Microsoft 365

從監督到洞察：管理影子 AI 風險

目錄

簡介

根據最近的《工作趨勢指數》報告，在 31 個國家/地區接受調查的知識工作者 (包括員工與領導者) 中，有超過 80% 表示他們覺得缺乏時間或精力來完成工作。此外，超過 50% 的受訪企業領導者表示，為了達成目標，生產力需要提升[1]。根據《2024 年 Microsoft 工作趨勢指數報告》，許多員工正在尋找生成式 AI 工具來彌補這一差距，並且在開始使用這些工具時並未等待公司 IT 部門的批准。

當工具在 IT 部門監控範圍之外運作時，可能會為組織帶來安全和合規風險。而影子 AI (指在未經 IT 部門批准的情況下使用 AI 工具) 正逐漸成為現今職場中最新形式的影子 IT。

隨著 AI 採用加速，企業領導者積極保持領先，並致力於緩解這些工具可能帶來的潛在風險。在最近的 iSMG 研究中，超過 70% 的受訪企業領導者表示，確保資料隱私與安全是將生成式 AI 與現有 IT 基礎設施整合時的首要挑戰[2]。此外，超過 90% 的受訪 CIO 和 CTO 表示，生成式 AI 已經或將會推動他們的組織加強資安投資[3]。

在這本電子書中，您將探索影子 AI 的常見應用情境，了解其對組織可能帶來的風險、五種管理這些風險的方法，以及 Microsoft 365 E3 如何協助您應對這些挑戰。

[1] **2025 工作趨勢指數年度報告，Microsoft, Inc.，2025 年 4 月。**Microsoft 分析了 2025 年 2 月 6 日至 2025 年 3 月 24 日期間，來自 31 個國家/地區共 31,000 名全職或自僱知識工作者的調查資料、LinkedIn 勞動市場趨勢，以及數兆筆 Microsoft 365 生產力訊號。

[2] **iSMG 第二屆年度生成式 AI 研究商業效益與資安風險,** 根據來自北美洲、歐洲、亞洲、南美洲、澳洲及非洲六個地區超過 360 位商業與資安專業人士於第三季的調查回覆

[3] **AI 安全平衡之道《從風險到創新》，NTT DATA，2025 年 6 月，** 根據 NTT DATA 對超過 2,300 位資深生成式 AI 決策者 (其中包括分布於 34 個國家/地區的 1,500 位最高層主管) 的調查資料。

什麼是影子 AI？為什麼可見性如此重要？

影子 AI 指員工在未經 IT 部門明確批准或監督的情況下，使用人工智慧工具和應用程式，且往往超出官方安全與合規框架的可視範圍。隨著員工尋求提升生產力及應對日益繁重的工作需求，他們可能會轉向這些未經授權的解決方案，以簡化工作流程、協作或產生新內容——但往往未意識到其中潛在的風險。影子 AI 對 IT 部門而言是不可見的，這使得組織難以掌握員工正在使用哪些應用程式，以及哪些應用程式帶來最大的風險。

影子 AI 可見性的重要性

當 IT 部門不了解某個應用程式或服務時，就無法提供保護或支援。這個*可見性缺口*使得準確識別、管理或減輕與敏感資料暴露、法規不合規以及失去專有資訊控制權相關的潛在威脅變得困難。IT 部門與企業領導者需要掌握組織中正在使用的影子 AI，處理與 AI 使用相關的新興風險，並決定哪些工具應該在適當的防護措施下獲准使用。組織有機會將影子 AI 從風險轉化為在安全的情況下創新工作方式的契機。為此，企業需要取得更好的平衡——讓員工能夠在受治理且安全的框架下善用有用的 AI 工具，以降低潛在風險。

見解

*看不見，就無法保護。*當 IT 部門未察覺某個應用程式或服務正在被使用時，就無法保障其安全。這正是影子 AI 問題的核心，也凸顯了為何需要一種新方法。如果員工認為這些 AI 工具對達成目標至關重要，全面禁止所有外部工具並非可行之道。相反地，組織需要將影子 AI 揭露出來——取得員工正在使用的工具的可視性，建立適當的控管措施，並提供安全且獲批准、能滿足組織需求的替代方案。簡而言之，挑戰在於賦能團隊使用 AI *不*犧牲安全性。

職場中的影子 AI：範例情境與潛在風險

影子 AI 源自於希望提升生產力與影響力，或嘗試新技術的員工。以下是幾個虛構範例，說明未經授權的 AI 工具如何被使用及其可能帶來的風險：

職務	案例範例	未經授權工具的潛在風險
行銷	使用生成式 AI 內容工具，根據公司品牌資料製作行銷文案或設計。	敏感品牌或產品資訊外洩；失去對外部 AI 服務如何儲存或使用公司創意資產的控制權。
財務	將企業財務資料上傳至 AI 驅動分析或視覺化服務，以獲得快速見解。	將機密財務資料 (預算、預測) 暴露給第三方；如果包含客戶或員工資料且未妥善保護，可能違反合規要求 (例如 GDPR)。
客戶支援	將客戶資料或支援聊天記錄輸入至 AI 工具，以撰寫回應或彙整案件。	違反隱私與資料管理規定——敏感客戶資訊可能被儲存於公司系統外部；AI 服務商無法保證資料保留或正確刪除。
前線零售	店經理在手機上使用 AI 排班應用程式來優化員工排班表。	公司人力資料 (員工姓名、班表) 被上傳至非獲批准的應用程式，可能引發隱私權問題。如果 AI 建議未符合勞動法規，可能導致排班衝突或原則違規。
前線醫療	護理師或醫生使用 AI 聊天機器人協助撰寫病患照護紀錄或回答醫療問題。	病患健康資訊 (PHI) 可能在沒有任何防護措施的情況下暴露於外部服務，違反合規與保密要求。AI 的醫療建議也可能未經驗證，帶來安全風險。

在上述各情境中，個別員工是出於良好意圖並尋求生產力提升，但組織可能因此承擔風險。

公司資訊可能分散於未經授權的平台上，造成*資料控管上的挑戰*。未經審核的應用程式可能會引入惡意軟體或資訊安全漏洞，將受攻擊面擴大到 IT 部門管理範圍之外。也可能存在合規風險。從 IT 支援的角度來看，如果影子 AI 工具發生故障，技術支援中心可能無法協助終端使用者，因為他們對此沒有了解或掌握權。

管理影子 AI 風險的五種方法

有了正確的策略與工具，您可以將影子 AI 從潛在威脅轉變為培養安全創新文化的機會。賦能您的團隊使用 AI 生產力工具*同時*維持保護企業所需的監督。這代表從過去的「不，絕不」轉變為「可以——但要有適當的防護措施」。以下五項建議旨在協助您管理並掌控組織中的影子 AI：

01 探索您的影子 AI 足跡，評估並優先排序風險

看不見，就無法保護。透過活動記錄，了解組織中正在使用的應用程式。一旦您了解正在使用的應用程式，就能辨識出處理敏感資料的合適工具，同時注意那些不符合您的安全與合規性政策的應用程式。有了這些見解，您就能做出更明智的決定，選擇要允許、監控或限制哪些應用程式，以降低潛在風險。

02 透過安全與合規性政策實現快速成效

啟用或套用原則調整，以更好地降低影子 AI 使用帶來的潛在風險。您可以使用條件式存取原則來限制高風險應用程式的使用，針對敏感資訊採用資料外洩防護原則以減少過度分享和資料外洩，並對所有使用者強制執行基本的多重驗證和裝置合規。即使尚未完全掌握組織中所使用的 AI 應用程式，這些措施也能迅速降低最明顯的風險。

03 教育員工認識影子 AI 的潛在風險

員工常常不了解使用未經授權的 AI 工具可能對組織帶來的風險。經常透過妥善設置的資料外洩防護警告、公司政策提醒及簡短培訓，傳達影子 AI 的風險，協助使用者轉向更安全的做法，避免過度嚴厲執行政策。

04 提供經核准的 AI 工具，進一步降低風險

在可能的情況下，提供員工經批准的 AI 工具，作為未經授權工具的替代方案。降低影子 AI 的有效方式，是以認可的解決方案因應組織中最常見的使用案例。這能讓 IT 部門持續掌握可視性與控制權，同時協助使用者解決遇到的問題。

05 推動持續治理

將檢查整合進您的 IT 治理例行程序——定期檢視活動記錄與報告，隨新 AI 服務推出及時更新原則，並隨時向領導層通報進展 (例如非授權應用使用減少或事件得到預防)。這將協助您在產業環境持續變化的過程中，持續降低當前與未來可能面臨的風險。

透過上述步驟，您可以同時賦能創新與安全。

員工可以在工作場所使用經核准的 AI 解決方案，而 IT 部門則維持對這些工具的控制與合規。

透過 Microsoft 365 E3 偵測與管理影子 AI 風險

Microsoft 365 E3 讓組織有能力發現影子 IT、評估潛在風險，以及實施安全與合規性政策，*而且不會*阻礙創新。這套整合的生產力、安全與管理功能，能讓您直接應對影子 AI 的挑戰。

Microsoft 365 E3 解決方案	它如何幫助您管理潛在的影子 AI 風險
Cloud App Discovery	**發現未經批准的應用程式並採取行動。**Cloud App Discovery 可供您上傳活動記錄並建立快照報告，讓您看到超過 31,000 個雲端應用程式，其中包括超過 400 個生成式 AI 應用程式。它能讓您看到組織中哪些應用程式被使用、由誰使用，以及使用頻率。這些資訊可協助您做出明智的決定，決定要允許或限制哪些應用程式的使用。
Microsoft Purview 資料外洩防護 (DLP)	**降低敏感資料外洩風險。**Microsoft Purview DLP 能讓您定義並套用原則，以偵測敏感資訊，並阻止或限制 Microsoft 365 服務中的電子郵件與檔案共享。例如，您可以設定規則來監控、稽核或阻止使用者透過電子郵件或檔案共用分享敏感資訊，並向使用者發出警示。
Microsoft Entra ID P1	**管理對雲端應用程式的存取。**Microsoft Entra ID P1 可啟用條件式存取原則，以控制誰能在何種條件下存取哪些應用程式。例如，您可以選擇要求多重因素驗證，或甚至限制使用企業帳號登入至您判定為高風險的應用程式。Microsoft Entra ID P1 可在合適的人員、合規裝置及核准條件下，提供雲端資源存取，同時限制對未核准應用程式的存取。
Microsoft Intune P1	**執行裝置與應用程式使用原則。**Microsoft Intune P1 可讓您允許受管理且合規的裝置用於工作，並提供管理這些裝置的工具。例如，它可以禁止在企業電腦上安裝未經批准的軟體，或推送限制存取特定網站或服務的設定。
適用於端點的 Microsoft Defender P1	**限制未經核准之網址的流量。**適用於端點的 Microsoft Defender P1 可封鎖受管理裝置到未經批准之網址的流量，協助您降低來自您認為具風險之網站的風險。例如，員工若試圖在公司筆電上存取已知風險較高的 AI 網站，將無法存取。

在 AI 採用之旅中踏出下一步 →

一切都始於意識、正確的工具和積極的計畫。Microsoft 365 E3 可提供工具，協助您的組織建立穩健的安全基礎與 AI 解決方案的治理架構。您將能掌握未經授權的工具的使用情況、啟用保護敏感資料的原則，並維持對使用者存取與裝置安全性的控制。準備好從被動 (在影子 AI 出現後發現並封鎖) 轉向更積極的策略，引導 AI 使用進入安全且受控的管道。參加 AI 安全評估並了解如何提升您的 AI 安全性態勢。深入了解企業用 Microsoft 365 的功能。