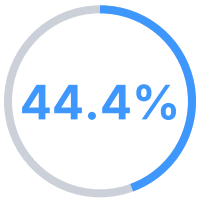
jamf

JAMF 的 AI 治理調查：

687 位 IT 與資安領導者對 AI 治理的觀察

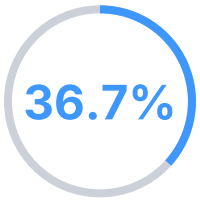
調查結果摘要

687 位來自 Apple 企業的 IT 與資安領導者，分享了他們在 AI 部署規模、目標與資安方面的現況。
以下是我們的調查發現。



自動化

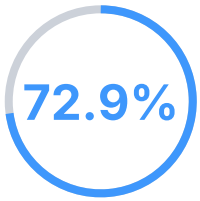
部署



治理

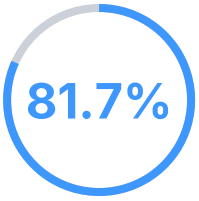
三大 AI 優先事項匯聚

受訪者將自動化 IT 維運（44.4%）、部署 AI 生產力工具（41.0%）與建立 AI 治理（36.7%）列為**前三大 AI 優先事項**。



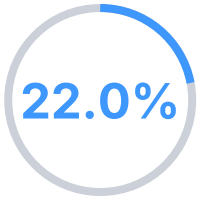
的組織已部署 AI

將近四分之三的組織已以某種形式部署 AI。產業已度過「是否導入 AI」的討論階段，建置治理機制勢在必行。



的組織暴露於 AI 風險中

22.0% 已發生過成本或資安事件。另有 59.7% 認為短期內可能發生。AI 風險若非已實際發生，就是企業普遍預期即將來臨。



的組織已發生過成本或資安事件

超過五分之一的組織已發生過與成本、資安或兩者相關的事件。影響同時落在預算與資安團隊身上。

事件發生率提升幅度

在已深度整合 AI 的組織中，27.1% 曾發生 AI 相關事件，而仍在探索階段的組織則為 19.4%。風險暴露程度隨導入深度增加而上升，而非下降。

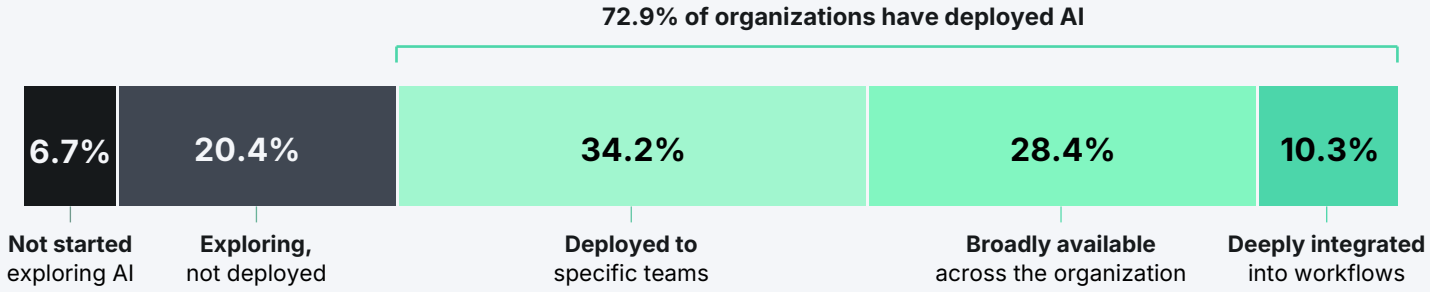
AI 使用越多，風險越大。

多數組織正積極推動 AI 導入，但風險也隨之增加。影子 AI、悄悄嵌入的軟體功能，以及端點裝置與代理型工具，都形成了難以治理、更難以稽核的盲點。隨著導入深度增加，風險暴露程度也隨之提升。問題不再是事件是否會發生，而是何時發生。

圖表 1

Apple 企業的 AI 導入現況

重點摘要： 將近四分之三的 Apple 企業已以某種形式部署 AI，從團隊層級的試行到深度整合於日常工作流程中皆有。討論焦點已超越「是否導入」的階段。



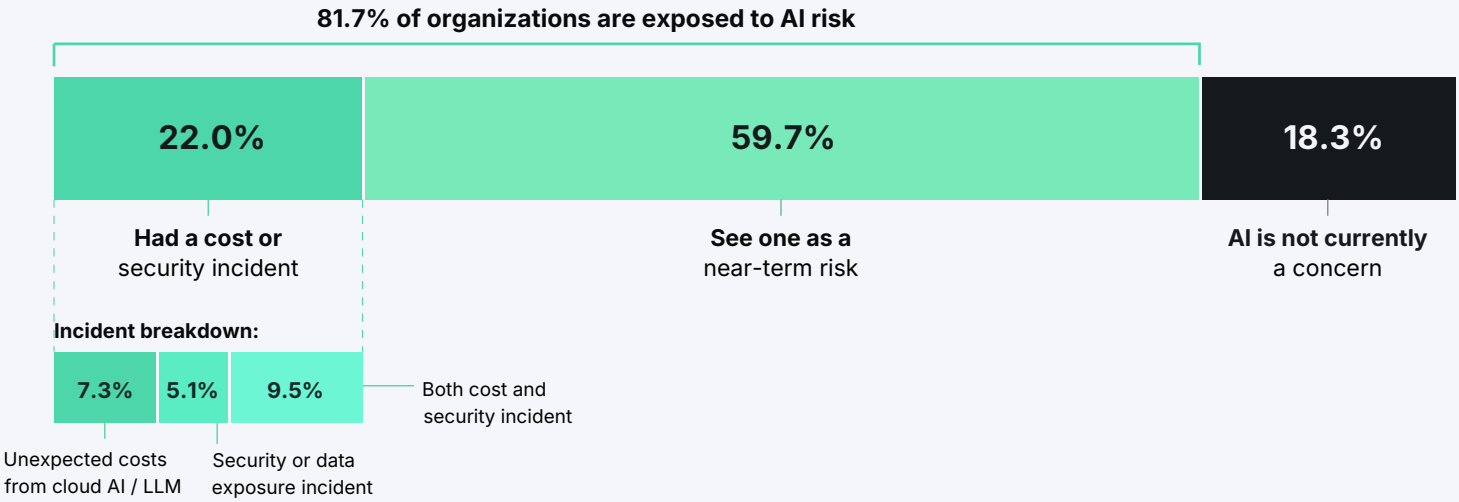
註解：樣本數 n = 687 位 IT 與資安領導者。2026 年第二季度。

儘管將近四分之三的組織已部署 AI，大規模部署並未降低風險，反而加劇了風險。22.0% 已發生過事件：7.3% 來自雲端 AI 或 LLM 的意外成本，5.1% 來自資安或資料外洩事件，9.5% 則兩者皆有。在尚未發生事件的組織中，仍有 59.7% 預期將會發生。

圖表 2

過去 12 個月的 AI 相關事件與擔憂

重點摘要：22.0% 的組織已發生過 AI 相關事件。另有 59.7% 預期會發生。僅 18.3% 表示 AI 目前並非其關注重點。



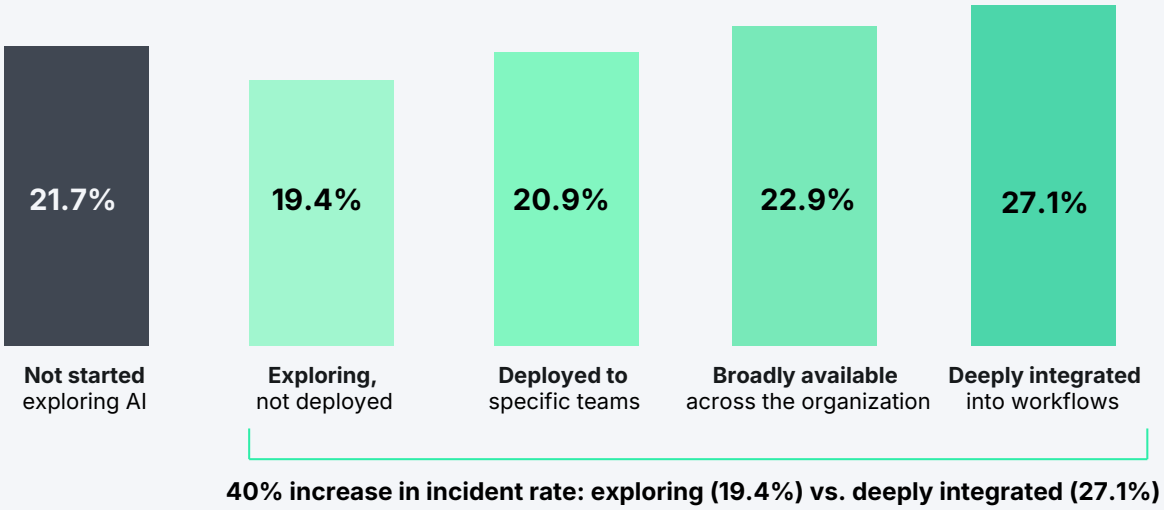
註解：樣本數 n = 681。此模式在兩個調查樣本中各自成立。

然而，資料呈現了一個反直覺的發現：AI 導入最深入的組織，事件發生率反而最高。

圖表 3

依 AI 導入深度的事件發生率

重點摘要：AI 部署程度較深的 Apple 企業，回報事件發生的比率也較高。在 AI 導入最成熟的企業中，27.1% 已發生過事件，而仍在 AI 探索階段的企業則為 19.4%。



註解：樣本數 n = 683 位 IT 與資安領導者。2026 年第二季度。

一旦團隊開始在組織內探索 AI，發生事件的機率便隨之上升。已深度整合 AI 的組織中，回報發生事件的比例（27.1%）比仍在探索階段的組織（19.4%）高出 40%。

AI 挑戰圍繞共同主題

受訪者針對事件預防的開放式回答，歸納為四大主題。

影子 AI

生產力提升的壓力、AI 工具的蓬勃發展，以及企業全面推動 AI 整合，都促使員工頻繁使用 AI。這通常未經 IT 核准；員工自行建立個人帳戶，並可能輸入敏感資料。其結果是 IT 對哪些 AI 系統被使用一無所知，使 AI 平台難以管控或封鎖。缺乏可視性，使得資安與治理幾乎不可能落實。

AI 工具過度擴散

除了大量新興 AI 軟體外，許多既有 App 也紛紛將 AI 功能嵌入原有產品中。逐一審查與部署每個 AI 工具對 IT 團隊來說既耗時又困難，尤其考量到 AI 發展的速度。受訪者表示，難以判斷哪些 AI 平台最適合員工，也難以推動員工使用經核可的 AI 工具。越來越多的進入點，使 AI 更難防護。

AI 代理程式與開發者 AI 工具

AI 代理程式與開發者 AI 工具的挑戰主要體現在幾個關鍵面向：安全部署/可視性、AI 功能，以及使用者教育。受訪者提到，在管理代理型 AI 部署時，如何在賦能使用者的同時不將資料置於風險中，是一大挑戰。對命令列工具、第三方套件、IDE 擴充功能、嵌入式 LLM 等的可視性不足，同樣是常見問題。若具備適當權限，AI 代理程式可能在程式碼庫中引入不安全或有問題的程式碼，或移除必要程式碼，構成嚴重風險。開發問題也延伸至非開發人員的使用者，他們會在未經適當審查與品質檢測的情況下自行建立 App。

成本失控

在成本、公司政策與資安之間取得平衡，對 IT 團隊構成壓力。雲端 AI 與 LLM API 以用量計價的收費模式使支出難以預測，而各部門快速採用新工具，導致付費授權重複累積。若無法掌握實際使用情況，IT 團隊便缺乏明確依據來決定哪些工具應予整合。

治理與生產力相輔相成。

在已導入 AI 的組織中，AI 嵌入越深，事件發生率就越高。

受訪者面臨的共同挑戰涵蓋可視性、部署、AI 工具過度擴散與成本等面向。

綜合以上調查結果，一個現實清晰可見：**AI 導入速度已超越治理機制的建置速度。**

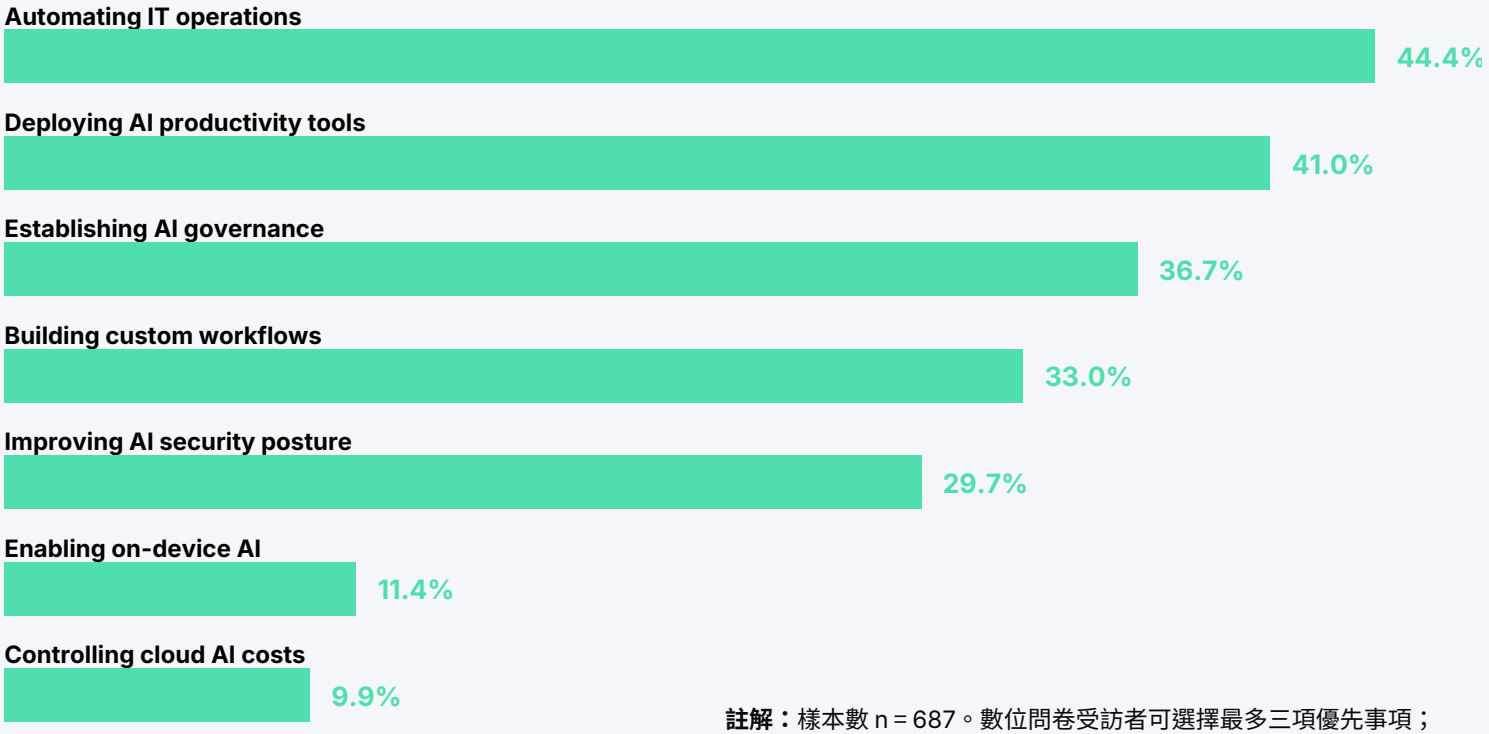
具體問題包含影子 AI、企業資料或系統的暴露點、重複採購高成本平台，以及 IT 部門無法察覺而難以量化的風險。

因應此局勢，IT 團隊需要在 AI 重塑工作方式的此刻，重新調整優先順序。

圖表 4

未來 12 個月的最重要 AI 優先事項

重點摘要： 自動化 IT 維運、部署生產力工具，以及建立治理機制，三者受重視的程度相當。
治理並未落後於賦能，而是同步推進。



註解：樣本數 n = 687。數位問卷受訪者可選擇最多三項優先事項；實體活動受訪者則選擇一項。詳細說明請參閱研究方法。

治理與賦能看似彼此對立。AI 工具越多，治理難度就越高。IT 團隊向來必須在各項相互衝突的優先事項之間取得平衡，AI 也不例外。AI 部署速度之快、功能與風險之多，都已進入全新領域。

正因如此，團隊才會同時推進這些優先事項。進度太快，事件發生的機率就會增加。進度太慢，員工就會尋求替代方案，進而損害您的資安狀況。

💬 同業心聲：AI 挑戰的真實面貌

在 178 份開放式回答中，調查獲得了豐富的細節與洞見，為量化數據提供了具體脈絡。
以下為開放式回答中的八則代表性心聲*：

員工希望立即使用 AI，把關的資安團隊承受不小壓力。核心困境始終未解：**嚴格管制會降低生產力，放寬規範則會引發實質合規風險。**

無論企業是否需求，各家廠商都在產品內建 AI 功能。全面禁用僅能暫時應急，無法長久維持。更大的隱憂在於雲端資料的處理方式，以及我們能否掌控資料的去向。

封鎖已知 AI 網站只是基礎作業。CLI 工具、IDE 擴充功能、瀏覽器外掛，以及從 GitHub 下載的套件等**大多難以偵測**；封鎖了一個管道，使用者就會找到另一個。

在受監管產業與特定司法管轄區，任何功能上線前都必須先建置特定的合規框架，而目前的**工具與框架尚未能滿足這些要求。**

影子 AI 與黑箱腳本執行位居風險清單首位。緊接在後的是非技術使用者自行摸索編寫 App，建構他們並未完全理解的東西，並在無意間暴露資料。

企業期望全面導入 AI，卻不願投入足夠預算購買授權。進展太快的團隊現在面臨多個功能重疊的代理程式，**成本高昂，卻缺乏明確規範**來判斷哪些工具值得保留。

開放 AI 代理程式存取開發與正式環境基礎架構，很難說服人。最令人擔憂的是，代理程式可能執行非預期動作，並在事後才告知資料已遺失。**如何在受控、可管理的前提下部署 AI 代理功能，至今仍是未解難題。**

當 AI 的幻覺輸出被當作事實，而 AI 又不斷深入日常作業，**風險累積的速度遠比使用者的認知提升來得更快。**

*以上內容由 Jamf 根據 178 份開放式回答中的模式歸納整理。每一則皆呈現反覆出現的主題，而非單一受訪者的逐字原話。

採取行動：四大治理原則

1.

取得可視性。

如同許多受訪者所言，取得可視性至關重要。看不見，就無法治理。當然，困難也在於此。定期稽核已安裝的 App與流量監控，有助於識別與 AI 平台的互動行為。隨著使用者採用本地 AI 平台，以及已核可的非 AI 應用程式陸續加入 AI 功能，必須更深入調查 AI 執行階段的偵測。

2.

治理工具，而非使用者。

對許多 IT 團隊而言，組織的 AI 政策來得很快，且未經 IT 部門充分考量。而這些政策鼓勵盡快擴大 AI 使用。即使提供使用者指引，指引仍不等於強制執行。這就是影子 AI 的溫床。

治理應以組織的風險承受度與資安準則為依據，並具體反映在 AI 工具的資料共享設定中：它存取哪些資料、如何處理這些資料，以及它能變更什麼。在影子 AI 的情境下，使用者不一定能被看見，但流量、資料與 API 呼叫是可以被看見的。您只能治理您看得見的東西。

3.

將治理內建於部署流程中。

導入 AI 過於倉促的組織，讓自己暴露於潛在的事件風險中。順序至關重要——治理必須伴隨 App 部署同步進行，而非事後應對。確實，說來容易做來難，您可能已在面對堆積如山的待辦事項。但透過盤點正在使用的工具、提供給使用者並建立存取政策，將使您能更安全地擴大 AI 工具的規模。

4.

選用專為 Apple 打造的，而非事後拼湊的工具。

基於網路層的工具能顯示流量：使用者存取了哪些雲端 AI 服務、何時存取、頻率為何。這確實是有用的訊號，但僅止於網路邊界。即使 AI 本身運行於雲端，存取行為仍發生在裝置上：安裝了哪些工具、這些工具產生哪些處理程序、存取了哪些檔案。這些都不會出現在 DNS 日誌中。Apple 原生的工具能補足此缺口：檢視工具、處理程序、檔案存取，並強制執行哪些是允許的。

治理您所賦能的；賦能您所能治理的。

AI 的發展速度，超越了多數治理框架原本的設計負荷。但您已遭遇的挑戰，不必定義您未來的部署方式。無需在使用者所需的 AI 工具與工具使用的安全性之間做出取捨。

表現領先的團隊，並非跑得最快或管制最嚴的。他們將治理與賦能視為同一個專案，從一開始就將可視性與存取控管內建於 AI 部署中。對 Apple 企業而言，這取決於能掌握您所管理之運行環境的工具：雲端流量、端點裝置模型與代理型處理程序各自留下不同的訊號，而非專為 Apple 打造的監控工具會遺漏其中大多數。您所建立的治理，其強度取決於工具的可視範圍。

您無法減緩 AI 的導入速度。但您可以治理它，而這正是行動的起點。

研究方法

本調查資料分兩波收集。第一波於 2026 年 3 月至 4 月間針對 Jamf 客戶社群發送（338 位受訪者）。第二波為 Jamf Nation Live 活動現場問卷，涵蓋北美六個城市（349 位受訪者）。合計受訪者：687 位 IT 與資安領導者。所有受訪者均任職於大規模管理與防護 Apple 裝置的組織，且均為 Jamf 客戶。

在優先事項問題中，受訪者被要求選出未來 12 個月內最重要的 AI 優先事項。3 月與 4 月的問卷允許最多選擇三項；Jamf Nation Live 現場問卷則允許選擇一項。此問題的百分比代表全體 687 位受訪者中，將該項目列為優先選擇之一的比例。為求透明，兩種選擇規則皆在此揭露。

統計檢定確認兩波受訪者分屬不同群體，Jamf Nation Live 的受訪者在 AI 成熟度上平均而言較為初期。方向性的發現各自獨立地存在於兩個樣本中。所有受訪者資料均以匿名方式收集與分析；個別回覆不會歸屬於特定受訪者或組織。受訪者未因參與調查而獲得報酬。