



# Jamf 與 Microsoft： 管理並確保 Apple 企業 裝置的安全

隨著企業邁向現代化工作型態，IT 和資安團隊也積極尋求最佳方案來支援 Apple 使用者。

企業在制定 Apple 策略時，常面臨相似挑戰：

- 如何有效管理並保護能從各地連線、存取敏感資料的裝置
- 如何將工具合併使用、達成事半功倍的效率，同時又能提升管理與資安的實力
- 如何支援員工自選裝置、行動裝置與 BYOD（自攜裝置）政策

雖然現代技術已大幅進步，企業卻仍在保障使用者與資料的安全上苦苦掙扎。

## 以致發生以下狀況...

- 配置完善的資安機制變得過度複雜
- 使用體驗不佳，不只讓使用者受苦，還增加 IT 管理的負擔
- 資安機制存在缺口，無法涵蓋整個基礎架構中的所有裝置
- 無法一致地控管企業敏感資源（包括資料）



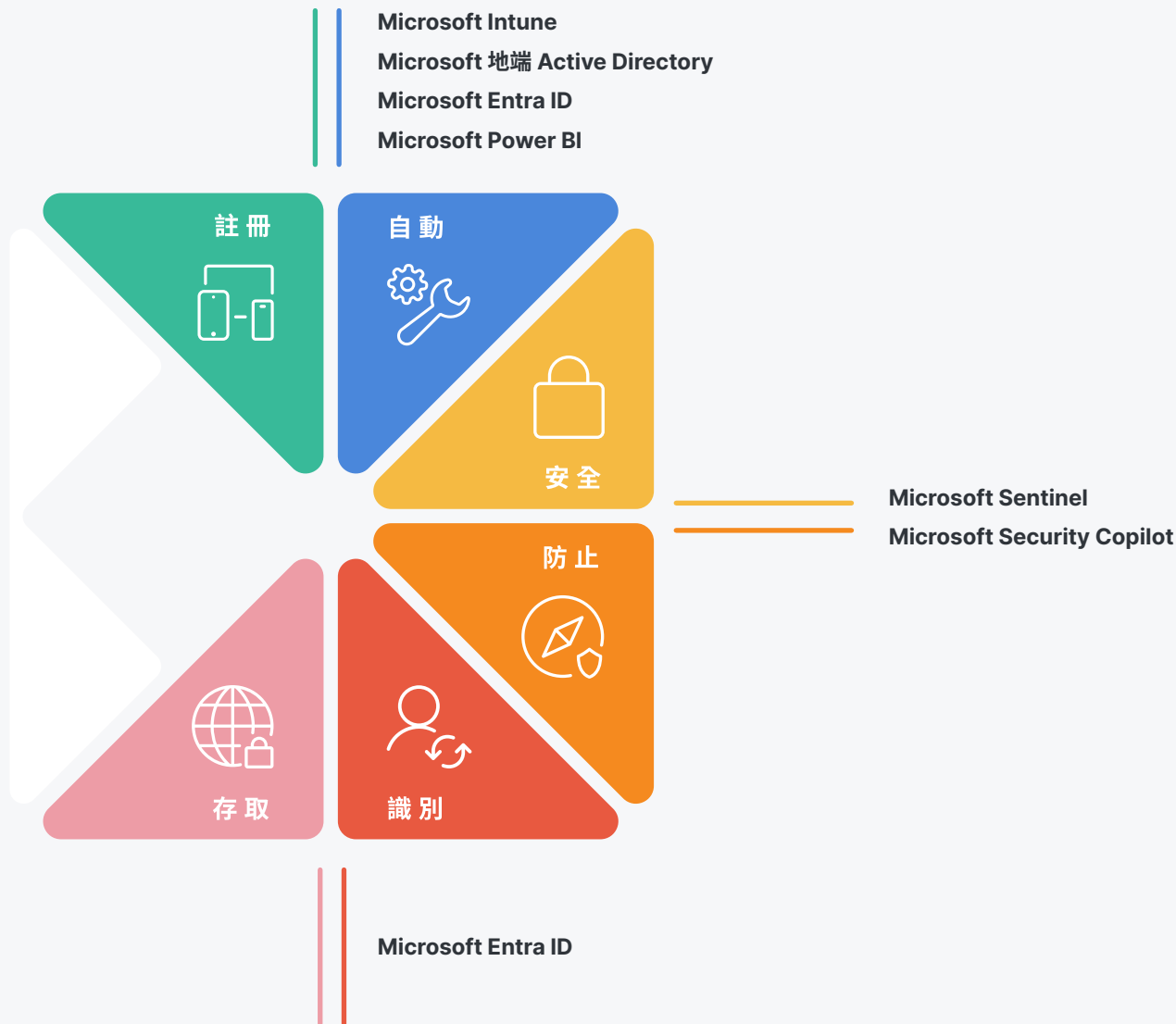
**Jamf + Microsoft 如何協助 使用 Microsoft 平台的企業有效支援 Apple 環境**

Jamf 具備獨特優勢，能整合 Apple 裝置管理、使用者身分識別與端點防護，與 Microsoft 攜手打造以 Apple 為核心的零信任架構。Trusted Access 可讓企業組織確保只有經授權的使用者、使用已註冊且安全的裝置，才能存取企業應用程式與資料。為實現零信任目標，雙方客戶會搭配雲端身分識別供應商（IdP）使用，因此 Jamf 與 Microsoft 的整合是再自然不過的選擇。所有註冊裝置都具備管理與端點防護機制，並透過零信任網路存取

（ZTNA）控管流量，不僅強化遠端連線安全，也彌補傳統 VPN 的缺陷，更符合現代資安威脅情勢。

對於採用 Microsoft 平台的企業而言，將 Jamf 與 Microsoft 整合，是實現 Apple 環境成功部署的關鍵。

不妨馬上看看可以簡化 Apple 流程的 Jamf 與 Microsoft 整合功能。



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。	<a href="#">與 LDAP 目錄 整合</a>	<a href="#">Jamf Pro</a>	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。	<a href="#">Microsoft Entra ID 整合</a>	<a href="#">Jamf Pro</a>	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	<p>免費獲取所有必要工具，創建並儲存無限份互動式報表。</p> <p>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。</p> <p>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</p>	<a href="#">Power BI</a>	<a href="#">Jamf Pro</a>	Microsoft Power BI	<p><b>Power BI 與 Jamf Pro</b></p> <p>「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。」</p> <p>C McBride</p>



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	<p>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。</p> <p>*該功能將於 Jamf Pro 10.4 版本取代 macOS 的條件式存取（Conditional Access）機制</p>	<a href="#">裝置合規</a>	<a href="#">Jamf Pro</a>	Microsoft Entra ID 與 Intune	<p>「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。」</p> <p>Samstar777</p>
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。	<a href="#">以 AD FS 配置 SSO</a>  <a href="#">Jamf Pro 與 Microsoft Entra SSO 整合</a>	<a href="#">Jamf Pro</a>	Microsoft Entra ID 與 Intune	<p><b>可與身分廠商 (IdP) 高度整合</b></p> <p>「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。」</p> <p>T Ellis</p>
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。	<a href="#">與 Microsoft Entra ID 整合</a>	<a href="#">Jamf Connect</a>	Microsoft Entra ID 與 Intune	<p>「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。」</p> <p>Tyler Verlato</p>

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	<b>Jamf Protect</b> 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 <b>警報</b> 與「 <b>Unified Logs（統一日誌）</b> 」，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。	<a href="#">適用於 Microsoft Sentinel 的 Jamf Protect</a>	<b>Jamf Protect</b>	Microsoft Sentinel	「 <b>Sentinel 可與 Jamf 流暢運作</b> 。 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。」 <b>Dominic Vasquez</b>
裝置遙測資訊轉發	Mac 在預設狀態下將蒐集有關 App 和裝置性能的各種資料。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。	<a href="#">將 Jamf Protect 與 Microsoft Sentinel 整合</a>	<b>Jamf Protect</b>	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	<a href="#">網路傳輸流</a>  <a href="#">威脅事件流</a>	<b>Jamf Protect 與 Jamf Connect</b>	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。	<a href="#">如何在 Security Copilot 中整合，如何將 Jamf Pro 整合進去</a>	<b>Jamf Pro</b>	Microsoft Security Copilot	



www.jamf.com/zh-tw/

© 2002-2025 Jamf, LLC. 著作權所有，並保留一切權利。

如欲深入了解 Jamf 與 Microsoft 合作關係的資訊，請[查看我們的 Microsoft 頁面](#)。若想體驗我們的產品，請[申請試用](#)。