jamf

為第一線工作者打造更創新的科技

安全洞察到位，使用者體驗如你所期待。

超過 60% 無固定座位的員工表示，他們對目前使用的科技產品並不滿意，認為仍有改善空間。

麥肯錫公司（McKinsey & Company） 2022 年科技趨勢展望

採用行動優先策略，能讓不在辦公室的使用者（如航空、製造業與外勤人員）也能擁有更彈性、更高效的工作方式。這些策略不只保護組織與客戶的資料，同時也能改善第一線人員 的工作體驗。

行動與資安團隊在推動行動化時常會遇到以下挑戰：

- 如何在裝置與 App 的安全性與使用體驗之間取得平衡
- 依照使用者需求或裝置 用途進行客製化
- 取得裝置與 App 的洞察報告，便於掌握並降低風險
- 為生產力工具與 資源提供安全且經授權的存取方式
- 建立能強化營運 流程的裝置工作流程

如果使用體驗、生產力與安全性能彼此加成，那會是什麼樣的成果？

Jamf 讓這一切成為可能。

Jamf 提供行動與資安團隊所需的平台，包括裝置與 App 的洞察、條件式存取與裝置管理，同時維持良好的使用者體驗。透過 Jamf 的 App 與合作夥伴生態系，組織能在各種情境中落實行動優先策略，無論是 1:1 派發、共享裝置，或是管理不同裝置類型與作業系統的混合環境。

發揮行動力的最大潛能。

註冊裝置與使用者

將裝置與 App 的管理自動化並擴大規模，確保所有工作裝置隨時處於就緒且設定正確的狀態。透過預先建立的角色或裝置類型設定，在共享裝置上提供更貼近需求的 App 使用體驗。

執行可接受使用政策

在所有裝置上阻擋禁止或高風險內容，落實可接受使用政策。設定限制類別或網域，並在所有 App 與瀏覽器中套用過濾規則。

建立行動基準設定

建立安全基準、驗證裝置是否合規並防禦進階威脅，同時符合 CIS Benchmarks、NIST、AC 91-78A、CMMC 等標準。

管控行動流量使用

管理行動裝置的數據流量，避免使用者在國內或漫遊時使用過量流量。有效控管成本，避免意外超量。

管理 App 與作業系統風險

自動更新過時或具風險的 App 與作業系統版本。監控漏洞、風險行為與 CVE，並封鎖或隱藏未授權或側載的 App。

安全地讓使用者連上應用程式

確保只有受信任的使用者，且裝置經核准，才能存取工作資源。Jamf 採用風險感知存取政策與依 App 建立連線，以零信任方式讓員工安全存取完成工作所需的 App 與資料。

網路威脅防禦

透過 Jamf 的機器學習引擎 MI:RIAM 即時保護使用者與裝置，在威脅造成影響前就阻擋釣魚攻擊、挖礦程式與惡意網域。

關鍵產業專業能力

Jamf 與頂尖製造業、安全帽產業、航空、零售與醫療機構合作，在多元情境中支援 Apple 裝置的導入與管理。我們的 Apple 專家會提供量身建議，協助你找到最合適的解決方案。

jamf

www.jamf.com/zh-tw/

申請試用 現在就和 Jamf 專業人員聊聊。

或者聯絡你偏好的經銷商