和 Jamf 與 Apple 一起實現行動 BYOD

工作裝置可以是 任何 裝置。

不僅限於公司配發的

員工的工作裝置不只是公司配發的筆記型電腦，還包括了任何可存取工作資源的裝置，如個人擁有的智慧型手機或平板電腦。無論您是否有正式的 BYOD 計劃，自備裝置 （BYOD）已經是十分常見的現象。

其實， **ZIPPIA 最近的一項研究**指出， **17% 的員工** 在沒有告知 IT 部門的情況下就使用他們的個人裝置工作。

使用者早就開始帶著自己的裝置上班了，這點是確鑿不移的。

這也帶來了嚴重的安全性問題。IT 部門無法保護他們不熟悉的裝置。舉例來說，Jamf 最近的 **Security 360** 報告發現，「21% 的員工正在使用配置錯誤的裝置，提高了風險性。」

但您可以選擇落實正規且完善的 BYOD 計劃，以保護資料和網路的安全這個解決方案既能讓使用者滿意，又能提升工作效率，同時保護他們的隱私與您的資料。

個人擁有的工作裝置需要什麼呢？

BYOD 必須是容易使用、安全，且具有隱私性的。

不只是具有更好的安全性，還要有絕佳的使用者體驗。您希望員工大幅提高工作效率，並以最安全的方式使用裝置。那您就必須讓這整個過程對他們來說是很輕鬆容易的。

企業組織必須配置、保護裝置上與工作相關的部分，同時，在工作與個人應用程式間可以順暢的交替使用。很重要的一點是，要讓員工清楚地知道，這些工作裝置與其他一般的 個人裝置享有同等的隱私性。

過去的 BYOD 選項

在採用過去的 BYOD 解決方案時，企業和員工都會有所顧慮。員工隱私、員工體驗和企業組織安全等挑戰都可能會阻礙 BYOD 部署。

那麼行動應用程式管理 （MAM） 呢？

使用 MAM：

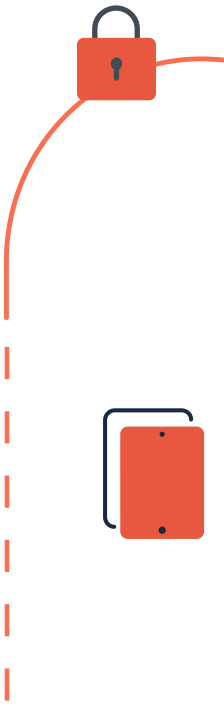
- IT 部門無法設定 Wi-Fi 或電子郵件，也無法自動安裝應用程式（即使是大量購買的也不行）。
- 使用者必須自行下載應用程式，且可供選擇 的應用程式數量也是有限的
- 企業的開發成本相對得高 — 必須專門為 MAM 開發 應用程式

全面的裝置管理：

- 也就是管理整個裝置，全面的裝置管理框架會侵犯隱私，侵入性太強。沒有員工願意接受這樣的 BYOD 。

無解決方案或未經授權的裝置：

- 當員工在沒有任何企業安全、IT 或資安概念的情況下使用個人裝置存取公司資源時



採用 Jamf 和 Apple——一個成功的 BYOD 計劃

Apple 功能除了能確保公司資料的安全，還能保護使用者的個人資料不受企業監控。將兩個裝置合二為一。

Jamf 如何支援 BYOD？

透過使用 Apple 的 **使用者註冊**工作流程和管理式 Apple ID （MAID），將工作與個人帳戶分開設定，進而保護員工的隱私。 然後，Jamf 會協助企業保護及配置該工作帳戶。IT 部門可確保裝置符合企業標準，也可以根據個人或部門需求調整存取和應用程式權限。

以 Apple 強大的安全態勢和無可批敵的隱私保護為基礎，Jamf 做到了：

- 嚴格保護員工隱私
- 在不影響使用者體驗的情況下提供公司存取權限
- 防範應用程式和公司資料受到威脅
- 安全地連接業務應用程式

Apple 十分重視個人隱私。

Apple 的使用者註冊和內建隱私權保護僅允許 Apple 管理員配置工作帳戶；他們無論在任何情況下都無法存取個人帳戶。

企業在使用行動裝置管理（MDM）時有嚴格的限制。

使用 MDM

企業 IT 可以：

- 配置帳戶
- 存取受管理的應用程式清單
- 僅刪除受管理的資料
- 安裝和配置應用程式
- 密碼長度須為六個字元
- 強制執行部分限制
- 配置每個應用程式的 VPN

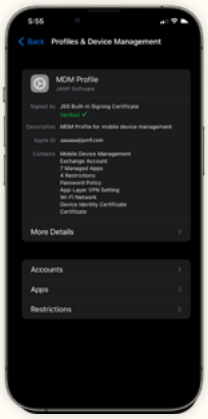
企業 IT 部門無法：

- 查看個人資訊、使用資料或記錄
- 存取個人應用應用程式清單
- 刪除任何個人資料
- 接管個人應用程式
- 須要複雜的密碼
- 存取裝置位置
- 存取單一識別碼（Unique Device Identifier，UDI）
- 遠端抹除 整個裝置
- 管理啟用鎖定
- 變更漫遊狀態
- 啟用鎖定模式

資料來源：APPLE「使用者註冊和 MDM。」

Jamf 如何實現 BYOD

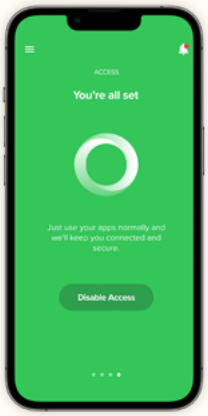
我們的解決方案可共同管理及保護應用程式、資料與業務聯繫，實現 **Trusted Access**（可信任的資源存取）還能保障使用者的隱私安全。



保護隱私的裝置註冊

Jamf Pro 利用 Apple 的使用者註冊功能，將工作帳戶和個人帳戶分開。以防止企業查看或監控個人帳戶 資料。

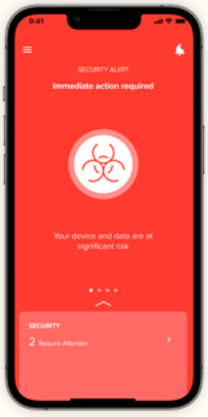
- 配置企業服務的存取權限，包括Wi-Fi、 電子郵件和通訊錄
- 分發並管理整個 iOS 或 iPadOS 應用程式庫
- 部署資料遺失防護政策，防止資料從託管應用程式流向非託管應用程式
- 從註冊到日常使用所需，都能享有完整的 Apple 體驗



安全存取和連接

Jamf Connect 能確保僅有受託管之裝置上之授權使用者才能存取工作應用程式和資料。Jamf Trust 是 Jamf Connect 的終端使用者應用程式。

- 藉由零信任網路訪問 （ZTNA）， 為業務應用程式提供安全、加密的連接
- 通過每個應用程式 VPN 配置 ZTNA，在應用應用程式中管理網路流量，進而保護隱私



行動端點防護

Jamf Protect讓 Apple 的安全性更加強大，輕鬆保護企業 資料。Jamf Trust 是 Jamf Protect 的終端使用者應用程式。

- 透過工作流程管理應用程式風險，審查應用程式，刪除易受攻擊或存在漏洞的應用程式
- 偵測並攔截中間人（MitM）攻擊
- 執行安全檢查，如監控過期或易受攻擊的作業系統 （OS） 版本

員工體驗

在員工存取工作資源時，同樣達到 Apple 使用者期望中的體驗。

唯有在使用者體驗不受影響，同時員工又能確信企業組織不會存取個人資訊的情況下，BYOD 才能真正發揮作用。這兩點，Jamf 和 Apple 都做到了。

用 Jamf Pro 進行使用者註冊：

- 無論是在註冊前或是註冊期間，都讓您清楚地了解 IT 部門是如何管理個人帳戶的
- 不管是處理工作業務或是個人事務，都能順暢地使用 Apple 本機應用程式
- 員工可以通過 **Seld Service**
- 自行下載經審查的應用程式，使用者能保留個人 Apple ID 以存取個人資料，而受管理的 Apple ID 則為工作用
- 帳戶驅動的使用者註冊，大幅降低了落入網路釣魚陷阱的可能性 - 使用者可以在「設定」中使用受管理的 Apple ID 對裝置進行身份驗證

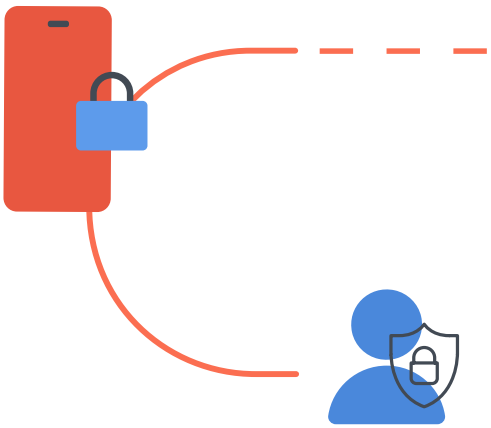
Jamf Trust：如何落實行動 BYOD 安全性

確保每個人的安全及保持員工效率其實沒有那麼複雜管理員將 **Jamf Trust** 部署到員工裝置：單單一個應用程式便可以提供 Jamf Connect 和 Jamf Protect 的存取和安全功能。Jamf Trust 僅適用於工作帳戶，保留個人帳戶。

Jamf 對 Apple 十分熟悉。

專為特定作業系統設計的 BYOD 解決方案，對企業組織的安全性、存取權限和裝置配置相當重要Apple 的易用性、安全性和隱私功能，為企業組織和員工註冊 BYOD 裝置打造了理想的環境。沒有人比 Jamf 更瞭解關於 Apple 的專業知識。

請聯繫您的 Jamf 業務或您偏好的經銷商 ，詳細瞭解 Jamf 如何提升組織安全性和個人隱私。



預約試用