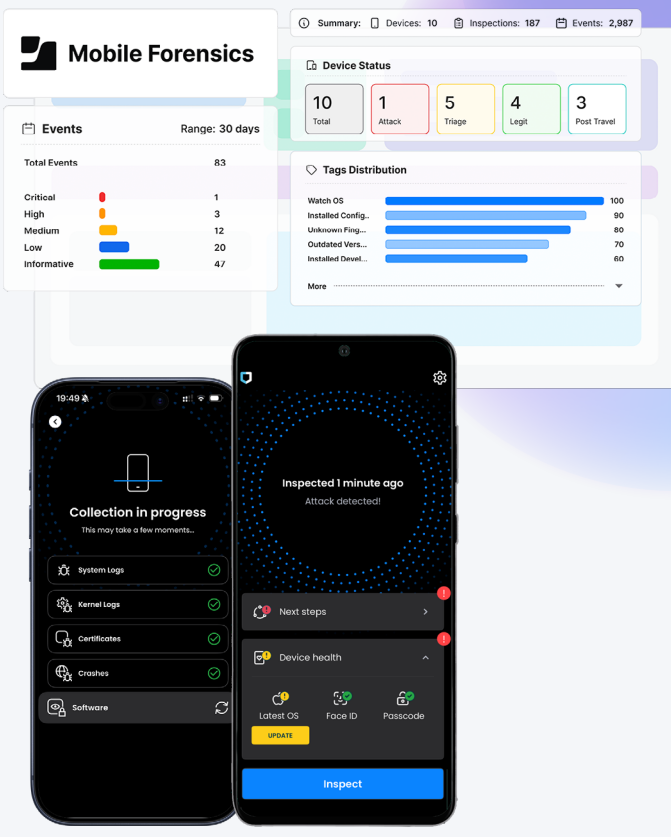
jamf

Jamf Mobile Forensics

保護行動裝置免受最精密複雜的攻擊。

高風險使用者 — 政府官員、企業主管、政治人物等 — **所面臨的威脅需要採取可行的防禦策略**。進階持續性威脅（APT）、傭兵間諜軟體、國家級攻擊以及零按一下利用，要求安全團隊在不干擾使用者、不部署侵入式代理程式或暴露個人識別資訊（PII）的情況下，持續分析裝置完整性並找出入侵指標（IOC）。

Jamf Mobile Forensics 為 Mobile Threat Defense 新增了進階防護層，協助安全團隊偵測並調查傳統工具可能遺漏的威脅。



☆ 主要優勢

- 在目標式攻擊和零時差進入網路前進行偵測
- 無需對裝置進行 Root 或越獄，即可分析深層系統、當機、核心與 App 記錄檔
- 簡化鑑識分析並減少人工研究
- 保護隱私權並確保高階使用者的裝置信賴度

將行動裝置鑑識分析的時間從數週縮短至數分鐘。

遠端數位鑑識與事件回應

減少停機時間並維持關鍵使用者的生產力

- 專有行為分析可偵測異常的裝置行為、零時差，以及 Pegasus、Predator 與其他間諜軟體的 IOC
- 透過探索裝置層級遙測，防止長時間的曝險
- 即時分析可讓安全團隊瞭解所需的步驟，並立即對進階攻擊做出回應

主動威脅狩獵

將複雜的安全資料轉化為具體可行的情報

- 全面的分析架構可強化威脅狩獵與情報能力
- 透過將事件時間軸、類型與嚴重程度歸納為單一事件，簡化調查工作流程
- 自動化事件時間軸，直接檢查裝置是如何及何時 遭到入侵的
- 透過分析檔案、App、程序、當機記錄檔等，偵測未知的 IOC

人工主導、AI 增強的分析

AI 分析可作為鑑識研究助理

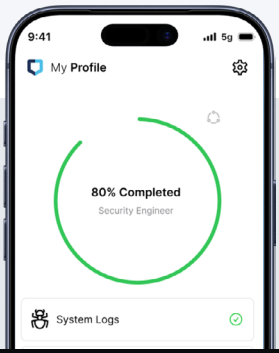
- 減少分析裝置當機和異常情況所需的人工研究
- 摘要事件並建議修復的後續步驟
- AI 分析預設為關閉，讓組織能保有對 AI 使用的控制權

*AI 分析為僅限雲端的功能。

隱私權優先設計的鑑識

為高階使用者提供全面保護，徹底解決所有隱私權與裝置完整性疑慮

- 不擷取 PII。分析不需存取密碼、相片、影片、訊息、聯絡人、通話歷史記錄、瀏覽器歷史記錄、雙重認證代號或 App 資料
- 遠端 DFIR App 會依組織設定的間隔執行靜默掃描，並提供使用者裝置安全資訊
- 此 App 可針對雲端與地端部署執行安全掃描



Jamf Mobile Forensics 由 **Jamf Threat Labs** 提供技術支援，我們的安全研究人員、分析師和工程師團隊致力於發佈行動惡意軟體與間諜軟體的研究，並開發和推動 Jamf Mobile Forensics 引擎的持續改進

jamf

www.jamf.com/zh-tw/

如需更多資訊，請聯繫您的 Jamf 通路代表。

或申請試用。