jamf

檢查清單：找出資安防護的缺口

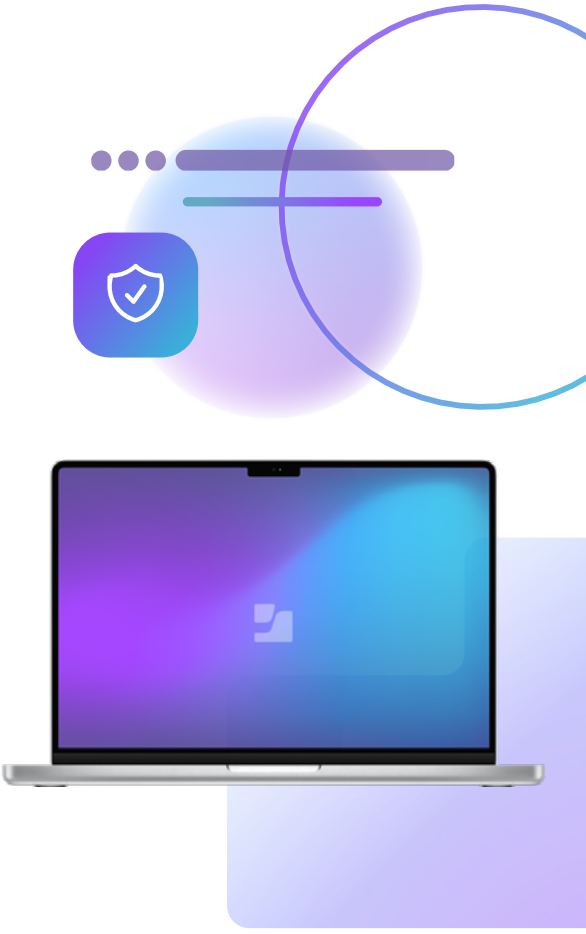
給管理 Mac 的 IT 管理員和 SecOps 團隊的一份簡短指南

工程師、行銷團隊、主管、創意工作者等等，都已經很習慣在工作中使用 Mac。Mac 的受歡迎程度持續上升：2025 年第 2 季相較 2024 年同期成長了 21.4% ，比所有其他電腦品牌都高。

其實這也什麼好意外的。畢竟，**員工就是喜歡用 Mac 工**作。Mac 在企業中的成長代表更多員工能使用自己偏好的裝置，也提升了滿意度和工作效率。 但這對 IT 和資安團隊來說代表什麼？

Mac 和 Windows PC 本來就不一樣。它們的作業系統、硬體策略、架構和設計理念都不相同。這也代表它們的資安維護方式也完全不同。主要管理 Windows 的 IT 管理員，可能會在面對大量 Mac 裝置時發現原本的策略有缺口。因為 Mac 的硬體與軟體都是 Apple 自家打造，管理員需要能夠理解並整合 Apple 生態系的工具。

在這份檢查清單中，我們會簡單介紹 Mac 特有的資安策略，幫你找出可能的防護缺口。我們會從佈署、身分與存取、端點防護以及法規遵循來逐一說明，並提供專門給 IT 與資安人員使用的檢查項目。



想更深入瞭解嗎？請參考我們的白皮書：

《多層式防禦：透過整合與分層方式補上資安缺口》

IT 管理員的資安缺口檢查清單

零接觸佈署與裝置設定

該考慮的面向：

- 將 Apple 商務管理與你的行動裝置管理（MDM）平台串接使用
- 透過自動化裝置註冊來設定相關承載資料與限制規範
- 在 Mac 進入設定輔助程式前強制要求最低 OS 版本

使用者驗證與身分識別供應商整合

該考慮的面向：

- 將平台級 SSO 與你的身分識別供應商（IdP）及 MDM 整合
- 使用支援可延伸單一登入（Extensible Single Sign-on）設定的 MDM
- 在初次登入後，對更高權限的操作再要求一次驗證

推送 Apple OS 更新

該考慮的面向：

- 推送自動更新與年度重大版本升級 —— 運作節奏和 Windows 裝置完全不同
- 確保管理與資安廠商都有針對最新 macOS 做相容性測試（尤其是重大版本的 beta 測試）
- 在不影響使用者工作的情況下發佈快速安全回應（Rapid Security Responses）

有32% 的企業 至少有一台裝置存在嚴重且可修補的漏洞

360 報告

SecOps 的資安缺口檢查清單

與法規與框架的符合程度

該考慮的面向：

- 透過整合 **macOS Security Compliance Project**（mSCP）來自動化裝置強化流程
- 支援像 **CIS Level 1 / Level 2** 或 **NIST 800-171 這類基準與標準**
- 在所有 Mac 上套用、維護並自動化管理設定，以確保特定的資安控制得以落實

將 macOS 的遙測資料串流到既有的 SIEM／SOAR 系統

該考慮的面向：

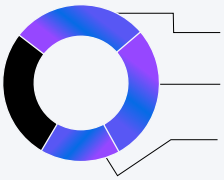
- 使用能直接從端點安全 API 擷取遙測資料的工具
- 將 macOS 的遙測資料映射到現有 SIEM 的資料模型
- 使用能將遙測資料轉成可立即使用資訊的工具
- 即時分析 macOS 安全事件，例如 Gatekeeper 被繞過、或 XProtect 偵測惡意程式的情況

專為 Mac 特有威脅設計的端點防護

該考慮的面向：

- 專為 Mac 打造的防護工具，可攔截已知威脅、新型威脅，甚至是零時差攻擊。
- 善用 macOS 內建的 XProtect、Gatekeeper、Notarization 等功能，實作即時端點防護
- 參考最新研究，針對 Mac 特有惡意程式進行威脅獵捕

最常見的 Mac 惡意程式：

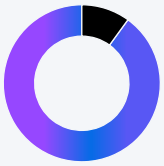


資訊竊取器（Infostealers） **28.36%**

廣告軟體（Adware） **28.13%**

木馬程式（Trojans） **16.61%**

360 報告



超過 **90% 的網路攻擊**來自 釣魚攻擊。

360 報告

應用程式的安裝與監控

該考慮的面向：

- 使用工具確保環境內的第三方 macOS 軟體都保持最新版本
- Mac App 的版本與使用情況報告
- 透過受管控的帳號與開發者憑證來管理 App 的發佈來源

確保使用者與裝置存取公司資源的方式安全可控

該考慮的面向：

- 運用 Apple 的 Network Relay 等技術來 打造零信任網路存取（Zero Trust Network Access）
- 透過 Secure Enclave 提供的硬體級裝置驗證來支援條件式存取政策
- 建立專為 macOS 平台設計的零信任模型

這份檢查清單能協助你開始打造多層式防禦的完整架構。

jamf

想更深入了解嗎？
請參考我們的白皮書。

www.jamf.com/zh-tw/