jamf

新興科技實戰指南：現代企業的管理、安全與規模化

新興行動科技的成長趨勢與企業發展

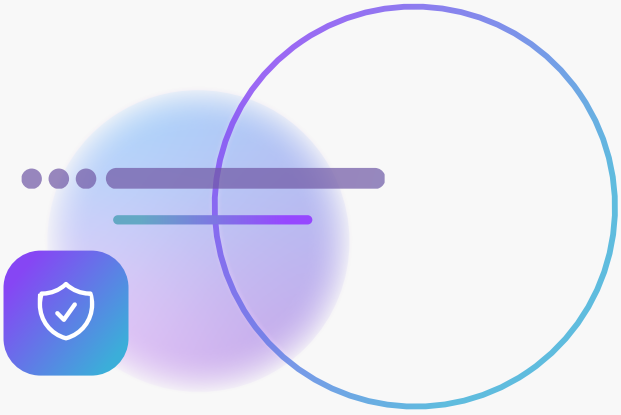
正如工作場所隨著工作型態不斷演進，穿戴式裝置、空間運算與 AI 等新興科技，也正在重新定義工作的進行方式。這些技術作為企業工具，不僅提升使用者體驗，也改變生產力模式，並在全球各產業加速創新。

然而，在導入這些技術的同時，企業領導者、IT 與資安團隊也必須同步調整端點策略，確保資料安全、裝置能被整體管理，並以更聰明的方式擴展規模，以因應攻擊面擴大、可視性破碎化與營運資源壓力增加等風險。

本白皮書不僅說明企業為何需要現代化管理，也提供不受平台限制的實務指引，協助組織建立並落實具備韌性的基礎架構，透過可執行的步驟降低複雜度、補足可視性缺口，並為混合運算時代做好準備。

在本白皮書中，您將了解如何：

- 讓管理與合規策略能因應新興科技發展
- 理解傳統作法為何無法提供一致的安全防護水準
- 將自動化與持續政策落實視為核心策略
- 讓管理、身分識別、安全與合規性與企業目標保持一致
- 將零信任視為 現代端點安全的核心原則



執行摘要

企業正邁入一個由混合運算模式快速發展所定義的新階段，其中包含穿戴式裝置、IoT 與 AI。這些新興科技正在重塑企業營運模式，並推動各產業創新，同時也帶來更高的複雜度、系統碎片化與全新的風險面向。隨著裝置種類與使用情境愈加多元，企業對於整體管理、情境式存取政策、持續安全狀態驗證，以及零信任架構的需求也同步提升。投資於自動化流程、深度可視性與政策導向控管的組織，將更有能力保護資料、因應不斷演進的法規，並安心擴展新興科技應用。

重點摘要：

- 強化型裝置預估至 2028 年的年複合成長率為 **8.4%**
- 空間運算預估 至 2030 年的年複合成長率為 **33.16%**
- 預計至 2028 年，**40%** 的企業將採用混合運算架構
- 預計至 2029 年，**80%** 的客服問題將能自動解決
- 2025 年穿戴式裝置預估出貨量為 **5.907 億台**

新興科技：2026 年及未來

隨著穿戴式裝置、IoT 與 AI 從試點專案走向正式企業工具，能實際帶來商業成果的新一代運算時代正快速加速。 這些科技正在改變人們工作的方式、學習模式與互動體驗，逐漸模糊實體世界與數位工作空間的界線，並釋放更高層次的創造力、生產力、協作能力、洞察力與自動化潛能。能夠掌握這股動能的組織，將更容易實現策略一致、強化韌性、智慧擴展規模，並把握下一波創新的關鍵機會。

空間運算

90 年代末期在大型電玩場常見的《Virtual Reality（VR）Vortex》遊戲，是許多人第一次接觸另類實境體驗的起點。這項技術涵蓋擴增實境（AR）與延展實境（XR），並進一步演進為混合實境（MR），串連起我們對實體世界與數位世界的理解。

這些技術統稱為「空間運算」，被視為學習與生產力的下一波進化，**預估到 2030 年的年複合成長率（CAGR）將達 33.16%**。

儘管空間運算仍處於發展初期，其影響力已**在全球多個產業中逐漸顯現**，包括教育、製造與醫療等領域。

以下是空間運算在實際應用中的幾個例子：

- **簡化新人到職流程：**透過虛擬導覽與探索工作空間，協助新進人員從第一天就快速熟悉環境。
- **快速原型設計：**工程師可更快開發與反覆迭代產品，同時進行操作測試並即時協作。
- **專業訓練：**外科醫師可在高度擬真的環境中練習，透過 3D 疊加影像打造沉浸式模擬，加強手術流程學習並提升精準度。
- **提升體驗：**零售消費者可使用智慧型手機掃描商品，在家中直接視覺化呈現， 或進行虛擬試穿，貼近消費者實際使用情境。
- **即時問題排除：**機台操作人員可透過 Apple Vision Pro 即時辨識問題並進行分析，直接在生產現場完成故障排解。

穿戴式裝置

試想一下：Apple Watch 內建的硬體元件，雖然體積大幅縮小，但在過去僅能出現在 Pentium 4 等級的桌上型電腦中。

具備多核心處理器、神經網路引擎、大量微型感測器，且可獨立運作成為運算來源，如今工作（與娛樂）已能在包覆於臉部、手部、手指或手腕上的高效節能設計中實現。

以下是 **2025 年出貨的 5.907 億台穿戴式裝置**的一些應用情境：

- **智慧手錶：**透過支援 GPS 與行動網路的智慧手錶，無論國內或國外旅行，都能與辦公室與親友保持聯繫，無需煩惱複雜或昂貴的漫遊方案。
- **追蹤裝置：**即時取得健康資訊，主動監測生命徵象、追蹤目標進度，或在發生意外與健康事件時快速回應，爭取關鍵救援時機。
- **耳機：**透過主動降噪降低外界干擾，幫助專注於重要事項；搭配智慧型手機使用時，還可進行即時翻譯，理解多種語言的即時對話。
- **智慧眼鏡**：在回覆緊急訊息的同時拍照或錄影，並依照導航前往會議地點，全程免持操作，搭配整合式 AI 助理，讓你用更短時間完成更多事情。

物聯網（IoT）

效率是企業營運持續性的關鍵推動力。 而自動化正是提升效率的基礎，因此企業仰賴物聯網裝置來建立商業洞察並不令人意外，例如應用於流程運作中，支援資料導向的決策，以大規模最佳化營運效率。

此外，在特定商業模式中，透過感測器與自動化的結合，可實現**約 20–30% 的能源成本節省**。 同時，透過如預測性維護等策略轉變，從被動回應改為主動預防，企業有機會將**維護成本降低高達 50%** ，並減少非計畫性停機。

以下是物聯網在企業中帶來效益的幾個例子：

- **資產追蹤與物流網絡：**簡化庫存監控，並搭配預測分析，提升產能規劃與庫存預測的準確性。
- **客製化客戶體驗：**透過量身打造的互動方式，更貼近客戶的個別需求，同時提升服務 品質並強化品牌忠誠度。
- **建築與設施管理：**透過自動化空調、照明與安全系統，在提升建築運作效率的同時降低能源消耗。
- **串聯複雜系統：**將感測器與物聯網整合至既有系統中，創造額外價值，並開啟全新的服務與營收機會。

人工智慧（AI）

AI 所帶來的潛力，同時影響企業與個人使用者。生成式 AI 的應用橫跨全球各行各業，其為企業帶來的轉型效益幾乎沒有上限：

- **創造更高價值：**員工可專注於策略性工作，重複性任務則交由自動化處理。
- **提升投資報酬率：**透過資源最佳化與效率提升，改善流程並降低營運成本，同時帶來創新與客戶體驗提升等質化效益。
- **簡化流程：**快速將概念視覺化、彙整內容或產生範例程式碼，充分發揮資源效益。
- **強化分析能力：**取得關鍵洞察、進行趨勢評估，並做出主動且以資料為基礎的決策，加速產品上市時程（GTM）。

此外，具備自主決策能力、無需人工介入的 Agentic AI，更進一步擴大了上述效益。例如，Gartner 研究預估，**到 2029 年，80% 的常見客服問題將能自動解決。**其關鍵優勢還包括主動性（威脅獵捕）與適應性（即時學習）。其中一個最有機會徹底改變企業關鍵流程的領域，就是資安軟體。以 Agentic AI 為基礎的資安解決方案可持續監控並評估風險，同時即時採取行動因應威脅，無需人工介入，大幅縮短反應時間並維持系統韌性。

混合式運算

全球企業在效率、工作負載處理、資源配置與擴展，以及法規要求與資本支出等面向，正面臨傳統運算模式（如地端或公有／私有雲）難以單獨解決的挑戰。即使是將資料處理更靠近裝置、以降低延遲的模式（如邊緣運算），也仍無法完全因應快速變動的數位環境需求。

混合式運算是一種新型態的運算架構，不僅納入新興技術，還整合既有運算模式，以解決上述挑戰，例如：

- **敏捷性**：透過多種運算模式的搭配，企業能在突發流量高峰時，以較低成本最佳化流量處理、提升回應速度並降低延遲。
- **效能**：導入 AI 驅動工具與自動化，將工作負載智慧分配至最有效率的環境，以提升整體生產力。
- **法規遵循**：透過資料與應用程式的地理配置控管，企業能掌握資料存放位置，在符合隱私與法規要求的同時，確保資料主權。
- **韌性**：整合雲端、地端與既有系統，在發生中斷時維持營運不中斷，強化整體持續運作能力。

Gartner 預測，**到 2028 年，超過 40% 的領先企業將在關鍵業務流程中採用混合式運算架構**，高於目前的 8%。

企業 IT 面臨的挑戰

當裝置未納入管理範圍時，便會產生可視性缺口，進而影響 IT 團隊的以下能力：

- 評估資安態勢
- 即時回應威脅
- 維持資料安全

平台與裝置的多樣性，加上不同的持有模式與混合式工作環境，帶來更多變數，進一步擴大組織的攻擊面。同時，也加重了原本就需因應不斷演變威脅環境的 IT 與資安團隊負擔。相對地，AI 與 IoT 在法規與標準上的持續演進與碎片化，也讓全球企業及其所屬產業在治理與負責任採用上承擔更高風險。

裝置註冊與佈署

完整的管理與資安策略，從裝置註冊開始，接著需能佈署必要的工具與設定，確保組織符合法規、資料受到保護，並讓員工維持生產力。這項最佳做法已深植於整體 IT 工作流程中，也是許多佈署標準與框架的核心。

當裝置未納入管理平台，或未佈署使用者完成工作所需的工具時，便會引發一連串緩慢但持續的風險，影響：

- 裝置可用性
- 資料機密性
- 通訊完整性
- 使用者隱私
- 端點可用性

上述每一項風險都會影響服務交付與法規遵循，最終對企業營運持續性造成層層放大的衝擊。

政策與可視性缺口

裝置洞察能力是所有資安策略的基石。一旦無法檢視或分析端點健康狀態，IT 與資安團隊實際上就無法掌握新興技術裝置在企業環境中如何連線、通訊，以及存取與使用公司資源。

由於遙測資料的盲點，管理人員在尚未了解潛在威脅、也無法判斷在資源或因應手段有限的情況下該如何排序優先順序前，往往無法有效處理問題。

以下是常見造成可視性缺口的原因：

- 多種作業系統平台
- 實體竄改
- 混合持有模式
- 不支援的裝置類型
- 裝置設定錯誤

威脅與風險因應

威脅行為者針對硬體與軟體尋找入侵點並非新鮮事，但在混合式環境下，加上多元裝置類型與各自執行不同軟體平台，讓風險控管變得更加複雜。

開放原始碼、專有系統與封閉系統並存的裝置環境，進一步加重 IT 與資安團隊在端點管理與防護上的負擔。若再加上端點健康狀態可視性不足，以及缺乏大規模安全設定裝置的能力，以下挑戰將大幅提高企業資源防護的難度：

- 資料安全
- 弱點利用
- 網路韌性
- 修補程式管理
- 擴大的攻擊面

法規與合規壓力

與既有或傳統系統不同，新興技術在全球範圍內正面臨多樣且快速變化的挑戰。在某些情況下，由於物聯網等技術本身高度碎片化，缺乏統一標準，進而引發多項資料安全疑慮。談到 AI，多數人認同其在效能與效率上的優勢，但對其對人類社會或環境所帶來的影響，理解與共識仍相對不足。

儘管許多議題仍在持續討論中，部分法規已跟上技術發展腳步，例如加州消費者隱私法（CCPA）與歐盟一般資料保護規範（GDPR），都對新興技術的使用方式施加高度監管。此外，企業領導者還需審慎評估下列因素，以判斷是否適合導入，以及可用於哪些情境：

- 資料駐留
- 營運韌性
- 第三方風險管理
- 治理因素
- 倫理考量

前瞻性解決方案與最佳做法

企業在因應新興技術導入挑戰時，應以經驗證的最佳做法為核心，最大化風險降低成效。這種有紀律的方法，能在裝置組合日益多元、應用情境不斷演進的情況下，支援可擴展且具韌性的端點管理，滿足企業成長需求。

端點盤點

在全面評估風險之前，企業必須先清楚掌握自身的基礎架構全貌。而最有效的方法，就是對所有硬體、軟體、服務與流程進行完整盤點。並深入了解：

- 每一台裝置
- 其相依關係
- 工作流程與政策

釐清各個元件及其彼此連結方式，可建立對整體基礎架構、通訊模式與裝置互動的全盤理解，為導入前瞻性解決方案奠定穩固基礎。

風險評估

下一步是評估各項風險因素，判斷其關鍵程度。此階段的目標不僅是降低風險，更是讓風險管理與組織整體的風險承受度相互一致。

透過質化與量化方法的結合，可建立系統化的資安風險指標，根據關鍵攻擊指標提供決策者資料導向的整體視角，例如：

- **攻擊向量**：用來發動攻擊或入侵系統的途徑或方法。
- **複雜度**：攻擊者利用弱點所需的技術能力與資源。
- **影響程度**：攻擊成功後對業務與營運造成的後果。
- **暴露程度**：環境中可被利用的弱點或缺口。
- **嚴重性：**威脅發生的可能性，以及可能造成的破壞程度。
- **修復能力**：是否有解法、解法為何，以及能多快佈署。

威脅建模

第三步是以主動方式識別並排序裝置、系統與應用程式中的風險。更具體來說，在進行滲透測試前先做威脅建模（下一節將詳述），可優先聚焦於高嚴重度風險。這不僅有助於降低裝置風險，也能維持組織整體穩固的資安態勢。

市面上有多種威脅模型，可用於評估特定風險，或整合使用以系統化識別與量化威脅；換句話說，最好的防禦方式，就是像攻擊者一樣思考。

常見的威脅建模方法包括：

STRIDE：

偽裝、竄改、否認、資訊洩漏、阻斷服務與權限提升。

用途說明：

依六大類別對風險進行分類評估。

DREAD：

破壞潛力、可重現性、可利用性、影響使用者數量與可被發現性。

用途說明：

根據五項因素計算平均分數，用以排序風險嚴重性。（通常會與 STRIDE 搭配使用，以優先處理高風險威脅。）

LINDDUN：

連結性、可識別性、不可否認性、可偵測性、資料揭露、認知不足與不合規。

用途說明：

透過分析資料在應用程式與系統中的流動方式，系統化識別並降低隱私相關威脅。

PASTA：

攻擊模擬與威脅分析流程。

用途說明：

聚焦於風險對企業的影響，涵蓋技術需求（如定義目標與範圍、分析弱點、模擬攻擊），以制定風險因應策略。

OCTAVE：

營運關鍵威脅、資產與弱點評估。

用途說明：透過三個階段（建立以資產為基礎的威脅輪廓、識別基礎架構弱點、制定風險管理策略），讓資安與業務目標保持一致。

滲透測試

最常見的風險評估工作，莫過於滲透測試，主要用於找出並排序裝置與軟體中的弱點。之所以將其列在最後，是呼應前一節對威脅建模的說明。在完成威脅建模後再進行滲透測試，能為整體風險評估流程帶來更高的效率與成效。

其效率提升體現在：

- 讓測試人員能聚焦於高嚴重度風險（因較低風險已在威脅建模階段識別）
- 讓 IT 團隊能在評估流程較早階段就開始進行風險因應

而成效提升則體現在：

- 驗證先前已佈署的修補與改善措施
- 進一步找出過去可能被忽略的弱點

裝置態勢與身分優先存取（零信任歷程）

新興技術需要以身分為核心的策略，並持續驗證裝置態勢，才能保護敏感資料並維持營運完整性。為支援日益多元的裝置組合，管理現代化必須自動化政策執行、降低營運負擔，並順暢擴展零信任架構。

以下解決方案提供不同層面的工具，協助 IT 進行新興技術的生命週期管理：

- **行動裝置管理（MDM）**：整合裝置與身分管理，並提供完整的端點資安能力，**從零接觸佈署到安全汰除**，支援地端或雲端環境。
- **統一端點管理（UEM）**：可部署於地端或雲端，提供跨平台支援，但通常需在功能深度上有所取捨。
- **Amazon Web Services（AWS）：**雲端架構，針對特定技術（如物聯網裝置）提供管理與安全能力，並支援多家供應商。
- **自動化端點管理（AEM）：** 雲端化 UEM 的下一個進化階段，透過自動化降低營運成本，並持續驗證與修正裝置狀態，在大規模、多樣化裝置環境中落實零信任。

應用程式與資料控管

回到最基本的本質，不論是哪一種裝置或作業系統，資料就是資料。在管理與保護新興技術的所有控管、流程與作業中，資料保護始終是核心。

部署設定檔是強化裝置安全、並保護裝置內與處理中資料的有效方式之一。雖然支援的方式會依作業系統而有所不同，但核心目標是一致的：依循標準與框架等最佳實務建立安全設定，跨平台守護資料安全。

建立安全設定時，常見可使用的工具包含：

- **Android**：**OEMConfig** 與 **Android Open Source Project**（AOSP）
- **Apple**：**Apple Configurator**、**Jamf Pro** 與宣**告式裝置管理**（DDM）
- **Linux**：Bash 指令碼、**SOTI MobiControl** 與 **Microsoft Intune**
- **專有系統：**請參考製造商的支援網站，以取得專為該技術設計的管理工具

監控與回應

掌握端點健康狀態的可視性，是主動式資安防護不可或缺的一環。問題越早被發現，事件回應就能越快降低風險或排除威脅。主動監控環境中的端點，不只是建議做法，更是零信任架構的關鍵要素。

零信任防護可分為兩個層面：裝置端防護與網路層防護。網路層的部分將於下一節說明，以下先聚焦在裝置端，說明如何在整體環境中維持良好的裝置狀態：

- 主動監控裝置健康遙測資料與合規狀態
- 整合管理與資安解決方案，自動化回應流程
- 在授予資源存取權限前，透過零信任機制驗證端點健康狀態
- 以固定節奏部署作業系統更新、安全修補程式與應用程式更新

網路安全

新興技術的發展速度往往超越既有標準，使部分端點更難管理，甚至與企業目標產生落差。由於風險本身具有主觀性，資安策略並不存在一體適用的標準答案。因此，保護從端點出發的資料安全就顯得格外重要。以下解決方案可單獨部署或相互搭配，協助在地端與雲端環境中強化資料安全：

- **非軍事區（DMZ）**：將 IoT 等高風險裝置區隔，只允許依政策進行受控的內外部通訊。
- **資安協同、自動化與回應（SOAR）：**透過自動化整合資安工具與流程，加速威脅偵測、回應與控管。
- **零信任網路存取（ZTNA）**：持續進行情境式裝置驗證、以連線為單位的微通道與健康檢查，確保只有合規裝置能存取受保護資源。
- **零信任網路存取（ZTNA）**：持續進行情境式裝置驗證、以連線為單位的微通道與健康檢查，確保只有合規裝置能存取受保護資源。

基準、指標、標準與框架

重要的是，這些階段應被視為循環流程，而非線性步驟。IT 與資安的生命週期本質上是反覆迭代的，它不是終點，而是一條持續前進、相互影響的路徑。因此，在導入新興技術的同時，下列要素之間的相互搭配與協同，對維持整體安全至關重要：

- **基準（Baselines）：定義基礎資安狀態的一組控管與流程。**
- **指標（Benchmarks）：**用來**衡量是否符合資安最佳實務的效能指標。**
- **標準（Standards）：**全球認可的最佳實務，用來規範硬體、軟體或服務應如何**達成特定安全要求**。
- **框架（Frameworks）：**以結構化方式說明如何部署控管、政策、流程與標準，**以降低風險**並提升安全性。

總結

在理解新興技術及其對企業目標的影響後，現在正是企業領導者與 IT 團隊採取行動、讓既有管理與資安策略與前瞻性最佳實務接軌的時刻。 及早行動，企業才能領先因應新興風險、簡化營運流程，並有信心迎接下一波創新浪潮。

檢查清單：企業領導者與 IT 管理者的下一步行動

1. 盤點業務使用情境

- 評估新興技術（AI、IoT、空間運算、穿戴式裝置）與企業目標的契合度。
- 分析在既有工作流程下，可能帶來的投資報酬率（ROI）與營運改善空間。
- 優先推動能帶來可量化業務成效，並具備法規遵循準備度的專案。

2. 建立跨部門評估團隊

- 組成由 IT、資安、法務與營運等關鍵利害關係人參與的評估小組。
- 明確指派風險評估、法規審查與生命週期管理的負責單位與窗口。
- 建立快速回饋與問題升級的溝通管道。

3. 執行完整的資產與相依關係盤點

- 完整記錄環境中使用的所有裝置、軟體、API 與雲端服務。
- 釐清混合環境（雲端、地端與邊緣）之間的整合與相依關係。
- 標示裝置持有模式（COBO／COPE／BYOD／CYOD），確保可視性與責任歸屬。

4. 執行風險與威脅評估

- 同時運用質化與量化方法，評估風險承受度與可能影響。
- 透過威脅模型進行風險對應，確保評估結果一致且準確。
- 依嚴重性、可利用性與修補時程，為弱點進行優先順序排序。

5. 進行威脅建模

- 使用主流威脅建模框架，模擬可能的攻擊路徑。
- 找出隱私、資料流向與營運層面的曝險點。
- 在正式上線前，記錄並落實降低風險的因應措施。

6. 確認法規遵循與治理要求

- 檢視各地區與產業相關的法規要求。
- 確認資料落地、資料主權，以及第三方供應商風險管理機制。
- 將 AI 與資料導向技術的倫理議題納入評估考量。

7. 定義裝置註冊與佈署流程

- 為所有裝置類型與持有模式建立標準化的導入流程。
- 自動化設定、修補節奏與存取控管，降低人工作業錯誤。
- 透過安全註冊機制與身分為本的驗證方式確認端點可信度。

8. 整合以身分為核心的存取策略

- 在存取資源前，持續驗證身分憑證與裝置狀態。
- 在所有端點與應用程式中落實最小權限原則。
- 將零信任與情境感知政策整合至存取控制系統中。

9. 建立安全設定與資料控管機制

- 制定資安基準，明確設定配置與合規期待。
- 對靜態與傳輸中的敏感資料進行加密。
- 建立細緻的資料分類、儲存與分享政策。

10. 進行網路區隔並強化通訊安全

- 透過 VLAN 與 DMZ 隔離 IoT、穿戴式裝置等高風險裝置。
- 運用微分段與零信任網路存取（ZTNA），建立具彈性的網路層安全控管。
- 確保資料安全是網路安全的核心，不論裝置類型、持有 模式、 作業系統，或使用者身處何地。

11. 導入持續監控與自動化回應政策

- 蒐集所有端點的遙測資料，提供即時可視性與健康狀態洞察。
- 部署自動化流程，用於異常偵測與事件回應。
- 將警示集中至中央平台，自動化威脅偵測與修復作業。

12. 套用基準與指標，並蒐集生產力數據

- 套用基準設定標準，建立全企業一致的整體安全防護。
- 以指標衡量效能表現與安全狀態。
- 檢視關鍵績效指標（KPI），評估合規狀況並呈現風險降低成效。

13. 定期執行驗證：滲透測試與稽核

- 在部署後定期安排滲透測試與弱點掃描。
- 驗證威脅建模階段所提出的修補措施是否確實生效。
- 依既定基準檢視發現結果，並據此更新相關政策。

14. 自動化生命週期管理與政策落實

- 運用整合式端點管理或自主式管理系統，持續維持合規狀態。
- 自動化修補流程、合規政策與裝置汰除作業。
- 隨著框架與標準演進，持續調整並對齊相關設定。

15. 文件化成果並定期進行教育訓練

- 建立回饋機制，追蹤新興威脅與實務經驗。
- 持續為管理者與使用者提供訓練，提升風險辨識能力。
- 隨著技術與法規演進，重新評估適用性並持續優化控管。