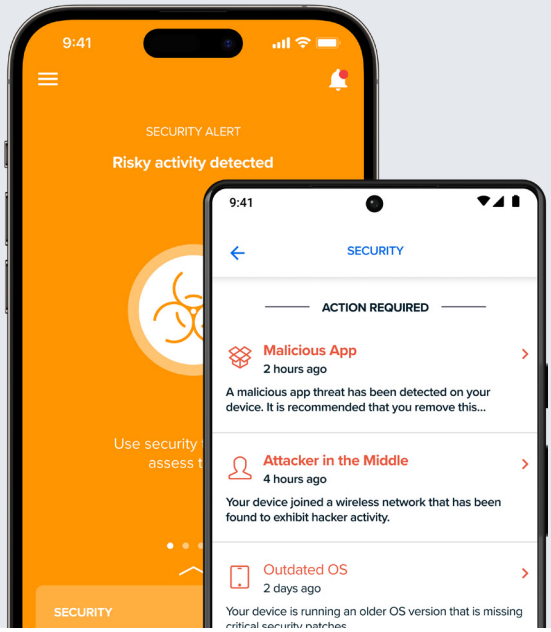
jamf

保護行動端點
免受現代威脅的侵害

預防網路攻擊、維持端點裝置合規性，
並識別及回應即時威脅。



現代員工適應混合與遠距辦公模式的速度出奇的迅速。

這樣更為靈活的工作模式，也代表著有更多的工作是在手機或平板上完成。行動裝置除了存有大量的工作與私人資料，另一個特性就是它時常都是連上網路的狀態，使得行動裝置成了十分適合攻擊人士下手的目標。行動裝置的體驗不像筆電或電腦，因此增加了使用者識別可疑攻擊的困難度，若沒有導入強化的保護機制，便無法妥善確保使用者與工作資料的安全。

Jamf Mobile Security 登場

這是一款專為行動裝置設計的安全解決方案，用以抵禦行動攻擊、強制執行可接受使用或流量限制政策，並提供裝置合規性的清晰可見性，同時針對任何應用程式提供即時條件式存取。保護所有工作中使用的行動裝置，無論是個人擁有的還是公司配發的，確保工作資源安全無虞。

化解任何棘手挑戰，確保行動裝置安全無虞

Jamf Protect 綜合多層安全機制，並藉由以下功能來確保使用者、端點設備及網路的安全：

行動端點防護
持續監測以建立不同的邊防關卡，確保行動裝置符合資安基準的要求。

網路釣魚防護
在裝置尚未被影響前，就搶先以先進的機器學習技術來即時阻擋新型或已知的釣魚攻擊、挖礦劫持攻擊以及惡意或不安全的域名。

網頁內容過濾
可依據網頁類型來選擇的內容過濾機制，讓你可以藉由導入 AUP 來預防使用者存取被禁止或不安全的內容。

越獄偵測
先進的掃描功能，可判斷行動裝置是否已被使用者或惡意行為者取得 root 權限或修改。

OS 漏洞回報
輕鬆回報在 macOS、iOS 及 iPadOS 上偵測到的資安漏洞。裝置上若搭載容易遭到攻擊的作業系統 (OS)，在回報時就會將該風險做升級處理。

App 風險監測
監測是否有側載 App、可疑的開發配置文件、惡意程式碼的跡象、不安全的動態行為或危險的權限設定。

公共 Wi-Fi 安全
防止攻擊者攔截網路流量，讓敏感的企業資料遠離風險。

傳輸網路威脅資料
將 iPhone、iPad 和 Android 裝置上的各種安全資料串流至 Jamf 或直接串流至 SIEM，藉此獲得更深層的資安可視性。

數據上限與報告
可管理行動裝置的行動數據用量，避免使用者在境內或漫遊時超出數據額度，藉此管控費用或預防產生額外的開支。

風險通報
透過完整的安全性資料來分析各裝置的風險評分，而這些評分也能協助你使用 Jamf Connect 或其他零信任存取 (ZTNA) 解決方案，做出更為妥當的零信任存取決策。

簡易部署
Jamf Trust 應用程式可通過 **Jamf Pro** 或任何現代行動裝置管理（MDM）解決方案進行部署與配置，，讓所有機構都能輕鬆享有完善的行動端點防護機制。

條件式存取將維持永遠啟用
Jamf Connect 採用風險感知存取政策與依循 App 的連線，使人員可透過零信任技術，存取高效作業所需的 App 和資料。

Jamf Protect 由 Jamf Threat Labs 提供支援，這個團隊由經歷豐富的資安威脅研究人員、網路安全專家以及資料科學家所組成，目標是探索未來資安威脅動向，並致力強化 Jamf 產品的防護能力

jamf

www.jamf.com/zh-tw/

Updated 01/2025.

立即預約試用以深入了解如何透過 Jamf Protect 來確保行動裝置的安全

或者聯絡你偏好的經銷商