jamf

Mac 與 iOS

整合指南：在 Windows 為主的企業環境中實現

全方位管理

介紹

當 Apple 裝置進入以 Windows 為主的企業環境時，「效率」才是決定 IT 運作順暢與否的關鍵。唯有高度自動化，才能避免因裝置增加而被迫增加人力成本，或讓 IT 小組陷入無意義的 額外 瑣事中。

本指南為《為何選擇 Jamf》系列的第一部分，旨在為各種技術層級的 IT 主管與管理員提供必要資訊，確保現有的身分驗證、資安、自動化及 觀測工具投資能發揮合規成效，並大幅減少手動作業。最終目標是在不增加營運負擔的前提下，建立一致的 Apple 使用體驗。

執行摘要

隨著 Apple 裝置在 Windows 體系企業中的普及率攀升，營運效率成為成功的決定性因素。本電子書概述了組織如何透過解決影響程序與工作流程的關鍵挑戰，在不增加人力、持有成本或複雜度的情況下整合 Apple 裝置。其成果包含更快的部署速度、更優異的可視性，以及能隨業務規模同步擴展、既一致且安全的 Apple 體驗。

Jamf 協助解決的整合痛點

透過整合**身分驗證**、**資安防護**及**現有 IT 解決方案**來消除「資料孤島」與工作流低效問題，建立全方位策略。

利用「零接觸」且順暢的裝置上線工作流程，**提升**員工生產力。

透過**生態系統整合**，實現 Apple 裝置從採購、軟體修補到安全除役的完整生命週期**自動化**。

在所有平台上統一落實結合**「零信任」**架構與**身分提供者** (IdP) 的全面存取政策。

透過持續評估豐富的遙測資料，標準化並維持基準資安狀態，藉此縮短**事件應變時間**。

與現有技術架構深度整合

裝置管理與現有資安、身分工具之間若缺乏連動，會導致資料孤島、工作流程低效以及合規性漏洞。

關於 Apple 裝置與傳統 Windows 網路環境，最常見的迷思就是兩者「不相容」。雖然這種觀念可追溯至數十年前，但現代企業技術的現實是：跨平台支援不僅是維持全球業務連續性的必要條件，更是理所當然的標配。隨著組織日益仰賴雲端架構、應用程式與服務來創造價值，這一點尤為重要。IT 必須確保分布在各地的員工不論使用何種裝置類型、平台或版本，都能獲得全面一致的作業環境與生產力。

與跨平台支援並行的關鍵點，在於您的現有技術架構與大規模導入的 Apple 裝置之間，是否具備深度整合的相容性。

Jamf 如何讓企業整合 Apple 的過程變得毫無阻礙？

關鍵就在：**平台 API** (Platform API)。

Apple 端點與您的技術架構能否順暢溝通，取決於管理、身分與資安工作流程之間，是否建立了安全且符合標準的連結。

面對現代威脅情勢，這對企業合規代表什麼意義？代表更簡約的解決方案，以及更低的複雜度。

透過將 Apple 與現有技術架構無縫整合，可在跨平台環境中實現：

自動化驅動：確保工作流程一致且環境規格對等。

以身分為核心的安全防護：提供統一的威脅保護。

運用既有投資：使用您**已擁有的解決方案**來維持合規。

改善應變時間：減少因 IT 團隊職責切分過細（Siloed teams）導致的延誤。

為什麼選擇 Jamf?

Jamf Marketplace 提供超過 300 種（且持續增加中）預建整合套件，消除在現有企業環境中導入 Apple 的複雜性。

改善裝置部署流程，減少員工停工時間

員工每等待一小時裝置配置，就是一小時的生產力損失。在純 PC 環境中，每台機器的平均等待時間為 2 到 4 小時。

在以 PC 為主的環境中整合 Apple 裝置時，部署階段是僅次於規劃階段的最關鍵任務。在此階段，員工通常只能乾等 IT 設置新裝置或更新裝置。根據需要套用的設定、安裝的 App 數量以及職務所需的特定組態，從員工拿到裝置到「全面就緒」之間的時間差，都會造成生產力中斷。

如果我告訴您，這些延遲可以縮短到每台 Mac 約 15 分鐘（iPad 和 iPhone 僅需 5 到 7 分鐘）呢？

部署神速的祕訣在於「零接觸佈建」。藉由將 Apple Business Manager (ABM) 連接至專為 Apple 設計的管理解決方案，IT 能啟動 Windows 環境完全無法企及的自動化架構。您可以將 ABM 視為 Apple 版的 Windows Autopilot，但由於 Apple 同時掌握晶片硬體與註冊服務，因此其硬體整合深度更勝一籌。IT 將 ABM 與 Jamf 整合後，即可在管理主機中定義「就緒狀態」：包含 App、環境設定、資安政策與身分設定。從那一刻起，當裝置從 Apple 採購後，ABM 會自動將裝置資訊同步至 Jamf 並加入預先註冊群組。

到這一步，IT 的工作基本上就完成了。

公司資產裝置會直接寄給使用者（不論在辦公室或遠端），他們只需拆箱、開機，就這麼簡單！裝置會自動註冊至 Jamf，並執行預設的工作流程，流暢地完成所有配置。得益於零接觸配置的自動化特性，終端使用者不需要執行任何複雜操作，也不必提交任何 IT 工單。

為什麼選擇 Jamf?

透過 Jamf 藍圖功能，裝置能利用「宣告式裝置管理」自主執行政策，將 Mac 的設置時間縮短至 15 分鐘左右，行動裝置則不到 7 分鐘。受管裝置證明 (Managed Device Attestation) 則提供了根植於硬體的合規證明，讓 IT 確信每台裝置在存取公司資源前皆為官方正品且安全無虞。

Apple 將證明、身分識別與管理整合為統一架構——從晶片硬體到軟體層級皆無縫串連。

宣告式裝置管理 (DDM) 允許裝置以非同步方式套用設定，並向裝置管理服務回報狀態，無需像過去那樣頻繁輪詢 Apple 支援伺服器。這代表著裝置的配置速度更快，且即使在沒有網路連線的情況下也能維持合規狀態。

受管裝置證明在信任評估中提供了強而有力的裝置屬性證據。它利用基於 Secure Enclave 與 Apple 證明伺服器的加密宣告，在裝置接觸任何公司資源前證明其真實性。

平台單一登入 (Platform SSO) 讓使用者能利用 Touch ID 實現免密碼登入。基於 Secure Enclave 硬體密鑰的抗釣魚憑證，讓員工只需在登入時驗證一次，即可無縫存取所有企業 App，無需再為管理多組密碼煩惱。

實現企業級 IT 任務與程序自動化

根據 Forrester 的報告，單次密碼重設的平均成本為 70 美元， 一般 企業每年平均編列超過 100 萬美元預算，僅為了支援手動處理密碼相關的問題。

「自動化」是一個宏大的概念，就像一個巨大的袋子，幾乎能裝進任何被放入其中的東西。理解自動化與「時間」之間的關係至關重要。這不僅關乎自動化任務能節省多少 IT 時間，還包含 IT 團隊學習一項技能、直到掌握開發自動化所需知識所投入的時間成本。

考慮到企業級別運作的裝置、技術與解決方案數量極其龐大，IT 團隊的時間顯得極為寶貴。自動化的報償不只是效率，它能讓 IT 從「到處救火」的雜事中解脫，專注於具策略價值的任務。它能實現：

一致的規範執行

政策能統一套用於 Mac、iPhone 和 iPad，不讓任何裝置 成為資安漏洞。

減少人為錯誤

透過標準化工作流程 消除手動作業帶來的風險 。

無須增加人力的擴充性

隨著企業擴張，輕鬆應對日益增長的管理與資安需求。

正確的自動化架構能處理各類重複性工作：部署裝置、執行政策、修補軟體以及重設密碼。Apple 甚至做得更徹底。透過 DDM，裝置不必等待伺服器指令，而是能自主執行政策並 即時回報狀態變更。這意味著當您的 Apple 裝置群規模擴大時，支援案件會隨之減少、合規速度更快，且需要的人工干預也更低。

為什麼選擇 Jamf?

Jamf 的智慧自動化工作流程透過政策化管理、智慧群組 (Smart Groups) 及 API 驅動程序 ，消除了手動設定的必要，旨在確保大規模環境下的部署與合規監控始終一致且零錯誤。

透過實施零信任架構強化存取政策

現代威脅情勢正不斷演變。攻擊者利用 AI 等先進技術提升威脅的精密程度、極大化破壞力，並 透過隱匿手段規避偵測。

請記住，攻擊者的目標涵蓋所有平台，沒有任何作業系統是絕對無敵的。這就是為什麼保持端點更新並實施「防禦深度」策略是現代裝置管理的基石。關鍵在於：在證明安全之前，將每個裝置、每個使用者與每次請求都視為「不可信」。「零信任」不是一種產品，而是一個架構。而 Apple 的架構正是為此而生。

受管裝置證明 (Managed Device Attestation) 透過加密技術，在裝置接觸任何公司資源前證明其真實性。平台單一登入 (Platform SSO) 將使用者身分與 Secure Enclave 中的硬體密鑰綁定，極大化提升盜取憑證的難度。宣告式裝置管理 (DDM) 則確保裝置即使在離線狀態下，也能自主執行安全政策。結合上述技術，便能建立一個持續驗證、而非盲目信任的安全基礎。

企業透過在裝置群中統一管理、身分驗證與資安防護，可從以下關鍵面向提升靈活性並加快事件應變速度：

實施零信任網路存取 (ZTNA)

- 執行「環境感知」存取政策，在 每次請求時驗證裝置狀態與憑證健康度。
- 使用加密通道隔離連線階段，減少常見的裝置端與網路內攻擊。
- 將防護延伸至 macOS、iOS、iPadOS、Android 與 Windows。

應用基準設定並進行基準測試合規

- 根據 法規或自定義合規需求，**自動部署基準安全設定。**
- 透過基準測試**稽核全企業裝置狀態**，驗證合規性。
- **利用 AI/ML 進行威脅獵捕、事件應變與 IT 支援**
- 主動偵測已知威脅，同時提升及早**識別並 阻斷未知威脅**的能力。
- **縮短應變時間、加速修復流程**，同時填補資安漏洞。
- 利用 **Jamf AI Assistant** 協助團隊探索技術細節、驗證配置建議，並開發更快速的修復方案。

為什麼選擇 Jamf?

生成式 AI (GenAI) 正在強化社交工程攻擊——釣魚訊息、合成媒體及 AI 生成的惡意軟體比以往更難察覺。

Apple 的 Secure Enclave 與受管裝置證明可在硬體層級驗證裝置身分；同時 Jamf 透過風險評估存取政策、裝置合規驗證及條件式存取整合，落實零信任網路控制，保護端點上的敏感資料。

掌握裝置生命週期全貌並改善應變效率

大多數的資安討論都集中在主動威脅上。但某些最大的風險與成本其實隱藏在細節中：過時的資產清單、未使用的軟體授權，以及未經妥善抹除資料便離開組織的裝置。

IT 與資安團隊往往過度專注於駭客攻擊，以至於忽略了裝置管理的其他面向。

「可視性」不只是了解網路中有什麼。它關乎了解哪些軟體已安裝、哪些已授權、哪些符合規範，以及哪些裝置已準備好退役。即時的端點資料（如最新的裝置清單或軟體過度擴張情況），能描繪出端點在整個生命週期中的健康全貌。透過宣告式裝置管理 (DDM)，Apple 裝置會主動回報狀態變更（包含 OS 版本、資安狀態、已安裝的 App），無需等待 IT 進行輪詢。這意味著資產清單能隨時保持最新，而非過時的資訊。

我們將分析缺乏可視性對組織造成的影響：

未使用的軟體授權

若無法精確追蹤軟體授權，將導致約 50% 的 軟體 授權處於未使用狀態，每月**損失金額約為 4,500 萬**美元。

裝置除役問題

近年來有 10-20% 的資料外洩事件與電子廢棄物 (e-waste) 或處理不當的裝置有關。相較於目前使用中的端點，這些退役裝置代表了企業的資安盲點。

合規漏洞

若組織在更新與重新配發裝置時管理不當，資料便可能落入錯誤的人手中（例如內部威脅）。例如，如果一位人資主管先前使用的筆記型電腦被轉交給新進的業務人員。該裝置中包含的個人識別資訊 (PII) 可能依然存在並可被新使用者查看；根據您所屬產業的法規，這可能違反隱私法（如 GDPR）。

Apple 的管理方式讓這類問題更易處理。裝置會自我回報，政策則會自動執行。當需要抹除資料並重新部署時，Apple 商務管理與管理解決方案之間的整合可確保裝置自動重新註冊——無需人工干預，亦無資安漏洞。

Jamf 讓 IT 在裝置除役前，能驗證搭載 Apple 晶片的 Mac 是否正以「完整安全性」模式執行，確保經 FileVault

為什麼選擇 Jamf?

加密的資料即使在裝置遺失或處理不當時，依然受到保護。鑑於 10-20% 的資料外洩與電子廢棄物有關，透過硬體層級監控「安全啟動」(Secure Boot) 狀態的可視化管理，能填補多數組織平時忽略、直到出事才驚覺的資安漏洞。

轉化為實質成效的產業工作流程

衡量裝置管理成效的指標不在於 IT 後端系統，而在於員工與客戶是否感受到工作效率的實質提升。
以下真實案例展示了裝置如何為工作流程增進效益：

醫療產業

當病患的病歷狀態更新為「出院」時，病床旁的 iPad 會自動抹除所有病患資料並重新整備，無需醫療人員手動介入，即可供下一位病患使用。醫護人員在換班時共用 iPhone，系統會根據其職務與憑證自動啟用個人化的應用程式。

航空業

飛行員以單一台 iPad 搭載的「電子飛行包」(Electronic Flight Bag) 取代笨重的查檢表、航圖與手冊。不論拿起哪一台裝置，維修人員、登機口人員與空服員都能自動獲得所需的正確 App。

零售業

鎖定於「單一 App 模式」的 iPad 可作為自助服務機 。這代表著不需要排解故障、不會出現不當內容，且在一天結束時也無需手動重置。店員在共用裝置上登入後，即可根據身分配置，在銷售時點情報系統 (POS)、庫存與客戶資料之間無縫切換。

製造業

生產線作業人員通常沒有網路帳號，也不熟悉行動技術的應用。安全充電櫃提供全自動的基礎支援。如果 iPad 無法運作，員工只需將其插回充電櫃，裝置便會自動重置、完成設定並進行自我修復。他們只需拿起另一台 iPad 就能立刻開工，完全不需要提交 IT 工單或專人支援。

金融服務業

理賠調查員、貸款專員與外勤顧問常需在充滿變數的環境中，透過共用裝置存取具備嚴格合規要求的敏感資料。理賠人員從公用裝置庫領取 iPad 後，只需感應憑證一次，即可立即存取理賠 App、照片工具與客戶紀錄。工作結束後，僅需數秒即可登出憑證，裝置便會準備好供下一位使用者使用，並保留完整的合規稽核追蹤紀錄。

總結

將 Apple 整合至以 Windows 為主的企業環境，並不需要大規模的組織轉型或增加營運負擔。相反地，這需要的是轉向高效、自動化且標準化的工作流程。藉由在 Apple 原生基礎上統一裝置生命週期管理、身分驗證與資安防護，並與現有工具整合，IT 團隊即可按部就班提升營運成熟度。這種做法能減少手動作業、提高一致性並實現主動式營運，讓組織能按照自己的節奏進行現代化轉型，同時維持跨平台的可用性、合規性，以及對桌機與行動裝置群的掌控力。

關鍵總結

- Apple 整合是效率問題，而非人力成本問題。
- 零接觸部署將長達數小時的設定縮短為數分鐘，大幅減少停機時間。
- 統一管理、身分與資安，消除營運上的橫向孤島。
- 自動化確保大規模環境下的規範落實，並減少人為錯誤。
- 零信任網路存取 (ZTNA) 在不增加複雜度的情況下強化安全性。
- 生命週期可視化保護了系統運作時間、合規性與軟體支出。
- 宣告式裝置管理 (DDM) 讓裝置即便在離線時也能維持合規。

準備好親身體驗了嗎？

立即體驗 Jamf