



採購指南： Enterprise Mobility

發掘行動裝置的無限可能

行動辦公的使用者正面臨越來越多樣化的資安威脅。

想讓行動裝置部署順利，就得掌握詳細資訊、保障應用程式存取安全，還要確保裝置能滿足使用者與企業雙方的需求。

不論是第一線人員還是辦公室員工，大家越來越仰賴行動裝置來完成工作。保護行動裝置的安全並不簡單，尤其是現在使用者面對的攻擊方式越來越多，裝置的使用情境也愈來愈複雜。現在的企業必須提供讓使用者喜歡的體驗，同時解鎖全新的工作流程與生產力。

完善的行動安全計畫應包含：

防堵行動裝置上的網路釣魚攻擊



行動裝置上發生網路釣魚的機率，比其他裝置高出 **50%**

阻擋各種
攻擊

實施可接受
使用策略
(AUP)

把裝置和使用者納入工作流程裡

從漏洞管理到防惡意軟體，**避免應用程式的各種風險**

用進階的鑑識手法
偵測是否遭入侵

控管行動網路的使用量，
避免超量產生額外費用

建立基本的安全標準，
並確保符合合規要求

讓員工能安全地連上重
要的應用程式和工作系統

避免因設定錯誤
而造成資安風險

關鍵功能特色

這些功能能幫你發揮行動裝置的最大效益



安全配置管理

強化行動裝置

- 建立良好的安全習慣
- 執行合規性審計
- 監控配置漏洞

修補程式管理

- 透過詳細的漏洞報告，確保修補優先順序
- 修補作業系統與應用程式漏洞

資料遺失防護 (DLP)

- 監控商務資料在應用程式之間的流向
- 根據使用者或裝置狀態限制應用程式存取

可接受使用政策 (AUP)

- 透過動態分類政策限制網頁使用
- 根據使用者、群組、地區或全球政策來強制執行 AUP



攻擊預防

惡意軟體和其他應用程式風險

- 阻擋惡意軟體
- 識別存在安全風險的應用程式
- 預防應用程式內的敏感資料外洩
- 監控非官方應用程式商店的使用情況

中間人攻擊 (Adversary-in-the-Middle, AitM)

- 識別惡意熱點和協議攻擊
- 透過加密通道減少中間人攻擊風險

網路威脅

- 防範釣魚攻擊 (包括零時差攻擊)
- 阻擋惡意網路流量 (包含 C2 指令與資料竊取)
- 防止隱密挖礦、垃圾郵件及其他網路威脅



裝置管理

部署與註冊

- 把裝置直接寄到使用者或指定地點
- 支援各種裝置擁有模式的註冊方式
- 讓裝置、使用者和應用程式都能順利加入工作流程

設置與設定

- 自動化裝置管理工作，提升效率與規模
- 限制裝置用途，只能用在指定情境
- 套用政策來確保裝置符合資安要求

裝置清單報告

- 蒐集使用者、硬體、軟體與裝置安全相關的資料
- 自訂清單欄位，掌握裝置全貌

隨選內容管理

- 讓員工能自行申請、下載和更新核准的應用程式



自訂工作流程

支援共享裝置的使用流程

- 根據使用場景，自動佈署、個人化與重設裝置
- 讓使用者馬上能使用需要的企業應用程式
- 針對不同角色設定專屬的裝置體驗
- 讓第一線主管在不靠 IT 協助下就能提供基礎支援

夥伴整合與 API

- [Jamf Marketplace](#) 提供現成的解決方案與整合工具
- 支援醫療、零售、工地與航空產業的主要廠商
- 整合電子病歷系統 (EHR/EMR)，簡化醫療裝置管理
- Jamf API 可讓企業把 Jamf 整合進任何平台或工作流程中



安全存取

保護資料傳輸

- 為關鍵商務應用程式與資料建立加密通道

審核關鍵應用程式使用情況

- 報告行動工作者存取的所有應用程式

執行即時存取政策

- 設立存取政策，包含使用者資訊與裝置安全性檢查



威脅偵測和應對

收集完整的遙測資料

- 蒐集詳細的日誌，供離線分析使用

異常偵測

- 啟用威脅搜尋與行為異常偵測，識別惡意活動
- 整合新的威脅情報與入侵指標（IoC），提升未來的偵測能力

修復威脅

- 當偵測到入侵時，阻止對關鍵應用程式與工作負載的存取
- 移除惡意軟體，讓使用者迅速恢復工作狀態



用 Jamf 達成零信任資安的目標

Jamf 協助企業保護其最重要的資產，確保只有授權使用者、已註冊裝置，且符合企業安全性要求的裝置，才能存取敏感的商務應用程式。



選行動資安功能前，要睜大眼睛

行動威脅環境與工作方式不斷演變，過去能防護的東西，不代表現在還有用。現在的工作方式，也不一定適合明天。挑選行動安全解決方案前，可以從這幾個面向來思考：

先了解每項方案的實際功能

別光看它宣稱有「行動安全」功能，要看它到底做得到什麼。確認其是否真正應對針對行動裝置的威脅，而不只是將電腦安全概念簡單套用到行動裝置上。

裝置管理為資安必須

單一安全解決方案可能無法滿足所有需求，安全軟體本身也不是萬能的。沒有可視性，就無法保護裝置。因此，裝置管理對於安全性至關重要，可確保裝置符合合規性並即時修復潛在問題。

使用者體驗十分重要。

員工之所以使用行動裝置，是因為行動性有助於提供工作效率。嚴重阻礙裝置功能的安全策略對使用者不僅沒有幫助，他們還可能會利用未經批准的解決方法來避免這些策略。

行動裝置已成為不可或缺的工作工具，使用者依賴它們來提高生產力。當裝置受到安全性政策影響時，建立工作流程以幫助使用者盡快恢復工作相當重要。

並非所有裝置都需要相同的安全工具。在部署工具和設定安全性政策前，應先考慮裝置的部署情境與使用個案。舉例來說：

- 請評估您的員工如何使用裝置。不同職務的員工所面臨的風險也不同，安全需求也就不盡相同。例如：
一般員工需要保護敏感資料與網路存取，應確保裝置合規，防範網路釣魚與惡意軟體攻擊，並透過內容過濾、威脅防禦與零信任網路存取（ZTNA）進一步強化安全性。
- 無辦公桌員工（如零售業）內容過濾和應用程式安全會有很大的幫助。畢竟如果裝置無法瀏覽網頁，落入網路釣魚陷阱的風險就較低。
- 高層主管與擁有機密資料存取權限的職員，通常是主要攻擊目標，他們需要額外的安全防護措施，還可能需要符合特定法規要求。



www.jamf.com/zh-tw/

© 2025 Jamf, LLC. 著作權所有，並保留一切權利

想用行動力改變您的工作模式嗎？
歡迎和我們的專員聊聊！