jamf

資安缺口持續擴大。本文說明如何 填補這些漏洞。

混合辦公、行動裝置與進階威脅瓦解了傳統邊界防護。分層防禦是可行的解決方向。

傳統方案失效原因

網路邊界已不復存在，但安全風險依舊存在。

設備數量變多 → **受攻擊面擴大**

移動屬性提升 → **管控難度上升**

環境複雜度提高 → **事件響應變緩**

雲端服務、遠距辦公、自攜設備（BYOD）與非可信網路，逐步瓦解傳統工具原本要守護的網路邊界。

威脅態勢

現階段威脅技術精密、類型融合且攻擊持續不斷。

逾 1 億筆

客戶資料在近年度資安外洩事件中遭竊

21 億次

2023 年存在已知漏洞的檔案下載紀錄

2500 萬美元

鎖定財務長之深度偽造攻擊所致損失

超過 90%

的現今攻擊以竊取資料為目標，而非加密勒索

主要威脅類別

社交工程與網路釣魚

郵件釣魚、定向釣魚、高層釣魚、簡訊釣魚、語音釣魚、QR 碼釣魚，以及偽飛航模式、偽鎖機模式等新型手法

國家級攻擊/APT 攻擊

90% 的警示來自關鍵基礎設施外部。主要目標：教育、政府及智庫。單起事件平均損失 160 萬美元

供應鏈攻擊

2023 年攻擊數量增至三倍，透過合作夥伴與供應商作為間接入侵管道

行動裝置威脅

43% 遭入侵裝置被完全惡意利用（年增 187%）。80% 的網路釣魚網站鎖定行動裝置。新型行動惡意軟體數量成長 51%

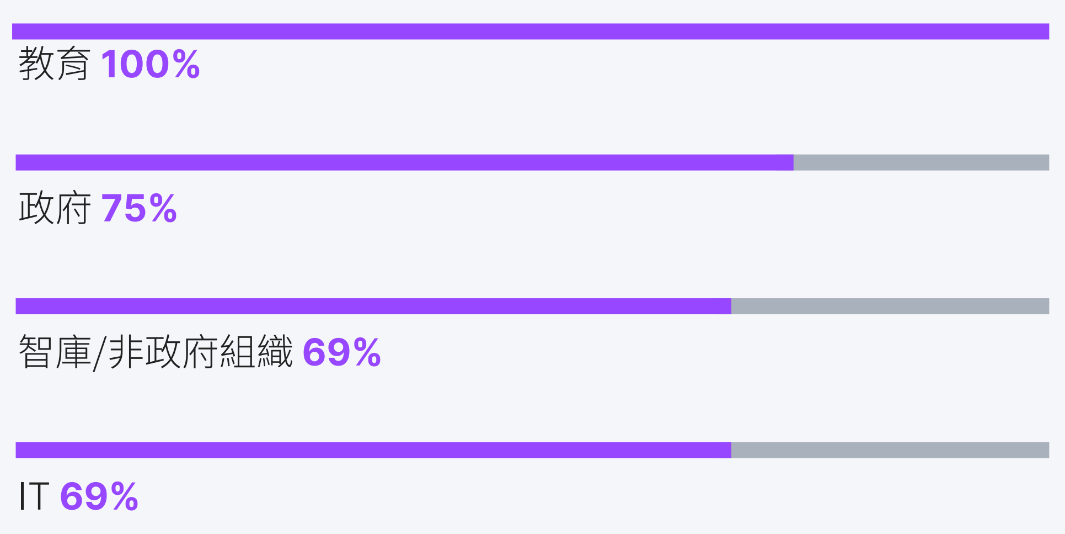
AI 強化型威脅

已觀察到 5 個 APT 組織運用 AI 強化攻擊能力

國家級威脅

定向攻擊相關數據。

主要受害產業



10 間機構有 9 間

認為自己遭到與國家相關的威脅行為者鎖定

160 萬美元

單起國家級攻擊事件的平均損失

為何單一方案無法適用全場景

裝置生態已然改變。

過去為固定辦公室桌面電腦打造的傳統解決方案，無法為現今動態、多裝置環境提供資安防護。

25%

macOS 在美國的市場佔有率

96%

的資訊長預期 Mac 裝置保有量在 12 至 24 個月內成長

3.6

2023 年全球每位使用者平均持有裝置數

96%

企業網路中的行動裝置為個人自有設備

行動裝置：未受控管的風險

行動裝置形同無人看守的前門。

使用者平均每人持有 3.6 台裝置。單人對應的攻擊入口因此增至 4 倍，多數缺乏專屬端點防護機制。

43%

遭入侵裝置被完全惡意利用（年增 187%）

80%

的網路釣魚網站鎖定行動裝置

51%

新型行動惡意軟體成長幅度（樣本數逾 92 萬）

96%

企業網路中的行動裝置為個人自有設備

策略架構

填補資安缺口的四個 C 原則。

1. **一致性管控（Consistency）**
不區分裝置類型、外觀規格、作業系統與持有模式，對所有端點採取統一管理標準。

2. **法規遵循（Compliance）**
建立基準規範、監控異常偏離，並透過遙測數據留存可供稽核的佐證資料。

3. **資源整合（Consolidation）**
將 IT 與資安整合為一體，打破部門藩籬、共享威脅情資並統一作業流程。

4. **成本優化（Cost Savings）**
透過原生工具、自動化、流程精簡以及自攜設備（BYOD）方案實現投資報酬率（ROI）提升。

分層資安防護架構

深度防禦＝透過多層防護攔截單一層遺漏的威脅。

若威脅突破單層防護，後續層級可阻擋入侵；三大基礎模組整合後，為整體基礎設施建構補強防線。

裝置管理

批量部署組態、強制執行政策並維持全域管控能力

身分識別與存取管理

授予受保護資源存取權限前，完成使用者與裝置驗證

端點資安防護

即時偵測並處理所有裝置上出現的威脅

管理 ＋ 身分識別 ＋ 資安 → **深度防禦**

關鍵技術

各防護層的實務運作方式。

零接觸部署

裝置自首次開機即處於安全防護狀態。配置、App 與政策於設定期間自動部署，全面支援企業與自攜設備（BYOD）。

威脅搜捕

透過基準規範、遙測資料和自動化修復工作流程，主動偵測未知威脅。

ZTNA（零信任網路存取）

永不信任，始終驗證。以加密微通道、最小權限存取與常態健康檢查取代傳統 VPN。

進階威脅應對

IoC/IoA 分析、時間軸建構及 APT 清除。調查時長由數周縮短至數分鐘。

落地成效

方案帶來的實質價值。

全裝置防護等級
提升

威脅偵測與應對
速度加快

營運負擔
降低

全環境資安規範
一致化

深入瞭解可於組織內建構整合式分層資安防護的完整架構。

下載白皮書

jamf

www.jamf.com/zh-tw/