行動安全解決方案購買指南

確保所有端點都受到保護

行動辦公的使用者正面臨著不斷日新月異的威脅。

成功的行動裝置部署關鍵在於需要清晰 的可視性與果斷的行動。

越來越多員工使用行動裝置在辦公桌或公司辦公室以外的地方工作，防禦這些分散的現代端點可能是一項挑戰，尤其是當使用者面對新的威脅策略時。

網路威脅不僅限於電腦，行動裝置面臨的風險是 確實存在的。

- **40%** 的 企業行動裝置存在 已 知的安全漏洞。
- 使用 行動裝置的員工遭受網路 釣魚攻擊的可能性比筆記型電腦高出 **50%** 。
- **1%** 的行動工作者會受到惡意軟體的影響，而「進階持續性威脅（APT）」則能夠精準鎖定目標，對使用者發動攻擊。

這就是為什麼 **行動安全性** 對於保護行動工作者、裝置和資料至關重要。完善的行動安全計畫應包含：

- 預防 安全性 錯誤配置
- 阻擋攻擊
- 透過強大的鑑識分析與 事件回應來偵測裝置入侵

主要特點

那麼，您應該為行動裝置實施哪些安全性功能呢？

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

攻擊防禦

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

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

收集豐富的遙測資料

- 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

透過 Jamf 實現 Trusted Access。

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。

精心選擇行動安全性功能

行動威脅環境與工作方式不斷演變，昨日的安全防護不代表今日仍然有效。選擇行動安全解決方案時，請考量以下幾點：

評估解決方案能力

不要只看它是否聲稱具備「行動安全」功能，請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。

最先進的行動防護與連線解決方案，為您的企業提供完善的保護，確保行動機群的安全性與合規性。免費試用 Jamf 。