jamf

打造現代化 Apple 資安計畫

免費的成熟度模型
以及 90 天實施藍圖 →

大多數以 PC 為基礎的工具皆支援 Mac。但只有 Apple 原生工具——行動裝置管理 (MDM)、端點資安框架 (ESF)、平台 API、平台 SSO——能在 Apple 架構中的適當層級運作，並為企業提供完整的資安涵蓋範圍。

準備好消除資安漏洞了嗎？

Apple 資安成熟度模型

使用 4 階段模型，找出您資安計畫中的漏洞：

第 1 階段

臨機

- 裝置註冊不一致
- 手動稽核
- 可視性有限
- 高風險

第 2 階段

已定義

- 基線已部署
- 自動修補
- 合規報告
- 基本 IdP 整合

第 3 階段

受管理

- 持續強制執行
- ESF 遙測數據傳送至 SIEM/SOAR
- 完整的 IdP 狀況共享
- 事件回應劇本

第 4 階段

最佳化

- 預測分析
- 自動修復
- 完整的 ATT&CK Mac 涵蓋範圍
- Zero Trust 已驗證

90 天實作藍圖

在 90 天內，從不一致的臨機裝置註冊，轉變為您適用您環境、完整最佳化且成熟的資安計畫。

第 1 至 30 天

設定基礎架構

- → 執行完整的 macOS 與 iOS 裝置盤點
- → 部署零接觸註冊
- → 建立 CIS 基準第 1 級基線
- → 連線至 IdP 以進行合規信號傳送
- → 設定裝置監控

第 31 至 60 天

加速營運

- → 設定 macOS 和優先 App 的自動化修補程式管理
- → 將基準擴展至法規架構
- → 設定主動式偵測 + SIEM 整合
- → 註冊 iOS 裝置
- → 移除不必要的本機管理員權限

第 61 至 90 天

最佳化以提升成熟度

- → 設定 iOS 威脅防護
- → 為前 5 大 Mac 事件回應情境建立 SOAR 劇本
- → 執行首次持續合規報告
- → 評估成熟度階段
- → 向管理階層呈報可衡量的改善成果

您現有的工具在它們原本設計的用途上表現優異，但Mac 和 iOS 裝置需要契合 Apple 架構的資安狀況。

Jamf 旨在透過整合來補強現有技術堆疊——整合對象包含 SIEM、SOAR、IdP、XDR 與 SSE 平台——而非取代現有技術堆疊。其可與 Microsoft、CrowdStrike、Palo Alto 和 Zscaler 完整整合。

立即與我們討論如何實現現代化的 Apple 資安計畫。

立即體驗 Jamf