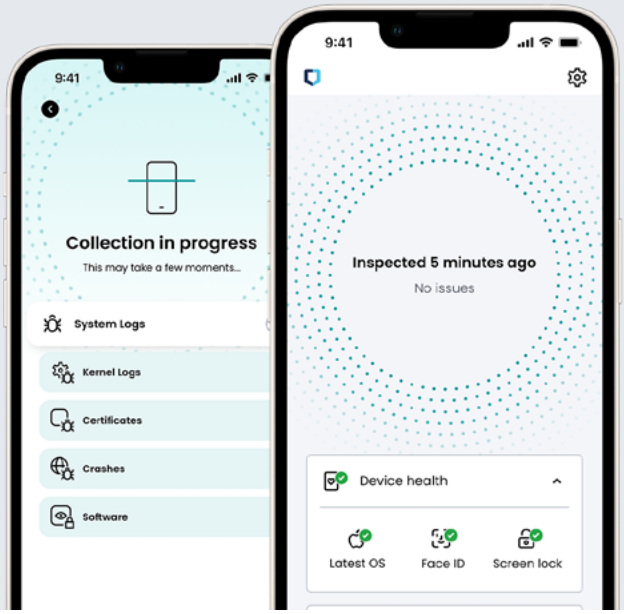
jamf

Jamf Executive Threat Protection

行動裝置上的攻擊，終於也能一覽無遺



行動裝置的應用場景非常多元，整天下來不論是工作還是私人任務皆適用，而遠端和混合辦公模式早已成為現在許多機構的常態。App 的誕生，使得電子郵件、會議等各種內容唾手可得。智慧型手機因為同時含有工作與私人資料，並且隨時都會與網路連線，這使得手機成了駭客理想的攻擊目標。

資安攻擊有多種形式，從企業 App、多重要素驗證 (MFA) 的請求到照片甚至是備忘錄，最危險的零點選、零日漏洞攻擊手法可遠端存取裝置上的所有內容。某些漏洞甚至可以悄悄地啟用網路攝影機和麥克風，因此能夠即時偵測裝置是否遭到入侵極為重要，若沒有配備適當的工具，則無法立刻採取行動來修正威脅。

Jamf Executive Threat Protection

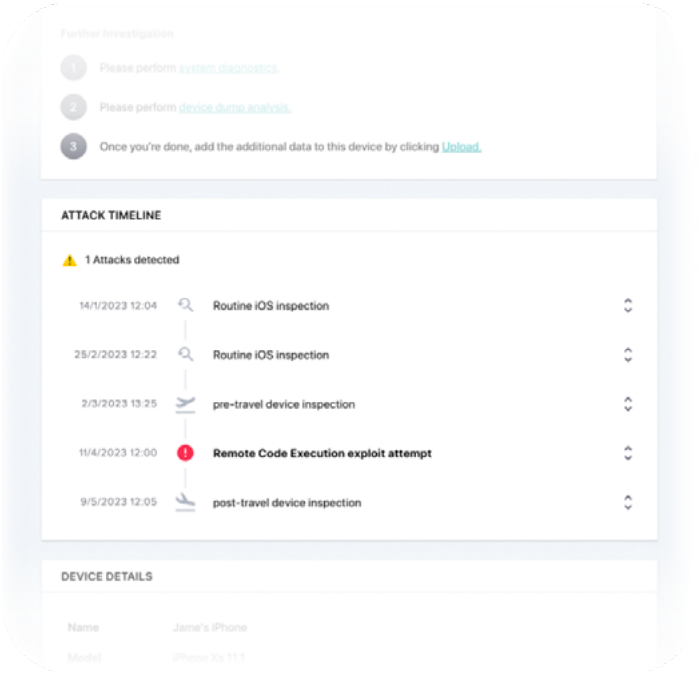
Jamf Executive Threat Protection 是一個偵測與回應解決方案，可遠端為機構提供精密的方法來了解並以適當的工具回應行動裝置上發生的狀況。

更完整的資料蒐集

鉅細靡遺的行動裝置遙測數據可將手動調查時間從數週縮短至數分鐘，讓您在哪都可以透視設備狀態。這個服務的功能遠超越一般 MDM 平台，可透過蒐集系統日誌來全面支援調查工作。

偵測並根除複雜的行動裝置攻擊

Jamf Executive Threat Protection 不只兼顧資安與裝置管理，還可以深層透視專門攻擊重要人物的資安威脅。



更快的偵測速度

不論攻擊者的經驗多麼老道，仍會留下蛛絲馬跡，因此更重要的是要知道怎麼找出線索。Jamf 可執行深入分析來識別入侵指標 (IOC)，並直接向資安團隊提供這些進階偵測內容，在不容易偵測到複雜的零日攻擊的情況下，Jamf Executive Threat Protection 更能夠發揮它的實力。

修復事件，好有自信

自動生成可疑事件的先後順序時間表，列出裝置被入侵的時間與原因。在不間斷執行設備監測的同時，內建的事件回應工具使資安團隊能夠攻破進階型的持續性威脅 (APT)，確保已根除威脅並維持使用者的安全。

我們的 Jamf Threat Labs 研究人員可提供深度分析與精闢見解，取得對行動裝置更高的可見度。現在就預約試用。

歡迎前往 jamf.com/zh-tw 以獲得更多資訊