



為 Apple 裝置建構完整的 Microsoft 堆疊。

Jamf 結合 Apple 裝置管理與資安能力，與 Microsoft Sentinel、Entra 以及 Intune 完成整合，讓 IT 與資安團隊能夠掌握各地所有 Apple 裝置的**完整可視**資訊。



在 Microsoft 環境下管理 Apple 裝置的組織，往往會面臨資安缺口。身分與存取控管的強度，取決於背後的裝置訊號；若缺少 Apple 原生的合規資料，條件式存取就無法針對整體裝置群完整落實零信任原則。

同時管理 Mac、iPhone 與 Windows 裝置的資安團隊，經常只能獲得不完整的狀態畫面，原因在於通用跨平台工具難以擷取 Apple 專屬的遙測資料。另一方面，主要為 Windows 環境開發的工具，需要手動變通方案，佈署至 Apple 裝置的速度也較慢。

通用型管理工具會拉高成本，卻無法帶來相對應的效益。雪上加霜的是，隨著組織擴大 Apple 裝置規模，不一致的驗證機制或裝置導入流程，會中斷員工生產力。



Jamf + Microsoft = Apple 專屬單一平台

Microsoft 與 Jamf 聯手，為共同客戶提供一套單一、具一致性且高度整合的技術堆疊，支援全體員工使用。IT 團隊可取得統一的可視化管理介面，資安團隊獲得全方位防護覆蓋，終端使用者無論身處何地，皆可在各款 Apple 裝置上享有順暢的產品導入與日常工作體驗。

合作更佳，設計使然

功能領域	效益簡述
大規模佈署與管理 Apple 裝置	裝置送達時即完成設定、符合規範並可立即投入作業。零接觸佈署由 Microsoft Entra ID 憑證與 Apple School Manager 提供技術支援。
透過 Entra ID 實現即時合規	Apple 原生合規訊號提供給 Microsoft Entra 條件式存取，當裝置暴露於風險時自動限制存取權限。
每位使用者享有流暢的身分體驗	使用者透過 Microsoft Entra ID 憑證登入；Jamf 自動完成帳戶佈建以及 FileVault 加密作業。
在 Microsoft Sentinel 實現 Apple 裝置深度可視化	Apple 原生遙測資料直接串流至 Sentinel，讓資安團隊能夠統一檢視 Mac、行動裝置與 Windows 的狀態。
透過 Security Copilot 實現統一資安作業	Jamf 外掛程式直接在分析人員工作流程中呈現 Apple 裝置相關脈絡資訊，加速事件調查與回應。

客戶效益

- 彌補 Microsoft 技術堆疊下 Apple 裝置的合規與可視化缺口
- 透過零接觸佈署與自動化強制規範，簡化 IT 營運作業
- 在不犧牲資安的前提下，提升員工使用體驗



整合功能	描述	產品文件或 Marketplace 頁面	Jamf 產品	Microsoft 產品	客戶回饋
用於查詢使用者 和群組的 LDAP	企業目錄中的使用者資訊（姓名、電子郵件、職位等）可用於確保正確的應用程式與設定推送到正確的終端使用者。管理員無需 手動重新建立這些資訊。	與 LDAP 目錄整合	Jamf Pro	地端 Active Directory	
用於查詢使用者 和群組的雲端 IdP	企業使用者的資訊（姓名、電子郵件、角色等）現在存放於雲端 IdP，這些資訊可確保正確的應用程式與設定套用到對應的使用者與裝置。透過將這些資訊與 Jamf Pro 連結，管理員無需手動輸入資料，即可確保身份驗證的精準性與安全性。	Microsoft Entra ID 整合	Jamf Pro	Microsoft Entra ID 和 Intune（Microsoft 端點管理員）	「Jamf 和 Microsoft 提供的文件是我參與過最清晰易懂的整合流程之一。」 I Borota
儀表板分析與報表	免費獲取所有必要工具，創建並儲存無限份互動式報表。透過 Jamf Pro 與 Power BI 整合功能，為整體部署提供更深層的資料分析。擴充 Jamf Pro 的報表功能，並將其整合進 Power BI 架構中。 可用的資料：電腦與行動裝置、詳細資料、應用程式、延伸屬性與群組	Power BI	Jamf Pro	Microsoft Power BI	Power BI 與 Jamf Pro 「Power BI 可與 Jamf Pro 高度整合，提供有關 Jamf Pro 物件實體各方面的詳細報表。你可以設定報表內容，例如 macOS 版本、病毒定義版本、各棟大樓的裝置數量等等。工具提供了大量的實用資料，讓人十分受用。」 C McBride



身分識別與存取整合功能	描述	產品文件或 Marketplace 頁面	Jamf 產品	Microsoft 產品	客戶回饋
iOS、iPadOS 和 macOS 專用的裝置合規性管理	企業希望在使用者存取公司資料前，先確認其使用的裝置已符合合規標準（如：OS 為最新版本、有啟用密碼等）。此整合讓 Jamf Pro 能驗證裝置是否合規，並將「是 / 否」的狀態傳送至 Microsoft，確保只有合規裝置能存取機密資料。 *該功能將於 Jamf Pro 10.4 版本取代 macOS 的條件式存取（Conditional Access）機制	裝置合規	Jamf Pro	Microsoft Entra ID 與 Intune	「這項整合可確保只有符合規範的裝置才能存取公司資料。Jamf 與 Microsoft Entra ID 的無縫整合，有效實現我們的資安要求。從資安角度來看，這是不可或缺的解決方案。」 Samstar777
雲端身分的 SSO	這項整合也讓機構管理員能使用 Entra ID（Azure 憑證）登入 Jamf Pro、macOS Security Cloud 與 Jamf Security Cloud。	以 AD FS 配置 SSO Jamf Pro 與 Microsoft Entra SSO 整合	Jamf Pro	Microsoft Entra ID 與 Intune	可與身分廠商 (IdP) 高度整合 「Microsoft Entra ID 幾乎能與所有支援外部 IdP 的服務整合，是最佳的身份提供者整合方案。Jamf Pro 不僅與 Jamf Protect 深度整合，其支援 SSO 的雲端身份功能，也能輕鬆將企業帳號串接到 Jamf 產品與其他第三方服務。」 T Ellis
適用於 Mac 的雲端身分	讓使用者可透過 Entra ID（Azure 憑證）登入其 Mac 裝置。	與 Microsoft Entra ID 整合	Jamf Connect	Microsoft Entra ID 與 Intune	「根據給出的指示操作，輕輕鬆鬆就能啟用。SSO 真的是徹底改變我們作業流程的關鍵。」 Tyler Verlato

Member of
Microsoft
Intelligent
Security
Association



端點防護 整合功能	描述	產品文件或 Marketplace 頁面	Jamf 產品	Microsoft 產品	客戶回饋
適用於 Microsoft Sentinel 的 Jamf Protect	Jamf Protect 與 Microsoft Sentinel 整合，能透過簡易流程，將 macOS 裝置上的詳細事件資料傳送至 Microsoft Sentinel。此整合讓安全團隊能透過 Jamf Protect 所記錄的 警報 與「 Unified Logs（統一日誌） 」，配合 Sentinel 的工作簿與分析規則，更全面掌握 Mac 裝置上的資安事件。	適用於 Microsoft Sentinel 的 Jamf Protect	Jamf Protect	Microsoft Sentinel	「 Sentinel 可與 Jamf 流暢運作 。Sentinel 與 Jamf Protect 這個組合，簡單來說可以改善工作流程，提升效率並深入掌握裝置資安狀態，有助爭取 SecOps 團隊的支持。我十分推薦這個組合。」 Dominic Vasquez
裝置遙測資訊 轉發	Mac 在預設狀態下將蒐集有關 App 和裝置性能的各种資料。雖然這意味著龐大的資訊量，但我們能夠藉由使用 Jamf Protect 對資訊進行篩選，並將關鍵資訊轉發至其選用的資安工具。	將 Jamf Protect 與 Microsoft Sentinel 整合	Jamf Protect	Microsoft Sentinel	「這個範例又再次演示了 Jamf 和 Azure 的運作真的相當的順暢。」 使用者 MrCcSti BF
網路威脅流事件 轉發	「Network Traffic Stream」（網路傳輸流）可讓機構傳輸、記錄和查看服務的基礎架構經由第三方日誌彙整工具與分析工具處理的網路活動。事件將以 CEF 格式編碼的 syslog 形式並藉由傳輸層安全性 (TLS) 憑證即時發送，以確保資料傳輸的安全。 Threat Events Stream 則可以 CEF 編碼的 syslog 或以 JSON 編碼的 HTTP 事件兩種形式即時傳送事件。兩種資料流都可以整合至 Microsoft Sentinel	網路傳輸流 威脅事件流	Jamf Protect 與 Jamf Connect	Microsoft Sentinel	「跟 Azure 和 Sentinel 的整合非常順暢。Jamf Protect 的整合真的幫了我們很大忙。」 Catherine Breese
用於 Microsoft Security Copilot 的外掛 程式	透過此外掛程式，安全管理員可在發生安全事件後，使用自然語言快速查詢 Jamf Pro 裝置資訊，並直接透過聊天介面獲取裝置清單資訊，無需進入 Jamf Pro 主控台。	如何在 Security Copilot 中整合，如何將 Jamf Pro 整合進去	Jamf Pro	Microsoft Security Copilot	

