jamf

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。

確保您的行動端點安全，同時保持現有 Mac 裝置的合規性是可能的。閱讀本文後，您將了解如何有效地保護行動裝置，與最佳的端點防護解決方案結合，確保整個機群（Mac 和行動裝置）安全 和資料 安全。

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 >

行動安全現況

隨著技術的進步，人們越來越頻繁地使用行動裝置。這些裝置具有桌上型電腦的功能，但設計更纖薄、輕巧、節能。它可供全天候使用、快速的網路連線，以及能隨時隨地存取各種應用程式和服務的功能。

從業務角度來看，行動裝置減輕了工作地點的限制，而網路連線功能則降低了對特定平台的依賴，這在一定程度上要歸功於雲端服務的即時存取功能。雖然公司為每位員工發放行動裝置存在著成本考量，但個人使用的行動裝置已相當普及，進而為企業組織發展出各種不同的擁有權模式，例如公司提供再由個人註冊的裝置（COPE）、員工自選方案，和自帶裝置 （BYOD） 方案。透過 BYOD，企業可以讓使用者用個人的裝置來工作，因而節省成本。相較之下，使用者可以選擇他們偏好的平台和外型規格來完成工作。

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
- 未經授權存取使用者個人資訊
- 行動裝置與 Mac 端點防護之間缺乏整合
- 難以評估及維持合規性
- 裝置受損可能導致資料外洩

企業組織往往有一種安全感的錯覺。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？

那些對於保護行動裝置還有所遲疑的企業，試想看看：如果 CEO 在旅行時使用平板電腦呢？他的孩子或許也用這台平板電腦做家庭作業，但這台裝置是可以存取公司電子郵件的。或者想想看，董事會成員和董事用來安排會議、討論機密業務的智慧型手機。這些裝置常常作為通訊用途，可能成為攻擊的潛在媒介，甚至是網路捕鯨攻擊。（網路捕鯨是一種針對性更強的網路釣魚，因為這類攻擊專挑企業高階主管或名人。）

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：

提高工作效率的行動裝置：

智慧型手機等行動裝置已成為工作的必備工具。使用者可以隨時隨地存取商務應用程式、連接網絡，進而更聰明、更有效率地工作。

行動商務應用程式的普及：

行動商務應用程式能夠適應各種多變的工作環境，因此也越來越受歡迎。行動裝置的便利性、個人化功能、高度互動性和成本效益，使其成為不可或缺的工具。

多種工作流程：

行動裝置能幫各種任務創建有效的工作流程。使用者可以在行動裝置上輕鬆地進行視訊會議、傳送商業訊息、協作文件編輯以及處理工作電子郵件等。

對行動效能的期望：

隨著越來越多使用者利用行動裝置來輔助桌上型電腦，人們也期待行動科技能拓展個人工作能力，更快速、有效率地工作。

工作場所創新：

在工作場所創新中，行動裝置是相當重要的，有助於提升員工的滿意度、生產力和留任率。行動裝置能讓企業找到更簡單、更有效率的工作方法，也能適應不斷變化的工作 環境。

行動裝置的持續成長：

行動裝置繼續主導市場，多數人使用行動裝置上網、執行與工作相關的任務，行動裝置市場逐年持續成長就說明了這點，根據 Statcounter GlobalStats 的資料，「全球行動裝置、桌上型電腦和平板電腦用戶的比例分別為 58.72%、39.18% 和 2.1%」 。

遠端和混合工作趨勢： 行動裝置的廣泛使用，加上 2020 年採用遠距工作解決方案，讓人們對靈活工作空間的需求大幅增長。行動裝置的廣泛使用是推動遠端和混合工作環境的關鍵因素， 員工對遠端工作偏好正好證明了這點。FlexJobs 發現，97% 的受訪員工希望能夠遠端工作，無論是完全遠端還是混合模式都可以。

全球行動裝置擁有量：

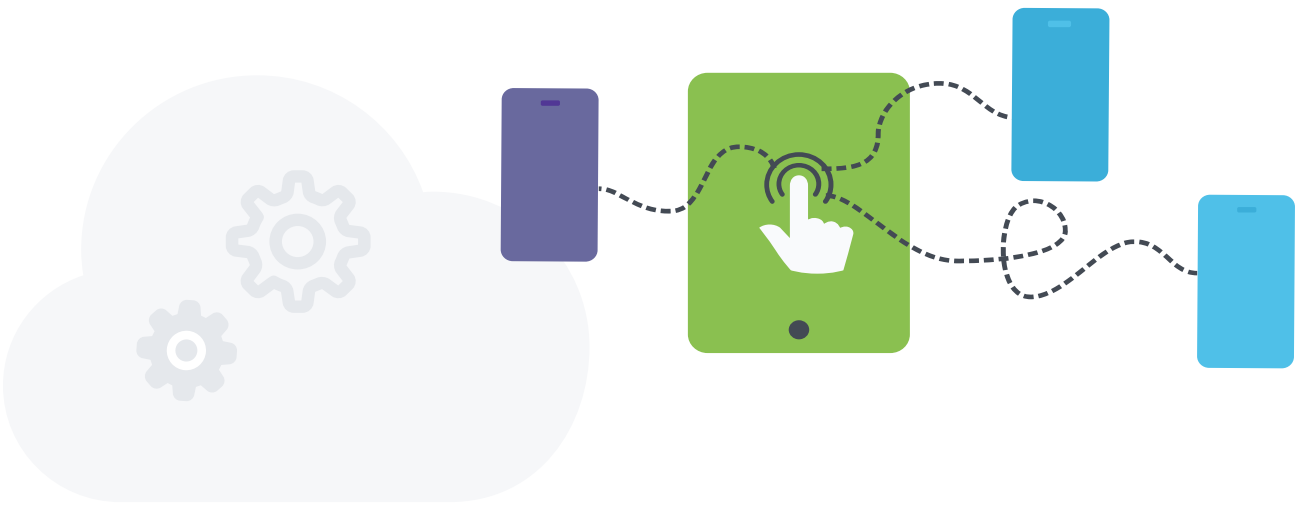
世界上絕大多數人口都擁有行動電話，其中又以智慧型手機為主，這凸顯了行動裝置的普及性。根據 Statistica 的資料，到 2023 年， 全球有 90.97% 的人口持有手機，其中智慧型手機佔了 85.88% 。

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：

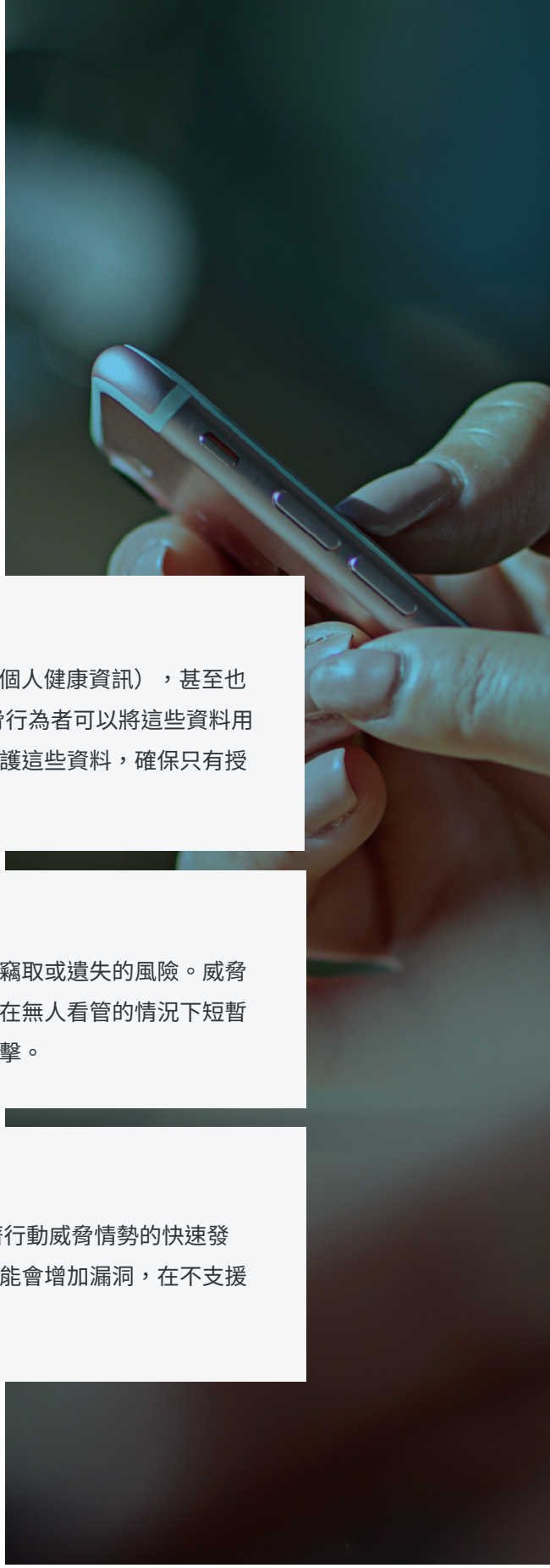
- **行動作業系統選擇的多樣性**
- **每個作業系統支援的版本之間存在差異**
- **各個作業系統的部署方法不斷變化**
- **各種不同的支援需求導致延後升級**
- **不同作業系統版本對業務應用程式的支援各不相同**
- **開發人員的更新計畫表和功能支援各不相同**
- **不同的裝置所有權模式也會影響其管理方式（例如，BYOD vs）COPE（公司所有，個人使用）**
- **MDM 解決方案支援的功能與不支援的功能（原生框架與非原生 框架）**
- **不同作業系統的安全等級也不同**
- **策略的合規性要求執行受限**



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：



1. **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。

2. **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。

3. **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

在行動科技以及更廣泛的安全和管理領域中，平衡是一個關鍵概念。儘管這通常被視為 IT 和資安團隊之間的拉鋸戰，但實際上，單單依靠 MDM 解決方案是不夠的。企業應將管理和安全性視為不可分割的關鍵要素，才能建立真正有效的行動安全解決方案。

挑戰在於找到適當的平衡。以拼湊解決方案來過度保護裝置安全，會導致使用者體驗不佳，而忽視行動安全，又可能會危及寶貴的資產。這並不是二選一的問題，而是必須在管理與安全性之間的取得平衡，作為有效行動安全的指導原則。

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		✓

整體方法：從 Mac 範例中汲取的經驗教訓

如果貴公司願意保護 Mac 電腦，為什麼不也保護行動 裝置呢？

無論您身處哪個產業或地區，世界各地的企業都將繼續採用 Apple 裝置來工作。根據蘋果的統計數據，不到兩年前，蘋果的年收入為 3,658 億美元！其中，iPhone（51.9%）和 iPad（8.8%）的總銷售額佔 60.7%。光是 Apple Watch 的銷量就超過了 iPad 和 Mac（9.8%），佔總收入的10.4%。

人們希望行動裝置能使用各種作業系統（包括 iOS、iPadOS、Windows、Android 和 ChromeOS等），這個需求是非常明顯的。

值得注意的是，用來保護這些作業系統的策略並沒有太大的不同這並不是說它們是完全相同的，但至少可以找出一些相似之處。例如，備受讚譽的 Apple 使用者體驗，以及對安全性、管理和隱私之間的平衡的重視，都可以直接有效地應用於行動安全。這種方法採取全面的策略，以保護機群中所有的端點免受潛在威脅。

有效的 Mac 安全性基礎始於 Apple 本身。這個概念植根於他們開發硬體和軟體的方式，從一開始就完美地整合了安全性和隱私保護元件，而不是事後再添加進去的。鞏固這項基礎的關鍵因素是使用 Apple 的原生框架。開發人員必須遵守這些框架，以確保使用者在使用裝置時資料的保密性、完整性和可用性。

為了讓這些框架符合 Apple 的核心原則，例如容易使用的特性和簡潔的設計，開發人員花費了大量心思。有趣的是，這些原則也解決了對安全措施的常見批評——過於嚴格的安全性限制讓員工無法有效率地工作再次強調，這就是取得平衡的重要性。

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抵禦新出現的行動威脅，只會讓您有安全的錯覺。

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（如個人資訊）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。

如果能像對待 Mac 電腦一樣對待行動裝置，可以預期以下結果：

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裝置上的資料。

企業組織可以以現有的 Mac 合規性計劃為基礎 ，來為行動裝置使用者制定專屬的合規性計劃。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。

如果能像看待 Mac 合規性一樣認真看待行動裝置合規性，企業就可以保護其行動端點免受最新威脅，不管是裝置庫存、使用情況、發放的設備、員工對企業資料的存取，以及部署的安全措施等，都有準確、詳細的記錄，就像 Mac 一樣。

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。這個願景的最終目標：打造終端使用者喜愛，企業又能信任的科技，消費者能夠輕易上手，又有高度安全性我們的願景，是在各種情況下都能同時做好管理和保護。我們稱這項服務為 —— Trusted Access。

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

jamf

www.jamf.com/zh-tw/

立即開始

或聯絡你偏好的 Apple 經銷商，來試看看 Jamf 的服務