資訊安全產業

零信任與平台化業者加速搶奪市占，評價已回到相對舒適區

焦點內容

1. XDR: CRWD F2H26 NNARR 財測年增 40%優於市場預期 11ppts，需求由客戶換約與 NG-SIEM 等新產品帶動。
2. SASE: PANW FY26 NGS ARR 優於預期 2%；ZS FY26 有機 ARR 財測在新任 CFO 上任下較為保守。
3. IAM: OKTA 聯邦政府優於預期，然 cRPO 展望仍相對保守；CYBR IMPACT 25 強化 PAM 於 AI Agent 地位。
4. Data Security: Rubrik F2Q/3Q26 營收財測優於預期 10/8%，F500 大型客戶滲透率持續增加。

Nasdaq 指數

資料來源：Bloomberg

ESG 分數評等

Company		Overall	E	S	G
CrowdStrike	CRWD US	25	20	29	23
Zscaler	ZS US	38	68	58	13
Okta	OKTA US	40	37	62	23

資料來源：Refinitiv、凱基

重要訊息

資安業者 CrowdStrike (美；CRWD US)、Zscaler (美；ZS US)、Okta (美；OKTA US)、Rubrik (美；RBRK US) 與 Palo Alto Networks (美；PANW US) 公布 C2Q25 財報，大致符合凱基產業觀點，即防火牆更新週期驅動 SASE 需求、次世代業者加速切入 SIEM 產業。我們亦參加 CyberArk (美；CYBR US) IMPACT25 更新身份資安產業動態。

評論及分析

XDR：CRWD 在 CWPP、NG-PAM 及 NG-SIEM 全方位布局。CRWD F2Q26 營收/NNARR 優於預期 2/6%，雖 F3Q26 營收低於預期 2%，然 F2H26 財測 NNARR 年增 >40%，優於預期 11ppts。Flex 客戶數突破 1k，Re-Flex 帳戶數倍增，近 10% Flex 客戶在平均 5 個月內追加 Re-Flex，帶動 ARR 提升 50%。產業趨勢上看到 AI 帶動雲端資安重點由 CSPM 轉向 CWPP、次世代 PAM 需求升溫、NG-SIEM 具破壞性定價有助搶佔市場。

SASE：PANW 併購 CYBR 完善平台化大艦隊；ZS ZTE 客戶數成長亮眼。PANW FY26 財測 NGS ARR 優於預期 2%，管理層表示需求 SASE、XSIAM 與軟體防火牆帶動，SASE ARR 年增 35%，取得該司史上最大 US$60mn 合約，XSIAM 業務客戶 400 名，年增 2x，平均 ARR >US$1mn；ZS F1Q26/FY26 營收及財測優於預期 3/2%，FY26 ARR 財測年增 22%，惟扣除 Red Canary 有機成長僅 19%略低於市場預期的 20%，考量新 CFO 甫上任較保守財測尚屬合理。ZTE 客戶數達 350+，Z-Flex 已帶動 >US$100mn 訂單，季增 50%，Red Canary 併購上將優先完成與 Data Fabric 的深度整合，打造統一弱點曝險管理與 AI 驅動 SOC。

IAM：OKTA 聯邦政府業務優於預期然 cRPO 展望仍較保守；CYBR IMPACT 25 強化 PAM 於 AI Agent 防護地位。OKTA F2Q26 營收優於預期 4%，美國聯邦政府需求優於先前擔憂，聯邦續約強勁且伴隨新產品加購，亦隨先前對總經與聯邦政府業務的保守假設未出現，全年營收財測上調 1%至 US$2,880mn，惟 F3Q26 cRPO 財測季增持平為相對負面之處。CYBR IMPACT 25 會議中強調 AI Agent 具機器身分之可擴張性與人類自主性，防護需採即時授權，調查顯示 65%台灣組織尚未建立 AI 身份防護，82%的組織認為身份系統孤島是資安風險根源，凸顯 PAM 以及平台化重要性。

Data Security：RBRK 財報優預期且 F500 客戶滲透率向上。RBRK F2Q/3Q26 營收財測優於預期 10/8%，F500 客戶持續採用身分與資料防護產品，管理層看好身分資訊與 DSPM 結合為該司切入資安領域之競爭優勢。

投資建議

C2Q25 財報顯示之產業趨勢符合我們先前所述，並持續觀察到零信任與平台化業者在 SASE, SIEM, 身分等次產業奪取市佔，凱基資安產業首選仍為 CRWD，看好其佔據較佳產業地位；ZS 持續受惠防火牆更新週期，並透過收購案強化 SOC 佈局。正向看待 PANW 為平台化趨勢主要受惠者之一。

投資風險

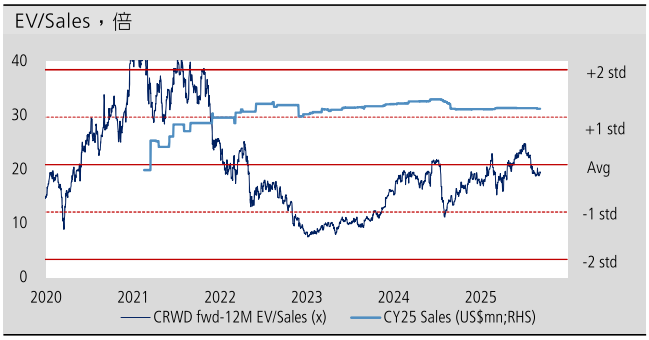
企業 IT 支出動能趨緩；競爭；GenAI 實際應用不如預期。

圖 1: 凱基財測及目標價調整

	KGI forecast		Chg. (%; pts)					Target price				Multiple	
	2025	2026	2025	2026	Rating	Shr px (US$)	Mkt cap (US$bn)	New (US$)	Upside (%)	Old (US$)	Chg. (%)	New	Old
Crowdstrike (FY ends Jan.)	**FY26**	**FY27**											
Revenue (US$mn)	4,788	5,830	0	0									
Gross profit (US$mn)	3,729	4,570	(0)	(0)									
Operating profit (US$mn)	1,025	1,400	3	2	OP	424	106	610	44	610	0	FY27 25x EV/sales 5yr +1.5std.	FY27 25x EV/sales 5yr +1.5std.
Pre-tax income (US$mn)	1,189	1,578	3	1									
Net income (US$mn)	937	1,245	4	1									
EPS (US$)	3.66	4.76	4	1									
Zscaler (FY ends Jul.)	**FY25**	**FY26**											
Revenue (US$mn)	2,673	3,276	0	2									
Gross profit (US$mn)	2,141	2,628	0	2									
Operating profit (US$mn)	580	732	1	2	OP	282	44	400	42	400	0	FY26 19x EV/sales 5yr avg.	FY26 19x EV/sales 5yr avg.
Pre-tax income (US$mn)	684	858	2	3									
Net income (US$mn)	535	619	3	0									
EPS (US$)	3.28	3.66	2	(0)									
Okta (FY ends Jan.)	**FY26**	**FY27**											
Revenue (US$mn)	2,881	3,153	1	0									
Gross profit (US$mn)	2,354	2,577	1	0									
Operating profit (US$mn)	734	823	2	1	N	94	17	110	17	110	0	FY27 6x EV/sales 2yr +1std.	FY27 6x EV/sales 2yr +1std.
EBITDA (US$mn)	839	917	2	1									
Net income (US$mn)	622	686	2	1									
EPS (US$)	3.36	3.62	3	1									

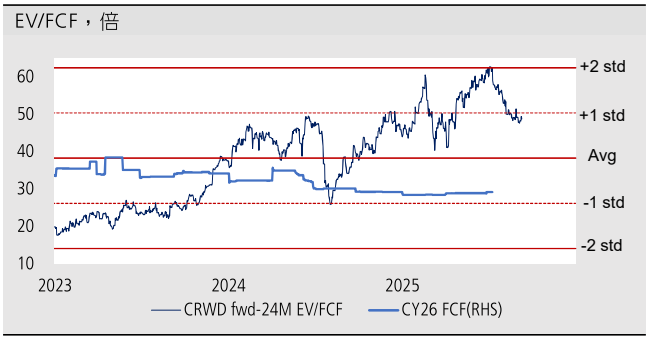
資料來源: Bloomberg；凱基

圖 2: CrowdStrike 未來 12 個月預估 EV/Sales



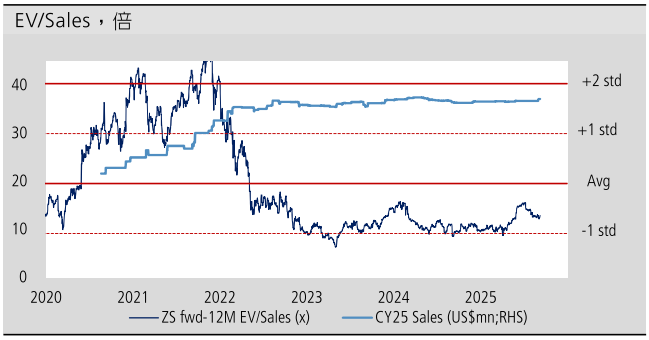
資料來源: Bloomberg；凱基
備註：財年止於 1 月

圖 3: CrowdStrike 未來 24 個月預估 EV/FCF



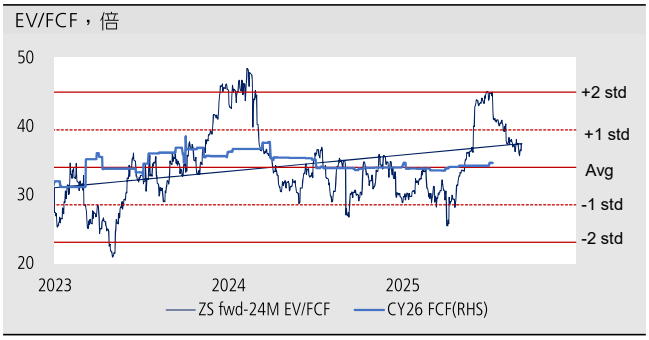
資料來源: Bloomberg；凱基
備註：財年止於 1 月

圖 4: Zscaler 未來 12 個月預估 EV/Sales



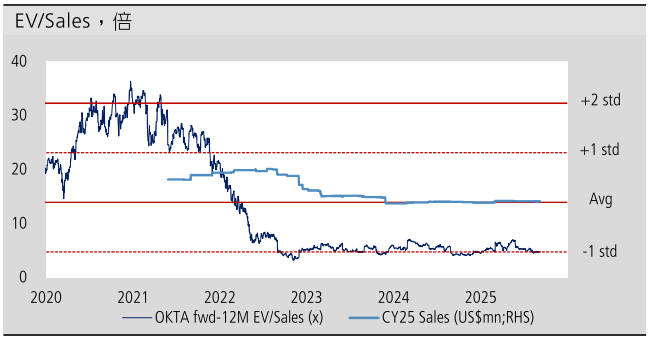
資料來源: Bloomberg；凱基
備註：財年止於 7 月

圖 5: Zscaler 未來 24 個月預估 EV/FCF



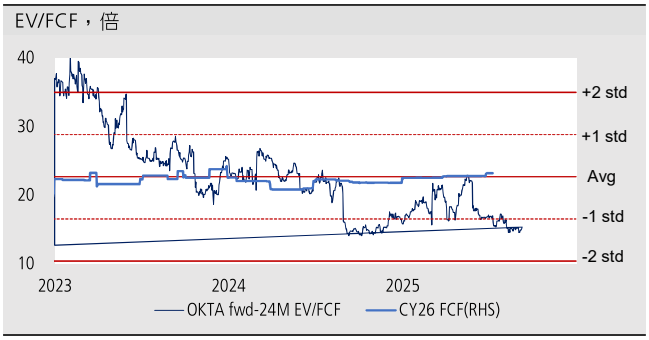
資料來源: Bloomberg；凱基
備註：財年止於 7 月

圖 6: Okta 未來 12 個月預估 EV/Sales



資料來源: Bloomberg；凱基
備註：財年止於 1 月

圖 7: Okta 未來 24 個月預估 EV/FCF



資料來源: Bloomberg；凱基
備註：財年止於 1 月

CyberArk IMPACT 25 Taipei 強化 PAM 於 AI Agent 防護地位與機器身分需求

- 所有身分（人、機器、AI）都必須以「適當層級」的控管被保護，而不是一體適用的重手段；控管強度需依情境動態調整。
- Palo Alto Networks 整合合作能提升覆蓋率、加速創新與服務能力，讓平台更無縫連接網路、雲端與 AI 環境，加速創新；對現有客戶/夥伴承諾不變，服務、支援、既定 roadmap 與既有解決方案均延續。

三大威脅／趨勢

- 人類特權的擴散：過去只需保護少數固定特權帳號；如今幾乎每個人每天都在某些時刻取得特權或敏感存取（可能是數分鐘到整天），傳統只管「常設存取＋共用帳號」的作法已不足。
- 機器身分大爆發：裝置、工作負載、VM、微服務、雲原生／無伺服器、IoT / OT 等機器身分數量呈指數級成長；去年的估算是每位員工對應超過 40 個機器身分，今年已超過 80 的量級。
- AI 無所不在：AI 不只改變工作方式，也加速攻擊、擴張攻擊面（新的工具與資料來源），同時帶來 AI Agent 這種須自第一天起就被保護的新身分。

主要產品／能力更新

- 現代化 IGA：
  - 目標是解決傳統 IGA 難上線、不易擴張的痛點；快速上線應用（API 優先，無 API 時以機械式自動化輔助）。
  - AI 驅動角色管理：把角色定義與維護自動化，降低人工作業負擔。
  - 流程自動化：存取審查、加入/調任流程等由系統驅動，提升體驗。
- Secure Workload Access（工作負載身分）：
  - 為雲原生與現代化架構簽發與管理工作負載身分，並與 Secrets 管理並行整合，單一平台同時管理「現代工作負載身分」與「密鑰／金鑰／Token」。

- Machine Identity Discovery & Context：
  - 對 Secrets、憑證、唯一 ID 等各類機器身分做發現/情境化/動作化（找得到、看得懂、做得到）。
- AI Agent Identity Solutions：
  - 把 AI Agent 視為會替人行動的身分主體，以機器等級的可擴張性與人類身分的治理原則自 Day-1 納管；與生態系夥伴合作建立標準。
- 機器身分不是新東西（如 service accounts、API keys），但在做零信任「五支柱」盤點（裝置、身分、網路、工作負載、資料）時最容易被漏掉，一漏掉就成了零信任的「例外/後門」。
- 常見錯誤是「永不更改密碼、權限過大」的服務帳號，這與「持續驗證、最小權限」原則衝突，會成為攻擊者首要目標。

2025 新調查洞察：身分風險的根因

- 調查樣本約 2,600 家（台灣約 100 家）。約 74%指出「身分擴散（Identity Sprawl）」是風險根因；72%指「身分安全與資安工具整合困難」。
- 三大成因：1) Hybrid 身分架構複雜 (雲/地混合、多目錄)；影子/未授權的 AI 應用 (缺乏可視性與治理)；過度依賴雲平台原生權限模型。
- 65%的台灣組織表示對 AI / LLM 尚未建立身分安全控管；許多新型數位身分因此處於未受保護狀態。
- 機器身分量級遠高於人類身分，台灣略低於全球平均，但仍非常高，多數未受管理，自動化擴張也放大誤用與未授權存取風險。
- 82%的組織認為身分系統孤島是資安風險根源，高於亞太與全球；割裂的身分系統造成盲區，難以一致施策與偵測異常。

ZSP（零常駐權限）在雲上的實作

- 沒有作業就沒有權限：目錄中預設不留任何持續性權限；當有合法需求時才「即時授權」，會話結束自動撤銷。
- 前後狀態對比：導入前使用者長期持有權限 → 導入後平時權限為 0，僅在工單/審批/情境條件滿足時動態賦權；降低誤用與外洩面積。

把 ZSP 延伸到 AI Agents

- AI Agent 不是單純機器帳號，其行為具自主性、可並行執行多任務且 24/7 運作，因此需採「像人一樣」的風險與行為治理。
- 做法：讓 AI Agent 也走即時授權 + 全程審計，權限與行為受同一平台治理。

CyberArk Core AI

- Core AI 助理：協助身分管理（例如建立 safes、指派權限、答覆產品／文件問題），用戶回饋正面。
- AI 會話摘要：自動把大量會話紀錄轉成可行動洞見，約 10% 的 Session Monitoring 客戶已使用，節省稽核／管理員時間。
- EPM（Endpoint Privilege Manager）策略建議：針對檔案提出 block / allow / trust / elevate 建議，依據最佳實務與社群知識；覆蓋約 65% 檔案、約 2,000 家客戶採用，能減人工、降錯誤、提安全。

用 AI 強化 CyberArk 平台能力

- 提升安全性（Boost Security）
  - 在 CyberArk 平台橫向偵測威脅，並以智慧化的權限控制即時回應，特別針對敏感或低頻使用帳號。
  - Demo 情境：某管理者取用 Vault 密碼後，開始連續存取不同高權限帳號（例如「CIS admin」），系統偵測異常、立刻告警；SOC／管理端可用自動流程或 Playbook 緩解。
- 最佳化動作（Optimize Actions）
  - 以 AI 精準個人化 EPM 策略建立，由「應用程式」轉為「發行者簽章」為主的建議，並附上可解釋理由，降低摩擦與處理時間。
- 提升效率（Enhance Productivity）
  - Troubleshooting Agent（Core AI 驅動）：互動式排錯，起步支援 SWS／RDP 與管理端問題；願景是從被動支援轉為主動，做 log 分析、自動建立偵測與處置。
- 2026 Agent 願景
  - Core AI 作為「Agent 協調器」，跨網域（domain）驅動專家型 AI Agents，自主執行營運決策與流程（超越 GUI / API 操作）。

為何 AI Agent 是「身分安全」議題?

- AI Agents 定義：能自主規劃、推理與執行任務的系統，行為具非決定性。
- 多重互動面：1) 與使用者 (回饋、提示)；2) 與組織環境 (郵件、資料庫、Sales 資料等)；3) 與 SaaS 應用 (如人類與機器既用的雲端服務)；4) 與自身框架資源 (記憶、資料庫狀態等)；5) Agents 彼此互動，以完成更大任務。
- 雙重本質：「像人一樣推理、非決定性」，同時「像機器一樣大規模、自主、無疲勞」—機器身分 + 人類行為模式的結合，本質是身分安全挑戰。

已發布 AI Agents 方案與實作（AWS Marketplace）

- CyberArk MCP Server for Secure Cloud Access（SCA）：將 SCA 能力以 MCP 方式暴露給開發者，支援 CLI／IDE／AI 助理。對人類與機器身分都落實「零常設權限」與更佳稽核性。
- Agent Guard（開源、免費）：面向自建 AI Agents 的團隊，提供完整稽核／追溯、動態祕密注入（整合 AWS Secrets Manager／CyberArk Secrets Manager），可 Docker 部署或以 SDK 內嵌。

機器安全身份

- 定義機器身分＝指派給「非人類實體」的數位身分，用於機器對機器的驗證、授權與存取管理。範圍包含 API、應用程式、Server、雲端服務與各式憑證／金鑰。透過機器身分彼此溝通與交換資訊，讓系統安全地完成任務。
- 今年「機器身分：人類身分」的比例翻倍；去年約 41:1，今年升至 82:1
- 94% 的受訪者表示過去三年內機器身分在其機構中大幅增長。
- 50% 的組織「已偵測並回報」機器身分遭入侵事件；實際情況可能更嚴重，因為不少組織尚未察覺自己已被入侵。
- Uber 案例：開發者電腦遭入侵 → 攻擊者在自動化 Script 中找到未加密的 PAM 特權密碼 → 進而入侵內部系統、下載資料並造成混亂。
- Epic Games 案例：憑證過期未自動更新導致旗下多人線上遊戲大量用戶無法登入（一晚接近 100 萬 用戶受影響），衝擊營收（例：微交易）。
- Alaska Airlines 案例：因過期憑證未更新而影響 IT 系統，導致全部航班取消。定義機器身分＝指派給「非人類實體」的數位身分，用於機器對機器的驗證、授權與存取管理。範圍包含 API、應用程式、Server、雲端服務與各式憑證／金鑰。透過機器身分彼此溝通與交換資訊，讓系統安全地完成任務。

CRWD 公佈優於預期的 F2Q26 財報，F2H26 NNARR 展望強勁

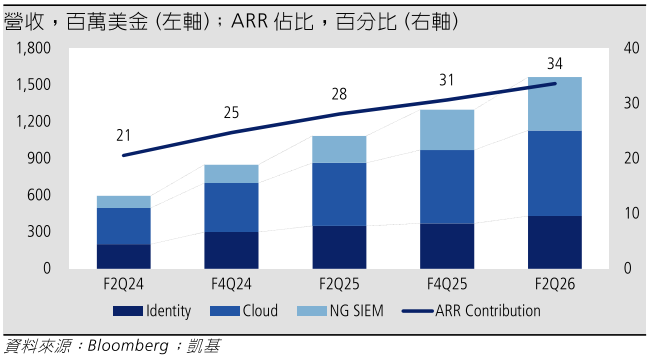
- CrowdStrike (CRWD US) 公布 F2Q26 財報（財年止於 1 月），盤後股價下跌 4%，係反應雖 F2Q26 營收/NNARR 優於預期 2/6%，然 F3Q26 營收低於預期 2%，FY26 財測營收微幅上調下緣 US$6mn 至 US$4,778mn，營業利益上調 3% 至 US$1,020mn，然對比 F2Q26 營收優於財測上緣 US$17.4mn 上修相對保守，亦對比樂觀投資人預期有所落差。管理層展望 F3Q26 NNARR QoQ 高個位數，優於預期的 QoQ -5ppts，F2H26 NNARR YoY >40%，優於預期 11ppts，FY26 ARR YoY >22%，優於預期 1ppts
- Cloud Security：ARR >US$700mn，YoY 35%，AI 帶動雲端資安重點由 CSPM (Wiz) 轉向 CWPP (CRWD 市佔第一 per Gartner) 的 run-time 防護，在產業變動期看到強勁轉換與整併需求，F50 客戶將 CNAPP/CSPM/ASPM/CDR/容器等 10+ 點產品整併至 Falcon 平台

- Identity Security：ARR >US$435mn，YoY 21%，優於預期 9%，身份防護產品擴大至非人類身分與 SaaS 應用，PAM 產品在市場對傳統 PAM 前景不確定下需求升溫。全球顧問公司，以 CRWD 產品涵蓋密碼輪替、身分風險評估、提權偵測、彈性 MFA 與裝置信任等，達成合規與整併

- NG-SIEM：ARR >US$430mn，YoY 95%，低於預期 4%，收購 Onum 擴大即時遙測資料 pipeline 管理，可在轉送過程即做偵測，降低資料搬移成本。SIEM 產品差異化在於不對 CRWD 自產資料收費具破壞性定價、利於替換傳統 SIEM。Charlotte AI QoQ >80%，透過 Falcon Complete SOC 的威脅遙測數據形成 AI 回饋迴路

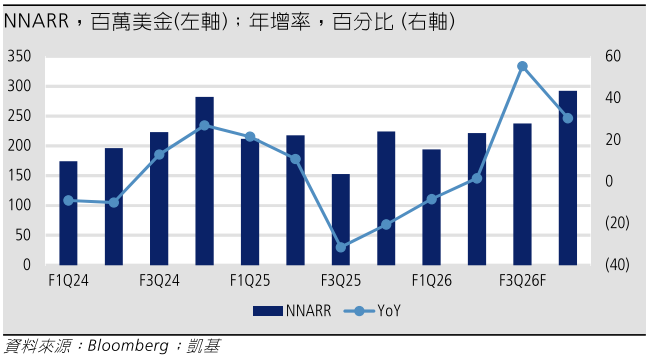
- 關注焦點：1) Flex 客戶數突破 1,000 家，本季新增 220+，整體客戶使用量 >75%，Re-Flex 帳戶數倍增、近 10% Flex 客戶在平均 5 個月內追加 Re-Flex，帶動 50% 的 ARR 提升；2) Exposure Management ARR >US$3mn，持續看到產業整併趨勢；3) 合作夥伴貢獻 >60% 的本季新業務，Red Canary 以 US$10mn 交易將 10 萬+ 既有 EDR 端點遷移到 Falcon、Amazon Business Prime 將 Falcon Go 納入會員權益以切入 <100 席市場；4) 6+/7+/8+ 模組客戶佔比 48/33/23%；5) F3Q26 對事故與計畫相關現金支出約 US$51M，GTM 將持續圍繞 Flex/平台啓用優化；6) 年度客戶大會 Fal.Con 2025 將於 9/15 開始、9/17 有投資人簡報

圖 8：CrowdStrike 新業務 ARR 佔比持續增加



資料來源：Bloomberg；凱基

圖 9：CrowdStrike F2H26 NNARR 將加速成長



資料來源：Bloomberg；凱基

OKTA 公佈優於預期的 F2Q26 財報，聯邦業務需求優於預期

- Okta 公布 F2Q26 財報，盤後股價上漲 7%，係反應在 F1Q26 相對保守的財測與市場預期下（過去一季股價 -27% vs. NASDAQ +12%），F2Q26 營收/cRPO 優於預期 4/7%，管理層表示先前對總經與聯邦政府業務的保守假設未出現，已自後續財測移除，因此全年營收財測上調 1% 至 US$2,880mn（上修 US$35mn vs. F2Q 優於財測 US$17mn），惟 F3Q26 cRPO QoQ 財測持平為相對負面之處

- GenAI 相關：1) Auth0 for AI Agents (原 Auth for GenAI) 提供 AI Agent 的驗證、憑證金庫與細粒度授權；2) 並發佈開放標準 Cross-App Access，管控 AI Agent 可觸達的資源，夥伴興趣濃厚，含 AWS、Boomi、Box、Zoom；3) Identity Security Fabric 讓人類與非

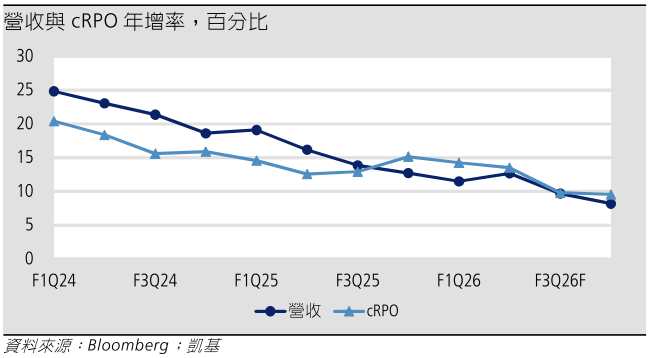
人類（NHI）身分皆可獲得盤點、註冊、授權、保護與持續治理；4) 企業當前痛點是服務帳號/機器身分與憑證治理，AI Agent 會放大此問題；5) AI-native 客戶成長快、內部也積極導入 AI Agent，Okta 協助其強化內部身分安全並支援以 Auth0 建構面向客戶的 AI 服務

- 聯邦政府業務：美國聯邦政府為 F2Q26 主要成長動能，呼應美國營收優於預期 3%，管理層表示需求優於先前擔憂，部分民事機關有合約重組/採購延遲，但聯邦續約強勁且伴隨新產品加購，前十大交易中有 5 筆來自美國公共部門，本季最大案來自國防部一年期交易，以 Okta Customer Identity 現代化其存取系統、符合零信任與聯邦法規要求

- 競爭擔憂：PANW 收購 CYBR 不致改變競爭態勢，持續強調當今大型企業面臨過度分散與舊平台成本高，Okta 以身分作為整合樞紐具中立性，可保留其他安全工具的選擇權，與大型科技公司合作整合 50+ 身份安全供應商

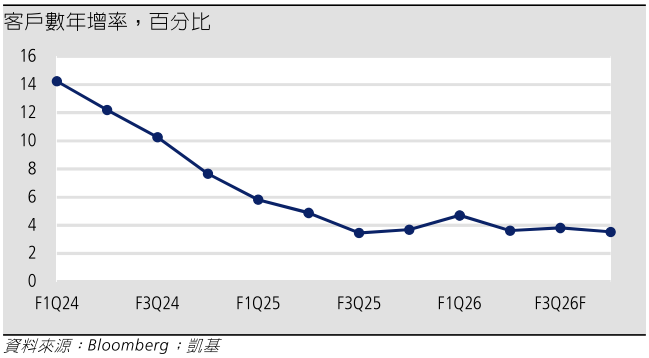
- 關注焦點：1) ACV >US$100k 客戶 4,945 名，YoY 7%，Workforce Identity ACV 佔比 59%，YoY 10%，Customer Identity ACV 佔比 41%，YoY 15%；2) 收購 Axiom Security (現代化 PAM 供應商) 將於 F3Q26 完成，將強化公司 PAM 產品；3) OIG 身分治理、OPA 特權存取、ISPM 身分安全態勢管理、ITP 身分威脅防護、細粒度授權等新產品連續四季表現強勁；4) F1Q26 導入的 GTM 專業化仍在爬坡階段，需要幾季時間完全發酵；5) F2Q26 pipeline 創新高、AE 自主開發管線占比提升，前 20 大交易全數有夥伴參與，通路生產力續增

圖 10：Okta cRPO 持續疲軟



資料來源：Bloomberg；凱基

圖 11：Okta 客戶數年增未見加速



資料來源：Bloomberg；凱基

PANW 公佈 NGSARR 優於預期的 F4Q25 財報，SASE, 軟體防火牆需求亮眼

- Palo Alto Networks (PANW US) 公布 F4Q25 財報，盤後股價上漲 5%，係反應在市場預期已被壓低下，FY26 財測 (不含 CyberArk 貢獻) 營收大致符合預期；NGS ARR 優於預期 2%；RPO 優於預期 2%；FCF Margin 38.5% 優於預期 1.8ppts。管理層表示總體環境尚可，需求由 SASE、XSIAM 與軟體防火牆帶動

- 防火牆更新週期：與防火牆同業 FTNT, CHKP 類似，C2Q25 營收表現較佳皆為防火牆所在之產品業務，而管理層表示 PANW 憑藉較佳之公有雲原生軟體防火牆技術 (市佔>50% vs. 於整體防火牆市佔 22%) 在多雲/混合雲環境獲得客戶青睞，取得優於產業之成長 (PANW 營收

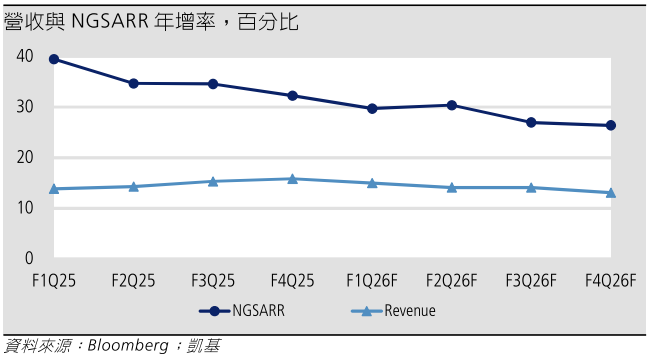
YoY 19% vs. FTNT/CHKP 13/12%)，軟體防火牆營收占比達 56%，YoY 12ppts。展望未來，管理層預期 F1Q26/FY26 產品營收 YoY 20/low-teens，隱含更新週期集中在 C2H25

- CyberArk 收購案：管理層認為未來 12-24 個月 IAM 市場將因 AI Agent 發生巨變，而專注於資安而非 SSO (OKTA) 更能滿足需求。收購後將發揮平台化綜效，擁有 10x 以上的核心經銷商，並導入 CYBR 產品於 PANW 75k 客戶中，預計在 FY28 達到 FCF Margin 40% 以上，符合市場預期

- GenAI 相關：1) AI ARR US$545mn，YoY 2.5x；2) 2024 年 GenAI 流量 YoY 840%，自去年以來與 GenAI 相關的資料安全事件增加一倍；3) 與專業服務公司達成八位數 Prisma AIRS 交易；4) AI 將加速產業整併需求，管理層看好 PANW 市占率由 6-8% 提升至 15-20%

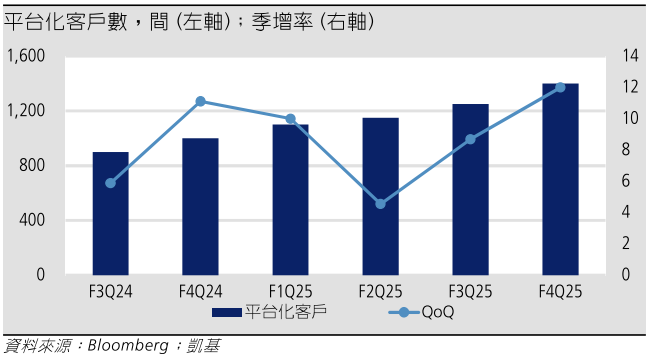
- 關注焦點：1) Bookings 達兩年半新高，RPO YoY 24% 較去年同期加速成長 4ppts，NRR 120%，平台化客戶 1,400 新增 150 名為新高；2) 大型交易顯著增加，US$5-10/20mn 客戶 YoY 50/80%，代表性客戶案例含全球顧問業者 US$100mn、歐洲銀行 US$60mn+，以及美國保險公司 跨三平台 US$33mn 交易；3) Cortex Cloud ARR YoY 25%，Cortex XDR >US$1mn 交易 YoY 30%，XSIAM 擁有 400 名客戶，YoY 2x，平均 ARR >US$1mn，其中 25% 為 G2k 企業；4) Network Security NGS ARR US$3.9bn，SASE ARR YoY 35%，客戶數 >6,300 名，涵蓋 1/3 為 F500；贏下史上最大 US60mn 及 20 萬座席 SASE 合約，Prisma Access Browser 單季售出 300+ 萬席，QoQ 2x，累計 >600 萬席；5) 共同創辦人 Nir Zuk 宣布退休，Lee Klarich 出任 CPO＋CTO 並加入董事會，延續產品與技術路線

圖 12：Palo Alto Networks 營收未見加速成長



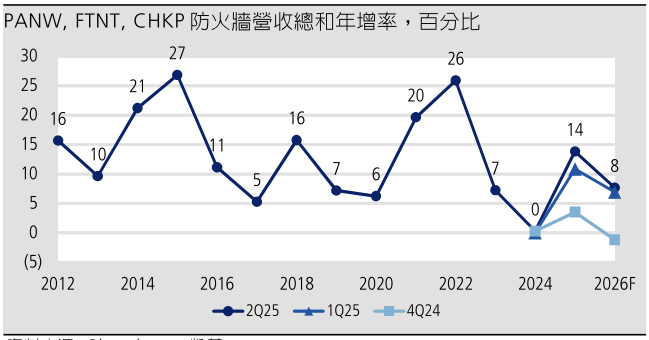
資料來源：Bloomberg；凱基

圖 13：Palo Alto Networks 平台化客戶數季增加速



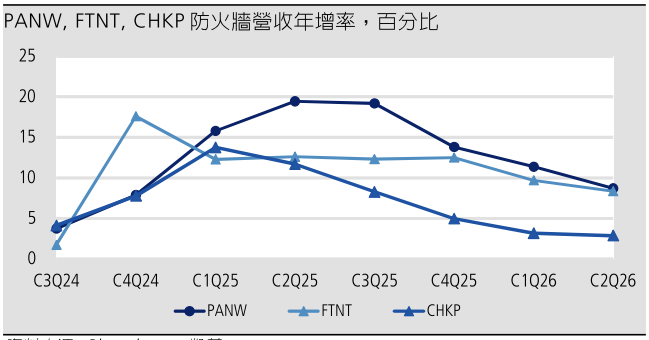
資料來源：Bloomberg；凱基

圖 14：防火牆業者 CY24-25 產品營收持續上修



資料來源：Bloomberg；凱基

圖 15：Palo Alto Networks 產品營收增速優於同業



資料來源：Bloomberg；凱基

圖 16: Palo Alto Networks 推出 SASE 4.0 強化瀏覽器防護, Data Security 與資安運營布局

版本	發布時間	重點 / 核心更新	主要技術突破	定位與差異
SASE 1.0	Sep-21	首度把 Prisma Access（雲端 SSE）+ Prisma SD-WAN 統一成「Prisma SASE」，加上 ADEM（體驗監測）與 Cloud SWG；單一雲後台管理	將 SD-WAN 與 SWG/CASB/FWaaS/ZTNA在雲端提供整合服務；啟動單供應商 SASE 路線	以「單一平台」切入 SASE，主打全球節點與雲交付、簡化分支與遠距存取部署
SASE 2.0 (ZTNA 2.0)	May-22	ZTNA 2.0（持續驗證、細粒度最小權限、持續檢測），Prisma Access 完整支援；強化「統一 SASE」與自助式 ADEM	從「一次放行」的傳統 ZTNA 跨越到行為/內容持續評估與檢測 的零信任實作。	與 1.0 相比，零信任做到更嚴謹與連續性，收斂管控面更完整
SASE 3.0	May-24	擴到未受管裝置、AI 資料防護（DLP/分類）、應用加速（與雲商整合）、更好的體驗與可用性（五個 9 SLA）	藉由收購/整合把瀏覽器層安全、應用加速與 ADEM 拉進單一服務，單供應商 SASE 能力成形	與 2.0 相比，版圖從存取管控擴到資料、體驗、與效能；更貼合「混合辦公＋多雲」情境
SASE 4.0	Sep-25	新一代 AI 驅動 SASE：推出/強化 Prisma Access Browser（SASE-原生安全瀏覽器），瀏覽器內組裝型威脅即時化解、AI 輔助資料分類、動態私有應用保護；強調統一、智能營運	把偵防範圍前推到使用者瀏覽器執行環境，搭配 AI 於資料/策略/運維全面加持，讓網路、安全、與運營 在同一雲端架構中閉環	與 3.0 相比，安全邊界前移到瀏覽器、AI 覆蓋更深（分類、檢測、運維），明確鎖定 AI 時代企業的威脅型態與營運複雜度

資料來源: Palo Alto Networks；凱基

ZS 公布 FY26 ARR 略低預期的 F4Q25 財報，ZTE 表現亮眼

- Zscaler 公布 F4Q25 財報，盤後股價上漲 2%，係反應 F1Q26/FY26 營收財測優於預期 3/2%，管理層提及客戶對 GenAI 資安需求強勁，帶動 ZTE/AI Security/Data Security ARR >US$1bn，全年財測上預計 ARR US$3,687mn，YoY 22%，投資人普遍預期約 YoY 20%；營收 US$3,275mn，YoY 22.5%，優於預期 2%；non-GAAP 營業利益 US$732mn，YoY 26%，大致符合預期

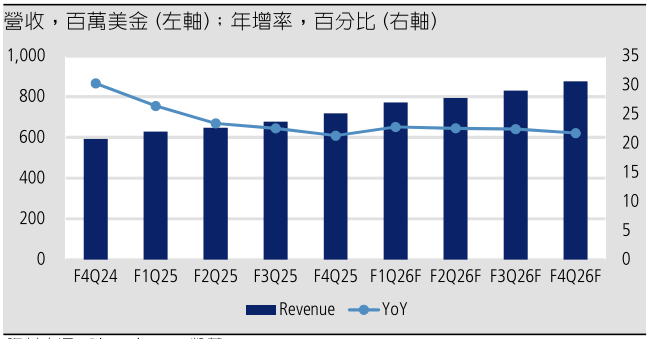
- Zero-Trust Everywhere：客戶數達 350+，QoQ 67%，客戶路徑多為使用者 → 分支 → 雲；成為 ZTE 客戶後常見 ARR 2–3 倍提升。客戶採用 Zero Trust Branch 取代舊有方案節省成本，Zero Trust Branch 可解決傳統 SD-WAN 管理負擔大且易於側移攻擊的風險。雲端產品於 F4Q25 加速。

- Data Security：ARR US$425mn，佔比 14%，在既有 8 個模組內，目前僅約 30% 客戶啓用 3+ 模組、約 10% 啓用 4+ 模組，擴充空間大，35 萬用戶大型服務業客戶整合 Email DLP、端點 DLP、分類與加密、GenAI 安全等多單點產品

- Red Canary 收購：SecOps/Agentic Ops ARR YoY >85%，將結合其 MDR 專長與 ZS 的 Data Fabric for Security，以 Agent AI 自動化偵測、分析與修復，加速並精準降低網路風險，FY25 認列 US$83mn ARR，FY26 假設 US$95mn ARR／US$90mn 營收貢獻。未來將優先完成與 Data Fabric 的深度整合，銷售上採專家型覆蓋以擴大全面平台交易，MDR 業務持續經營，SecOps 以 Data Fabric 打造統一弱點/資產曝險管理與 AI 驅動 SOC，以成果計價、不以 GB 數據量

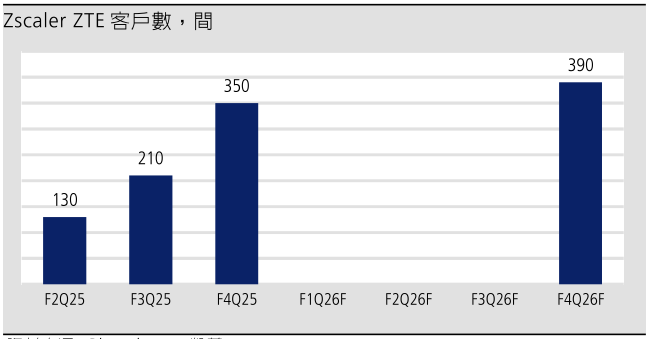
- 關注焦點：1) Z-Flex 已帶動 >US$100mn 訂單，QoQ 50%，五年期八位數 TCV 的能源客戶把啓用模組 由 14 擴至 19，ARR 提升 >100%；2) SASE 替換防火牆將由分支→資料中心→虛擬防火牆，ZS 零信任分支與 AI 安全產品需求強勁， 零售業分支防火牆同質性高、佈署簡單，先從小型門市開始推進，在 5 年汰換週期下，FY26 對 Branch 成長具貢獻；3) 聯邦約占 FY25 業務高個位數，通過美國國防部 CMMC Level 2，成為首家同時取得 AWS ISV Competencies 醫療、教育與政府新版各子類別的 ISV；4) F4Q25 毛利率 79.3%，因一次性政府私有雲部署含硬體而下滑，F1Q26 目標回到 ~80%；5) 發布 2025 ThreatLabz Ransomware 報告，勒索攻擊 +146%、公開勒索 +70%，凸顯以 Zero Trust Everywhere 防側移、保護敏感資料與應用的重要性；6) IT 端以 ZDX Copilot 與 端點自動修復加速工單處理，ZDX Advanced Plus 訂單 YoY 58%；7) FY26 NNARR 有機成長高個位數，將集中於 F2H26，對總體環境假設保持不變；8) AI Security 保護順序由安全使用公共 AI (DLP) → 保護私有模型與應用 (AI Guardrails) → A2A/MCP 零信任通訊，目前正處 AI Guardrails 的早期階段

圖 17： Zscaler 營收將自 F1Q26 落底並略微加速成長



資料來源：Bloomberg；凱基

圖 18：目前 ZTE 客戶數 210 間，目標於 FY26 達到 390 間



資料來源：Bloomberg；凱基

RBRK 公布優於預期的 F2Q26 財報，「資安韌性」延伸為「Security + AI」

- Rubrik (RBRK US) 公布 F2Q26 財報，盤後股價下跌 4%，係反應雖 F2Q/3Q26 財測營收優於預期 10/6%，然管理層表示雲端轉型期的非經常性營收將貢獻全年營收年增 6ppts，較先前僅數個百分點預期有所提升，反應在全年營收財測上調 4% 至 US$1,232mn，訂閱 ARR 僅上調 2% 至 US$1,412mn

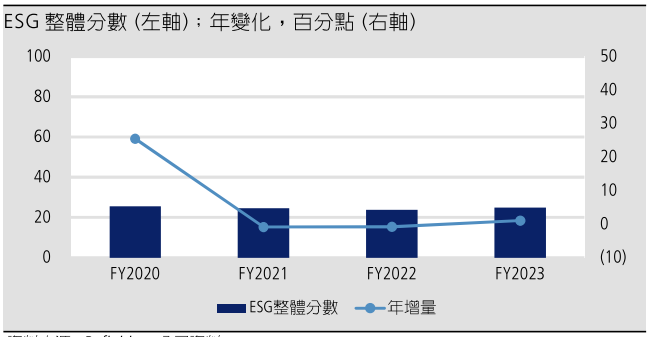
- DSPM：1) 公司定位正從「資安韌性」延伸為「Security + AI」，核心平台 RSC 結合 DSPM 與身份復原，呼應客戶預設被入侵的思維；2) 管理層認為資料＋身分一體化視圖才具可持續競爭力：例如特權提升時即時評估新增暴露的敏感資料與潛在衝擊，並串接資料復原／身分修復能力

- GenAI：1) 結合 Anapurna (embedding 搜尋) + Prebase (微調與服務) + Agent Rewind Agentic Ops 能力，定位為 Security + AI 公司；2) 近期併購 Prebase 與自家安全資料平台，推進企業 AI 加速：推出 Agent Rewind，協助在不轉返 (rollback) 整個系統下撤銷 AI Agent 的錯誤動作；3) AI 產品仍在找產品市場契合的早期階段，將持續多年度投資

- 關注焦點：1) 身份業務推出數季即達 200+ 客戶，F500 金融客戶因應審計與實際攻擊風險導入，將 AD/Entra ID 關鍵服務復原時間降至 <2 小時、大型物流公司導入身分復原，把復原時間由數週縮至數小時，新功能把身份與 DSPM 敏感資料脈絡關聯，持續監測人類／非人類身分組態與高風險變更；2) 公有雲資料防護擴充至 AWS RDS 與 Amazon DynamoDB；「Code-to-Cloud」一體化韌性平台持續擴展，大型運輸客戶加購 M365 on Azure、GitHub／Azure DevOps 原始碼復原與 Jira 防護；3) 近期有聯邦機構以 Rubrik 取代新世代競品以保護使命關鍵資料庫，主因是資料庫快速復原能力；4) 由過去半年度薪酬計畫改為全年，上半年運作順利、干擾輕微；因此 Q2 與 Q3 走勢更趨相近、Q4 仍季節性最強，已反映於財測；5) GTM 採三階段模式，Rubrik X（孵化）→ PLS（產品線銷售擴大）→ Core Sales（主力銷售接手規模化）；6) 競爭格局未變，對傳統與新世代競品皆維持高勝率；7) 近半數新單落在 Enterprise，Foundation 仍是預算受限客戶的切入點，無論起點為何，後續可升級版本與橫向擴到更多工作負載

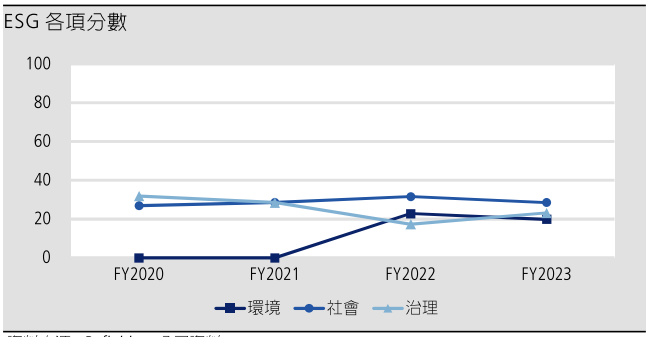
Crowdstrike (CRWD US)

圖 19：Crowdstrike – ESG 整體分數



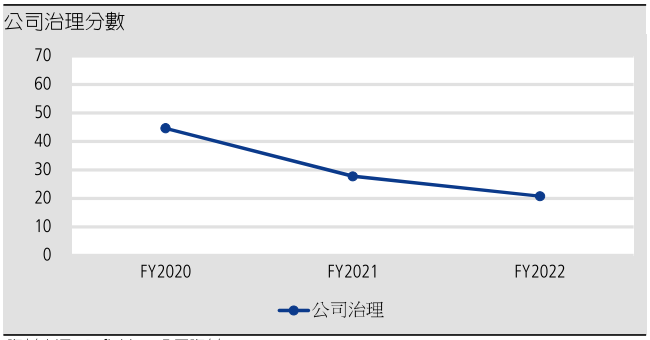
資料來源：Refinitiv、公司資料

圖 20：Crowdstrike – ESG 各項分數



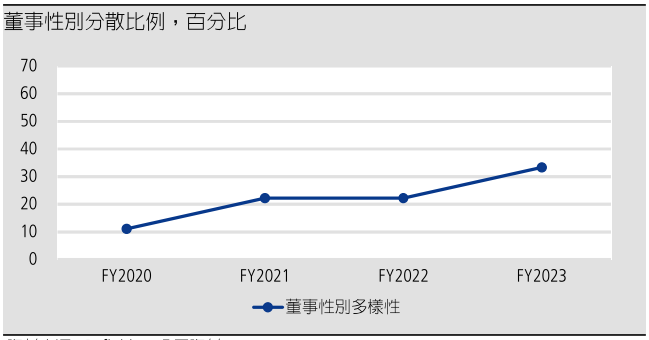
資料來源：Refinitiv、公司資料

圖 21：Crowdstrike – 公司治理



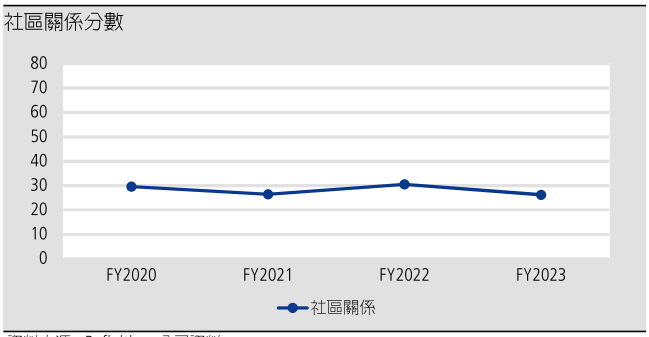
資料來源：Refinitiv、公司資料

圖 22：Crowdstrike – 董事性別多樣性



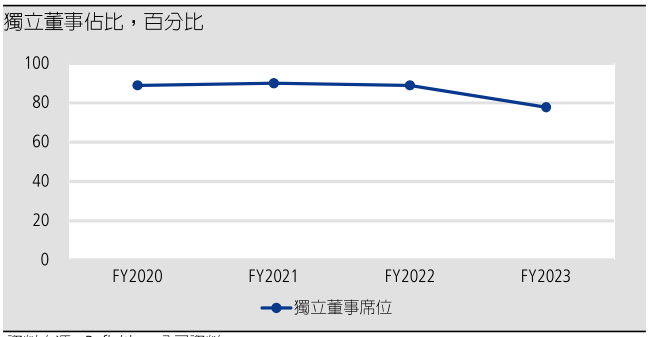
資料來源：Refinitiv、公司資料

圖 23：Crowdstrike – 社區關係



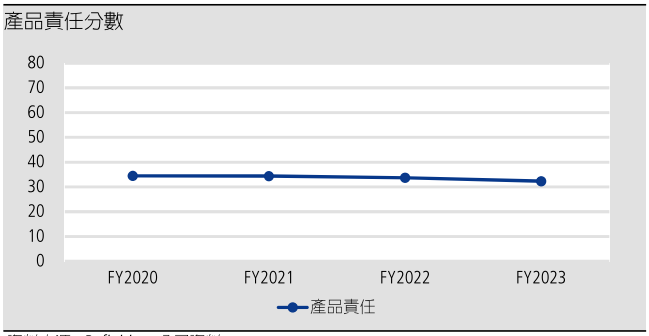
資料來源：Refinitiv、公司資料

圖 24：Crowdstrike – 獨立董事



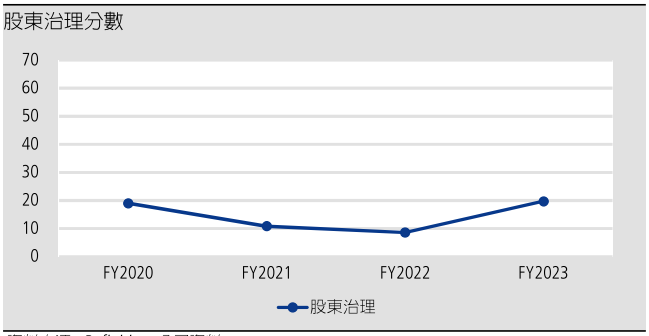
資料來源：Refinitiv、公司資料

圖 25：Crowdstrike – 產品責任



資料來源：Refinitiv、公司資料

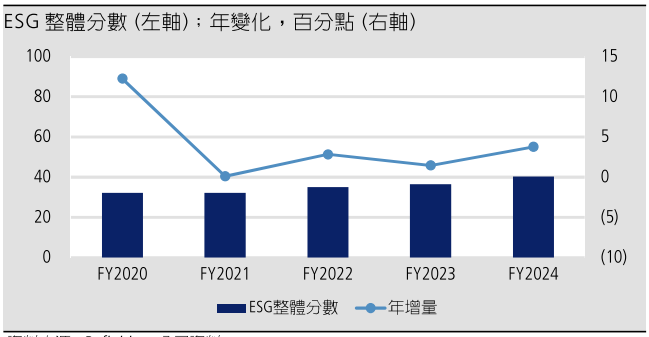
圖 26：Crowdstrike – 股東治理



資料來源：Refinitiv、公司資料

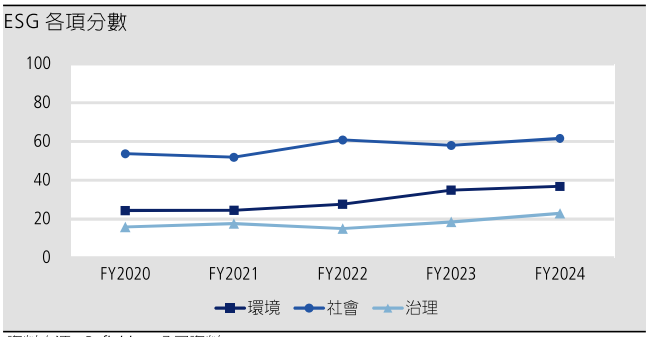
Okta (OKTA US)

圖 27：Okta – ESG 整體分數



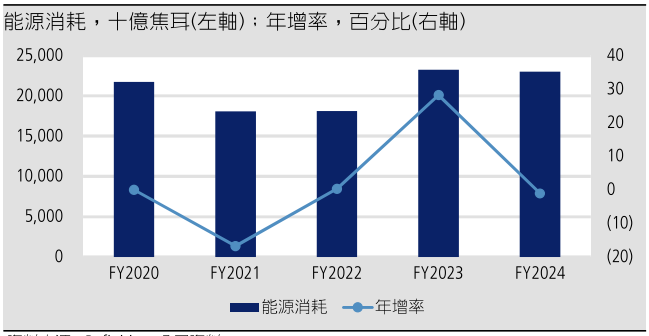
資料來源：Refinitiv、公司資料

圖 28：Okta – ESG 各項分數



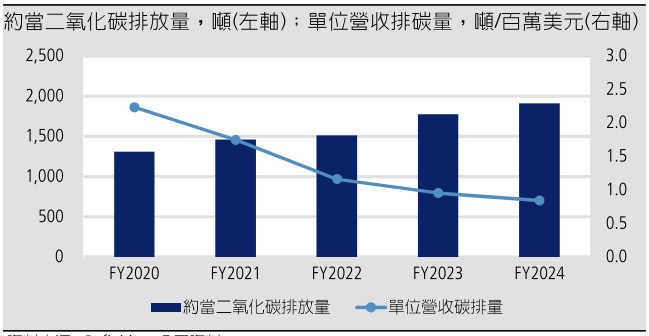
資料來源：Refinitiv、公司資料

圖 29：Okta –能源消耗



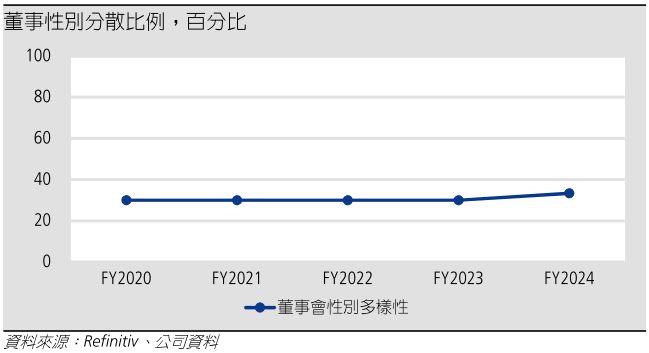
資料來源：Refinitiv、公司資料

圖 30：Okta –碳排量



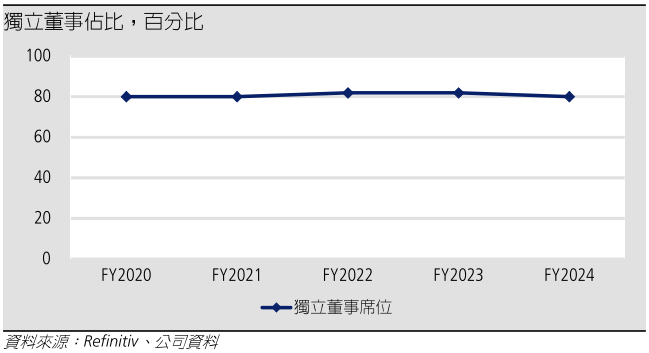
資料來源：Refinitiv、公司資料

圖 31：Okta – 董事性別多樣性



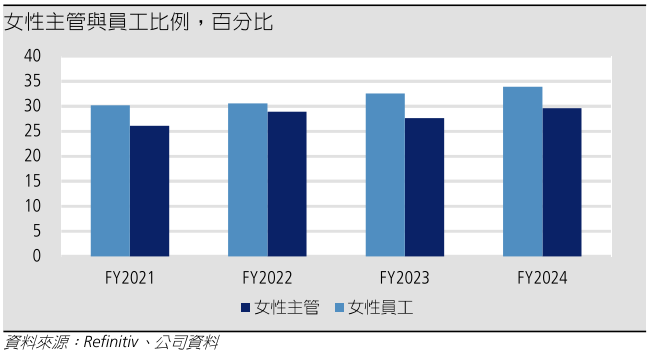
資料來源：Refinitiv、公司資料

圖 32：Okta – 獨立董事



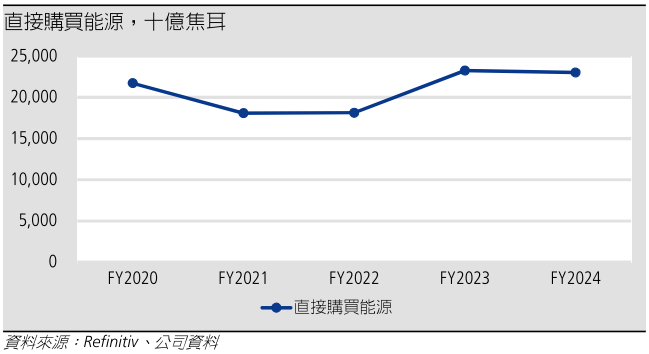
資料來源：Refinitiv、公司資料

圖 33：Okta –性別多樣性



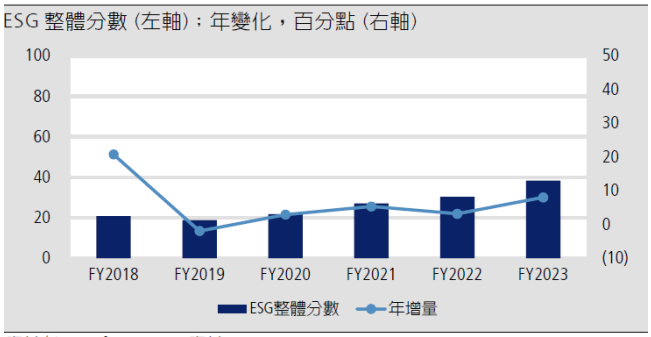
資料來源：Refinitiv、公司資料

圖 34：Okta – 直接購買能源



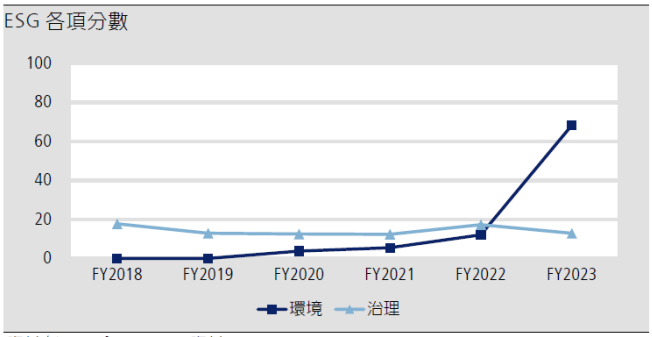
資料來源：Refinitiv、公司資料

圖 35：Zscaler – ESG 整體分數



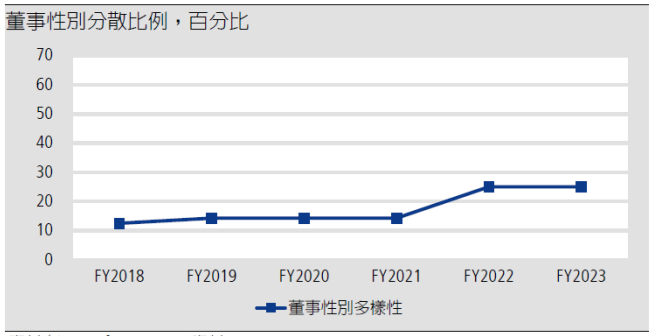
資料來源：Refinitiv、公司資料

圖 36：Zscaler – ESG 各項分數



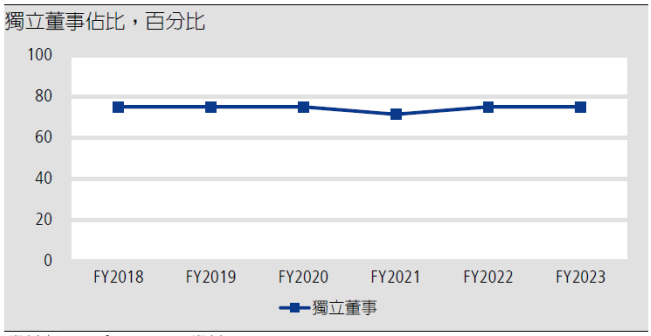
資料來源：Refinitiv、公司資料

圖 37：Zscaler – 董事性別多樣性



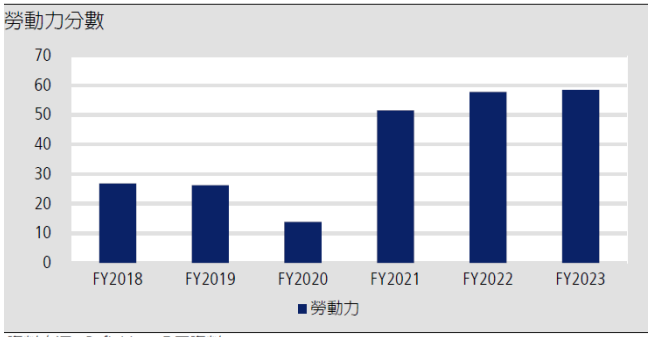
資料來源：Refinitiv、公司資料

圖 38：Zscaler – 獨立董事



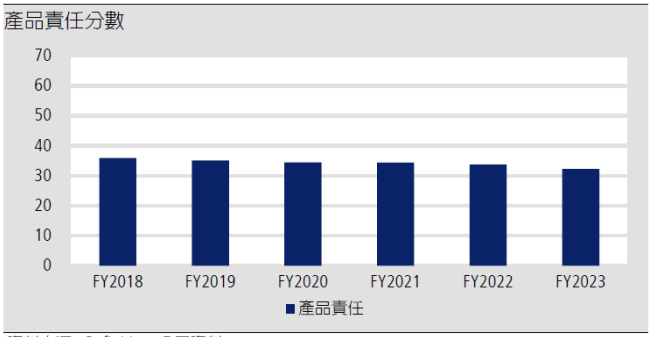
資料來源：Refinitiv、公司資料

圖 39：Zscaler – 勞動力



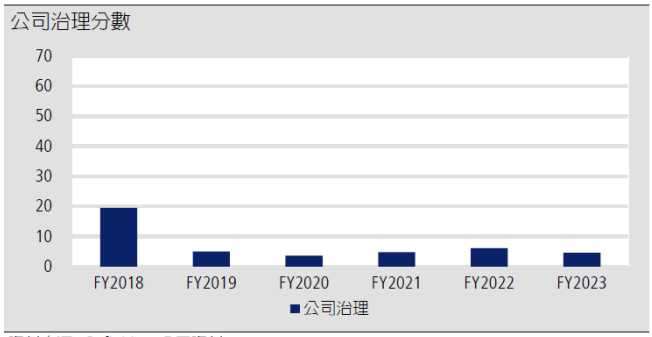
資料來源：Refinitiv、公司資料

圖 40：Zscaler – 產品責任



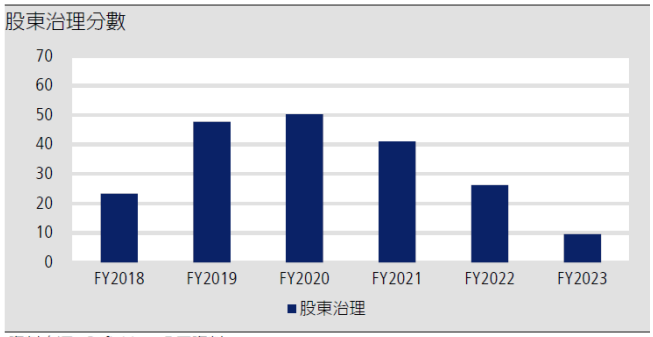
資料來源：Refinitiv、公司資料

圖 41：Zscaler – 公司治理



資料來源：Refinitiv、公司資料

圖 42：Zscaler – 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。