評估端點管理：

為什麼傳統解決方案已無法回應現代企業的需求

介紹

現今的工作型態更加行動化、分散化，對彈性的需求也比以往更高。

無論組織採取遠距、混合，或全面回到辦公室的工作模式，行動裝置早已成為企業營運中不可或缺的一環。智慧型手機、平板與其他行動端點已廣泛應用於各行各業，不僅簡化工作流程，也讓使用者能隨時隨地即時存取資料，全面提升生產力。

隨著行動裝置快速普及，問題已不在於它們是否該進入企業，而是企業是否具備足夠能力，在超越原本設計用途的情況下，妥善管理與保護這些裝置。

行動裝置已在醫療、金融、營造與 運輸等產業中，轉變為關鍵的業務工具，但這樣的演進也帶來高度複雜性：IT 團隊必須在裝置種類高度分散、所有權模式混合的環境中維持法規遵循，同時兼顧生產力、安全性與使用者隱私，並確保行動技術與 IT 流程能與企業目標與成果一致。

本電子書將探討企業行動管理與資安的關鍵轉變，說明為何傳統工具或「一套適用所有情境」的做法，已無法滿足現代企業的需求。同時也 強調可擴充、整合式解決方案的重要性，這類方案不僅能支援現代工作流程、賦能終端使用者，也能讓 IT 掌握必要的可視性與控制力，確保所有行動裝置與企業策略目標保持一致。

如果你目前使用的工具並非為行動優先、混合辦公環境所設計，本指南將協助你評估它們是否仍具備價值，或是否該重新思考管理策略。

無界限的工作模式

不論組織是全面遠距， 或 遵循 回到辦公室的政策 ，也不論你 實際身在何處 ， 行動裝置早已全面融入我們的 日常生活 ，這點無庸置疑。這股趨勢強大到早已跨入專業應用場景，憑藉效能、功能、行動性與效率的優勢，成為許多產業的首選工具，也模糊了個人與工作的使用界線。

行動裝置對企業營運持續性究竟有多關鍵？

根據 **Verizon《2024 行動安全指數》報告指出**，

「80% 的受訪者認為，行動裝置對組織順利運作至關重要。」

既然行動裝置在維持營運、交付產品與服務上扮演如此關鍵的角色，企業就必須確保行動端點不只是被管理與保護，而是能與業務目標一致，在法規遵循的前提下，全面支援組織與使用者不斷演進的需求，並因應持續變化的威脅環境。

角色演進與工作方式的改變

近年來，許多產業透過導入行動裝置，以前所未有的方式推動業務發展與成長。以下是部分產業、角色，以及導入行動裝置後所帶來效率提升的實例：

航空業

行動裝置讓飛機維修、飛行作業與旅客服務更加順暢，從登機門到駕駛艙，都 **能即時存取資料並進行溝通**。透過將傳統飛行資料袋改為電子飛行包，飛行員能將約 40 磅的紙本地圖與手冊，整合到一台僅約 5 磅重的 iPad 中，大幅提升營運效率與法規遵循能力。

營造業

平板與智慧型手機透過數位文件與專案管理工具，提升團隊協作、 **降低延誤，並強化現場與非現場的專案掌控能力** 。iPad 讓現場人員即時查看藍圖，主管也能隨時處理文件與簽核，同時保持與利害關係人及供應鏈夥伴的即時溝通。

金融服務業

智慧型手機透過多種加密通訊平台，提升客戶服務品質、生產力，同時支援法規遵循。金融專業人員（如分析師）可安全存取客戶資料，並隨時掌握市場動態。同樣地，經紀人也能透過受管控的 iPhone，隨時隨地安全地執行交易，提供 **更貼近 客戶需求的服務**。

餐旅管理業

智慧型手機與平板協助飯店 **提升顧客體驗，透過行動系統串聯各部門流程** ，讓員工能提供更快速、更個人化的服務。Kiosk 模式的 iPad 也讓旅客可自助辦理入住，提早享受住宿體驗。此外，客房中的受管控 iPad 能簡化房務管理，並透過專屬 App 提供即時資訊與禮賓服務。

零售業

行動裝置為零售業者與顧客帶來更快速的交易流程、更佳的互動體驗，以及 **橫跨實體與數位通路的高度營運彈性**。從傳統 PoS 系統轉向行動系統後，銷售人員可在服務顧客的同時，即時管理庫存，無需離開現場。所需資訊一目了然，包括更新客戶資料與行動結帳，全都能透過 iPhone 或 iPad 完成。

企業面臨的挑戰

過去以單一管理工具管理同質裝置的做法，早已無法反映 現今行動優先企業的實際狀況。員工使用各式各樣的行動裝置、不同所有權模式與作業系統，使 IT 必須在高度碎片化的環境中，同時維持業務一致性、法規遵循與生產力。在威脅環境不斷演變、端點日益多元的情況下，企業必須重新檢視現有管理解決方案，是否仍能因應複雜需求並持續為 業務創造價值。

通用方法並不適用於每個狀況

過去，IT 普遍認為，只要企業內使用的是單一裝置類型、單一作業系統，就能透過一套管理解決方案進行有效管理。無論管理的是 100 台、1,000 台，甚至數萬台裝置，這樣的思維在當時確實合情合理，也讓 IT 能夠在同質化的端點環境中，維持管理與資安控管。

但先停下來看看，僅就「行動裝置」這個範疇，就包含了哪些不同的裝置類型：

- **智慧型手機**
- **平板電腦**
- **筆記型電腦**
- **穿戴式裝置**
- **物聯網（IoT）裝置**
- **電子書閱讀器**
- **掌上型遊戲主機**
- **數位相機**

再將這些多樣化的裝置類型，與全球 **人均持有裝置數**（3.6 台）一併納入考量，並與過去的企業環境進行對比。你會發現，兩者幾乎沒有共通點，而這也直接反映在現代運算環境與資安威脅樣貌的巨大差異上。

「85% 的受訪者表示，過去一年來，來自行動裝置的資安風險持續上升。」

—《Verizon 2024 行動安全指數》

這也引發一個關鍵問題：你目前的管理與資安解決方案，是否 仍能 與業務目標保持一致、落實法規遵循，同時支援生產力需求？

在不同裝置所有權模式下維持法規遵循

在回答前一節提出的問題之前，我們不能忽略不同裝置所有權模式，對企業行動裝置使用情境所帶來的影響。

本節重點在於，當工作用行動裝置同時包含公司配發與個人持有時，**企業該如何維持一致的資安水準**。進一步增加複雜度的，還包括必須同時支援：

- 各式不同的裝置類型（筆記型電腦、智慧型手機、平板、穿戴式裝置）
- 來自不同廠商的裝置（Apple、Microsoft、Samsung 等）
- 多種作業系統平台（Apple、Android、ChromeOS 與 Windows）
- 版本各異的應用程式與作業系統
- 分散式的工作型態（回到辦公室、遠距工作與混合辦公）

毫無疑問，現代企業就是由各種裝置、所有權模式與工作環境所組成的大熔爐，這些因素以無數種方式影響企業的需求與管理要求。這也讓 IT 必須獨自面對一項重大挑戰：不論裝置屬於公司或個人，都要確保端點能讓終端使用者順利存取企業資源，維持工作效率。同時，必須在整個企業範圍內，全面保障員工使用行動裝置時的生產力。最後，還要確保這些關鍵的業務工具（行動裝置）能以符合業務目標的方式被使用，支援營運發展，並與組織成長與擴展需求同步前進。

「87% 的關鍵基礎設施受訪者認為，若發生涉及行動裝置與 IoT 裝置的資安事件，將對其業務造成重大影響。」

—《Verizon 2024 行動安全指數》

解出關鍵解方

傳統工具的設計初衷，並不足以因應現今以行動為優先、混合辦公的工作環境。IT 團隊需要的是可 擴充、具備資安能力，且能簡化管理流程的整合式解決方案。現代化管理解決方案可透過簡化零接觸部署、自動化修補流程，並在跨平台環境中落實合規基準，協助企業達成預期的業務成果。同時，與身分識別服務的深度整合，也能支援 Zero Trust 架構，讓使用者在任何網路環境下都能安全存取資源。行為式威脅偵測與即時端點監控，進一步提升事件回應效率。結合對 CIS 基準的支援，IT 就能持續稽核並證明法規遵循，同時在各種裝置類型、所有權模式與 工作環境下，維持生產力與效能。

讓 技術 流程與業務目標一致

IT 與企業的其他面向一樣，都是組織成功不可或缺的關鍵。 為了達成使命，IT 流程必須超越傳統裝置管理策略，全面支援行動裝置、分散式工作環境，以及不斷演變的資安威脅。

為了保持競爭力，IT 必須與核心業務目標緊密對齊，並直接貢獻於：

1. 策略性成長
2. 營運效率升
3. 長期韌性

同時提升企業敏捷度、支援生產力並降低風險，且不犧牲使用者體驗。

將支援行動多樣性的管理解決方案，與企業策略同步整合，能在各關鍵產業中創造可量化的成果，例如：

製造業

iPad 讓產線人員能即時存取供應鏈資料，並將工作流程全面數位化。 IDC 的一項調查發現，85% **投入數位轉型（DX）技術** 的組織指出，「更好的員工體驗與更高的員工投入度，能轉化為更佳的客戶體驗、更高的客戶滿意度，以及更高的營收」。

醫療產業

iPad 與 iPhone 讓醫護人員能即時且安全地存取電子個人健康資訊（PHI）與遠距醫療工具。 根據美國國家衛生研究院（NIH）針對**〈臨床實務中醫師使用智慧型手機與行動 App〉**一文所分析的十項研究指出，「有 70% 的醫師表示使用行動 App」，藉此透過循證醫學支援臨床決策，提升病患照護成效並簡化照護流程。

政府機構

iPhone 能在確保安全的前提下，讓人員遠端存取機構資源，同時支援現場資料蒐集作業。根據 **《Verizon 2024 資料外洩調查報告》**，超過 90% 通報遺失或遭竊的行動裝置，最終都導致「確認的資料外洩」。因此，具備可擴充性的全面性安全防護，必須能因應裝置數量成長與政策演進，同時維持一致且完整的保護水準。

最佳化整體行動裝置群的支援與管理

現代化的行動裝置策略，是 IT 團隊在個人裝置與公司裝置並存的情況下，擴大支援規模、落實法規遵循並維護使用者隱私的關鍵。跨平台安全機制可確保各平台具備一致的防護水準並持續符合規範，同時透過簡化共用裝置的重新設定，降低風險、提升可用時間，讓無固定座位的工作人員更有效率。這樣的做法能提升營運效率並確保防護一致性，讓 IT 領導者能將行動裝置車隊管理，與不斷變化的業務與人力需求維持一致。

可擴充的裝置所有權模式支援

現代企業在支援個人裝置與公司裝置混合的車隊時，經常面臨擴充性上的挑戰。為此，具備針對性設計的解決方案 **（例如支援不同註冊模式）**，對 IT 團隊而言至關重要，可協助：

- 降低整體複雜度
- 全面性擴展安全防護
- 區隔企業資料與個人資料
- 落實法規遵循
- 兼顧使用者隱私

在兼顧資安與隱私的前提下，一項關鍵作法是：**保護企業資料、加密連線** 至／來自公司資源的網路流量，同時讓個人裝置上的非業務流量直接連線至網際網路。這樣的做法能在不同裝置所有權模式下，以規模化方式維持一致的裝置安全狀態與政策執行。

跨平台端點安全一致性

除了不同所有權模式帶來的挑戰外，現代企業也經常處於異質、混合的作業環境中，像是 iOS/iPadOS、Windows 與 Android 同時被各方人員使用。當裝置數量一增加，複雜度也隨之倍增，各種變數讓風險控管變得更加困難。

透過縱深防禦策略，搭配合適的控管機制，例如：

- 進階遙測資料
- 行為式威脅偵測
- 統一的存取政策

再加上跨平台支援，即可確保行動端點在裝置端與網路層，都能獲得一致的安全防護，**不受平台限制**。這種跨平台支援，能在 **維持高安全標準**的同時，降低行動裝置群的碎片化問題。

共用裝置與無固定座位工作人員

在大量使用共用裝置與多使用者環境的產業中，降低使用者之間的空窗時間至關重要。無論是：

- 在 購物旺季，快速設定 iPhone 以支援客戶服務
- 將 iPhone 部署給機組人員，用於簡化機上餐飲銷售流程
- 即時將 iPad 從 kiosk 模式切換設定，以更好地支援護理照護

在分秒必爭的情境下，**讓使用者能自行快速切換角色**，或 **在無需 IT 介入的情況下清除並接管裝置**，簡化重新設定流程，甚至可能成為關鍵救命措施。專為此情境打造的解決方案，能確保共用裝置隨時安全可用，準備好交接給下一位使用者，同時降低支援需求並提升整體營運效率。

解鎖全新工作流程，驅動生產力提升

簡化行動裝置管理，可全面提升 IT 效率與使用者生產力。 與身分識別與資安工具的無縫整合，可加速佈署流程、合規報告與存取控管。自動化部署可縮短設定時間、降低人為錯誤，而自助服務功能則讓使用者能即時取得必要的應用程式與資源。最終，解鎖的工作流程能善用效率優勢，同時降低停機時間，讓 IT 團隊能專注於打造真正為業務目標創造價值的流程。

與既有工具的無縫整合

不存在所謂的「萬靈丹」解決方案。

因此，**整合能力成為成功管理與保護行動裝置的關鍵**，因為它能：

- 全面性延伸服務能力
- 增加多層次、完整的安全防護
- 讓企業能在既有工具基礎上持續擴充
- 依合規需求客製化工作流程

例如，與 Microsoft Entra ID、Okta 等 **身分識別服務整合**，可集中管理存取控管、強制條件式存取政策，並在驗證流程中加入具備防釣魚能力的多重要素驗證（MFA）。降低未授權存取受保護資源的風險，只是與資安平台整合所帶來眾多效益之一，IT 還能：

- 簡化裝置上線流程
- 加快佈署速度
- 簡化合規報告流程
- 降低整體技術堆疊的摩擦與阻力
- 與業務工作流程保持一致

自動化裝置部署與佈署流程

視組織需求而定，手動讓行動裝置上線，每台可能需要超過 30 分鐘，導致生產力延遲並增加 IT 負擔。

但透過 **Zero-Touch 與 Apple Business Manager（ABM）自動化部署行動裝置**，可大幅縮短佈署時間，有效降低停機狀況。 這種做法 **不僅提升 IT 效率**， 也為組織帶來以下效益：

- 免除手動設定，降低人為錯誤風險
- 加速上線流程，包括應用程式安裝與設定
- 確保每台裝置從第一天起就符合資安與合規標準
- 使用者在啟用後即可取得所需資源，立刻投入工作

在需要的時候，讓使用者即時取得所需資源

一般來說，IT 需求的 **良好回應時間**約為 24 小時，也就是一個工作天。但當利害關係人需要某個應用程式或設定才能完成工作時，每延遲一分鐘，就代表生產力流失，進而影響營運，甚至影響最終營收。

Self Service 透過提供以下功能， **讓使用者更有自主性**：

- 經過核准、精選的應用程式目錄
- 企業資源與服務
- 安全的設定與組態

— 完全不需要提交支援工單！

使用者能在安全的前提下取得所需資源、維持生產力，同時 IT 仍能掌控可用內容，降低服務台負擔，也讓使用者更有信心自主完成工作。

落實全面性的資安策略

企業必須持續進化並擴展資安作法，才能有效因應多元行動環境中的現代威脅。 自動化修補管理可確保裝置與應用程式維持在最新狀態，降低漏洞風險，同時減輕 IT 負擔。進階威脅偵測需要即時分析、深度整合與多層防禦，才能有效辨識並降低風險。
以裝置健康狀態與使用者身分為基礎的 Zero Trust 策略，能確保不論地點、平台或 裝置所有權模式，都能安全存取資源。

自動化修補管理

人為錯誤是企業資安計畫中，最可避免卻也最常見的威脅來源。 過期的軟體正是其中一環，會讓行動裝置暴露於風險之中，也削弱組織的合規目標。 好消息是，只要將 **作業系統與應用程式的修補流程自動化**，就能透過以下方式降低這類風險：

- 即時監控與警示
- 主動檢視整合式紀錄
- 善用 **Smart Groups**
- 強制套用動態政策
- **App Installers** 工作流程
- 最低應用程式版本鎖定

透過自動化，IT 能減少人工操作，同時確保裝置持續更新並符合內部與法規要求，且將對使用者的干擾與停機時間降到最低。

威脅偵測與防護

根據 Kaspersky 的資料，網路攻擊在 2020 年達到高峰後一度下降，但到了 2023 年， **行動裝置攻擊從第一季到第四季暴增 147%** 。行動威脅的手法越來越精密，往往能繞過傳統惡意程式防護工具。有效的行動資安必須同時防範已知威脅，並結合裝置端與網路層的行為分析，即時偵測進階風險。管理、身分與安全之間的深度整合，能為 IT 團隊帶來：

- 更深入掌握行動裝置的使用行為與活動狀態
- 即時評估整體風險態勢
- 在多平台環境下更快的事件回應速度，

不論裝置所有權類型或工作環境為何

- 可無縫整合第三方 SIEM 系統
- 在不影響裝置效能的前提下，提供完整、分層的安全控管

零信任網路存取 (ZTNA)

工作型態與裝置使用方式都已經改變，企業是否 還該 繼續依賴為不同年代設計的舊式工具，來管理與保護今天的行動裝置？

答案很簡單：不該。

雲端運算、混合式工作環境與行動裝置的轉變，使得以「使用者身分」與「裝置健康狀態」來控管存取，成為維持法規遵循的關鍵。現今沒有明確邊界的企業，通常透過以下方式達成：

- **以加密微型通道取代傳統 VPN，將網路流量有**效隔離
- 實施條件式存取政策，只允許核准的使用者與驗證過的裝置存取資源
- 將身分管理無縫整合至管理與安全架構中
- 建立一套完整的 **零信任策略** ，無論員工在哪裡工作、使用哪種裝置、裝置屬於誰，都能全面保護企業資源。

全面標準化並落實法規遵循

有效的法規遵循，始於建立以產業標準為基礎的安全基準，確保所有行動裝置從第一天起就符合可強制執行的政策。主動監控端點健康狀態，提供即時可視性與 AI 驅動的風險偵測，協助 IT 快速維持合規並回應威脅。最後，透過 CIS 等基準進行驗證，讓組織能稽核、修正並回報合規狀態。

透過建立基準強化整體安全態勢

技術控管與政策對法規遵循與落實執行至關重要，但企業該從哪裡開始，才能符合特定產業的要求？ 答案就是：從基準開始，並以業界普遍接受的標準與框架為基礎。

建立設定基準，能確保每一台端點裝置——無論是公司或個人持有—— **在納入 MDM 管理時，就符合可執行的安全要求。**這是建立縱深防禦資安策略中，一個基礎且關鍵的步驟。它能協助 IT：

- **透過結構化的設定檔，** 部署至指定的智慧型群組，以建立合規機制
- 自動化一致的佈署流程，降低大 規模環境下設定漂移的風險
- 讓行動裝置管理流程與資料安全接軌，支援營運持續性
- **依據組織需求與產業法規，量身打造安全策略**

主動監控端點健康狀態

完成基準設定後，下一個關鍵步驟就是主動監控行動裝置群，持續掌握健康狀態，以確保長期合規，並在偵測到不合規端點時快速回應。透過管理、身分與安全之間的緊密整合，打破 IT 團隊之間的隔閡，並 **善用 AI 強化整體安全態勢** ，同時實現：

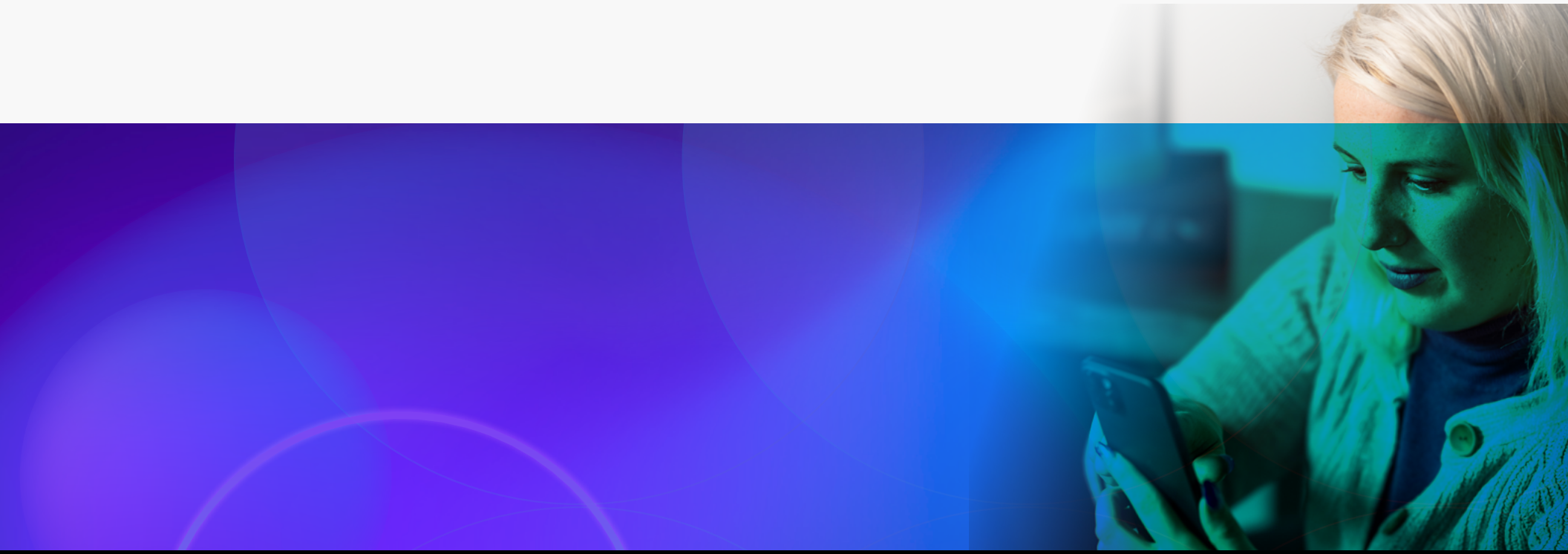
- **即時遙測資料與端點行為洞察**
- 以機器學習（ML）驅動的風險偵測與更快速的修復
- **主動進行行動端點威脅獵捕**、分析與進階威脅回應

透過基準驗證並落實法規遵循

第三個關鍵步驟，透過持續稽核機制，串起「執行、檢視與改善」，完整閉環行動裝置的合規生命週期。 同時，也能協助 **組織在高度監管的產業中，提供必要的合規證明**。

現代化管理解決方案不僅能標準化與監控合規狀態，也內建工具可依據 CIS Level 1 與 Level 2 等產業基準進行驗證，協助內部治理與法規準備， 包含：

- **讓 IT 能彈性客製基準，** 以符合企業的獨特需求
- 自動化基準量測**，並自動修正與基準不符的項目**
- 一鍵產出 PDF、HTML、Adoc 格式的稽核指引文件



便利性 vs. 安全性：數據告訴你

選擇方便或低成本的工具，往往會犧牲安全性，導致長期風險與營運中斷成本更高。不同裝置之間防護不一致，會削弱整體安全態勢，並製造可被攻擊者利用的漏洞。資安事件不只影響安全，也會拖慢裝置效能、降低生產力，進而衝擊營運持續性。 為避免這些問題，IT 領導者必須優先選擇能保護所有端點的解決方案——不論裝置所有權或作業系統——以確保成效、韌性與長期組織健康。

為什麼在「簡單」上省錢，最後反而比「安全」更花錢

成本往往是企業選擇行動裝置管理與安全解決方案時的重要考量。延用舊系統或選擇「一套通用」的工具，雖然可能降低初期成本或部署時間，但往往是以犧牲全面行動資安為代價。

而安全漏洞，最終可能導致代價高昂的資安事件。根據 IBM《2025 資料外洩成本報告》，**全球平均一次資料外洩成本為 444 萬美元**，美國平均更高達 1,022 萬美元。

同一份報告也指出，採用 AI 與自動化的資安團隊，可縮短 80 天的事件處理時間，平均節省 190 萬美元 成本。

重點整理：投資資安與企業營運、品牌信譽與法規遵循息息相關，最終都會反映在企業的獲利表現上。

缺乏一致性，會削弱整體安全態勢

當行動資安依賴平台差異，而非平台無關的安全能力時，就會產生防護落差。

簡單說：有些裝置的防護，就是比其他裝置少。

《Infosecurity Magazine》 指出，41% 的受訪者認為「裝置遺失且含有敏感資料」是資料外洩的主因，甚至高於帳密外洩與勒索攻擊。這正是平台控管不一致所導致的結果，讓企業誤以為安全無虞，實際上卻留下可被利用的漏洞。

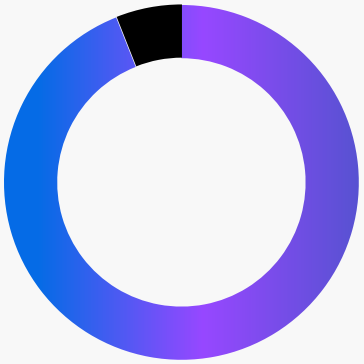
重點整理：企業資安必須涵蓋所有存取組織資源的端點——不論裝置類型、作業系統或所有權。風險就是風險。

對裝置效能與員工生產力的影響

資安事件不只帶來財務衝擊。它們確實會影響裝置與整體組織的資安防護態勢，但同時也會拖慢效能、降低使用者生產力，而這些影響最終都會反過來持續衝擊企業營運。

IBM 在涵蓋多種環境（包含公有雲、私有雲以及地端環境）的資安事件研究中發現，資料外洩的平均識別時間（MTTI）長達 207 天。而平均控制時間（MTTC）還需要額外 70 天，使得在各種環境中，從發現到控制資料外洩的平均總時程拉長至 276 天，期間也因受影響的裝置與企業系統效能下降，衍生出龐大的財務成本與機會成本。

前面提到的影響會以直接或間接的方式波及員工，但某些特定威脅與攻擊所造成的後果，對使用者生產力的直接衝擊其實更為嚴重。以勒索軟體攻擊為例。在一篇探討長時間網路與業務中斷影響的文章中，**Help Net Security** 指出：



「94% 曾 遭遇勒索事件 的組織，都經歷過一段明顯的系統停擺，以及生產力延遲的狀況。
其中更有 40% 的受害者表示，他們曾出現完全停工、生產力歸零的情況。」

重點整理：資安攻擊的影響不只限於眼前的損失，還包括商機流失、生產力下降、公眾信任受損，以及市值下滑，而這些後果往往在事件被控制後，仍會持續發酵。

重點整理

1. **行動裝置已成為關鍵任務工具：**

行動裝置在各行各業中都是不可或缺的工具，支援即時溝通、彈性工作流程，並確保在遠距、混合及現場工作環境下的業務持續運作。

2. **傳統工具已力有未逮：**

在面對現代行動裝置車隊的高度複雜性、多元裝置擁有模式，以及跨平台作業系統的情境下，傳統且一體適用的管理方案已無法維持一致的資安水準。

3. **資安必須是全面性的：**

現代企業需要跨平台、與身分整合的資安策略，並納入即時威脅偵測、條件式存取政策，以及自動化修補管理。

4. **法規遵循沒有妥協空間：**

有效的行動裝置管理能透過部署安全基準、監控端點健康狀態，以及驗證是否符合產業標準，協助企業隨時做好稽核準備。

5. **擴充性與自動化是 關鍵 ：**

專為需求打造的解決方案能簡化部署流程、降低設定複雜度，並減少人工負擔，讓 IT 能夠全面性地擴展對分散式團隊的支援。

6. **使用者體驗同樣重要：**

透過自助式工具與一致的企業資源存取，賦能員工提升生產力，同時不犧牲隱私與資安，也能減輕 IT 團隊的工作負擔。

7. **與業務目標對齊才能創造價值：**

將行動裝置管理與企業策略目標對齊，能提升營運效率、支援成長，並讓 IT 成為推動創新的關鍵角色。

總結

企業對行動裝置的依賴持續增加，使 工作 不再受限於辦公桌前，而是隨時隨地都能進行。 以成果導向來驅動業務，已不再只是趨勢，而是現代企業的核心特徵。

隨著裝置類型、擁有模式及多作業系統支援的複雜度不斷提高，傳統管理工具已無法滿足現代企業在資安、法規遵循與使用者體驗上的基本需求。

IT 不再只是被要求「管理裝置」。

IT 團隊被期待能將技術與管理流程，與企業策略及業務目標緊密結合。在保護關鍵資產的同時，也必須支援員工隨時隨地、使用自己最熟悉且最有效率的裝置與作業系統，無縫存取所需資源。

1. **風險更高。**
2. **挑戰也更嚴峻。**
3. **可容許的錯誤空間正在快速縮小。**

現代化的 端點 管理解決方案，正是為了回應這些不斷演變的需求而設計。從零接觸部署、進階威脅偵測，到跨平台支援與零信任資安架構。這些專為需求打造的工具，能讓 IT 團隊在 不 犧牲資安、效率與生產力的前提下，擴展、保護並最佳化行動環境中的企業營運。

問題是：

你目前使用的管理解決方案，是否仍能滿足企業、IT 團隊與員工持續演進的需求？如果答案並不確定，現在正是重新檢視管理策略的時候——企業的成功，取決於此。

試用 Jamf