Apple 裝置安全

入門

jamf

無論是縝密規劃的網路攻擊，或是不小心下載到惡意軟體，都可能導致原先豐碩的成果瞬間陷入停頓。駭客的手法愈趨複雜，獲利虧損狀況與使用者 (如客戶、員工及學生) 的資料安全成了組織憂心的問題，因此資安防護力必須要更勝一籌。

Apple 系統與其他系統的資安疑慮一樣真實存在，並且會構成機構資源與相關人士嚴重的威脅。

Apple 的作業系統十分注重安全性，這點毫無疑問，它對軟體和硬體安全與隱私的重視正是 Apple 在企業、教育機構與其他行業廣受歡迎並大量採用的關鍵原因。也正因為 Apple 逐漸成為個人或辦公硬體的首選，以致它成了攻擊者下手的目標。這意味著管理者必須在資安事件出現時迅速做出回應，而不是毫無防備的坐等問題發生。若使用專門抵禦針對 Apple 系統的解決方案，Mac 管理者與資安團隊 (以及他們提供支援的相關人士) 才能更有效並主動的防範威脅，避免日後衍生成更嚴重的問題。

若你是想強化組織 Apple 裝置安全性的主管、管理者，或是想取得基本資訊的新手及想快速複習知識的 Apple 管理老手，那麼這份電子書非常適合你。

Apple 裝置安全入門

為確保機構的裝置與資料的安全，以下多個條件須同時作用：

1. **Apple 原生安全機制：**
   iOS、iPadOS、macOS 及 tvOS 內建的安全性系統
2. **已註冊的裝置：**
   以匯集眾多功能的單一平台來註冊和部署設備，並提供高資安可見度與安全的管理功能
3. **保護裝置：**
   保護實體裝置並確保你的使用者遠離資安威脅
4. **資料加密：**
   持續確保裝置上與網路內、閒置或傳輸中資料的安全
5. **合規性監測：**
   監測裝置，再依判定出的裝置健康度來實施合適的資安防護基準
6. **App 安全與漏洞修補：**
   確保 App、軟體及作業系統的修補程式皆維持在最新版本

jamf

1

基本要素一：

APPLE 原生安全機制

Apple 硬體是市面上最安全的開箱即用選項，選擇專為 Apple 設計的管理與資安方案更可進一步延伸 Apple 的強大功能

macOS (Mac 作業系統)、iOS (iPad 與 iPhone 作業系統) 及 tvOS (Apple TV 作業系統) 內建的安全性功能用途廣泛並具備諸多效益如：

- **Apple 作業系統是由 UNIX 系統發展而來，這個已成熟發展、經過充份研究且十分穩定的平台因具備深厚的開發基礎，造就了 Apple 的豐富運算能力。**
- **強大的 OS 資安框架：**
  - 公證
  - 門禁
  - XProtect
  - 惡意軟體移除工具 (MRT)
  - TCC 防護
  - 快速安全回應
  - 封閉模式
- **確保實體裝置安全的方法：鎖定或在遺失時以「尋找」追蹤裝置**
- **可透過行動裝置管理 (MDM) 平台的配置選項，執行並配置安全性控制**
  - Apple 裝置上已內建安全的裝置註冊模式，例如「自動裝置註冊」與「使用者自助註冊」，因此不論是公發或個人裝置，我們都能支援相應的所有權模式 (如 BYOD、CYOD 和 COPE)，並免除不安全的註冊連結、可疑的電子郵件邀請等風險
  - 以深度整合的「Apple 商務管理」或「Apple 校務管理」輔助並集中管理全部機構所有的硬體設備，再於空中啟用「監管」並安全交接給 MDM 解決方案來實現裝置管理功能，比如管理 App 部署、安全開通裝置及零接觸入職工作流程

我們的 MDM 平台專為 Apple 裝置設計，可運用 Apple 裝置既有的安全性配置，參照行業基準並根據不同機構的特殊需求，在少數或無數台裝置上部署與執行這些安全性配置，因此不論是設置上千台或一台 Mac，都一樣的輕鬆。透過 MDM 平台，你可以獲得更廣泛的安全控制內容，這個工具可讓你在偏好的任何裝置上輕鬆執行管理任務。舉例來說，你可以遠端鎖定與清除遺失或應從資產清單上移除的裝置，藉此簡化重複性工作任務，當然還有許多其他功能。如果你有興趣深入了解，歡迎參閱我們的《Apple 裝置管理入門》電子書。

安全性功能一覽

macOS、iOS、iPadOS 及 tvOS 裝置的原生安全性功能

macOS	iOS 與 iPadOS	tvOS
軟體更新	軟體更新	軟體更新
系統完整保護 (SIP)	安全的系統	App Store
「門禁」	App Store	AirPlay 設定與密碼
App Store	生物辨識技術	App 限制條件
「檔案保險箱」加密	硬體加密	螢幕保護程式
「監管」	「監管」	「監管」
XProtect 和惡意軟體移除工具 (MRT)	App 沙盒測試	
「尋找」	「尋找」	
隱私權設定	隱私權設定	
公證和文件隔離	「安全隔離區」和生物辨識技術	
Endpoint Security API	公證	
App 沙盒測試		
「安全隔離區」和生物辨識技術		

2

基本要素二：

安全的已註冊裝置和裝置部署

成功的關鍵在於是否奠定穩固基礎，而穩固的基礎與後續其他項基本要素，甚至是訂定管理與資安的主調息息相關，因為這些步驟之後可能都會影響到 App 生命週期和硬體

要正確配置裝置並以標準化、高效的方式安全部署整批設備，第一步就是使用「自動裝置註冊」，這是我們透過免費的「Apple 商務管理」與「Apple 校務管理」達成的服務。

藉由「自動裝置註冊」，Apple 便可以得知你的機構內擁有的裝置數量、我們等等會提到的其他所有權模式，並將裝置指派讓 MDM 管理。接著當使用者啟用註冊於此計畫的裝置時，系統將：

- 自動將裝置註冊到 MDM
- 啟用「監管」，這是實現更為嚴格安全控制不可或缺的一部分
- 允許管理者套用設定描述檔並強化資安設定
- 在開始使用裝置前，便確保已部署關鍵的安全性設定和承載資料
- 簡化作業系統更新和安全修補程式的管理與部署流程
- 一個平台就能處理 App 的購買、配置及部署，進而減少開通裝置的步驟，也確保 App 的安全性已經過審查
- 讓使用者不需 IT 人員協助也有能力維護自己的裝置，藉此縮短裝置設定流程
- 可執行遠端管理，無論使用的是哪一種裝置，或是在哪裡使用以及透過哪個網路來連線

裝置所有權模式

隨著裝置數量不斷成長、辦公地點逐漸呈現分散趨勢，越是凸顯裝置管理與資安自動化流程的必要性。市場產業十分多元、使用者族群形形色色，而企業選擇工作裝置的現象也是如此，有越來越多的機構已經改使用 Apple 平台與行動裝置。

有些機構透過實施員工自選裝置方案來導入 Apple 系統，此方案會派發運行 macOS、 iOS 及 iPadOS 的公司所有裝置給使用者，其他機構則是透過支援 BYOD 方案，讓員工能夠以個人裝置存取企業資源。有了 BYOD 方案，使用者可持續以自己熟悉、信賴且喜愛的軟體與硬體來辦公，機構也不必為每一位使用者都購入裝置，進而能抵銷開支。

這也促使問題從「我們該怎麼提供職員工作用的裝置？」轉為「我們該怎麼確保企業資源維持安全？」

從下列裝置所有權模式可以看得出來，為什麼機構應該選擇靈活一點的 MDM 平台，否則無法支援不同模式：

員工自備裝置 (BYOD)

可以說是企業最常採用的模式，這個方案可讓員工使用個人裝置來存取企業資源。在員工存取企業資源前，便要求他們手動將裝置註冊至機構的 MDM；另外一個優勢就是，使用者再也不必擔心是否可以存取工作必要的資料、工具及服務，而機構也不必擔心註冊裝置是否已搭載完善的資安系統與配置設定，以確保使用中、閒置中與傳輸中的資料皆維持安全。

員工自選裝置 (CYOD)

此方案是變化版的 BYOD，只不過多數的案例中，這個方案的裝置通常所有人是機構或組織。在企業環境中，使用者會透過這台裝置辦公，在教育環境中，則是會以這台裝置進行學習。如果導入這個方案，那麼使用者就能選擇最適合自己使用需求的 Apple 裝置。每一台裝置都會註冊並受機構的 MDM 系統監管，再指派給使用者。所有必要的 App、描述檔、裝置設定將連同資安系統一同開通，並確保建立在適合各機構資安態勢的基準上，佈建時也會給予使用者對應的辦公權限。

公發裝置 (COPE)

COPE 模式在大型機構中目前呈增長趨勢，尤其是那些已經選擇完全遠端或混合辦公的企業。這些機構會購入工作裝置，所以他們會是裝置的所有者，後續再將裝置註冊至機構的 MDM 以進行監管。與 CYOD 一樣，使用者辦公所需的工具會根據裝置和公司的資安態勢來進行安裝和管理。但與 BYOD 類似的一點是，選擇這個方案的機構會鼓勵使用者無論私事還是公事，都以這台裝置來執行，這個做法可確保企業資源存放在監管的 App 上，並且會受到描述檔的箝制，因而能夠維持安全。雖然這個做法會促使企業可以藉由 COPE 裝置存取員工的私人資料，我們還是可以透過適當使用原則 (AUP) 與資料管理來為這些裝置提供妥當的管理與隱私等級，因此考量到員工個人隱私可說是格外重要。

靈活的註冊方式

為了能夠在單個 MDM 環境中，簡化多個所有權模式的管理事務，Apple 開發了兩種互相彌補的裝置註冊方法，讓機構在管理與實施安全機制的同時，也不會損及使用者隱私。

自動裝置註冊

大多數企業更偏好選擇的方式。以 MDM 的 PreStage 從 Apple (或授權的第三方) 購入裝置、在裝置啟用時即開始註冊流程，此方法的每個步驟都會經過驗證，從 Apple 到 MDM 再到管理者，整段旅程都可自動化，確保管理流程不間斷。由於整段流程已經過驗證，所以裝置在透過「自動裝置註冊」註冊時，便已經啟用「監管」狀態，而監管裝置可讓 IT 人員獲得管理該裝置的完整掌控權。「監管」是信任的根基，也是執行部分管理任務必不可少的要點。

User-initiated Enrollment (使用者自助註冊)

對於個人 BYOD 裝置來說，這個註冊方式更新也更為普遍。User-initiated Enrollment 這個註冊方式需要裝置的使用者或所有者在「設定」App 中手動註冊這台裝置，並使用公司憑證來進行身分驗證。在完成自助註冊流程後，機構的 MDM 和使用者裝置之間的雙向通訊便會受到保護。

一旦裝置註冊完畢，即使是個人裝置也可以透過 MDM 來管理，管理者可藉此安裝合格的 App、部署描述檔，還可以使用一組配置修改特定的設定內容，讓機構可以按照裝置要求和相關管理動作來達成「使用者」而非整部裝置的必備條件。Apple 的設計可讓機構適時採取必要動作，確保資料的存取和儲存方式、與 App 的連線、在網路間傳輸時，都能安全無虞，並兼顧裝置上私人的 App、資料以及個資安全。藉由將私人資料綁定至私人的 Apple ID，企業資料綁定至管理式 Apple ID，機構便可訂定對監管裝置的可見程度。

3

基本要素三：

保護裝置

保護裝置、資料及使用者遠離資安威脅

「駭客只需成功一次就足夠，但是我們連半次失誤都無法承擔。」

——惠普 Chris Triolo

如果回顧近代歷史上一些最大規模、最複雜甚至是最致命的資料外洩事件，我們會發現一個共同點。諸如 Stuxnet 這類的攻擊，便是透過感染約聘人員的筆電來對 SCADA 裝置進行更新，以停止伊朗的核濃縮計畫。某位開發人員就是濫用 API 從 LinkedIn 成功抓取七億筆用戶的個人識別資訊 (PII)，然後再到黑市兜售。印度的 Aadhaar 為全球最大的身分資料庫，此系統存有超過 11 億名印度公民的 PII 和財務資料，威脅人士在藉由未受保護的網站成功連線到資料庫後，便竊取並兜售個資。上述這些攻擊事件，都僅僅只是成功針對或入侵一台裝置而起。

繞過機構的資安框架來存取敏感資料，同時將使用者的安全置於危險之中最常見方法之一就是針對單一台裝置。若不論你的機構代表哪個行業，也先不論你的機構是否有向學生、教師、醫療人員、遠距員工、零售人員、知識型員工或經常旅行的旅客，提供資料和/或資源，你的設備在任何時候都可能位於世界上的任何角落、透過任意數量的不受信任網路進行連接，使得裝置和公司網路面臨的威脅風險因而倍增。

裝置遺失或失竊

iPhone、iPad 或 Mac 遺失或遭竊不僅會造成財務上的損失，它還意味著巨大的資安風險，其後果可能是無法估量的。下方舉例降低裝置遺失或失竊風險的重要性：

現實生活場景

一名遠距員工正為法庭上進行中的責任案件準備法律檔案，並在附近的一家咖啡店工作。在需要續杯咖啡時，他們會離開位置，讓公發的 Mac 裝置暫時無人看管，扒手可能就會趁這時把筆電偷走，也因為裝置沒有上鎖，攻擊人士可以不受限制的存取敏感，甚至高機密的企業資訊，因此對當前的法律程序和企業聲譽可能產生負面影響。

第二個例子為甲同學使用個人的 iPhone 前往教育平台上存取學習相關的資源，卻在換班時把裝置放錯位置，另一名乙同學找到該手機，並開始查看甲同學的帳號資訊、存取敏感的 PII，比如甲同學的住址、電話號碼或學生 ID。未經授權的使用者可利用 PII 資訊，進行身分盜用或冒充成甲同學來犯罪。這支手機甚至可能進一步受到惡意軟體的影響卻依然返還給受害者，讓威脅人士能遠端追蹤學生，危害他們的人身安全。

再更白話一點來說：裝置搞丟或被偷。意外事故和注意力不集中不時會發生，因此，意外前的規劃十分關鍵 (不把問題的核心放在「萬一」，而是認定「遲早」會有人粗心搞丟裝置)，如此才能確保策略有到位，並在裝置遺失或被竊之前就將風險降至最低。

其他使用者和資料安全的考量點在於，多數的裝置，尤其是學生或患者用裝置，又或者是多人共享裝置，這些環境都需配備安全機制來抵禦錯誤使用、意外發現他人個資、存取和查看不當與不安全內容的情形。

在配置使裝置符合合規要求時強化安全性設定，可能會是一項相當耗時和勞累的工作，尤其當裝置數量增長時，但是具體將取決於你的機構的需求。

若要手動執行保護裝置的措施或限縮裝置使用，你需要：

Mac

- 所有裝置都需要密碼
- 從「系統偏好設定」>「iCloud」中啟用「尋找我的 Mac」
- 使用者須能夠登入 iCloud 並記住密碼 (並已事前啟用「尋找」)
- 如果裝置遺失或遭竊，則需要向 Apple 回報，同時須啟用清除功能
- 依照 Mac 序號或資產標籤來追蹤所有設備
- 在裝置上啟用家長/監護人控制，以阻擋不當內容和惡意網站 (使用 Safari 瀏覽器)
- 讓 Mac 及時更新所有 App 和系統，以最大程度降低漏洞的風險
- 配置和強化裝置設定，以最大程度減少可能使資料不安全的錯誤配置
- 部署可支援的 App 並確保它們維持在最新狀態
- 安裝和配置端點防護平台，以監測裝置、識別並修復威脅事件

手機與 iPad

- 所有裝置都需要密碼
- 從「系統偏好設定」>「iCloud」中啟用「尋找我的 Mac」
- 使用者須能夠登入 iCloud 並記住密碼
- 依照裝置序號或資產標籤來追蹤所有設備
- 如果裝置遺失或遭竊，則需要向 Apple 回報，同時須啟用清除功能
- 在個人裝置上啟用家長/監護人控制，為每部裝置建立不同的帳號
- 讓 iOS 裝置及時更新所有 App 和系統，以最大程度降低漏洞的風險
- 配置和強化裝置設定，以最大程度減少可能使資料不安全的錯誤配置
- 部署監管的 App 並確保它們維持在最新狀態
- 安裝和配置端點防護平台，以監測裝置、識別並修復威脅事件

Apple TV

- 在所有 Apple TV 上都要求輸入密碼
- 設定限制條件：
  - 從主選單前往「設定」>「一般」>「取用限制」
  - 選取後即可啟用
  - 若被要求，則請設定四位數密碼
  - 請再次輸入四個數字，然後選取「確定」
  - 記住密碼
  - 為所有 Apple TV 重複此步驟

如要限制 Apple TV 的 Airplay：

- 從主選單前往「設定」> 選取「AirPlay」

- 開啟或關閉「AirPlay」

選項如下：

- 所有人
- 連接相同網路的人
- 為所有 Apple TV 重複此步驟

同業最佳 MDM 解決方案 (如 Jamf Pro) 藉由執行管理任務，來限縮裝置使用和確保安全的做法如下：

Mac、iPhone、iPad 及 Apple TV

- 初次使用就設定好所有限制與安全性功能，或者可藉由「監管」、可信的描述檔或政策來自動啟用
- 無論裝置實際位置、也不論是否已經登入 iCloud (且無需使用 Apple ID)，便可遠端鎖定或清除任何遺失或不當使用的裝置
- 憑證與配置設定是依循使用者，而不是裝置，以此方式在交接與清除裝置時，讓多人共享裝置也能維持安全
- 將管理式 Apple ID 設為處理與辦公相關的任務，同時讓使用者也可以透過消費型 Apple ID 存取儲存在 iCloud 上的個人 App、資料及設定
- 維護所有設備資產。除了可透過序號、資產標籤等類別來分組，還能蒐集與裝置相關的必要資訊，舉例來說，像是指派使用者、作業系統版本或已安裝的 App 等
- 執行管理類任務。派發指令給一台或是多台裝置，例如部署安全更新、升級至全新 OS 版本、清除已上鎖裝置上被忘記的密碼等
- 實施家長/監護人控制。可選擇根據特定條件或一次對所有裝置套用限制條件，以封鎖不當或不安全 App 的存取連線
- 部署使用者在家中、辦公室、學校，或其他任何維持高效工作地方所需的監管 App，預先批准要在 Self Service 自助服務區上陳列的 App，讓使用者能夠在需要時隨時取得想要的軟體
- 可將端點防護方案與你偏好的 MDM 整合，確保裝置持續受到監測並可抵禦資安威脅，同時將詳細的遙測數據與 MDM 分享，藉此啟用政策型管理，將事件回應流程自動化
- 集中一處管理裝置任務的各個方面，確保裝置、使用者和資料免受網路威脅，同時兼顧使用者隱私

這樣良好的體驗不僅簡化了員工和 IT 團隊的工作，而且還能確保提供終端使用者完整的支援。我們不僅延續了大眾喜愛且愛戴的 Apple 體驗，也沒有因此犧牲組織、行業合規性和安全要求或使用者隱私，並轉而採用更嚴格的安全控制。

4

基本要素四：

資料加密

有關閒置資料與傳輸中資料的基礎知識，以及如何確保兩種類型的資料皆安全無虞

不論你是保護學生相關資訊的校園、維護患者病史的醫療機構，或者是希望能保護智慧財產權的企業，加密都不再只是選項，而是有其必要性。任何一間企業如果想確保敏感、機密、關鍵任務型的資料或任一類別的資料獲得安全保護，最佳做法就是將裝置上的所有資料進行加密。

以下是裝置上三種資料狀態的摘要：

閒置資料：(通常) 存放於本機，一台閒置、未使用的裝置

傳輸中的資料：透過通訊管道 (有線或無線網路) 來接收或傳送資料

使用中的資料：既沒有存放在永久存放區，也沒有透過網路傳輸，這通常是指當前 App 或其他處理程序正在使用的資料

每個州各自有固有的風險，也就是說，適合某個州的解決方案，可能也不一定完全符合其他州的需求。雖然量身打造可能會增加資安策略的複雜性，但請不要擔心，因為有效解決方案的核心，都是以基本加密功能為出發點。

現實生活場景

公司的人資部門來了一位新員工，在收到新的 Mac 後，他完成設定步驟後隨即開始辦公。他們的工作職務之一是需要**使用試算表軟體**建立緊急聯絡人樹狀圖，上面需包含每位員工的姓名、職稱、公司電子郵件地址、私人地址和聯絡電話，並說明他們是主要聯絡人還是備用聯絡人。這份資訊將**備份於本機**，其中包含 C 字輩和管理階層的個人資訊，而授權的相關人員必須**可透過雲端儲存庫安全取得副本**。

在上述的場景中，粗體標示部分代表不同的資料狀態。首先，「使用試算表軟體」正是「使用中資料」的一例，意即在 App 內使用資料時必須確保維持安全；要達成這一點，便須要檢查、驗證軟體的完整性，以確定內部安全機制沒有被威脅人士或惡意程式碼入侵。「備份於本機」是「閒置資料」的一個例子，為了避免資料遭未授權人士存取或讀取，啟用加密程序至關重要。「可透過雲端儲存庫安全取得副本」則是「傳輸中資料」的一個例子，這是泛指透過網路來接收與傳送的資料。所有網路通訊連線，都必須進行端到端加密，確保只有參與通訊的兩端才能成功解密訊息，避免這筆資料遭未經授權者攔截或竊聽。

雖然第三種資料狀態聽起來和傳統 VPN 沒有兩樣，但兩者的差別就在於「已取得授權的相關人士」一詞。零信任網路存取 (ZTNA) 為「傳輸中資料」提供加密，也可與你的身分供應商 (IdP) 進行整合，因此使用者和裝置都須要經過成功驗證並開通必要的存取權限，才能通過多個防護層存取請求的資源，徹底落實最小權限原則。此外，有別於傳統授權存取整個網路的 VPN，ZTNA 的安全連線可為每個受保護的 App 或服務建立獨特的微型通道。除了實施最小權限原則來提升安全性，同時也會執行運行狀況檢查來確保裝置在每次發出請求和授予存取許可權時，都至少符合最低要求和使用者身分驗證要求。

如何加密三種不同狀態的資料

閒置資料

裝置或磁碟區加密

建議的最佳做法為替電腦上的磁碟區或整部裝置的資料加密，這麼做有幾個原因：由主動和被動措施組成的加密啟用流程十分容易配置，並可為永久存放區的閒置資料將安全性最大化。我們使用了演算法，因此攻擊者可能需要花費數百年，甚至是數千年的時間，使用最強大的電腦日以繼夜的工作才能攻破，相較之下，啟用加密流程可說是相當省力。如果你問是否要將安全性控制納入深度防禦策略的一部分，那麼答案應該是不假思索的「是」，而這就像是象徵德州誕生的阿拉莫之戰，又或者是成語「背水一戰」的概念一樣。

以下我們以一些常見的資安事件為例，這些事件可透過啟用磁碟區或完整裝置加密來有效降低傷害：

裝置遺失或遭竊

iPhone、iPad 或 MacBook 放錯地方，其中手機和平板尤其常見。移動的頻率越高，遺失或竊取發生的機率就越高，也就是說，一旦裝置脫離使用者的掌控範圍，威脅人士越有機會趁虛而入，取得存放在裝置上的資料。

或許你會說，複雜或高強度密碼也可以保護裝置，雖然這一點會因不同裝置而異，但是有心的攻擊人士仍可以使用其他方法攻破密碼保護層，存取裝置上部分甚至全部的資料，除非今天裝置有另外經過加密。啟用加密這個簡單的步驟，會將資料打亂到無法讀取的程度，唯有解密密鑰才能再次復原資料。不論裝置是否已開啟到登入畫面，或 SSD 固態硬碟有沒有出於不明原因而接上另一部裝置，在尚未解密或使用復原密鑰前，其餘任何情況都會讓資料無法讀取、無法使用，資料將維持在加密狀態。

實地存取

與裝置遺失或失竊的情形類似，不是只有放錯地方才會讓他人有實地存取裝置的機會。如果是工作區的共享裝置，那麼分配給你的電腦或任何運算裝置，都可能成為威脅人士趁無人查看時下手的目標。當你結束工作，登出、關機，或是當你不在螢幕前需要鎖定裝置時，裝置上或儲存區裡的資料都能維持在加密狀態。如果要解密資料，則必須要有解密或復原密鑰才能取得對受保護資料的可讀存取權。

法規遵循性

端看你的機構的行業別，你可能會受特定法律約束，我們稱之為法規，這些法律規範了保護資料和資料處理方式的最低要求，同時還規範並限制哪些職位才可處理受保護的資料類型。特定行業會比其他行業面臨更嚴格的監管，如金融業和醫療產業，而其他行業可能只會著重在資料安全的部分層面，例如專門確保學生權益和與這方面相關的 PII 教育法規。

如先前已經提到的，規範是以法律為基礎，如果機構不遵守治理機構訂定的規則，則後果不堪設想。加密是在資料閒置或傳輸中等不同狀態時，必備的基礎資安機制，它可最大程度降低受管資訊因資料外流、洩露甚至曝光而落入惡意人士之手的風險。

資料加密與 Apple 裝置

- macOS 的磁碟區加密已內建於「檔案保險箱」，你無需安裝任何軟體即可加密 Mac 上的資料夾、完整磁碟或磁碟區
- 較新版的 Mac，比如搭載 Apple 晶片的機型，則仰賴「安全隔離區」；這個具備專門用途的硬體零件，可用於處理加密密鑰的建立和存放，並同時執行演算法
- 搭載 Intel 晶片的 Mac 則是採用名為 T2 的安全晶片來執行與「安全隔離區」類似的功能
- 「檔案保險箱」已通過 FIPS 140-2 認證。也就是說，Apple 加密系統不僅已通過認證，還符合美國聯邦政府的加密最高標準
- 你可以手動或遠端啟用「檔案保險箱」：個人使用者可以自行在配備的裝置上選擇是否要啟用，或者 IT 人員可透過 Jamf，一次為數百甚至數千部裝置啟用「檔案保險箱」
- 只需在 macOS 裝置上進行身分驗證或在 iOS 和 iPadOS 裝置上輸入密碼，即可授權使用者加密或解密磁碟區。如果使用者的裝置有支援生物辨識功能，則可運用 Apple 的 Touch ID 或 Face ID 技術，為資料防護額外增加一層安全機制

如何在 macOS 裝置手動啟用「檔案保險箱」：

- 前往「系統設定」>「隱私權與安全性」>「檔案保險箱」
- 點選「開啟...」按鈕以啟用加密
- 為所有裝置重複此步驟

若要在所屬機構的全部裝置上啟用「檔案保險箱」磁碟加密，請多加利用 MDM 解決方案來部署、執行並將流程自動化。你可以部署啟用「檔案保險箱」的描述檔或政策。如果員工之後有需要進行解密，可以向 IT 人員取得復原密鑰。

- 在 Jamf Pro 上簡單點選幾個按鈕，即可建立設定描述檔
- 不論有多少台裝置或 macOS 電腦，都能以更精細的方式來進行部署
- **連步驟三都沒有**

有了 Jamf Pro，即便使用者自行啟用「檔案保險箱」，你也可以設定讓復原密鑰重新導向，IT 人員接著會將密鑰存放在管理解決方案中，以便後續快速取用。

如果是 iPad 或 iPhone 呢？

替 iOS 和 iPadOS 裝置加密，不代表比較輕鬆。iOS 裝置在密碼設定完成時，加密流程就會隨即啟用。你可以獨立執行此動作，也可讓 Jamf Pro 替你執行此動作、設定密碼強度的參數，例如最小長度和複雜性要求。

傳輸中的資料：

加密端到端網路連線

傳統作法會要求使用 VPN 來保護從一台裝置轉移到另一個服務的資料。這個方法可追溯至幾十年前，VPN 當道的時代，它可透過不可信的網路 (如網際網路)，安全橋接兩個截然不同網路。

雖然許多個人與企業用戶時至今日仍以 VPN 作為安全性控制，但是過去幾年來在辦公環境採用 Apple 裝置、個人和企業用行動裝置呈爆炸性增長、機構逐漸轉型為完全遠端和混合辦公模式，這些運算環境的轉變都凸顯 VPN 技術已無法有效保護現代威脅環境中的裝置、使用者及資料。

種種變化逐漸顛覆我們使用電腦和行動裝置來工作和玩樂的方式。那麼，我們還有什麼理由非得繼續仰賴陳舊的安全策略，來保護傳輸中的資料？

對此，我們提出的應對解決方案為零信任網路存取 (ZTNA)。更詳細一點的說，ZTNA 是完全依照現實中的需求來開發，它可確保各類型的裝置、本機和分散型使用者和團隊的安全。此外，在透過不可信網路來存取資料、仰賴雲端服務來拓展基礎架構的同時，機構的網路安全邊界也將越趨模糊。所有這一切，以及針對 macOS 和行動裝置的威脅可見顯著增加，卻依然能夠確保遠離並抵禦已知和新型的資安威脅。

簡單來說，保護網路連線不再只是為了維持員工出差或一些特殊案例時的遠端生產力。

ZTNA 不只是加密通訊連線的兩端這麼簡單而已，它在執行更精細的安全防護機制，保護相關人士、避免不當存取企業資源的同時，也將威脅發生的可能性降至最低。ZTNA 是透過以下做法，來實現這些目標：

- 可與雲端身分廠商 (IdP) 整合，集中一處便能管理使用者帳號，權限原則將依循使用者帳號
- 頻繁的查驗裝置，確保端點符合最低要求，並藉由以下方法來維持安全完整性，例如確保修補程式維持在最新狀態、查看是否有越獄或破解 Root 權限的情形、端點防護是否已正確安裝和配置
- 如果裝置未通過運行狀況檢查或被斷定為已遭到入侵，ZTNA 與 Jamf Pro 這類同業最佳的 MDM 解決方案的整合將啟用政策型管理，透過共享遙測數據，中止存取連線，再執行必要的修復任務使裝置回歸合規狀態，確保解決所有偵測到的問題
- 屏棄傳統 VPN 的絕對信任模式，在每次請求存取公司資源時，都遵循「永不信任，一律驗證」原則，並且只有在成功進行驗證後，才會授予存取所請求的資源

你需要為傳輸中的資料準備什麼

連至 VPN 伺服器的安全網路連線

若要手動建立 VPN 連線：

iOS 與 iPadOS 裝置	macOS 裝置
▸ 前往「系統設定」>「VPN」	▸ 前往「系統設定」>「網路」>「VPN」
▸ 選擇「加入 VPN 設定」	▸ 選擇「加入 VPN 設定」
▸ 在裝置上輸入 VPN 的伺服器位址	▸ 在裝置上輸入 VPN 伺服器位址
▸ 從網路選項選取該位址	▸ 從網路選項選取該位址
▸ 為每部裝置重複此步驟	▸ 為每部裝置重複此步驟

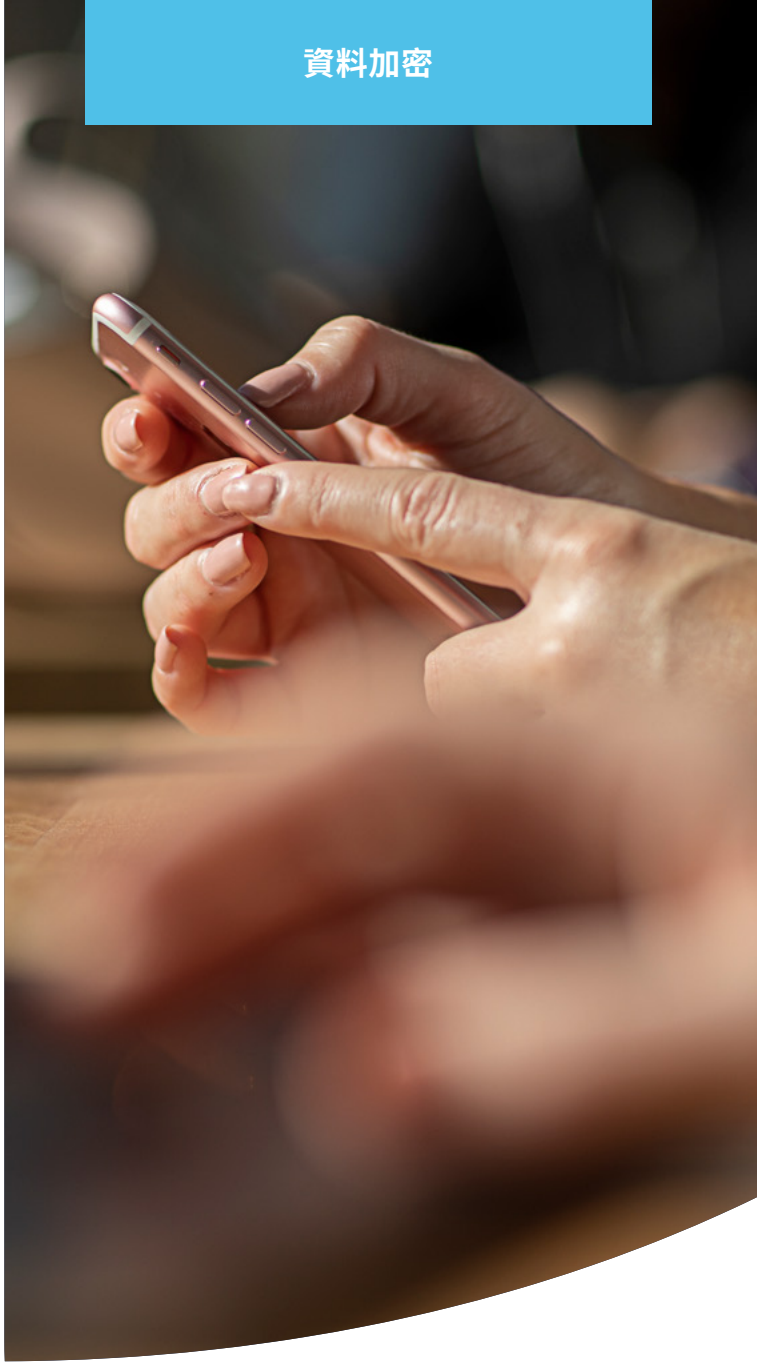
若要將多部裝置連線至 VPN

在設定好 VPN 廠商後

- ▸ 在 Jamf 這樣的 MDM 平台上，為 iOS 或 macOS 裝置建立設定描述檔
- ▸ 將描述檔部署至無限台裝置
- ▸ 你猜對了——沒有步驟三

我該如何確定我的加密防護安全無破綻？

確保安全性和加密一致性的重要方式之一，便是由雲端託管 MDM。使用 Jamf Cloud 可確保你的伺服器和資料安全無虞，任何更新或修補內容在推出之際，你也能馬上取用，實屬值得你信賴和讓你高枕無憂的好產品。



ZTNA 相較於傳統 VPN 的優勢：

- 對安全驗證的態度從絕對信任轉換到抱持保留態度，零信任模型在授予請求資源的存取權前，會先要求驗證裝置和使用者，藉此增強安全性
- 分流技術可確保業務流量的安全，私人流量會直接路由到網際網路，而不是回中央網路，藉此減少開銷與節省頻寬，這也意味著更高的效能和更加嚴謹的使用者隱私保護
- 永不中斷的防護機制，代表在發出存取請求時，資源都是受到保護的 (即使服務已停用)，系統會自動啟用防護以確保每次的流量都受到保護
- 使用最少的數位足跡且託管於雲端，代表著你無需再管理昂貴的支援合約、複雜的配置或硬體
- ZTNA 支援 macOS、iOS、iPadOS、Android 及 Windows 裝置，不僅可以降低總體擁有成本 (TCO)，還可為 IT 團隊減輕支援多廠牌硬體和軟體的負擔

在本節中，我們探討了資料加密的基礎知識、原生於 Apple 的解決方案，也說明了在 macOS、iOS 和 iPadOS 裝置上啟用此安全控制的步驟。ZTNA 除了可持續確保遠端網路連線的安全，還額外增加了安全保護層，在授予存取權前，就先對使用者和裝置進行驗證，確保閒置與傳輸中的資料都能安全無虞，並幫助你釐清新型 ZTNA 技術更勝於傳統 VPN 的原因。那麼，如果是 App 正在使用、處理中的資料呢？

解鎖其他兩種資料狀態；使用中的資料並沒有特定的安全控制來緩解風險，反而是跟隨著持續性管理任務和安全性流程。

當 App 在存取和處理資料時，資料會從 RAM (記憶體) 傳至 App 來進行處理，接著回到 RAM，再永久保存在設備的儲存區中。只要是由已知、受信任開發人員所開發的 App，都會納入安全機制，以確保 App 內部的安全性不會受到干擾；其中一個原因在於確保 App 內處理的資料不會洩漏給裝置上運行的其他 App、服務、流程，也不會相互共用資料。這樣一來，不僅能維護資料的完整性，也能維護 App 的完整性。

利用漏洞成功入侵 App 的攻擊程序，不是會對內部安全機制動手腳，就是本身為流氓 App，它們原先宣稱為執行某項任務的 App，實際則是執行其他秘密任務，導致安全機制面臨風險。

那麼，你可能會好奇，什麼樣的解決方案才最有效？下列回覆綜合了建議的最佳作法、深度防禦策略，以及善用 Jamf Pro 來盡全力確保使用中資料的流程和工作流程維持安全：

- 實施持續性修補程式管理政策，規範必須從可信來源取得 App，例如 Apple 的 App Store、開發人員網站或像是 Jamf 這樣可信的管理供應商提供的「App 安裝程式」
- 使用你偏好的 MDM 解決方案部署受監管 App，並實施政策型管理，確保 App 維持在最新狀態
- 透過安裝描述檔來驗證裝置安全配置，將配置錯誤所造成威脅的可能性降至最低
- 強化裝置設定以限縮可能引入威脅的風險行為，例如越獄 iOS 或 iPadOS 裝置、從未經授權或不安全的來源側載 App
- 持續實施內部資安教育訓練，讓相關人員了解常見的威脅類型和特定操作 (例如影子 IT) 會如何造成風險
- 制定讓相關人員簽署的適當使用原則 (AUP)，讓員工明白違反公司政策的行為可能面臨的後果

5

基本要素五：

合規監測

了解所有裝置上通訊協定和管控措施的狀態

安全性系統的優劣，端視系統最薄弱的環節而定。管理者必須監測組織的裝置，確保每部裝置都已更新、已接收最新的修補內容並已啟用正確的配置選項，如此才能締造最佳的安全覆蓋範圍

「察覺自身的無知，
才是智慧的開端。」
——蘇格拉底

透過持續蒐集遙測數據，取得豐富的裝置詳細資訊以深入了解安全控制、設定和裝置健康狀況，IT 團隊得以更適當的保護裝置、使用者及資料，同時確保在威脅造成更糟糕的局面之前，快速修復超出範圍的端點設備，並迅速讓他們恢復至合規狀態。

就如同本電子書中其他項的基本要素，監測端點合規性不只有一種途徑，你既可手動執行，也可自動執行。合規性監測的成效可能受到多個因素影響，單看各機構的需求，例如知識庫、選用的裝置管理和資安解決方案、預算考量等，都可能是問題的成因，此處僅舉最關鍵的幾個為例。

手動監測與管理合規性和設備資產意即：

- 藉由不斷查核裝置，確保機構的所有裝置都受到保護
- 實際追蹤每台裝置，以符合資產管理需求
- 更新個別裝置上的軟體，以確保維持在最新狀態
- 驗證個別裝置上像是加密這樣的安全性設定等配置都維持一致
- 監控並確保沒有人引入如可疑 App 或惡意軟體這樣的風險

- 在作業系統、關鍵安全性更新釋出時即立即更新，修補已知漏洞並修復軟體中的錯誤
- 部署充足的人力，確保在偵測到問題和裝置遭到入侵時，可以有人支援問題分類、裝置隔離及修復任務，讓受影響的端點設備恢復合規

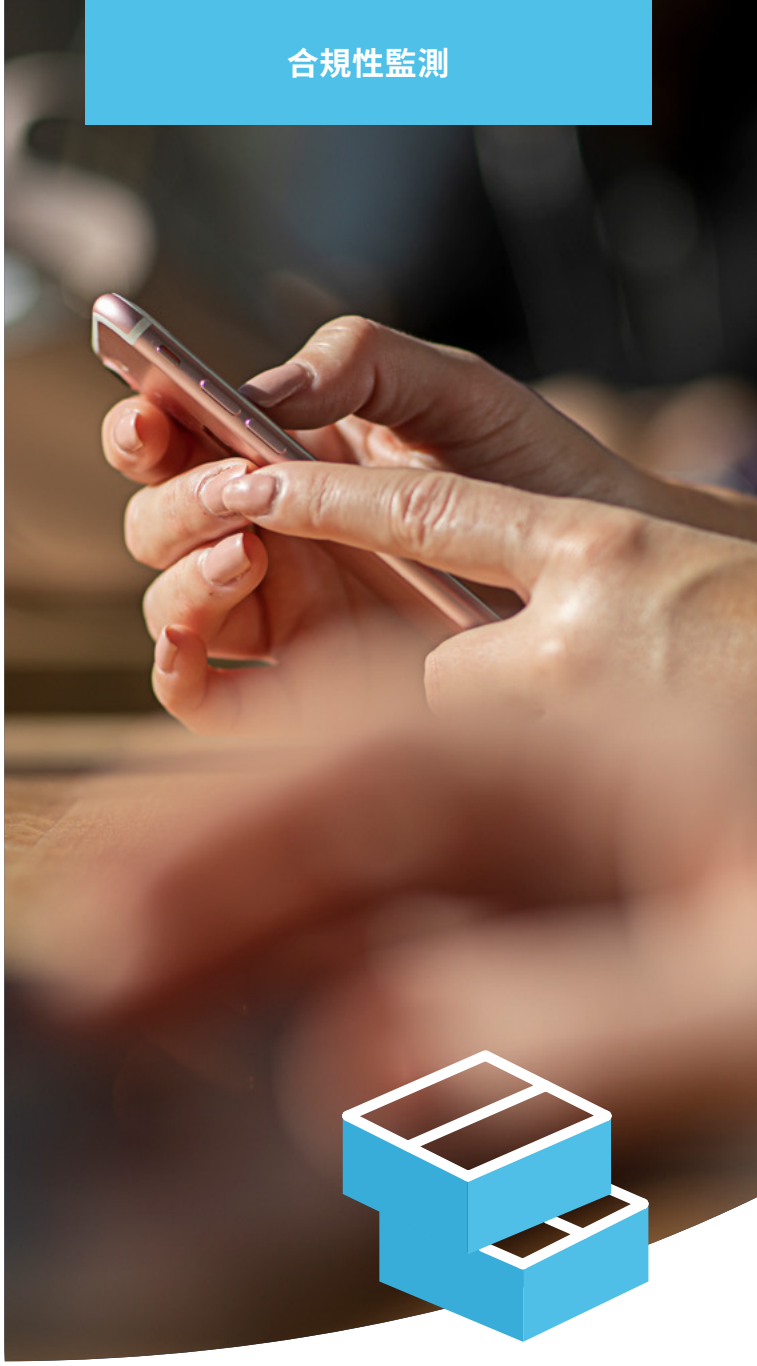
此方法需要人員始終保持警惕，還會為了完成管理任務而花費大把時間和管理開銷。若要以這個方法取得成功，則需要相關人員和管理團隊之間協同合作和取得所有人員的贊成票。還有一點需要注意的是，這種方法在本質上就需要頻繁的做出回應，也就代表具時效性的問題 (如事件回應時間) 在被偵測到之後，鮮少是在偵測到之前，還拖延到處理時間。

最後一個需考量的要點是，如果今天裝置數量和類型有顯著的增長，那麼 IT 和資安團隊手動回應問題的時間也將呈指數增長，這會使威脅人士在攻擊鏈中獲得更多展開威脅的時間，同時還增加了資料外洩的風險。

使用 Jamf 來監測資產設備，代表你只需要：

- 同時查看所有裝置上的最新即時資訊
- 為防護不當的裝置，部署更新內容與安全性配置
- **請跟著我們一起說：沒有步驟三了**

查看資產設備狀態的功能，可讓管理人員掌握每台 Apple 裝置的命脈。透過了解裝置的當前狀態，管理者可得知分別要將哪些更新發送到哪裡以及要配置哪些安全性功能，才能有效地管理裝置和安全性。根據動態條件來建立「智慧型群組」，代表管理者可以重點或盡可能完善的推送更新。無論是藉由精細的權限設定、裝置類型，還是任何其他分類方法，Jamf Pro 作為強大的工具，都能加速與合規相關的任務，同時保留一定的靈活度，利用可自訂標準重點傳送任務到所有裝置上。如果你有興趣深入了解，歡迎參閱我們的《資產管理入門》電子書。



使用 Jamf 來管理合規性，代表我們將：

- 以網際網路安全中心的 CIS Benchmarks 標準來查核裝置
- 將所有合規數據傳輸到雲端，以便進行集中管理
- 存取 macOS 統一日誌和完善的端點遙測數據，藉此快速且高效的識別威脅
- 透過政策實施合規規範，自動執行修復任務並確保端點維持在合規範圍內
- 執行共有漏洞披露 (CVE) 以了解環境中存在的漏洞
- 使用對應至 MITRE ATT&CK 框架的分析資料來預防資安威脅
- 以 API 在管理 (Jamf Pro) 和資安 (Jamf Protect) 解決方案之間安全的分享遙測數據，藉此發展進階工作流程，自動將事件回應時間最大程度降低和即刻解決已識別的問題

只會保護裝置是不夠的，許多法規都要求機構要有能力證明裝置可以持續維持在安全狀態並滿足合規要求，這代表機構必須提供文件，以證明在特定時段裝置確實維持在合規狀態。如果你無法提供裝置在特定時段為合規的佐證，那麼實質上就不能被認定為合規。

Jamf 可從個別裝置獲取遙測數據，我們的資料和報表可為你的機構提供必要的工具，並藉由修補級別、偵測到的漏洞、在整個生命週期內已執行動作的時間戳記等關鍵分類法來組織這些資料。此外，強大的整合功能可確保第一和第三方工具都能安全共享這些數據，並以集中式儀表板呈現延伸訊息，還可將數據視覺化、輸出為其他格式，以便傳送合規報告給監管調查人員。

6

基本要素六：

App 管理與安全性

三大功能：漏洞修補報表、政策及 App 安裝程式，確保 App 維持在最新狀態，同時可輕鬆實施安全措施

App 安全性

就裝置的資安態勢而言，能夠知道是否成功修補已知漏洞，是一項極其重要的資訊。但是你可知道自己使用的 App 來自哪裡嗎？你能保證這些 App 完全沒有暗藏惡意軟體或程式碼嗎？這些問題的答案對任何機構來說都至關重要，如果你無法信任 App 的來源，基本上就是置裝置安全和使用者隱私於風險之中、讓敏感資料暴露在外。

Apple 把維護安全性與隱私視為首要任務。而 App 安全性方面，Apple 則致力讓 App 的下載與使用都安全無虞。

App 的安全和管理功能：

1. **在沙盒執行 App：**每個 App 各自在獨立的空間中運行，且無法和其他 App 互動。在允許 App 讀取/寫入其他人的共享資料前，必須獲得已驗證使用者的明確贊同

2. **安全的集中式 App 採購：**為了降低資安風險，App Store 上僅陳列經過審查的 App。這個模式其中一個環節是將 App 進行公證，另一部分則是將已通過嚴格安全測試的 App 託管於一個由 Apple 管理的安全雲端倉儲。開發人員還可以輕鬆將最新版本的 App 直接交到使用者手中，消除了從不安全來源下載非法軟體帶來風險的可能性

3. **公證作業簽署以確認安全完整性：**對 App 進行公證可讓使用者放心知道，經過開發者 ID 簽署、並下載到 Mac 的軟體，已由 Apple 審查是否存在惡意元件和程式碼簽署。只要經過公證作業，你大可以放心認定 App 沒有被篡改或遭到入侵

4. **「門禁」將驗證並阻擋可疑的 App：**任何 macOS App 在首次運行前和後續的每次更新後，都將比照「門禁」要求驗證所分配到的公證票證，以確定票證的有效狀態。如果票證有效，則核准讓該 App 正常運行；如果票證已遭到撤銷，則該 App 的運行將受限制，此時系統會通知使用者 App 可能已遭到未經授權的一方竄改，內部安全性和完整性可能已受影響

5. **套用 App 使用限制：**在 iOS 裝置上，獲取 App 的唯一安全方法就是透過 App Store 來下載。也就是說，iOS 和 iPadOS 越獄雖然可讓你存取第三方 App 商店，但是這些 App 商店通常是用來派發「破解版」或內部安全機制已被移除的 App，像是免費提供原先要付費的 App，實際上這些 App 已被威脅人士注入用來竊取資料或監視使用者的惡意程式碼。借助像 Jamf Pro 這類的 MDM，管理者可以設置警報，在識別越獄裝置時收到通知，讓管理者可以執行修復作業，即時糾正安全問題

在 macOS 裝置上，使用者 (或有使用 MDM 的管理者) 總共有兩種「門禁」選項：

- Mac App Store
- Mac App Store 和已識別的開發者

限制 macOS 使用者只能在 Mac 的 App Store 上取得 App，好讓管理者管控整部裝置的 App 安全，同時將來自可疑、不安全和/或已遭到入侵 App 和可能帶來的種種威脅與風險降至最低。如果有需要從開發者網站取得第三方 App，第二個選項可允許使用者從 App Store 和 Apple 核准的已識別開發者取得 App，並建立以開發者 ID 簽署的軟體套件來提升安全性。

最佳做法

我們建議將 macOS 裝置設為允許從「App Store 和已識別的開發者」下載 App，若你的 App 為自家開發，或者你會重新打包 App，則更該選擇這個選項。此外，請向 Apple 申請一組開發者 ID 並以機構之名向他們簽署你們開發的 App，如此一來「門禁」才能識別並信任這些 App。最後，選擇 Jamf Pro 作為你的 MDM，就能將 Self Service 部署到所有裝置上，讓 IT 人員預先為使用者核准 App、設定、配置等，使他們能夠隨需求輕鬆存取和安裝自己需要的工具和服務，也不需要開支援工單、變更權限或使用 Apple ID。

手動設定「門禁」選項：

- 前往「系統設定」>「隱私權與安全性」>「安全性」
- 從兩個選項中做選擇
- 為機構的每部裝置重複此步驟

以 Jamf Pro 設定「門禁」選項：

- 設定和部署含有「門禁」設定的描述檔到所有裝置上
- **這樣就可以了！**

App 和安全修補檔案及更新

作業系統更新、使用 MDM 指令進行版本管控、「快速安全回應」還有更多。

機構必須導入修補程式管理策略，來測試和儘快更正錯誤，確保硬體、資料及使用者都受到保護。在部署修補檔案時，測試作業經常被忽視，但它其實是個必不可少的環節，尤其是當錯誤為迫切需要修補的類型時。只要能盡快執行這兩項動作，IT 部門就可以將資安威脅的影響降至最低，避免衍生成更龐大的問題 (比如修復一個事件但無意中又破壞了其他更關鍵的功能)。

在本電子書中，IT 團隊執行管理任務所需要時間的趨勢，與需要管理的裝置數量有直接的關聯性。在管理修補檔案時，也幾乎是比照這個規律，但其中有一個變數：需要部署的修補檔案量，可能在極少到極多之間浮動，個別裝置的管理任務甚至可能呈指數般無限增長。

讓我們來回顧一下，當管理者手動或透過 MDM 管理修補程式時，一些可用的選項：

以手動管理修補程式：

- 教育使用者，當裝置一收到更新通知，就儘速自行更新
- 當發佈新的修補程式時，便收集所有裝置，然後一部一部手動部署
- 修復缺少修補程式的裝置，並將此作為持續性合規監測流程的一部分

透過 MDM (即 Jamf Pro) 來管理修補程式：

- Jamf 會自動接收更新和修補通知，再透過我們的工具來部署修補程式到機構的所有裝置上，你可以按照自己的時間表，而不是他人的時間表，來進行更新
- Jamf 的 Self Service 自助服務區可在新的修補程式可用時，就發送提醒通知給使用者，讓他們不會忘記要更新
- 消除對使用者的依賴，同時將派發修補程式流程自動化，以減低 IT 人員的負擔。以修補程式作為政策發送到所有裝置，或使用動態「智慧型群組」來確保裝置維持在最新狀態

如要了解有關 App 生命週期和自動部署 App 的更多資訊，歡迎閱讀我們的白皮書

提升你的資安防護力

你有發現什麼端倪了嗎？安全性問題，不太適合以「一體適用」解決方案來處理。一個完善的策略應該具備多個防護層，才能夠全面的保護你的裝置、使用者和資料並提供徹底防護，以編織出數位安全網。我們稱之為深層防禦策略，這意味著如果其中一層防護層沒有捕獲威脅，則此防護層的上層或下層，都有機會再次嘗試攔截。

你很有可能已經熟悉多層防護的概念而不自知。就讓我們拿你熟悉的事物為例——你的家。

新舊安全措施融合以確保家的安全，對於保護心愛的人和自己，想必家中一定也有一些保護措施：

- 門鎖
- 家庭警報系統
- 監視器
- 四處巡邏的保安人員
- 一氧化碳偵測器
- 滅火器
- 屋主或租客的相關保險

理論上來說，上述每一項都可以作為獨立防護措施來確保家的安全，但個別來看，每一項都只是完整防護鏈的一個環節而已。如果將所有環節組合在一起，那就會像拼圖一樣，呈現出完整樣貌，並有能力處理多種問題。網路安全和 Apple 裝置管理與資安都是遵循類似原則，成為強化的核心要素，通報使用者、實踐良好的資安方法，藉此減少威脅的發生，並將風險降至最低。

其中一層端點防護層，正是在偵測到風險時發出警報。舉例來說，某些使用者可能有能力辨識網路釣魚攻擊，因此未曾按下惡意連結；某些使用者可能因為過度信任，所以乖乖的按照指示按下惡意連結，並給裝置、使用者和資料帶來風險。這名受影響的使用者，該如何知道自己已經按下惡意連結，又或者執行了破壞裝置或憑證的動作？

我們正好有個專為此打造的 App。Jamf Trust 可抵禦由使用者造成的風險，Jamf 在偵測到使用者裝置上存有威脅時，便會以 Apple 推送通知的形式通知使用者，例如釣魚連結在點按後以惡意程式碼安裝鍵盤側錄軟體時。

Jamf Trust 此時會判定有威脅存在，並進一步通知使用者 (以及管理人員)。推播通知將提醒使用者應留意風險和注意這類型的事件，同時 IT 團隊也能透過 Jamf Pro 和 Jamf Protect 快速回應並進行修復，將裝置從網路上隔離、清除感染源、修補所有偵測到的漏洞，再將裝置回復至安全基準線。最後，利用此次事件，在未來提升相關人士的資安意識。

保護資料和裝置，勢在必行

機構可以選擇透過 Apple，盡可能實現最強的資安防護，防範可能的攻擊或盜竊於未然，而 Jamf 可以用比手動作業還簡單、高效又安全的方式，協助你完成這項任務。

在網路安全方面，沒有人喜歡驚喜，當然也不希望自己在能提供協助時，反而手忙腳亂的應對攻擊事件。我們的資安方案無人能及，不妨免費試用看看，也歡迎你聯絡 Jamf 業務人員，一同討論如何為你的機構量身定制完善的 Apple 管理和資安解決方案。

如果市面上的產品你都試過了，那麼是時候該試試最頂尖的方案！

試用 Jamf

或者聯絡你偏好的 Apple 裝置經銷商來預約免費試用。