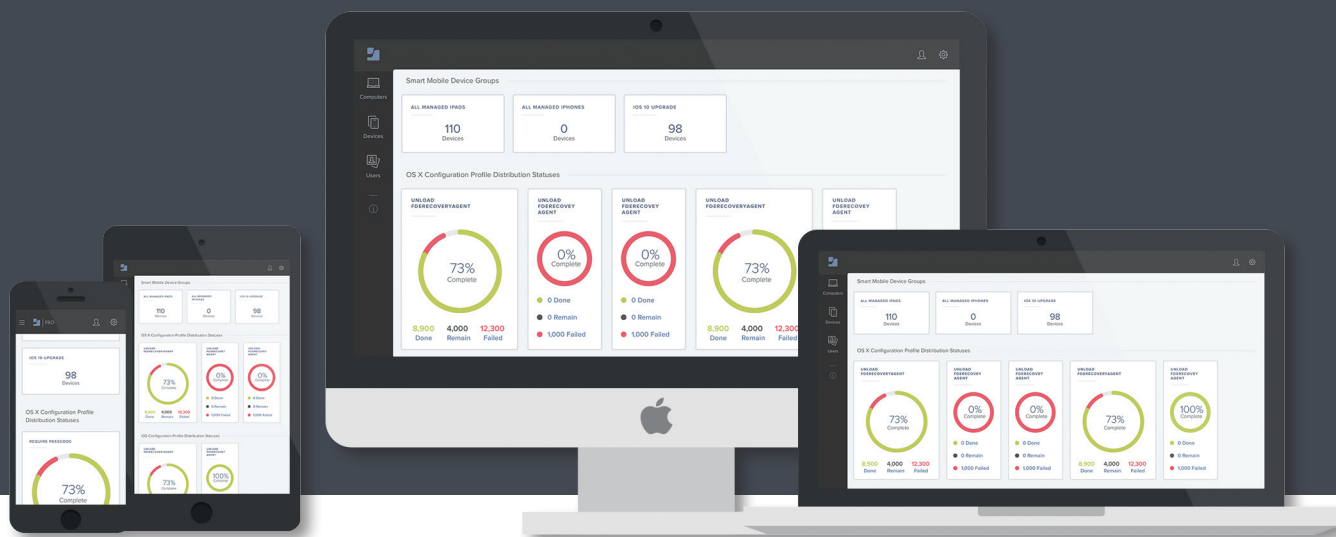




幫助企業使用 Apple 取得成功



輕鬆存取、部署與確保 蘋果電腦的資訊安全

基於對蘋果的熱愛，Jamf 成立於 2002 年，僅專注於蘋果設備管理。至今已有超過 26,000 個國際品牌使用 Jamf 管理超過 1300 萬部蘋果設備。在全球數十個不同的國家裡，共擁有超過 1,000 名員工，幫助企業、學校或政府單位在使用蘋果電腦做為工作設備，提供 IT 團隊強大的管理能力，協助企業同仁高效的使用蘋果設備，同時保障資訊安全。

此外，企業 IT 團隊也能從 Jamf Nation 受益；Jamf Nation 是全球最大的蘋果 IT 管理社群，超過 85,000 名會員，能互相學習並分享管理觀點、最佳實例，或是建議新功能，幫企業使用者選用最合適的管理策略。

Jamf Pro — info

Level 12, Infinitus Plaza 199 Des Voeux Road Central
Sheung Wan, Hong Kong

+852 3008-5865



www.jamf.com/zh

組織企業導入 評估設備的資安思維

- 搭配 Apple Business Manager (ABM) 實現零接觸自動化部署設備

我們應該如何管理蘋果的設備？

Apple 從硬體到軟體，所有產品線皆高度整合，包含我們熟知的 macOS、iOS 及 tvOS 設備。確保產品的穩定度與安全性，讓 IT 團隊可以輕鬆的進行部署。員工也會得到與市面上相同的使用者體驗。

Apple 規劃了一項專門計畫簡化整個部署過程，讓用戶獲得完全無需 IT 人員協助的開箱即用體驗，其名稱為 Apple Business Manager (ABM)。

過去，許多公司與組織都在尋求使用單一工具，同時管理所有的 Apple、Microsoft、Google 設備。然而，這會造成公司組織在管理、使用者體驗與安全性上面造成漏洞。使用單一管理工具管理多個平台時，各項安全功能也將無法正常作用，這也讓 Apple 設備優異的安全強項跟著消失。



Apple 系統框架

Apple 框架 ▶ 為了闡明 Apple 所採用的安全措施，我們必須先來瞭解一下 Apple 框架的基礎知識。



Apple 是否需要部署第三方安全軟體？

Apple 設備內建加密與防毒功能，不同於其它作業系統，Apple 設備通常不需要額外的安全層或第三方外部工具。

除了無需第三方介入，就能立即工作。透過 MDM 更能進一步的監控內部資料保密狀況。此外，Apple 將管理框架直接內建在作業系統上，IT 人員只需透過蘋果推播服務 (APNs)，就能將管理政策推送到設備，達成 MDM 支援的各項管理功能。

避免使用容器化技術添增管理風險

當企業或組織討論資料外洩問題時，經常會提到容器化技術。但這項技術使得 App 架構於該打包技術之上，在作業系統升級時出現程式碼不相容、或是簽章不符合等問題，造成企業管理困擾。Apple 由內而外的整合了軟硬體技術，兼容使用者體驗與資訊安全。只要透過 Jamf Pro 等解決方案就能在原生的方法直接把避免資料外洩，避免因為使用這類技術導致使用者體驗低落、性能下降。

MDM 框架不等同設備管理的完整解藥

Apple 的 MDM 框架十分強大，但對企業與組織來說，許多進階的功能，像是啟用 EFI 密碼等，並沒有包含在 MDM 框架裡面。

Jamf Pro 會在納管電腦裡面安裝 Agent，讓 IT 人員可以設置更進階的策略，配置非 App Store 的軟體（像是 Adobe），延伸天生的 MDM 能力。

一手掌握所有納管設備情況

了解企業環境內有多少設備、如何被使用、軟體安裝狀態、套用了哪些策略與限制，全面並即時了解設備十分重要。IT 人員可以透過 Jamf Pro 要求所有設備定時回來報到，接著分群分組的定制各項報表。

即便發現設備處於不合規定的狀態，Jamf Pro 的智慧型分組（Smart Group）擁有自我治癒的機制，可強制恢復該設備到合規需求，免去 IT 人員逐一修正的必要性。

Jamf 第零天支援最新版本的 macOS

蘋果每年發表的 macOS 作業系統。Jamf Pro 與 Apple 緊密結合，確保每一代新版本上市，IT 人員都能立即思考升級的可能性，導入最新的安全科技。

蘋果電腦設備管理

設備資產報表

macOS 設備具備哪些安全特徵足以我們思考？

AppStore 與企業開發軟體派發

應用程式、系統更新管理



使用 256 bits 的加密金鑰進行全盤加密。在搭配具備有 T2 安全晶片上的 macOS 電腦，亦會使用自身的硬體加速引擎，完整保護資料安全。



Apple 數位簽章

Apple 使用數位簽章保護設備在進行軟體更新及安裝時，辨識合法及安全性，遏止潛在的惡意軟體修改 Mac 上受保護的檔案和檔案夾。



GateKeeper 門禁技術

IT 人員可以透過內建的門禁技術（GateKeeper），確保只有受信任的軟體得以在 macOS 上執行。



XProtect

自動偵測並阻止已知惡意軟體的安裝，若惡意軟體突破重圍進入 Mac，在 macOS 裡另外內建了惡意軟體清除工具修正感染狀況。

更多關於 macOS 安全資料請見：

<https://www.apple.com/macOS/security/>



設備合規管理

我們該如何制定安全標準管理 Apple 設備？

落實 Apple 設備管理之前，我們需要訂定安全標準加以落實。參考 CIS 是一個很好的開始。CIS 全名為 Center for Internet Security，定期出版的 macOS 安全評量，從八大面向探討，被認作是管理 Apple 設備的完整檢核清單，Jamf Pro 在各面向都有完整的對應方式，滿足資訊安全考量。



軟體更新

Jamf 對應 ▶ 延時或強制所有蘋果設備更新最新版作業系統，維持最佳安全性。



日誌與稽查

Jamf 對應 ▶ 收集納管設備或擴充上百項資訊並自動匯出報表，掌握資源狀況。



存取與認證

Jamf 對應 ▶ 設定密碼規則，定期要求員工更改密碼、不得重複使用密碼等。



偏好設定

Jamf 對應 ▶ 開啟磁碟加密、關閉共享及藍牙傳輸，提昇資訊安全、維持員工效率。



網路設定

Jamf 對應 ▶ 藉由程式碼部署，禁止設備使用無線網路或成為網路伺服器。



其它考量

Jamf 對應 ▶ 維持資產編號及名稱與報表一致，並設定 EFI 密碼確保資產可用性。



iCloud 雲端

Jamf 對應 ▶ 關閉 iCloud 雲端等相關功能，減少資料外流風險。



使用者帳號

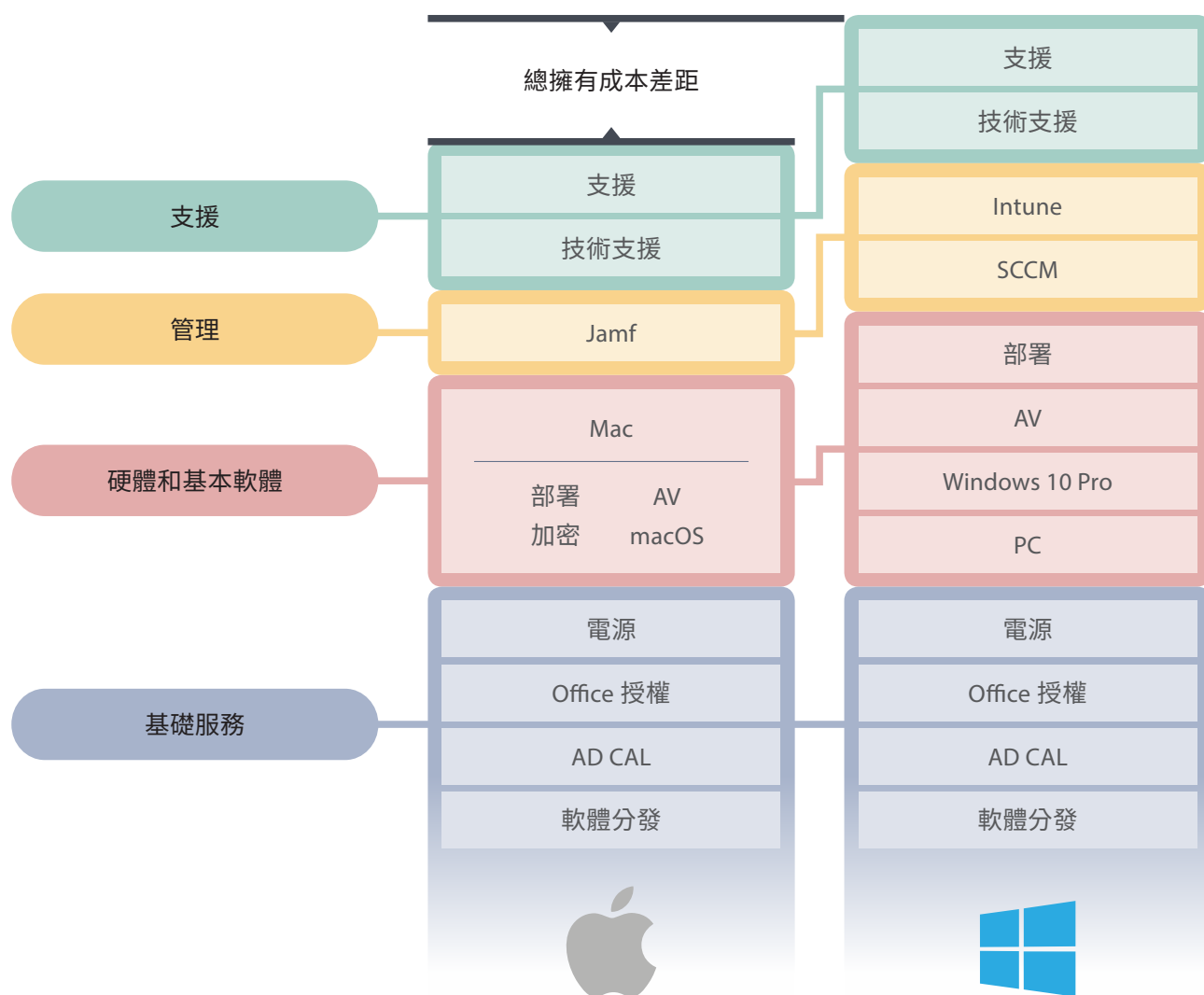
Jamf 對應 ▶ 整合目錄服務避免員工取得管理權限，但仍能自行安裝軟體。

更多 CIS 的資料請見：

<https://www.jamf.com/resources/white-papers/macOS-security-checklist/>



員工擇其所愛、企業節省成本



當計畫向員工提供 Mac 時，不可避免的需要考慮成本問題。多數的企業在考慮到切換到 Mac 時，心裡總想著：Mac 非常棒，但是購買一台 Mac 的價格是 PC 的兩倍。然而，這樣的迷思可以用 IBM 的真實案例打破，IBM 副總裁 Fletcher Previn 在為公司內部導入 21 多萬台 Mac 後，曾於 2016 年的 Jamf Nation User Conference 提及，現今每導入一台 Mac 的總成本相較於 PC，可減少 273 至 513 美金。

每一台蘋果電腦都已經內建了合法且免費的 macOS 作業系統，不同於 Windows 作業系統有多種版本，例如家用版或是專業版，macOS 僅具備單一版本，因此在功能上沒有差異，所有的 macOS 都能綁入至 Active Directory 服務、全硬碟加密、內建商

用等級的防護功能，無需另外採購防毒軟體，避免系統受到侵害。

在管理 Windows 方面，微軟提供 System Center Configuration Manager (SCCM) 以及 Intune 擴充 MDM 功能延伸 SCCM 能力，多數企業都會採購這兩套軟體進行管理。這再一次證明了 macOS 與 Windows 的不同之處，包含 macOS、iOS、tvOS 等都已內建了 MDM 管理框架，Jamf 做為蘋果專門的 MDM 服務提供商，得以利用此框架遠端管理蘋果設備，加上第零天部署的特色，所有蘋果設備推出新版作業系統的當下，Jamf 就能立即提供支援，享有完整的管理功能。