jamf

Mac 管理的頂尖資安最佳實務

介紹

隨著企業營運模式不斷演進、資安需求持續提升，以及員工可選擇的裝置越來越多元，大型企業**導入 Mac** 的比例已成長到 76%。根據 Computerworld 的研究顯示，「有九成的 IT 專業人員肯定 Mac、iPhone 與 iPad 在職場上的商業價值」。這對員工與企業來說，都是好消息！當企業提供更多元的技術選擇時，員工就能使用自己最熟悉、最順手的硬體與軟體工作，發揮最高生產力。

從 IT 與資安團隊的角度來看，任何變動都會帶來變數，若沒有妥善管理，就可能 演變成風險。好消息是，企業可以透過主動式、縱深防禦的策略來降低 macOS 特有的風險，整合行動裝置管理、身分識別與存取，以及端點安全的完整解決方案，全面保護整個基礎架構中的裝置、資料與使用者，因應不斷演變的威脅環境（下一節會進一步說明）。

整合解決方案後，就能實施更細緻的資安措施，維持端點健康狀態的基準水準。這不僅能確保法規遵循，也能讓員工保持高生產力，同時釋放 IT 人力，打造更貼近業務需求的工作流程。本白皮書將說明以下關鍵資安實務：

- 修補與更新管理
- 威脅偵測與事件回應
- 資料保護與加密
- 網路與應用程式安全

Mac 管理與資安的基礎

在進入資安實務檢查清單之前，先了解為什麼建立穩固的基礎對於打造 Mac 管理流程與工作流程如此關鍵。例如，若可擴充的解決方案無法在當天就支援最新修補程式，將會同時削弱裝置與整體組織的資安防護能力。這通常是因為開發商延遲支援最新 macOS 版本，或對關鍵功能的支援不足所導致。

行動裝置管理 (MDM)

在 **2024** 年，macOS 在前 50 大 CVE（常見漏洞與曝險）產品中排名第 9，共發現 508 個獨立漏洞，是榜單中相當顯眼的一項。截至 2025 年 5 月，macOS 已攀升至前 10 名中的第 2 名，累計 **243 個獨立 CVE**，接近 2024 年總數的一半。請注意，這個排名會隨著時間推移而變動，CVE 的數量與名次也可能持續 調整。

這再次強調，保持作業系統與應用程式在最新狀態對裝置來說相當重要。像宣告式裝置管理（DDM）這類現代化功能，能讓裝置自動套用設定，並即時回報狀態變更。這不僅能降低 MDM 的負擔，同時提升更新速度與可靠性，IT 團隊也能即時掌握關鍵狀態 變化。

MDM 不只負責修補管理，它在簡化作業流程、提升決策效率，以及集中管理 Mac 各項關鍵功能方面，同樣不可或缺。以下功能正好說明了 MDM 作為基礎架構 的重要性：

- 部署安全設定與 組態
- 安裝受管理的應用程式
- 執行以政策為基礎的法規 遵循控管
- 維護最新的資產清冊

身份識別與存取

資料保護與確保員工能存取所需資源看似是兩件事，但其實背後的共同關鍵是：權限控管。 根據 **Verizon《2024 資料外洩調查報告》** 指出，「68% 的資安事件都與人為因素有關」。這個數據不包含惡意內部人員，而是聚焦於權限設定錯誤（最小權限原則未落實）以及終端使用者在存取憑證上的操作失誤。

從資安角度來看，這並不是靠要求員工上資安教育訓練、學會辨識威脅就能解決的問題。企業需要超越「只啟用雲端身分」的解決方案，才能真正因應這些資安挑戰。例如 導入：

- 具風險感知能力的存取政策，阻擋已遭入侵的裝置與 帳號
- 智慧型分流通道，在加密企業流量的同時，兼顧非企業 流量的使用者隱私
- 多重要素驗證（MFA），確保存取資源前完成身分驗證

端點安全

在 2024 年，**針對 macOS 的惡意程式**約占全球惡意程式偵測量的 11%。雖然比例不及其他平台，但 IT 與資安團隊絕不能輕忽這個趨勢。相較兩年前，這個數字已成長超過一倍，加上惡意程式即服務（MaaS）與 AI 驅動的進階惡意程式，攻擊者對 Mac 的鎖定**明顯增加**，資訊竊取型惡意程式的攻擊 活動也大幅成長。

除了試圖繞過 macOS 程式碼簽章保護的木馬程式與 APT 攻擊之外，防範惡意程式已成為對抗演進中威脅環境的關鍵任務。此外，還有其他關鍵控管措施，能維持裝置與組織的資安防護態勢。例如：

- 透過行為分析辨識未知威脅
- 將可疑應用程式與偵測到的威脅隔離並移除
- 主動監控、警示並回報完整的裝置健康資料（遙測）
- 過濾高風險網頁內容，例如零時差釣魚網址

Mac 管理的頂尖資安最佳實務

本節內容涵蓋範圍廣，因此我們將以檢查清單的方式呈現最重要的資安實務。這樣的呈現方式，讓 IT 與資安團隊能彈性取得實作所需的所有關鍵資訊。這個格式讓 IT 領導層能清楚掌握重點，並將內容依三大基礎解決方案整合後，拆解成七大類別，一目了然。

裝置註冊與佈署

- 透過 MDM 註冊實現安全的零接觸裝置佈署
- 自動化系統設定流程，包含受管理應用程式與設定檔佈署
- 在公司裝置與自攜裝置（BYOD）之間，一致落實企業標準與資安政策

裝置端保護與合規檢查

- 強化 macOS 資安設定（FileVault、Gatekeeper、XProtect）
- 透過客製化分析，在裝置端與網路層打造專屬的威脅防護策略
- 產生資安設定指引，依產業框架與標準建立客製化安全基準，讓端點達到所需的合規等級

身分識別與存取管理（IAM）

- 建立角色型存取控制（RBAC），落實最小權限原則
- 透過 SSO 與無密碼驗證，降低帳密風險
- 以零信任架構 驗證裝置與身分憑證的健康狀態

修補與更新管理

- 自動化 OS 與應用程式更新流程，降低已知漏洞風險
- 即時追蹤遙測資料，並安全地與整合解決方案共享
- 當偵測到不合規時，透過自動化、以政策為基礎的修復流程確保持續合規

威脅偵測與事件回應

- 運用機器學習自動化蒐集與分析威脅情報，並提供資料導向的建議與決策指引
- 透過無縫整合的 EDR 工具快速處理資安事件
- 結合 AI 與政策型工作流程，加速威脅獵捕並自動化修復

資料保護與加密

- 強制啟用 FileVault 加密，並安全地在裝置紀錄中儲存與更新復原金鑰，自動化金鑰管理
- 將零信任網路存取（ZTNA）全面延伸到整個基礎架構，在存取受保護的企業 資源前，先驗證裝置與身分憑證狀態
- 透過資料外洩防護（DLP），確保資料只儲存在受保護的磁區，並限制未授權的分享與複製行為

網路與應用程式安全

- 為所有網路連線啟用持續加密，並集中管理防火牆政策，確保整體網路安全
- 管理第三方應用程式權限與 macOS 資安基準設定
- 將每個資源請求透過獨立的微型通道進行傳輸，分段網路流量，防範中間人攻擊等網路型威脅

Jamf 成效實證！來自第一線的實際成果

透過縮短裝置佈署時間提升效率

「與手動 佈署相比，我們每台筆電至少省下一整天的時間。」

— 數位簽章與文件自動化平台產品負責人

大規模導入 Mac 的企業，已**明顯看到效率提升**與資安防護 能力的強化。

專注創新，而不是重複性工作

「現在每台裝置只要花 10 分鐘，真的省下非常多時間。」

— 財務管理與會計 平台 IT 經理

展現**透過自動化、零接觸佈署流程所帶來的實際時間節省與資源最佳化**成果。

透過完整的風險控管，兼顧資料安全與使用者生產力

「即時威脅偵測、合規監控與集中式政策控管，在保護資產與確保法規 遵循方面發揮了關鍵作用。」

— 數位公共圖書館 IT 經理

運用 **Mac 管理強化資安**與法規遵循，突顯即時威脅偵測與集中式政策控管的價值。

在整個裝置生命週期中落實組織合規要求

「這套架構不僅符合，還支援 SOC 2 Type II、ISO 與 HIPAA 等嚴格標準的合規要求。這也展現了 Jamf 強化組織資安並確保關鍵產業法規遵循的能力。」

— 數位健康公司 IT 資深經理

主動提升合規基準的一致性，並依產業公認標準與框架**建立安全基準**設定。

總結

隨著企業導入 Mac 的比例持續成長，組織必須優先採用主動且整合式的方式來管理與保護 Mac 裝置群。在威脅環境不斷演進、混合與遠距工作型態日益複雜的情況下，一套聚焦明確、能與業務目標對齊，同時具備彈性的資安策略，將帶來極大的價值。

這不只是套用一套「一體適用」的方案就能解決。

而是需要一套多層式解決方案，在裝置與應用程式生命週期的每個階段都原生支援 Mac。從建立行動裝置管理（MDM）、身分識別與存取管理（IAM）與端點安全的穩固基礎開始。接著，企業就能安心支援使用者選擇，而不必在資安與隱私之間做痛苦的取捨。

簡單來說：

- **裝置符合規範**
- **資料安全無虞**
- **使用者受到保護**

本白皮書說明了維持端點完整性與確保法規遵循所需的關鍵資安實務。這讓 資安團隊能快速回應威脅，也讓 IT 團隊專注於創新，同時提供高品質支援。同時，員工能在不中斷 工作流程的情況下，發揮最高生產力。

當解決方案無縫整合運作，企業就能打造安全且可擴充的 Mac 生態系，與 Windows 並行運作，在任何工作環境中兼顧生產力、易用性與防護力，為創新與韌性鋪路。

重點總結

企業導入 Mac 的比例成長 **76%**，主因是員工選擇與生產力提升的 效益。

在資訊竊取型與 AI 驅動 惡意程式威脅攀升的情況下，macOS 端點安全比以往任何時候都更關鍵。

九成 IT 專業人員認同 Apple 裝置在職場上的商業價值。

零信任架構與自動化在維持合規、偵測威脅與縮短回應時間上扮演關鍵角色。

整合基礎解決方案可實現自動化，並在最小影響使用者的情況下簡化合規流程。

68% 的資安事件涉及人為因素，使權限與存取控管成為首要重點。

完整解決方案必須包含 MDM、IAM 與端點安全。

IT 與資安團隊必須因應 Mac 帶來的新變數，透過整合式、縱深防禦策略降低風險。

整合式的 Mac 資安策略，讓企業能在安全無虞的前提下擴大規模並最大化使用者生產力。

縱深防禦策略是降低 企業內 macOS 特有風險的關鍵。

jamf

www.jamf.com/zh-tw/

縱深防禦策略是降低企業內 macOS 風險的關鍵。