jamf

Apple 裝置群中應檢視的 5 項隱藏資安缺口

勾選所有符合貴企業現況的描述，
再於下方統計總分。

1.

配置偏移

裝置仍會正常簽入。配置已不再是 IT 原先設定的狀態。

- [ ] 部分裝置的設定可能在註冊後於我們不知情的情況下發生變更。
- [ ] 我們依賴排程的資產盤點檢查而非持續監控來偵測配置變更。
- [ ] 目前沒有自動化流程來修正已偏離配置的裝置。

2.

未修補裝置

多數裝置已完成修補。少數例外裝置即為風險暴露的來源。

- [ ] 必須透過人工逐一確認，才能掌握整個裝置群的修補覆蓋程度。
- [ ] 離線或位於不同網路的裝置有時會錯過更新週期。
- [ ] 難以輕易確認單台裝置已執行過時作業系統版本多久。

3.

MDM 無法偵測的威脅

裝置即便完成註冊、監控面板顯示正常，仍有可能正處於遭入侵的狀態。

- [ ] 我們的 Mac 裝置群除 MDM 外，未部署專屬的端點資安工具。
- [ ] 現有的工具組合無法偵測行為特徵、可疑程序以及各項入侵指標。
- [ ] 若威脅正運行於 MDM 儀表板顯示為合規的裝置上，我們將無從得知。

4.

過期存取權限

員工調整職務後，舊有的存取權限時常沒有同步撤銷。

- [ ] 當員工變更職務或離職時，存取權限不一定會隨之調整。
- [ ] 當使用者狀態變更時，裝置存取權限不會自動調整。
- [ ] 已結案的外包人員或調動崗位的員工，仍可能保有不再適用的資源存取權限。

5.

各自獨立的零散工具

不同工具的銜接空隙往往會累積潛在風險。

- [ ] 裝置管理、身分管控與資安防護三類工具彼此獨立運作。
- [ ] 被 MDM 標記為不合規的裝置，仍有可能通過身分管控環節而未遭到攔截。
- [ ] 端點偵測到資安事件時，管理平台不會自動執行對應處置動作。

5

為何這些缺口容易被忽略

這些缺口依附在看起來毫無異常的裝置狀態之下，包含已註冊、正常回報、持續上線等狀態。相關風險鮮少主動觸發警示通知。大多數狀況下，只有經過稽核、發生資安事件或是執行資安審查之後，缺口才會浮現。

評分結果

0 至 3 分 → **風險暴露有限**
隱藏缺口的跡象雖少，但部分盲點仍可能存在。

4 至 8 分 → **盲點逐漸浮現**
部分缺口可能在沒有明顯警示的情況下已存在。

9 至 15 分 → **多項隱藏缺口**
多個風險暴露點可能隱藏在看似健康且合規的裝置背後。

這些缺口不會以警示形式呈現，而會以資安事件形式出現。

《填補缺口：macOS 資安》可識別並說明如何修補現有工具未呈現的缺口。

jamf

www.jamf.com/zh-tw/

下載白皮書