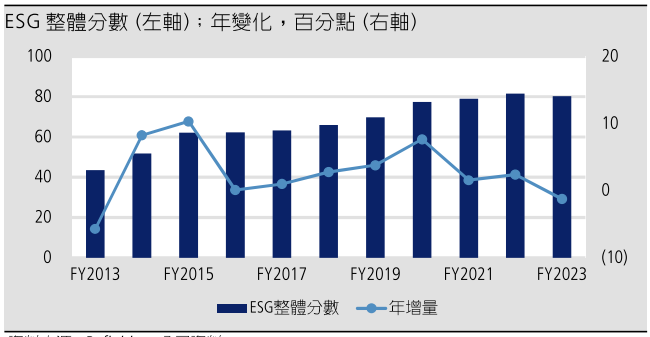
圖 28：Microsoft – 捐款



資料來源：Refinitiv、公司資料

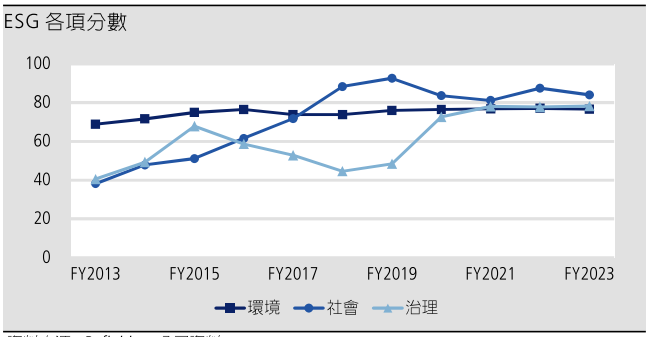
Alphabet (GOOGL US)

圖 29：Alphabet – ESG 整體分數



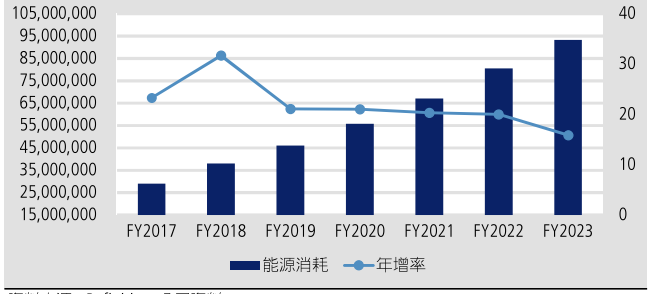
資料來源：Refinitiv、公司資料

圖 30：Alphabet – ESG 各項分數



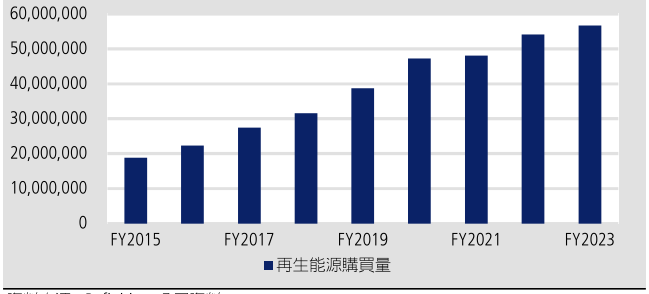
資料來源：Refinitiv、公司資料

圖 31：Alphabet – 能源消耗



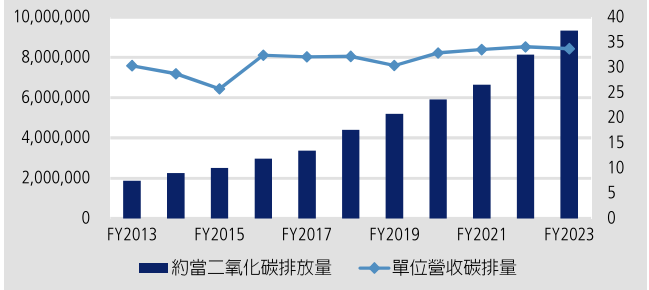
資料來源：Refinitiv、公司資料

圖 32：Alphabet – 再生能源使用



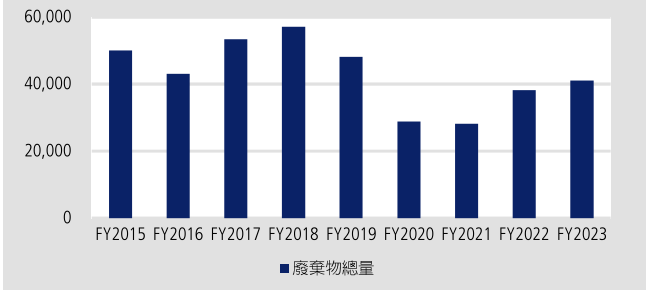
資料來源：Refinitiv、公司資料

圖 33：Alphabet – 碳排量



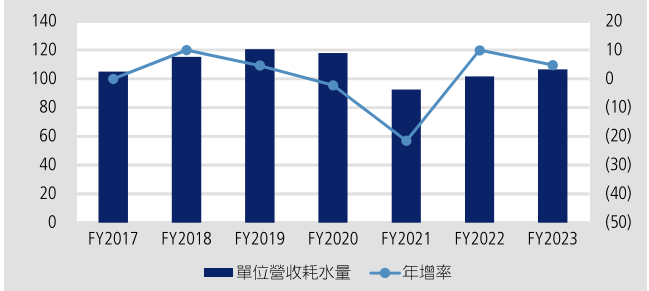
資料來源：Refinitiv、公司資料

圖 34：Alphabet – 廢棄物總量



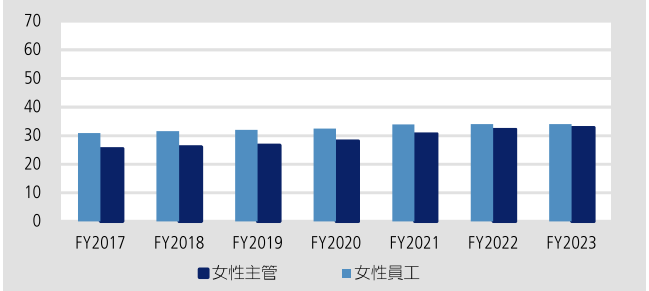
資料來源：Refinitiv、公司資料

圖 35：Alphabet – 耗水量



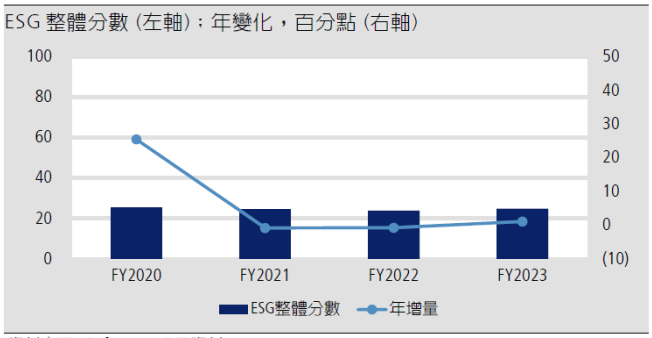
資料來源：Refinitiv、公司資料

圖 36：Alphabet – 性別多樣性



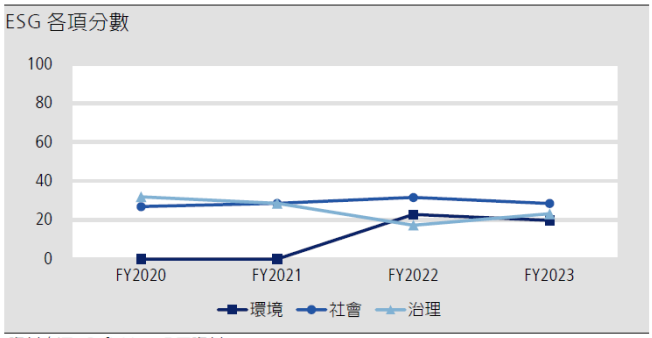
資料來源：Refinitiv、公司資料

圖 37：Crowdstrike – ESG 整體分數



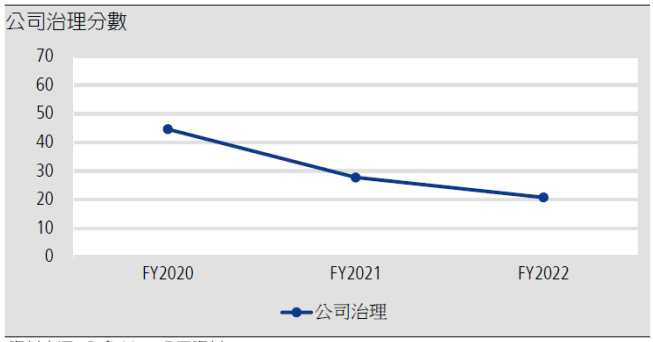
資料來源：Refinitiv、公司資料

圖 38：Crowdstrike – ESG 各項分數



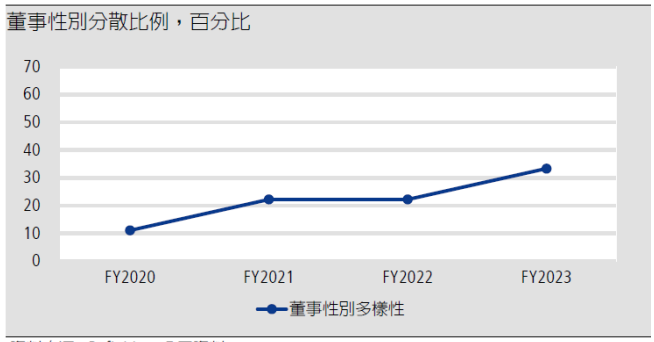
資料來源：Refinitiv、公司資料

圖 39：Crowdstrike – 公司治理



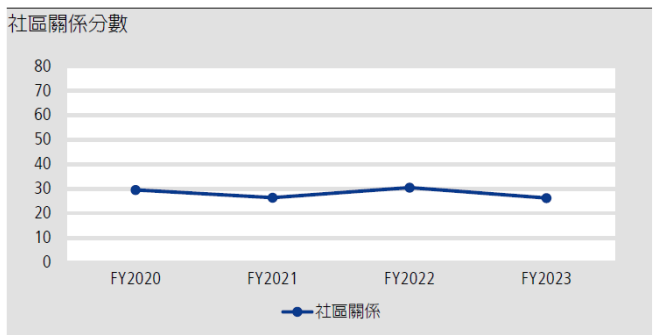
資料來源：Refinitiv、公司資料

圖 40：Crowdstrike – 董事性別多樣性



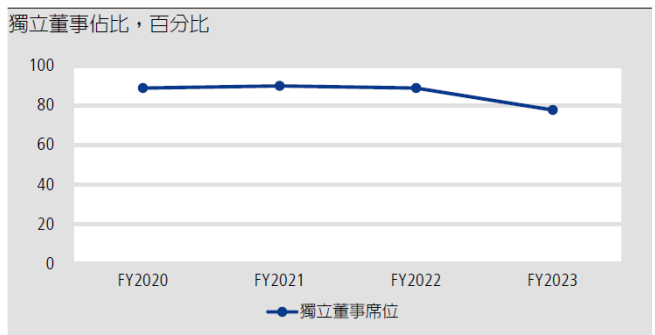
資料來源：Refinitiv、公司資料

圖 41：Crowdstrike – 社區關係



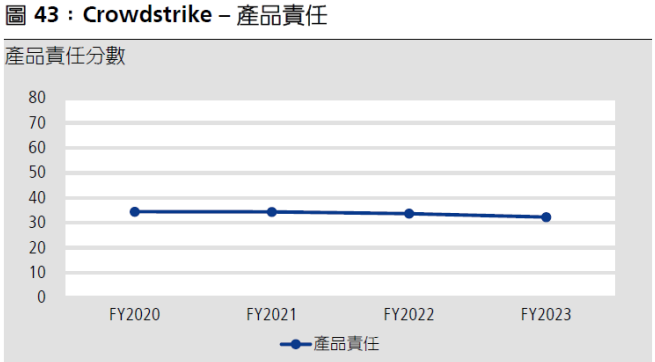
資料來源：Refinitiv、公司資料

圖 42：Crowdstrike – 獨立董事



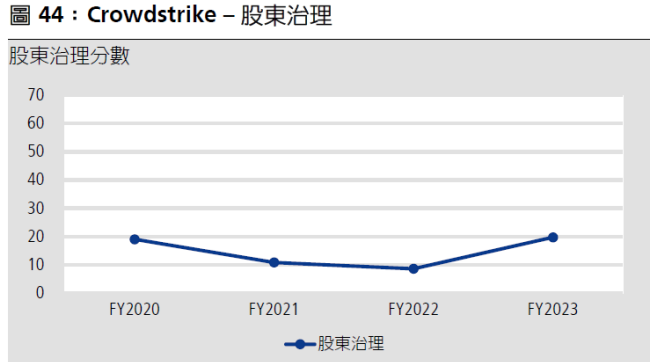
資料來源：Refinitiv、公司資料

圖 43：Crowdstrike – 產品責任



資料來源：Refinitiv、公司資料

圖 44：Crowdstrike – 股東治理



資料來源：Refinitiv、公司資料

上述為證監會持牌人，隸屬凱基證券亞洲有限公司從事相關受規管活動，其及 / 或其有聯繫者並無擁有上述有關建議股份，發行人及 / 或新上市申請人之財務權益。