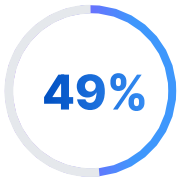
為什麼選擇 Jamf for Mac

企業 IT 領導者的任務是要盡量減少裝置停機時間，確保終端使用者工作順利又開心，同時降低風險與抵禦各種網路威脅。

隨著越來越多員工選擇使用 Mac，IT 團隊需要在既定預算下，提供無縫體驗與企業等級的資安防護，兩者缺一不可。這就是 Jamf 的用武之地。

IT 團隊花太多時間在日常瑣碎的 IT 任務上。

現代 IT 環境講求效率，但老舊流程、工具不整合、 缺乏即時資料，讓團隊只能耗費時間拼湊解法。這樣的模式難以擴展。



的組織表示他們在需要時無法即時取得關鍵資訊。[1]

若無法清楚了解各個裝置的狀態，IT 團隊只能靠臨時解法與人工 API 呼叫來拼湊資料，才能產出最基本的報表。缺乏即時資料，更會讓裝置資安面臨更高風險。

的 IT 領導者表示，系統整合困難會拖慢數位 轉型的腳步。[2]

沒有清楚的技術文件、原生整合機制或政策框架，IT 團隊就得花很多時間想辦法讓各種工具彼此協同運作，耗時又沒效率。

的 Mac 裝置未啟用 FileVault 。[3]

的 Mac 裝置未啟用防火牆 。[3]

IT 團隊還得花太多時間手動加強與修補裝置，以符合資安合規標準。其他廠商雖然提供合規樣板，但內容不完整，或是不符合 macOS 安全性合規專案（Security Compliance Project）的基準。結果讓 IT 團隊工作更繁重。

每 年 Apple 裝置的風險暴露程度都在逐漸上升。

Mac 在企業中越來越受歡迎，對 IT 團隊來說是種成就，但同時也吸引了駭客投入更多資源，因為他們覺得破解 Apple 裝置現在「值得一試」。

如果缺乏針對 Apple 威脅的防護，風險就只會越來越高。如果遙測資料中沒有 Mac 專屬的事件資料 （例如 Gatekeeper 與 XProtect），那就只能等到攻擊者觸發其他資安控制項，才會發現威脅。大多數資安廠商沒有專責的 Apple 威脅獵捕團隊，因此難以跟上攻擊手法的演變。

如果未遵守資料保護規定的話，平均需付出的代價為1,480 萬美元。[2]

缺乏詳細記錄與稽核軌跡，會讓稽核準備不足。不過若能整合 SIEM 系統，就能補足這塊缺口，實現真正的資安全視圖。

有 39% 的組織至少有一台裝置存在已知漏洞；[3] 若無法掌握 CVE 清單，又缺乏 自動化的軟體修補流程，就容易讓裝置暴露在漏洞風險中 。

300

Jamf Threat Labs目前追蹤超過300 種 macOS 惡意程式 。[3]

21

光是2023 年，Jamf 威脅實驗室就發現了 21 種新的 macOS 惡意程式家 族。[3]

1,480 萬美元

如果未遵守資料保護規定的話，平均需付出的代價為 1,480 萬美元。[2]

的企業至少有一台裝置存在已知漏洞。[3]

所以，為什麼你該選擇Jamf for Mac？

Jamf 與各種 IT 架構能無縫整合，[4]讓 IT 團隊與終端使用者的生產效率比其他競爭對手高出兩倍。 這讓團隊能大幅減少資料彙整、裝置停機、一線支援與人工作業所需的時間。

我們的資安解決方案能有效降低 Apple 裝置風險，整體效能是其他產品的 2 到 3 倍，涵蓋範圍包含：降低 Apple 專屬威脅、加快回應速度、減少漏洞風險，以及強化合規能力。

我們之所以能達成這樣的成果，是因為我們提供了：

- 由 Apple 專責威脅獵捕團隊執行的多面向即時威脅監控
- 完整的裝置清單盤點、報告產出、記錄與稽核功能
- 豐富的 IT 與資安系統預建整合
- 強大的政策架構，支援自動化即時執行與使用者自助服務功能
- 自動化應用程式擷取、驗證、重新打包與部署

我們強大的支援與服務團隊，在業界有口皆碑。我們還有 Jamf Nation —— 全球最大的 Apple 管理員社群，成員之間會互相分享經驗與專業。

「Julie（技術支援工程師）的支援非常到位， 讓我更加確信自己選擇 Jamf 來管理 Mac 是正確的 決定。我 也能很有信心地告訴管理團隊：Jamf 是 值得 信賴的選擇。」

—— 政府機構 IT 分析師

Jamf 的生產力效益勝過其他方案。

Jamf 勝出的理由包括：

- 裝置停機時間更短
- IT 作業效率顯著提升
- 減少對終端使用者提供一對一支援的需求
- 更完善的監控與可視化功能

更快完成部署流程

即時取得完整的裝置資訊，再加上自動化工作流程，大幅減少手動報表、稽核與流程管理的需求

以下是我們怎麼做到的：

- **自動化的入職工作流程，**根 據職位、部門、使用者與地點來設定裝置，大幅節省 IT 時間，也能讓新員工立即就位上工。
- **精準的目標對象設定** 可自動處理疑難排解、裝置加固與軟體更新，節省 IT 和使用者的時間。
- **Tier one 支援**延伸到基本使用之外，讓使用者也能透過 Self Service 自行安裝需要的生產力應用程式。

Jamf 在降低資安風險方面也領先其他廠商。

Jamf 擁有強大的政策架構，能涵蓋裝置管理、依據政策執行腳本，以及網路控管等功能。我們的資安團隊具備專業行為分析能力，能主動 阻擋針對 Apple 的攻擊手法。

透過 Jamf，IT 負責人可以做到以下幾點：

- 即時阻擋已知與未知（zero-day）的 Apple 威脅。
- 快速回應資安風險，精準執行修補作業。
- 透過 CVE 報告與 自動化更新機制，減少未修補漏洞。
- 內建 Apple 專用的安全連線機制，能依據更多風險資料點進行動態評估，降低資料外洩 的機率。
- 透過與 macOS Security Compliance Project 整合，讓裝置加固流程自動化，不但能避免人為錯誤，也能藉由完整的日誌與稽核紀錄強化查核準備度。

---

1. 《自動化：趨勢、挑戰與最佳實務》（Automation: Trends, Challenges and Best Practices），IDC，2023 年
2. 《IT 現況報告》（State of IT Report）第三版，Salesforce
3. 《Jamf Security 360：年度趨勢報告 2024》，Jamf，2024 年
4. 9.《提升投資報酬率：打造 Apple 企業管理最佳解方》（Driving ROI: The Case for a Proven Apple Enterprise Management Solution），Jamf 白皮書，2021 年

Jamf 是你正確的選擇。但也不要只聽我們的片面之詞。

G2 評論：

「Jamf Pro 仍然是 **Apple Mac 最頂尖的行動裝置管理解決方案。**」

「各大廠商提供大量支援，Jamf 幾乎總是被明確寫進廠商文件 中，因為 它就是**Apple MDM 的首選產品。**」

jamf

立即體驗 Jamf