



管理並保護 最容易受攻擊的端點：行動裝置



談到行動裝置時，我們通常會想到筆記型電腦、平板電腦和智慧型手機。雖然這些都屬於行動裝置，但本文重點放在討論智慧型手機和平板電腦。全球數百萬使用者仰賴這些裝置來完成日常工作、個人任務，還有學習。然而，對行動裝置的依賴也引起了人們對行動安全的擔憂。

在確保行動端點安全、維持合規性，同時提供良好使用體驗之間，其實可以兼顧。閱讀完這篇內容後，你將學會如何有效且高效率地，讓行動裝置的防護標準與整個裝置群一致。

行動安全現況

行動裝置可協助企業簡化各項業務功能的操作流程。憑藉其易用性、可攜性，以及隨時隨地存取應用程式與資源的能力，行動裝置幫助第一線團隊與企業員工保持聯繫與工作效率。

深入瞭解：

[行動安全現況](#)

[行動企業部署 環境](#)

[管理和保護行動裝置的整體方法](#)

[統一行動裝置和 Mac 管理及安全性的關鍵](#)

各組織通常支援多種行動裝置的所有權模式，例如提供給第一線員工（如護理師或門市人員）共用或一人一機的部署方式，以及企業擁有、個人啟用（COPE）或自攜裝置（BYOD）等企業員工使用方式。負責部署與管理的 IT 團隊必須根據各種模式的不同需求，採用客製化的安全設定。無論裝置是共用且嚴格管控，還是屬於個人並受隱私法規保護，都必須兼顧整體使用者體驗的提升。

但是，隨著行動裝置的普及，以及對其日益增長的高度依賴，都指向更大的安全隱憂。影響企業的一些較常見的因素包括：

- 資料外洩的額外風險
- 資料未經授權存取使用者個人資料
- 行動裝置與使用者體驗之間缺乏一致性
- 合規性的執行與維護挑戰

為了保護電腦而設計的安全策略，套用在行動裝置上執行的話，兩者之間的效果還是存在著差距，這會削弱行動裝置的安全態勢，甚至可能降低企業整體的安全態勢。另一個考慮因素是支援多個平台的複雜性，這會影響行動部署的速度——既要為使用者配置公司發放的裝置，還要確保公司資料在個人裝置上的安全。這些都不應該影響使用者隱私或裝置的使用。

另一個關鍵的考量，在 BYOD 方案之外的使用行動裝置，貴公司是否有配套政策來限制使用？如果您以為您的企業能夠免受行動威脅的影響，請再仔細思考一下。首先問問自己，我們允許個人使用行動裝置嗎？



裝置可能包含敏感資料，或需用於執行關鍵業務流程。例如，董事或副總裁用於日常業務的行動裝置。這些裝置常用於企業內部溝通，同時也是更具吸引力的攻擊目標。或者，也可以是針對特定用途所部署的裝置，例如外勤業務或工廠作業員使用的 iPad。這些裝置雖位於現場環境，但仍需符合特定需求——包括合規性與易用性。

驅動移動力的因素

傳統的企業「移動力」正面臨著重大挑戰，企業模式也要跟著轉型才能跟得上改變，這與我們工作方式的演變息息相關。推動這一轉變的因素有很多，其中包括

- 將業務遷移到雲端服務
- 採用分散式人力（為遠端工作者組成，「分散」在傳統集中式工作場所之外的不同地點工作。）
- 日益普及的原生行動應用程式

隨著行動業務應用程式的開發和普及，與現今不斷變化的工作環境相輔相成，讓行動裝置成為不可或缺的工具。這主要是因為行動裝置的方便性，在各個場合都可以使用，具有高度互動性，當然還有成本效益。

本文的重點是行動裝置和商務應用程式在現代全球工作場域中的重要性：



行動裝置提升工作效率：行

動裝置讓使用者可隨時隨地存取業務應用程式與網路，是更聰明且更有效率工作的關鍵工具。



行動應用程式的普及：

行動裝置承載關鍵工作流程與敏感資料，因而成為首要攻擊目標。高階主管或外勤團隊所使用的裝置必須兼顧使用體驗與合規性。



多元工作流程：

行動裝置支援高效率的工作流程，使用者可即時視訊會議、通訊、管理庫存、存取客戶資訊、編輯文件及處理電子郵件。



行動效能的期待：

越來越多使用者仰賴行動裝置來輔助甚至取代桌機，因此行動技術必須如同延伸的工作平台一樣流暢高效。



職場創新：

行動裝置提升員工滿意度、生產力與留任率，促進職場創新，有助企業更高效地運作並因應變化。



行動裝置持續成長：

根據 Statcounter GlobalStats，2024 年全球行動裝置的市佔率達 62.22%，遠超過桌機與平板，成為網路與工作應用的主要載具。



遠距與混合辦公環境：

行動技術的採用對於實現遠距與混合辦公仍至關重要，95% 的員工傾向擁有遠距工作的選項。行動裝置推動協作與彈性，無論身處何地皆可工作。



全球行動裝置普及率：

截至 2024 年，全球有 74 億人擁有手機，其中智慧型手機佔 71%，約為 67 億個用戶，凸顯行動裝置的全球普及規模。

行動企業部署狀況

在過去，企業大多會選擇使用單一平台來滿足其業務所需，該平台通常是專為 Microsoft Windows 設計的。這就需要採購與所選作業系統（OS）相容的電腦。當與 Microsoft 簽訂企業協議，企業就可以延後部署最新的 Windows 版本，直到為過渡期做好準備。這樣做的好處是，舊版作業系統可以持續得到支援，以便滿足企業的需求。

然而，挑戰就在這裡：行動領域一直被認為是以消費者為導向的領域，一旦作業系統修補程式更新，就應該立即套用。由於使用者可以自行決定更新的時間，以及在更新發布後多久安裝，企業在採用的過程中可能會遇到以下障礙：

- 行動作業系統選擇的多樣性
- 每個作業系統支援的版本之間存在差異
- 各個作業系統的部署方法不斷變化
- 各種不同的支援需求導致延後升級
- 各作業系統版本對業務應用的支援程度不一
- 開發人員的更新計畫表和功能支援各不相同
- 裝置所有權模式不同，將影響管理方式（例如 BYOD 裝置等）COPE（公司所有，個人使用）
- MDM 解決方案支援的功能與不支援的功能（原生框架與非原生 框架）
- 各作業系統的安全等級不一
- 以政策為依據的合規執行能力有限



日益嚴重的問題

我們剛剛也談到了，在企業環境中，行動裝置使用量快速成長所伴隨的相關安全問題。在本章節中，我們將深入探討針對行動裝置的威脅，以及使用行動裝置相關的風險。我們也會討論在工作場所中，關於行動裝置安全的常見誤解。

第一個問題源自於這些裝置的移動特性，由於以下幾個原因，它們容易成為攻擊的目標：



寶貴的資料：

行動裝置包含大量個人、業務和受法規保護的隱私資料（如 PHI 個人健康資訊），甚至也包括 PII（個人識別資訊）等雖未受法規保護但敏感的資料。威脅行為者可以將這些資料用於各種目的，對使用者或組織發動潛在攻擊。透過多層防護來保護這些資料，確保只有授權使用者才能存取，這一點相當重要。



易遺失或被竊：

行動裝置的便攜性讓使用者可以在不同地點工作，但也增加了被竊取或遺失的風險。威脅行為者可以抓住機會竊取設備，對資料安全構成直接威脅。即使在無人看管的情況下短暫地存取裝置，也可能會危及裝置，或著讓它在未來更容易受到攻擊。



關於安全性的誤解：

有些人認為，光是多樣化的安全解決方案是不夠的。然而，隨著行動威脅情勢的快速發展，端點框架也需要原生支援。仰賴缺乏支援的解決方案，就可能會增加漏洞，在不支援的功能和特性中有機可乘。

過度保護還是管理不足：找到平衡點

平衡裝置管理與安全，是最佳化行動技術以支援第一線員工的關鍵概念。雖然看似 IT 管理與資安需求可能相衝突，但實際上僅聚焦於其中一方都是不夠的。組織必須無縫整合管理與安全兩大要素，打造兼具效率與效能的行動資安方案。

挑戰在於找到正確的平衡點。如果使用過於嚴格的安全限制，可能會妨礙使用者體驗，進而降低第一線員工的生產力。另一方面，若忽視安全，則會讓寶貴的資料與業務處於風險之中。關鍵不在於選擇安全或效率，而是將兩者協調一致，使行動管理與安全共同發揮作用，同時支援前線團隊並保護企業資產。

問題	過度保護	管理不足
性能受損		✓
易用性		✓
影子 IT —— 員工在未告知內部 IT 人員的情況下，使用未經批准使用軟體、硬體或其他系統和服務（隱私問題可能促使員工使用個人裝置）		✓
避開公司的安全措施		✓
削弱行動工作空間的潛力		✓
符合法規要求	✓	
減少不斷變化的行動威脅	✓	
將業務資料與個人資料分開加密處理	✓	
確保定期進行修補、緩解	✓	
簡化行動端點的 部署	✓	
防止未經授權使用者或裝置存取公司資源	✓	
充分保護使用者隱私，同時也保護業務資源		✓

以下是一些策略，可以幫助企業的行動安全轉型，在提高安全性的同時，也能優先考慮使用者隱私。

1. 方便使用者操作的資安工作流程：

將易用性和簡易性整合到安全流程中。這不管是對使用者還是負責管理及保護行動裝置資安的團隊都很有幫助

2. 將「以資料為中心」的概念納入安全措施：

不要只專注於裝置安全，而是採取資料安全的思維模式。保護裝置固然重要，但裝置是可以更換的。而另一方面，保護敏感資料是始終不能鬆懈的。

3. 採用多樣化的裝置所有權模式：

對不同的所有權模式持開放態度，為其量身定制安全措施，不管用什麼所有權的裝置存取公司資源都能夠受到保護。忽略某些裝置所有權的話（如沒有為 BYOD 裝置制定專屬的安全策略），可能會造成整體安全策略的漏洞。

4. 全方位的資料保護：

確保所有形式的資料都是安全的。這包括加密磁碟區、將業務資料與個人資料分開，以及確保任何以網路傳輸的資料都是安全的。

5. 採用現代行動科技：

專為滿足現代行動裝置需求而設計的技術。傳統的安全工具往往無法有效防禦新興的行動威脅，只能提供片段、非全面的保護。

6. 採用分割通道（Split-Tunneling）：

了解移動效率的重要性。路由需要保護的業務資料，而非業務資料（如個人資料）則不受公司安全協定的規範。這種分流方法既能維護資料安全，又能尊重 BYOD 使用者的隱私。

若將行動裝置視為與電腦等同的重要端點來管理與保護，會帶來哪些成果：

macOS 和 iOS 之間的整合度越來越高，這對未來的行動裝置和端點防護有什麼影響？

雖然將 Mac 桌面作業系統與行動裝置比較就好像拿蘋果與橘子做比較一樣，但實際上，macOS 和 iOS 的每一次新迭代都會提升這些作業系統之間的融合度。隨著每個版本的發布，整合也變得越來越重要。

然而，更關鍵的問題是企業如何利用這種更深入的整合。以下是將這種整合套用到各種裝置類型的一些方法：

- 快速修復安全漏洞
- 輕鬆恢復生產力
- 改善員工體驗
- 建立員工信任
- 在基礎架構內的強制執行合規性
- 更符合企業組織的政策
- 全面、分層的安全流程
- 雙邊應用程式管理
- 無論裝置所有權 模式為何，均採用深度防禦策略
- 靈活且強大的安全性和管理解決方案，提供全面性的 支援

行動裝置合規性

並不是只有受監管的產業才需要考慮合規性。雖然合規性於金融、醫療保健和教育等行業的組織十分重要，但遵守組織內部的規則和政策也是必須，才能滿足不同的業務需求，盡可能降低業務連續性的風險。（業務連續性 Business Continuity 指企業有應對風險的能力，如自然災害、停電、網絡攻擊、系統故障、流行病和其他不可預見的緊急情況，以確保業務持續運作。）有鑑於此，在企業內實施和執行行動政策（像是現在處理 Mac 裝置的方式一樣），對於建立全方位的行動安全策略是相當重要的。

舉個例子：在混合和遠端工作場景中，行動裝置失竊、遺失或外洩風險更高，可能危及敏感的企業資料。IT 部門可以利用 MDM 工作流程，對裝置和使用者執行加密標準及安全性認證，以部署標準化的安全性配置。此外，遠端抹除功能可在必要時安全地刪除受影響裝置上的資料。

無論用途為何，企業都可以為行動裝置使用者制定合規性計畫。

這種方法既能解決固有風險，又能有堅實的基礎作為後盾。這對於降低新興技術的相關風險來說尤其重要，例如 **新設計的行動應用程式，與已經符合《加州消費者隱私法案》（CCPA）等法規的網站。**

此外，在問題演變成關鍵漏洞或違反法規之前，能夠先辨識問題及緩解，這也是合規性的一部分。在這種情況下，安全（監控）和管理（執行）相結合，共同偵測和減輕威脅，確保行動裝置保持合規。

也因為行動裝置的多功能性，使用者可能會不小心在公司批准的平台上執行個人任務，或將未經批准的應用程式用於與業務相關工作。這兩種情況都會帶來風險，如資料混和、侵犯使用者隱私，或讓企業面臨資料外洩及違反法規的風險。

若企業將行動裝置的合規性視為其他端點同等重要，就能確保所有存取企業資源的裝置都擁有相同層級的防護，能抵禦最新威脅，並準確記錄裝置清單、使用情況、發放裝置、員工對公司資料的存取，以及所部署的安全措施。

行動裝置合規性的最後一個考慮因素，是持續地為使用者安排資安培訓課程。這一點經常被忽視，但在全方位的行動安全計畫中卻十分重要，這可以讓 **使用者了解安全最佳實踐**、安全工作流程等，以及在遇到潛在安全威脅時應遵循的程序。這種培訓也是一種關鍵的保障措施，補足管理和技術安全措施缺乏的部分。

簡而言之：網路安全不僅是 IT 部門或公司的責任，也是每個人的責任。



統一行動裝置和 Mac 管理及安全性的關鍵方法

如果還不夠清楚，讓我們再次表明：資訊安全的關鍵在於統一整合整個機群的管理和安全性。

1. 融合：

在以行動裝置為中心的現代工作環境中，如果管理和安全性能與強大的安全協議完美地整合，就是通往成功的入場卷。

2. 克服：

唯有全方位的解決方案才能克服行動裝置安全問題，不要再採用傳統的零敲碎打的方法，將多個工具堆在一起，卻沒有任何一個工具真的有效。

3. 一致性：

要確保一致性，就必須測量各裝置的安全基線，並且主動監控端點的變化，這些變化可能代表著存在問題，也可以告訴您是否需要對安全威脅、漏洞或異常情況進行調查。

4. 可用性：

優先考慮使用者體驗，再加上安全性，一個全方位策略不可或缺的一點。強調 IT、資安團隊和終端使用者在效能和簡單易用的特性之間的微妙平衡。

5. 對應：

快速解決安全威脅非常重要，把重點放在確定優先順序、調查和解決方案，這包括所有裝置類型、跨不同平台，還有整個基礎設施。

6. 平衡：

取得適當的平衡，在顧及安全性的同時不去影響使用者體驗，將安全性和使用者滿意度完美融合。

我們想像，在未來，每台裝置都能受到無懈可擊的保護，無需為了安全性而做出任何取捨。這個願景就是最終目標：在整個基礎架構中的每一個裝置上實現平衡、全面的資料與隱私防護。

讓 Jamf 幫助您評估組織的安全需求，以及如何管理和保護所有端點



www.jamf.com/zh-tw/

©2025 Jamf, LLC. 著作權所有，並保留一切權利

立即開始

或聯絡你偏好的 Apple 經銷商，
來試看看 Jamf 的服務