jamf

在以 PC 為主導的企業環境中，如何為 Apple 裝置打造卓越的用戶體驗

介紹

體驗即生產力。

透過將 Apple 對使用者經驗的關注延伸至 IT 流程，企業得以減少摩擦，進而最大限度地提高生產力和投資報酬率（ROI）。

本指南是「為什麼選擇 Jamf」系列的第二部分，旨在為各個技能水平的 IT 主管和管理員提供所需的資訊，以確保在身份、安全、自動化和可觀測性方面的現有投資能夠幫助員工保持生產力，同時克服挑戰並減少常見障礙。

執行摘要

當裝置佈建、存取管理、軟體更新和威脅防禦都依賴手動流程時，生產力就會下降。本指南闡述如何整合裝置管理、身分和安全，從而簡化 IT 維運並提升使用者經驗。Jamf 提供零接觸部署、角色式存取控制和自動化 App 生命週期管理，從而加快使用者產品導入速度，並確保裝置安全及合規。Self Service+ 讓員工得以隨選安裝已批准的 App 並解決常見需求，從而在確保政策有效執行的同時，減少服務台工作單。最終，您將建立起一個可擴展的工作流，不僅增強了安全性、簡化了管理，更能讓員工從第一天起就保持生產力。

Jamf 解決生產力痛點

透過開箱即用的「工作就緒」裝置，**讓員工無縫導入產品**。

實施 **Zero Trust**，驗證裝置和憑證的健康：降低受保護資源的風險。

從首次登入開始，**即可設定安全**可靠的基礎配置，以及針對特定角色的最佳化。

獲得**即時可見性**，從被動回應轉變為主動解決問題，而非僅對事件做出反應。

自動**保持軟體最新狀態**：最大限度縮短停機時間，並最大限度地確保合規。

透過 Self-Service，讓使用者隨時隨地獲得所需協助，進而**降低服務台**負擔。

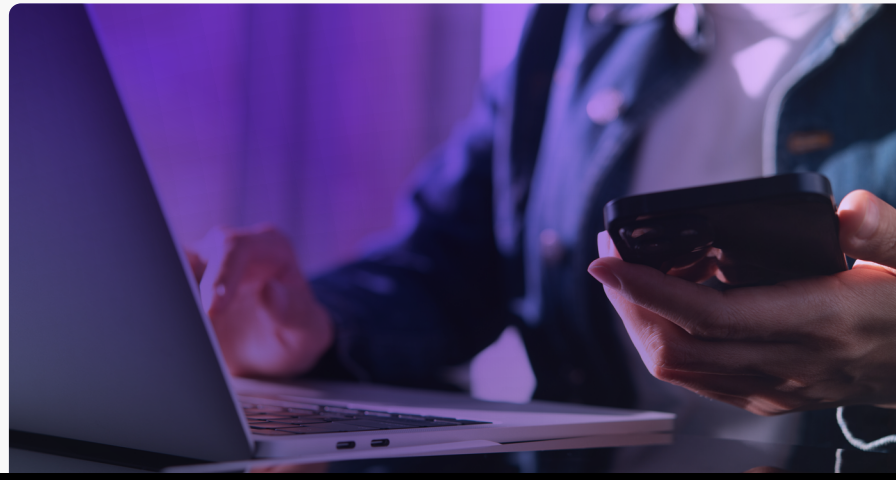
無縫導入產品，從第一天起即可高效工作

對於 IT 而言，典型的手動佈建流程如下：

1. **採購硬體。**
2. **拆箱每個裝置。**
3. **集中部署。**
4. **完成初始設定畫面。**
5. **安裝：**
   - 作業系統更新
   - App
   - 端點防護
6. **配置：**
   - 硬體設定
   - 軟體設定
   - 安全基準設定
7. **確認端點正在被監控。**
8. **指派給用戶。**
9. **確認用戶能夠通過認證。**
10. **確認用戶擁有必要工具的存取權。**

理論上，為新進員工準備一台裝置需要十個步驟，這看起來或許不算什麼。然而，在實際操作中，管理著上千台裝置的企業，即使只是手動處理十台裝置，也會因為耗時、效率低下和預算緊張而望而卻步。

根據您的獨特需求，僅每台裝置的步驟 5-6 就可能需要花費數小時才能完成。這意味著，即使是像套用 OS 和軟體修補程式、安裝辦公室套件及配置軟體設定以確保合規這樣簡單的操作，也可能需要花費半天的時間，因為重啟裝置、等待流程完成都需要耗費大量時間。



如何解決資源影響問題？

以管理、身分和安全為核心，採用整合式產品導入策略，根據用戶的角色實現零接觸部署的自動化佈建。這不僅能將新員工等待硬體「準備就緒」的時間從數小時縮短至數分鐘，還能大幅縮短他們投入工作的時間窗口。

這代表：

- 無需等待 IT 提供支援，**避免產品導入延遲**。
- 員工無需前往辦公室領取裝置。
- 消除人為錯誤和重複性工作帶來的疲勞。
- 員工在產品導入第一天即可有效率地工作並積極貢獻力量。
- 高效率的工作流能夠為企業節省時間和金錢，而不是浪費。

為什麼選擇 Jamf？

Jamf 擁有靈活且強大的工作流，可減少 IT 部門解決與產品導入相關的支援工單所花費的時間。透過將常見的設定任務轉移到自動化部署模型，IT 能夠建立更完善、更便利的工作流，使用戶能夠自行註冊裝置，並透過 Self Service 安全地存取所需的軟體、工具和配置。

在不影響使用者操作的前提下保護資料的存取政策

存取控制清單（ACL）是資料安全的基石，它定義了使用者帳戶對受保護資源的授予權限（或未授予的權限）。雖然在確定 IT 支援人員比例時通常會考慮裝置總數，但在身分管理方面，討論的重點則轉移到 IT 支援的使用者數量，以便制定資料安全策略。

手動配置時，主要考慮因素是所需權限乘以用戶總數。隨著員工人數的增加，IT 需要手動處理的權限數量也會增加。這會對效能造成巨大影響、導致嚴重的延遲，並因人為錯誤和重複性作業疲勞，而導致風險攀升。此外，由於這種方法依賴 IT 手動處理發現的變更，任何觸發修改的事件（例如員工晉升或風險承受能力變更）都需要對每個帳戶甚至每個裝置進行修改，這使得該方法難以普及。

那麼，最佳的可擴展解決方案是什麼？

將身分存取管理（IAM）與裝置管理和端點安全整合，可最大程度地滿足企業需求。它還將手動操作從每個帳戶/每個裝置的變更簡化為集中式安全模型，利用角色式存取控制（RBAC），根據使用者角色而非個人身分和/或工作使用的任何單一裝置來定義其對安全資源的存取權。

這代表：

- **權限指派**得到簡化，基於中央儲存庫中的角色和群組成員資格。
- 強制執行最小權限原則，**僅授予必要的存取權**，不多不少。
- 存取權在**使用者進行認證**時生效，並隨使用者在任何裝置上及角色變更期間生效。
- 即使在更大規模的情況下，**管理負擔也得以降低**，因為 IT 只需處理一次變更。
- 稽核控制得到**簡化**，提供集中式的合規執行可見性和記錄。

為什麼選擇 Jamf？

對雲端身分提供者（IdP）的原生支援意味著，用於管理使用者憑證和端點的集中式身分式安全控制，也適用於您的 Jamf 物件實體。Jamf 基於身分整合建置，提供無縫的使用者經驗，並將 IAM 策略應用於公司資源，全面支援 Mac 和行動裝置以及 Windows PC，從而實現真正統一的身分範式，該範式既可自訂又可擴展。

輕鬆管理 App 生命週期

使用者經驗的最大關鍵因素之一在於用於完成工作的軟體解決方案。平衡難題：

- **公司需求**
- **多種平台**
- **使用者偏好設定**
- **不同的裝置類型**

這意味著合規之路並非一帆風順。此外，支援原生 App、內部程式碼和/或雲端託管軟體也進一步增加了合規的難度。

針對多個作業系統的修補程式管理，包括安全性版本和 App 更新，很容易從幾分鐘就能完成的任務演變成耗時數小時甚至數天的專案，因為其範圍和規模會超出 IT 團隊的掌控。

即使 IT 與裝置的比例很低，手動更新 App 或執行全機群 OS 升級也會導致用戶無法運作，並使組織面臨來自各種方面的風險，例如：

- **源自**缺失更新的未修補漏洞
- 不完整或部分更新導致的軟體損壞
- 修補程式部署分散導致的**安全狀況減弱**
- **未經授權的** App 使用（影子 IT）
- 應用程式完整性受損或 App 安裝不安全

哪種解決方案能夠協調 App 生命週期管理？

一種策略，既能集中管理應用程式並以原生方式部署，又能整合端點可見性、政策式合規執行，並在軟體更新可用時自動執行更新，從而確保裝置始終保持最新狀態（對使用者而言無縫銜接），並且能夠以統一的方式緩解可能危及公司資料的已知漏洞，覆蓋整個基礎架構（無論 OS 或裝置類型如何）。

這代表：

資產資訊**即時更新**，讓您清楚瞭解管理式裝置上已安裝的 App 及其版本。

應用程式均**來自合法開發人員**，並透過數位簽章驗證其真實性和完整性。

軟體以原生方式安裝並**自動更新**，簡化管理式 App 生命週期，進而降低 IT 負擔。

合規透過政策強制執行，確保管理式 App 在每個支援的裝置上均可用且配置一致。

稽核追蹤得到**簡化**。藉助統一的記錄確保合規得到驗證，並可輕鬆與稽核人員共用。

為什麼選擇 Jamf？

成功的修補程式管理策略必須具備安全性、有效性、可擴展性和一致性。Jamf App 安裝程式符合上述所有特性，並結合自動化功能，確保部署第三方軟體時強制執行合規，從而實現安全的端點基線。此外，它還結合了強大且靈活的政策，利用基準來維持 OS 和系統安全修補程式的更新，從而維護強大的裝置狀況，使其與企業的整體安全狀況保持一致。

在威脅到達使用者之前將其攔截

沒有什麼比惡意威脅更能迅速扼殺生產力了，惡意威脅會阻止使用者存取資料、將網際網路連線速度降至無法使用的程度，或損害公司資料的完整性—甚至三者兼具。

前三節討論了裝置部署、存取權限和 App 生命週期管理。本節重點在於威脅防禦和預防，因為這對於在面對現代威脅時維持員工生產力至關重要。尤其需要關注的是那些利用多種行動裝置、不同平台，以及現代企業對雲端式服務的依賴，從而攻擊辦公室和遠端辦公用戶的複雜威脅。

有效的事件回應對於減緩現有威脅演變成更嚴重的後果至關重要。然而現實情況是，當易受攻擊的端點被攻破時，用戶已經受到了影響。此外，修復問題需要更大的中斷，從而延長延遲加劇影響。**這會導致：**

- **生產力下降**，
- 導致長時間**停機**，
- 進而對各團隊造成**疊加影響**，
- 對企業營運產生**負面**影響，
- 造成**收入損失**，
- **損害**客戶信任，
- 並導致更高的修復**成本**。

哪一種解決方案能夠幫助 IT 領先一步抵禦威脅？

要有效阻止威脅，IT 首先必須能夠識別威脅。無論威脅是來自不合規的 App，還是使用者關閉的設定，防止企業資料面臨風險的關鍵在於防患於未然。

這代表：

- **主動監控**包含上下文資訊的遙測資料，包括端點健康。
- 深入瞭解端點風險矩陣，**以評估威脅嚴重程度並確定其優先順序。**
- **對**存取安全資源的裝置進行全面透視至關重要—無論裝置是否為管理式。
- **整合解決方案**，打造涵蓋裝置管理、身分和端點安全的無縫策略。
- **利用機器學習（ML）**技術，加強並有效率地擴展對未知威脅的識別和解決能力。

為什麼選擇 Jamf？

Jamf 透過多層防護驗證端點合規。即時監控確保裝置健康始終處於掌控之中。系統會記錄並向 IT 回報所有發現，以防止對公司資源帶來風險。此資料用於透過自動使裝置合規來修復風險—在無需 IT 干預的情況下，用戶無需感知即可解決問題。

零停機時間：保障員工（及收入）持續運轉

以下因素：

- **跨平台支援**
- **桌面和行動裝置**
- **混合雲端技術**
- **分散式勞動力**
- **裝置所有權模式**

給全面的管理策略帶來了挑戰。從維持混合團隊的生產力，到無縫整合不同供應商的解決方案，再到全面擴展基礎架構的安全性—企業 IT 需要應對許多複雜挑戰，才能確保業務營運持續高效運作。

現代企業在全球舞台上開展業務，其業務結構如同章魚般複雜多元。每一隻觸手都代表著一項策略性舉措，共同構成了數位轉型的有機整體。

過去那種僅靠防火牆、防毒軟體、內部部署網域和 VPN 連線，就能將安全流量限制在邊界網路安全壁壘之內的時代已經一去不復返了。如今，每隻「觸手」或獨特領域都需要動態、靈活的解決方案，以便能夠從任何裝置、執行任何作業系統、全球任何地點進行有效管理和保護，同時還要確保使用者獲得他們期望和需要的所有便利、存取權和安全保障，從而保護計算裝置、公司資源和使用者隱私權。

哪一種解決方案能夠跨平台動態保護受保護的資源？

傳統解決方案存在安全漏洞，導致資料外洩風險。現今的企業需要基於 Zero Trust 架構的自適應技術，利用 IAM、裝置管理和端點安全，提供超越緩解現代威脅和攻擊的全面解決方案，從而確保合規。

這代表：

- 從隱式信任模型切換到**預設拒絕存取**的模型—永不信任，始終驗證。
- 每次允許存取請求之前，明確**驗證憑證**和**裝置健康**。
- 加入**情境感知**層，利用行為分析來應對複雜的威脅。
- 實施**網路內防禦**，將流量隔離到獨特的微通道中，防止竊聽和橫向移動。
- 透過自動化**加快**事件回應速度並執行修復工作流，從而減少停機時間。

為什麼選擇 Jamf？

藉助 Jamf 的 Zero Trust 網路存取（ZTNA），現代威脅防護可擴展至所有支援的裝置類型，提供跨平台支援，確保性能一致，從而簡化跨裝置機群的安全策略—無論裝置位於何處，也無論連接到何種網路。透過設計中融入分層防禦，用戶可以原生存取公司資源，而 IT 團隊則可以更好地協調業務營運和合規需求。

最大限度地減少服務台工作單，從而最大限度地提高使用者生產力

IT 的核心職責之一是支援使用者需求。在大多數組織中，員工人數遠遠超過 IT 專業人員的數量。因此，IT 能否及時、有效率地回應、分類和解決問題，並取得較高的成功率，會顯著受到以下因素的影響：

- **平均工作單吞吐量**
- **工作流效率**
- **IT 團隊規模**
- **公司整體文化**
- **團隊成員技能水平**

這些因素中任何一個或多個方面的潛在缺陷，都會因彼此之間的不協調而加劇。這會導致業務營運效率降低，進而影響業務目標的持續性。

雖然這些影響是長期的，但利害關係人會感受到更直接的影響，例如延遲工作相關任務的完成：

- 軟體**未安裝**
- **未配置的**設定
- **不正確的**權限
- 系統**錯誤**訊息
- 硬體**不相容**

哪一種解決方案能將 IT 轉變為生產力引擎？

傳統觀點認為，增加使用者存取權限並不能解決使用者經驗問題。IT 試圖「解決」某個問題，卻反而增加了風險，提高了資料完整性受損和安全事件發生的頻率。

然而，建立一個集中式儲存庫，讓利害關係人能夠自行解決問題（那些不需要技術背景的問題），不僅可以為使用者提供所需的即時解決方案，還能讓 IT 騰出精力，專注於開發更有效率的工作流，從而最大限度地提高使用者生產力，更緊密地與企業目標保持一致。

這代表：

- **將利害關係人納入解決方案**—這並非需要防範的問題。
- 用戶無需修改權限標準即可**安裝已核准的 App** 並**配置已授權的設定**。
- 透過使用者友好的介面實現**應用程式更新**自動化，只需按一下即可完成更新。
- 將企業介面與**雲端式 IdP** 連結，以便更好地滿足他們所在的使用者需求。
- 提供與使用者經驗相符的**原生介面**，並提供 App 更新通知。

為什麼選擇 Jamf？

適用於 Mac、iPhone 和 iPad 的 Self-Service+ 佈建 Apple 原生、企業管理式介面，並進行自訂，使用戶只需按一下即可存取應用程式、工具、腳本、耗材（例如印表機）和更新—無需管理員權限。透過與 IdP 整合，IT 可以無縫地臨時批准請求，而不會永久影響合規，即提供完整的稽核追蹤。

總結

高效率的組織能夠消除 IT 操作和員工體驗中的摩擦。透過統一裝置管理、身分和端點安全，企業可以實現產品導入自動化、強制執行一致的存取控制、維護應用程式健康，並在威脅中斷工作之前將其扼殺在萌芽狀態。Jamf 透過旨在跨各種裝置機群擴展的工作流提供這些功能，同時確保使用者有效率且安全地運作。憑藉零接觸部署、主動防護和 Self Service（使員工能夠隨選解決常見需求），IT 可以降低營運負擔，同時增強合規和彈性。最終，企業將擁有一個安全、精簡的環境，讓員工從第一天起就能專注於真正重要的工作。

重點總結

- **加速大規模裝置機群的產品導入：**零接觸部署無需耗時的手動佈建即可交付可立即投入工作的裝置。
- **擴展存取權而不影響使用者經驗：**角色式存取可隨著組織規模的擴大自動將權限與身分對齊。
- **維護數千個端點的 App 健康：**自動化修補和更新可確保軟體安全，同時不會影響生產力。
- **在威脅中斷營運之前將其攔截：**持續監控和合規執行可減少分散式員工的停機時間。
- **賦能使用者，同時減輕 IT 工作量：**Self Service 允許員工安裝已批准的 App 並解決常見需求，而無需建立新的工作單。
- **跨平台和位置提供一致的體驗：**統一的工作流可確保裝置安全且有效率，無論員工是在辦公室或遠距辦公。

準備好親身體驗了嗎？

立即體驗 Jamf。