# Mac 資安核對清單

隨著 Mac 裝置於各組織內的角色日益重要，IT 主管必須保護從裝置到其所存取資料的每一層安全，同時使資安策略與業務目標一致。

## 裝置管理

- 使用 MDM 解決方案強制執行資安政策
- 部署安全組態與裝置設定
- 安裝受管理的應用程式與設定
- 建立固定的軟體更新週期
- 追蹤裝置庫存與使用者指派狀況

## 端點防護

- 安裝端點資安軟體
- 即時監控端點狀態
- 防禦網路內與裝置上的威脅
- 運用 AI/ML 快速回應資安事件與未知威脅
- 將完整遙測資料串流至 SIEM 解決方案進行分析

## 使用者身分認證

- 將身分及存取管理整合至資安架構中
- 在整體基礎架構中全面執行高強度密碼政策
- 要求多因素認證，為資料提供額外保護
- 透過加密所有網路連線資料維持資料完整性
- 在授權存取企業資源前，透過 ZTNA 驗證裝置與憑證狀態

## 合規標準

- 符合產業標準與框架
- 建立符合可接受風險容忍度的客製化基準
- 執行資安政策以確保合規
- 定期執行稽核以評估資安狀況
- 透過反覆回饋持續優化流程

## 其他注意事項

- 多層防護提供多重安全機制，降低整體資安架構的風險
- 與整合式解決方案安全共享完整遙測資料，實現進階工作流程
- 自動化任務以提升效率並降低人為錯誤
- 導入 SSO 與無密碼身分認證，同步強化資安與使用者體驗
- 將防護延伸至公司自有裝置與自帶裝置（BYO），確保不同擁有模式下的資料安全具備同等標準

主動整合式 Mac 資安方案可保護裝置與資料，同時提升組織整體效率與生產力。

jamf

立即開始建置更堅固的資安基礎。

取得《頂級資安實務指南》

www.jamf.com/zh-tw/