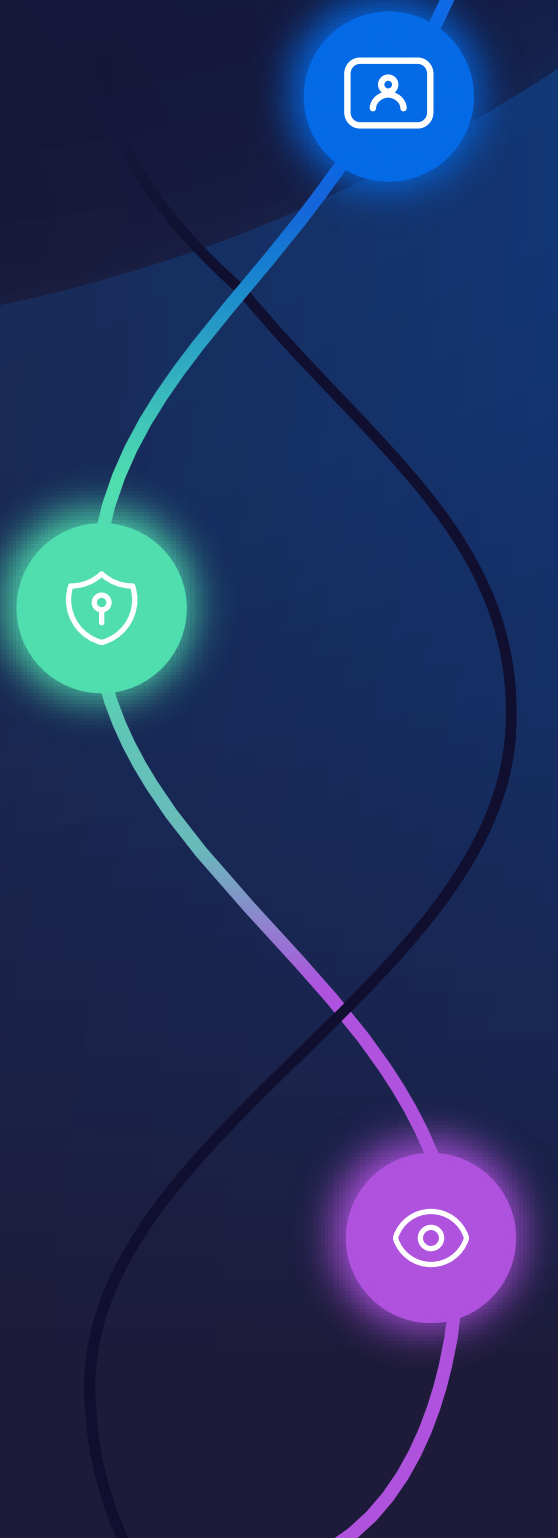
jamf

想在以 PC 為主的環境中導入 Apple 裝置嗎？

您的環境目前已擁有一套成熟的**身分識別**、**資安**及**可視性**系統。

現在，您需要以**更快的部署速度**、**更少的人為介入**、**更低的風險**來導入 Apple 裝置。

透過這份自我評估，了解如何將 Apple 快速串接至現有系統，避免產生「多套系統各自為政」的負擔。



jamf

檢查存取權限與信任機制

Apple 裝置應無縫融入 您現有的存取模型中，而不是依賴「手動排除」 或「個案處理」 。

請思考以下問題：

1. 我們能否對 Mac 與 Windows 使用者執行一致的**存取政策**？
2. 我們能否直接依**身分群組**來劃分政策，而無需重整組織架構？
3. 我們能否將存取權限與**裝置合規性**掛鉤（而不僅僅是帳號密碼）？

jamf

檢查資安態勢、偵測與回應能力

Apple 裝置應直接串接您的資安維運模型，而不是游離於體制之外。

請思考以下問題：

1. 我們能否在**同一個主控台**中，同時檢視 Apple 與 Windows 的風險狀況？

2. 資安警報是否**具備應變價值**，還是只是無意義的資訊通知？

3. 針對 Apple 裝置，我們能否**自動化執行應變動作**，還是所有操作都必須手動？

jamf

檢查資產管理與工作流程

Apple 裝置的數據應完整、正確地納入 IT 維運與資產生命週期管理中。

請思考以下問題：

1. 我們是否能掌握**完整的資產**清冊（包含 App、系統版本、加密狀態及所有權）？

2. 我們能否將 Apple **端點直接納入現有的 ITSM 流**程，而無需額外步驟？

3. 系統**整合是「雙向」的**（同步＋動作），還是只能單向匯出數據資料？

jamf

整合就緒度自我評估

各類別評分：1-5 分

身分識別：

- [ ] 我們能針對 Apple 裝置執行一致的存取控管與裝置信任機制
- [ ] 執行群組化原則劃分與自動化生命週期管理非常順手
- [ ] 對於 Apple 使用者，幾乎不需要任何手動例外處理

資安防護：

- [ ] Apple 的風險與資安態勢已完整呈現於資安維運工作流程中
- [ ] 我們能善用 Apple 的「宣告式裝置管理 (DDM)」執行自動化回應（而不僅是發出警報）
- [ ] 報表內容完全符合內部控制與稽核需求

可視性：

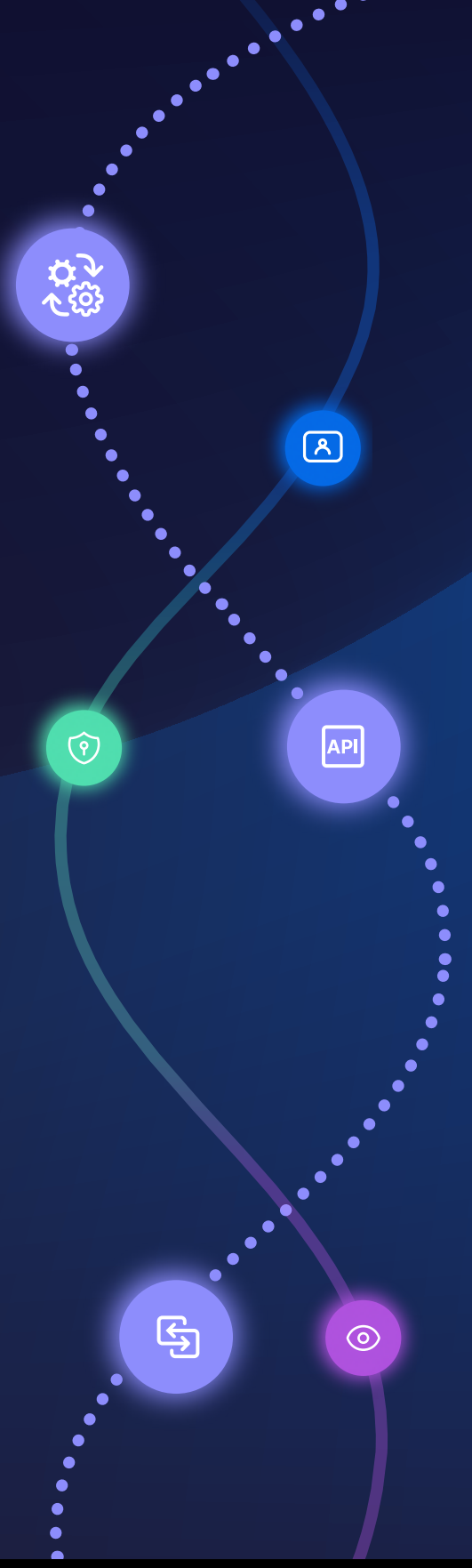
- [ ] Apple 資產清冊完整、精確，並可直接應用於 CMDB/ITSM 系統
- [ ] 我們能根據「裝置狀態」即時驅動工作流程（而不是看試算表辦事）
- [ ] 數據資料能長久保持一致，無需人工定期清理

評估結果： 若任一核心項目評分低於 3 分，代表您可能正走向「手動土法煉鋼」或累積「整合債（Integration Debt）」，這將嚴重拖累規模化的速度。

jamf

企業透過 Jamf 實現成功的整合轉型

Jamf 利用成熟的**市場化整合方案**與**彈性的 API**，在身分、資安與可視性等領域加速 Apple 裝置的導入。這能精簡工作流、降低整合債，協助團隊使用現有的信任工具來延伸管理 Apple 裝置。



別只聽我們說： 了解為何 Jamf 在《IDC MarketScape：2025–2026 年全球 Apple 裝置統一端點管理 (UEM) 軟體供應商評估》中被評為**領導者**。