



白皮書



## Jamf 與 Microsoft 攜手合作， 成就更好的體驗



就在今年，工作模式有了巨大的轉變，在企業中管理 Apple 裝置的日常也發生了變化。支援遠端員工的能力更是空前的重要，管理者需要最好的利器來幫助他們的機構取得成功——管理 Apple 裝置找 Jamf，其他裝置交給 Microsoft。

許多人認為這是非此即彼的選擇，若仍在討論該選哪一種裝置，或是使用無效的平台來管理所有設備，可能顯得有些過時，畢竟這些設備運作的方式，有著根本的不同。讓各家系統的裝置都能獲得最佳管理之道，並讓像 Microsoft 和 Jamf 這樣合作關係與整合能力的巨頭引領前路，才是解決問題的上策。

本白皮書將說明：

- 為什麼 Mac 的數量在企業中不斷增長，以及如何因應這種狀況？
- 看看 Jamf 與 Microsoft 如何攜手合作，實現易用、高效和靈活的解決方案

## 企業 Mac 的數量不斷攀升

更多員工開始要求改用更為友善使用者的裝置，工作中科技應用的輪廓也進而產生了變化，而通常他們的選擇會是 Mac。

### 選擇的力量

員工自選裝置方案在工作場所逐漸成為常態，您的企業網路也將來迎來更多的 Mac。數量有多少？若員工可以在 PC 與 Mac 之間做選擇，72%\* 會選擇 Mac。企業和 IT 團隊何以需要更加重視 Mac？因為感到幸福、工作效率高的員工，才能帶來更豐碩的成果。此數據擷取自一項針對企業中 Mac 的全球研究\*\*。來看看 Mac 使用者怎麼說...

**97%**

認為有助於提高生產力

**95%**

認為有助於提高創造力

**94%**

認為有助於獨立作業

**91%**

認為有助於提升協作能力

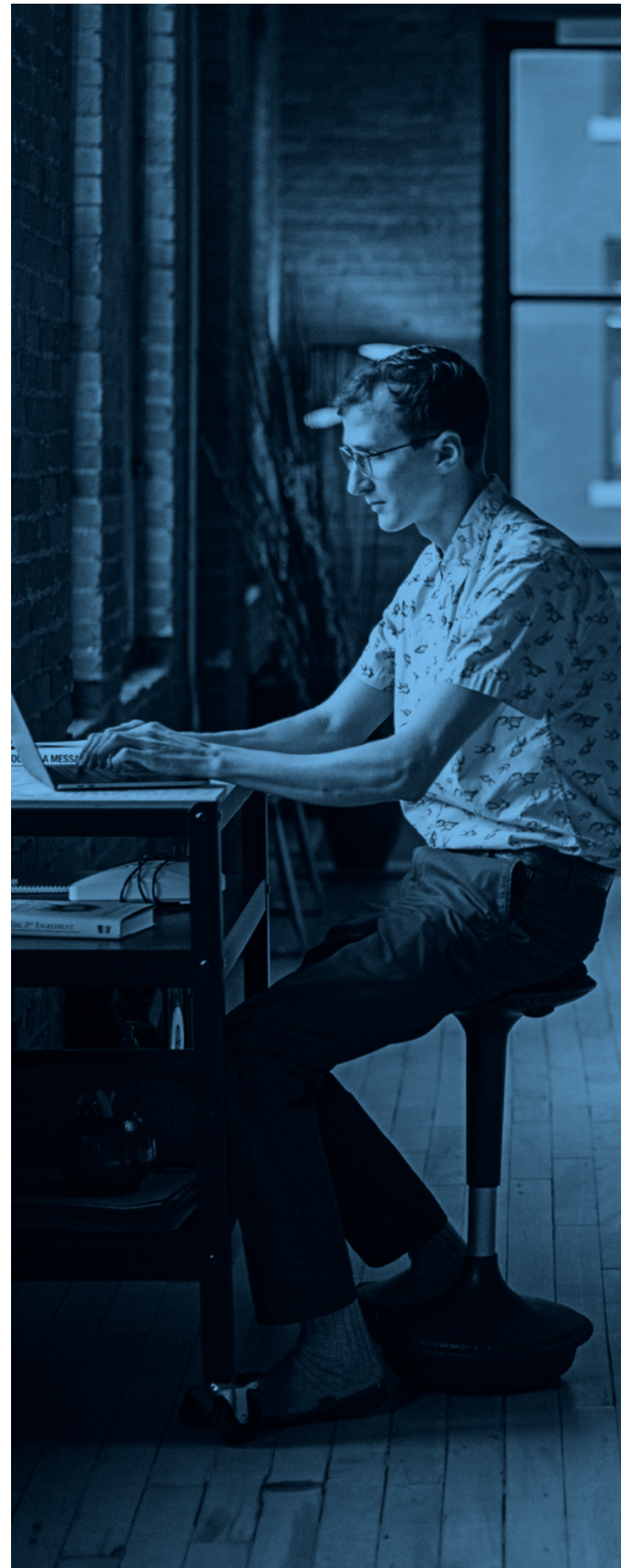
Mac 也被認為在工作場所中，比任何其他設備品牌來的有效率。在接受調查的人當中有 79% 認為，使用其他品牌的裝置將無法達成像使用 Mac 時的高效率。有 83% 的 IT 和人力資源部門受訪者認為，使用 Mac 對他們的工作來說至關重要。

### 提供員工 Mac, 可以提升留任率

給予員工選擇設備的自由，甚至是提供員工 Mac 電腦，皆為提升留任率的重要推手。

**95%** 的受訪者同意，如果給予員工選擇裝置的自由，他們會更有意願留下

重點是，使用 Mac 也並不影響使用者使用他們所愛的 Microsoft 服務。





## Jamf 與 Microsoft 並肩合作

Jamf 與 Apple 的密切關係眾所周知，光是這一點，就足以證明協助使用者執行既安全又具策略性的 Microsoft 整合只是必然。

Jamf 與 Microsoft 於 2017 年宣佈將「條件式存取」導入 macOS，其中還包括將 Jamf Pro 上的設備資料共享至 Microsoft Intune、套用「條件式存取」並提供修補管道，確保只有信任的使用者透過信任設備上的授權 App，才可以存取企業資料。接著到了 2018 年，Jamf 再次拓展與 Microsoft 兼容的技術廣度，為終端使用者創造更加流暢的登入體驗，合作關係並延續到了 2020 年的 Device Compliance for iOS，這個部分我們將稍後為您詳細介紹。2021 年，Jamf 將 Jamf Protect 提供的詳盡裝置資料、偵測與修復能力，以及專門為 Mac 打造的資安機制與 Azure Sentinel 的雲原生資安事件管理 (SIEM) 方案和資安協調、自動化與回應 (SOAR) 功能一塊整合，為資安機構提供豐富的 Mac 設備控制項目和安全性解析。

多年來隨著工作與使用者流程不斷變化，企業的「新常態」也更加普遍，Jamf 與 Microsoft 之間的距離將持續縮小，為使用者和 IT 人員創造更簡化的體驗。

### 從 IT 團隊的角度來看

對 IT 管理者來說，建立可靠、安全且易於更新、保護、維護的設備管理流程非常重要。無論是 Mac 還是 Windows，使用者期望的就只是一致的服務、安全性和可管理性。

不管是 Apple 或 Windows，互相了解對方的過程時而會演變成犯錯的溫床。不少管理 Mac 的 IT 人員者都十分了解並早已習慣 Jamf Pro，隨著 Apple、Jamf、Microsoft 之間的合作關係不斷昇華，許多習慣 Microsoft 系統的人雖然透過 Intune 管理 Mac，卻仍在期盼兩者進行整合。

作為 Windows 管理員，最重要的即零信任環境中的安全性。而 Microsoft Intune 並非最適合管理 Mac 的平台，它最多可以提供的

只是從 Mac 到任何 App 的 Identity Protection 服務。

對身為 Windows 管理員的您來說，則首先必須了解 Apple 生態系的運作原理。Apple 生態系如何進行加密？如何確保防毒機制有效？如何偵測並修復惡意行為？如何進行簽署？

## Jamf Pro 與 Microsoft Intune

Jamf Pro 是管理設備的引擎，並將蒐集得來的數據送回 Microsoft Intune，接著 Microsoft Intune 會負責審查該數據並判斷設備是否合規。

而合規遵循規定則完全取決於管理者，特殊設定、複雜密碼、加密或定時進入睡眠狀態都可以視需求決定要不要執行。這些合規設定內容，便是 Microsoft Intune 和 Jamf Pro 之間的溝通據點。套用這些政策後，管理者便可得知設備是否已正確配置或是否需要進一步採取動作。

其中不同的地方在於，合規或不合規的狀態與使用者掛鉤的這個動作。進入「條件式存取」。只使用 Microsoft Intune 雖可與其他服務進行整合，但操作控制只能在 Intune 內進行。透過這些策略、合規與資安措施，我們看到 Intune 和 Jamf Pro 之間的溝通管道、雙方合作關係、安全層級也都逐漸成形。

共創良好的合作關係是件多麼美好的事。藉由 Jamf Pro，您可獲得完整的管理功能，還可從 Mac 透過 Microsoft Intune 和 Azure AD 來保護存取服務的連線及身分，也就是說，統一使用一種設備其實根本沒有必要。

## Microsoft Enterprise Mobility + Security 與 Device Compliance for iOS

遠距勞動力的資安重點早已從過去的企業安全網擴大至辦公室之外。而因為這個轉變，機構正著手尋找簡化的方法來管理並保護設備。Jamf 身為管理企業 Apple 裝置的業界指標，為了能夠全力支持各機構，我們宣佈推出 Device Compliance for iOS 來拓展與 Microsoft Enterprise Mobility + Security 之間的兼容廣度。





Microsoft 副總裁 Brad Anderson 表示：「『員工自選裝置方案』與『IT 消費化』等趨勢持續增長，機構需要的管理工具必須能夠適應混合辦公環境。Microsoft 與 Jamf 並肩合作，使 IT 團隊可以統整管理員工設備的平台，但卻仍享有各生態系特定的主要功能。」

由於「Microsoft 端點管理員」會與 Jamf 共享設備資料，機構早已可在 macOS 設備上實施「條件式存取」。現在有了 Device Compliance for iOS，IT 團隊還可以防止授權使用者使用任何不符合資安政策的 macOS 或 iOS 設備，並利用 Jamf Self Service 進行修復。

Jamf 會要求使用者註冊他們想要用於存取 Microsoft 365 App、與 Azure Active Directory 連接的 App 的設備。首先，合規標準會透過 Jamf 在 iOS 設備上建立和衡量。接著，由 Jamf 蒐集得來的設備資訊將發送到「Microsoft 端點管理員」。最後，「Microsoft 端點管理員」會查看設備的合規狀態，並運用 Azure Active Directory 動態授予或拒絕存取請求。如果設備不合規，則會向用戶發送通知，並要求在 Jamf Self Service 中進行修正。

透過這項整合功能，機構得以選擇 Jamf 來管理 iOS 裝置，同時還能夠藉由「Microsoft 端點管理員」共享重要的設備資料，如裝置合規狀態。IT 團隊可以借助 Jamf 的功能來管理 Apple 生態圈，同時可運用 Azure Active Directory 和「Microsoft 端點管理員」提供的「條件式存取」，確保只有來自信任裝置的受信使用者才能使用批准的 App 存取企業資料。

## Jamf Protect 與 Microsoft Azure Sentinel

隨著機構的設備和網路基礎設施日益複雜化，資安團隊越來越依賴 SIEM 及 SOAR 等工具來保護其環境。為了確保完整實現 Mac 世界的資安與控制能力，Jamf 已將其端點防護工具 Jamf Protect 整合至 Microsoft Azure Sentinel 的數據流中。

Jamf Protect 是專屬 Mac 的端點防護平台，只需最少的配置即可將所有特定的 Mac 安全性數據和警報資料原生推送到 Azure Sentinel 中。所有惡意或可疑的 Mac 活動以及惡意軟體通知都可以輕鬆地與預訂好的工作流程整合，您的資安團隊幾乎不需要付出任何精力和時間。

得益於 Jamf Protect 的攻擊偵測和日誌紀錄，Azure Sentinel 可更進一步拓展其識別和修復針對客戶環境中所有 Mac 設備廣泛攻擊的能力，同時為機構各方面維持更好的安全性。

藉由 Microsoft 與 Jamf 的整合，客戶可透過早已熟悉的單一管理平台 Azure Sentinel，完整透視其 Mac 資產中的安全活動。

### 總結

有了 Jamf 與 Microsoft 這樣密切的整合功能，再也沒有理由不將 Mac 導入您的環境中。即使是 Windows 管理員，管理 Mac 也可以像管理任何 Windows 設備一樣安全、易於管理、流暢好操作。

沒試過不知道，現在就試用看看。或者也可聯絡您偏好的 Apple 裝置授權經銷商，立即開始使用。



來源出處：

*\*<https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/>*

*\*\*<https://www.jamf.com/resources/e-books/global-survey-mac-in-the-enterprise/>*