jamf

您的行動資安架構是否具備超越 MDM 的防護能力？

勾選所有符合的項目，並於下方計算勾選總數。

1.

威脅防禦

行動威脅不會在裝置註冊後就此消失。

- [ ] 我們僅依賴 MDM 保護行動裝置，未搭配額外的行動威脅防禦機制。
- [ ] 若使用者在 iPhone 或 iPad 上點擊網路釣魚連結，我們的自動偵測與回應能力有限。
- [ ] 我們難以快速辨識受管裝置上會增加資安風險的應用程式。
- [ ] 我們對不安全 Wi-Fi 或其他網路型行動威脅的掌握狀況與防護能力有限。

2.

合規性與裝置健康狀態

無法即時掌握狀態，就難以即時處理問題。

- [ ] 我們無法即時掌握哪些行動裝置目前為合規狀態。
- [ ] 配置偏移在影響使用者或合規性之前，難以被事先察覺。
- [ ] 我們通常在使用者回報後才發現行動裝置問題。
- [ ] 我們無法在所有行動裝置上一致落實作業系統與應用程式版本要求。

3.

更新與漏洞管理

每一次延遲更新都會產生不必要的風險。

- [ ] 我們無法確保所有行動裝置的作業系統更新皆維持在最新狀態。
- [ ] 關鍵應用程式更新仍仰賴使用者自行安裝。
- [ ] 我們未能在行動裝置群上一致落實更新期限。
- [ ] 裝置偶爾會因更新未即時部署而落入不合規狀態。

4.

身分識別與存取管理

身分識別僅是資安防護中的一環。

- [ ] 我們的身分平台在驗證過程中不會評估行動裝置的資安狀況。
- [ ] 遭到入侵或不合規的行動裝置仍可能存取企業應用程式。
- [ ] 存取政策預設已註冊裝置為可信任，不論其當前資安狀態為何。
- [ ] 我們不會自動限制高風險或不合規行動裝置的存取權。

為何這些問題至關重要

行動裝置管理是必要的基礎，但現代行動資安不能只仰賴裝置配置。威脅防護、持續合規、即時更新與身分感知存取，四者相輔相成以降低風險。

勾選項目愈多，代表您的環境愈可能存在單靠裝置管理無法填補的資安缺口。

您的評測結果

0–4 項勾選 → **基礎穩固**

您的行動資安策略已涵蓋現代 IT 團隊所需的多項能力。本白皮書可協助驗證您的做法，並提供進一步強化防護的建議。

5–9 項勾選 → **尚有強化空間**

您的環境存在若干常見資安缺口，長久下來可能增加營運風險。多數企業在行動裝置規模擴張時，都會來到這個階段。了解如何在無需增加不必要複雜度的情況下強化防護。

10–16 項勾選 → **該更新現行管理策略了**

現行裝置管理機制承載了超出設計範圍的資安責任。將威脅防禦、持續合規與身分感知存取納入策略，有助於在簡化維運的同時降低風險。這份白皮書提供務實的藍圖，協助您將行動資安策略升級。

準備好超越 MDM 了嗎？

了解如何整合行動裝置管理、威脅防禦與合規性管控，打造適用 iPhone 與 iPad 的現代資安策略。

jamf

www.jamf.com/zh-tw/

索取白皮書