

以安全基礎釋放 AI 的潛能



目錄

- 01** AI 契機與安全性當務之急
- 02** 具有潛在風險的良好意圖：AI 案例範例
- 03** 透過 Microsoft 365 E3 打造安全的 AI 就緒基礎
- 04** 繼續您的 AI 採用旅程



前言

AI 契機與安全性當務之急

當今勞動力在生產力產能方面的差距正持續擴大。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¹。同時，受訪的企業領導者中有**超過 50%** 表示必須提升生產力才能達成目標¹。這也提供了一個契機，讓我們檢視目前的工作方式，並尋找有助於縮小這項差距的潛在解決方案。AI (包括代理程式在內) 做為解決方案具有相當大的潛力。**超過 80%** 的受訪領導者表示有信心，他們的組織會在未來 12–18 個月內開始使用 AI 代理程式來擴充人力產能¹。

這股奔向 AI 的熱潮也伴隨著一項警示：創新必須與強而有力的安全性與資料保護並行，才能降低潛在風險。在最近的 iSMG 研究中，**超過 70%** 的受訪企業領導者表示，確保資料隱私權與安全性是將生成式 AI 與現有 IT 基礎設施整合時的首要挑戰²。領導者正面臨雙重使命：加速採用 AI 以推動生產力，並在這個新時代保護資料。

本電子書將深入說明可能帶來潛在風險的 AI 範例情境，提供運用 Microsoft 365 E3 降低這些風險的實用建議，並附上檢查清單，協助組織開始或持續為大規模採用 AI 做好準備。為自信擁抱 AI 做好準備：讓您的組織在不犧牲安全性或合規性標準的前提下，運用 AI 推動創新。





具有潛在風險的良好 意圖：AI 案例範例

在使用與採用 AI 的過程中，最大的風險往往源自那些出於善意、努力把工作做好並創造更大影響力的員工。在急於提升生產力的情況下，團隊成員可能會不經意地向 AI 工具過度分享敏感資訊，或使用尚未經過 IT 部門核准的應用程式。這可能會帶來風險，並讓組織暴露於新的威脅之中。

讓我們透過兩個範例情境來說明這一點——一個是辦公室中的資訊工作者，另一個是前線工作者。

在這些虛構範例中，您將了解：1) 若缺乏妥善控管，出於善意的 AI 使用如何可能導致安全性遭到破壞；以及 2) 如何透過穩固的安全性基礎來降低這些潛在風險。



以安全基礎釋放 AI 的潛能

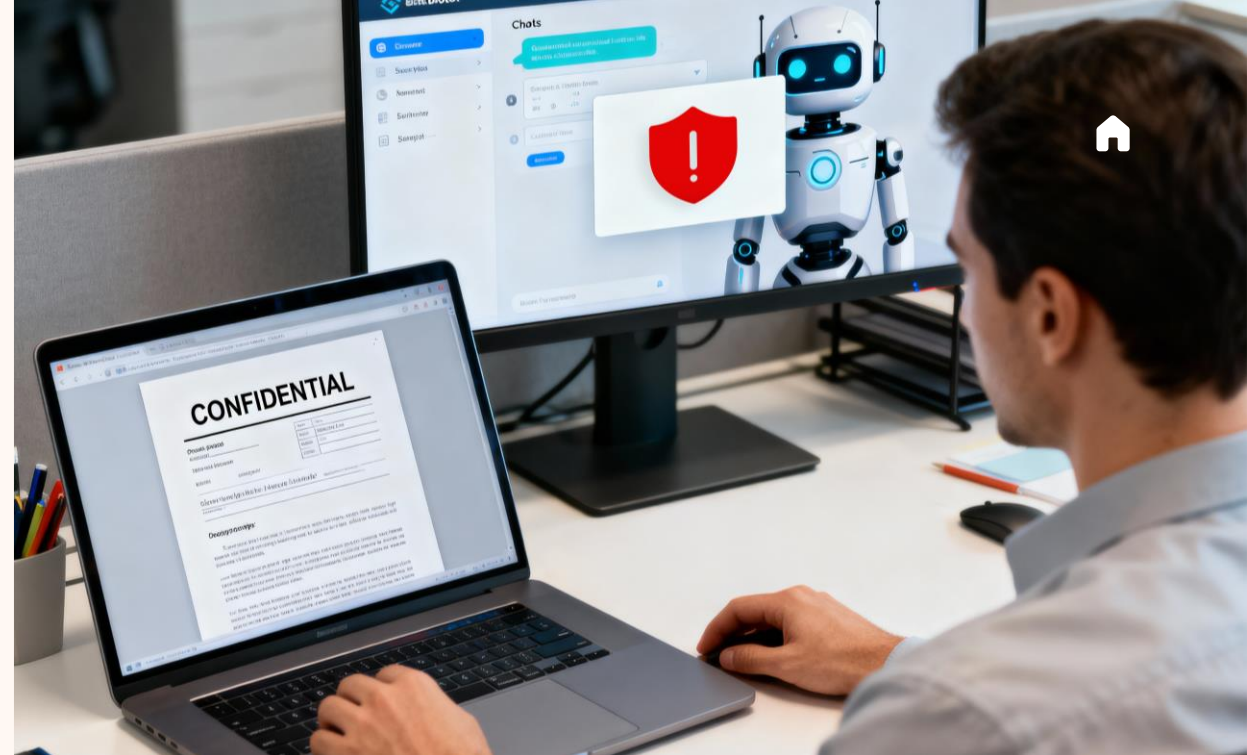
範例情境 14

產品行銷經理利用 AI 工具來草擬新聞稿

某家製造業公司的產品行銷經理正面臨緊迫的期限，必須撰寫一則關於未來幾個月即將上市的新產品的新聞稿。為了發想點子並加快撰寫流程，這位員工將機密的產品藍圖與內部財務預測的部分內容複製貼上到一個免費的線上 AI 寫作助理中。該 AI 工具很快產出數段潤飾過的文字，這位員工隨即將其用在新聞稿的草稿中。然而，這項工具尚未經其組織審查或核准。

潛在風險：

透過使用這項外部 AI 服務，該員工已經將公司的敏感資料 (產品規劃與財務資訊) 上傳至一個 IT 團隊無法掌握、也無法加以管理或控管的第三方系統。一旦這些資料被分享給該 AI 工具，由於已超出授權範圍，公司便喪失對其的掌控能力。該組織現在無法得知這些資料會被保存多久、可以由誰存取，或是該第三方將如何使用這些資料。原本看似快速提升生產力的做法，卻演變成一樁資料外洩事件。這個情境反映出，當出於善意的員工將敏感資料分享給未經核准的 AI 工具時，可能產生的內部風險，並使組織暴露在安全性弱點之中。



Microsoft 365 E3 的風險緩解措施：

Microsoft 365 E3 內建多項功能與能力，可協助避免出現這樣的情況。**Microsoft Purview 資訊保護方案 1** 可讓您對產品藍圖與財務預測等文件套用敏感度標籤與加密。如果這些文件事先已透過敏感度標籤加以分類並加密，例如透過加密套用 **機密** 標籤，其存取權限就能被限制為僅限授權使用者。此外，**Cloud App Discovery** 可協助識別正在使用哪些生成式 AI 雲端應用程式 (從雲端應用程式目錄中的眾多應用中找出)、是由哪些使用者使用，以及使用的頻率。那麼 IT 就能發現員工正在使用這個特定的 AI 工具，並可透過 **Microsoft Defender for Endpoint P1** 採取措施限制其使用，或提供經核准的替代方案。Microsoft 365 E3 提供各種工具與功能，協助組織提升可見度並降低風險。

以安全基礎釋放 AI 的潛能

範例情境 2⁴

零售門市經理使用 AI 擬定員工排班表與績效評語

一家大型零售連鎖店的門市經理因繁重的行政工作感到不堪負荷，此時發現了一款免費的 AI 生產力應用程式，聲稱能協助處理排班和各類文件作業。為了節省時間，該經理將一份包含員工姓名、電話號碼、時薪、可排班時段偏好，以及近期績效評語的試算表上傳到該 AI 工具中。他們請這個 AI 應用程式為門市產生一份最佳化的工作排班表，並協助撰寫即將到來的一對一會談所需的績效評估摘要。

潛在風險：

藉由將這些員工資料上傳到未經審查的 AI 應用程式，這位經理已經把員工的敏感個人資訊暴露給一個不受公司控管與監督的第三方系統。這可能導致潛在的隱私權侵害，以及與勞動法相關的合規性問題。公司的人資與 IT 部門無從得知這些員工資料目前儲存在何處、會被保存多久，或是可由哪些人員存取。原本只是為了提升效率的做法，卻造成嚴重的法律、隱私權以及員工信任問題。



Microsoft 365 E3 的風險緩解措施：

Microsoft 365 E3 的裝置與應用程式管理功能，有助於降低此類前線情境中的風險。透過 **Microsoft Intune P1**，零售商的 IT 團隊可以強制套用應用程式防護原則，針對存取工作資料的應用程式制定規則，例如限制複製/貼上，以及禁止將資料傳輸到未受管理的應用程式。透過 **Microsoft Entra ID P1**，零售商的 IT 團隊可以強制套用應用程式防護原則，針對存取工作資料的應用程式制定規則，例如限制複製/貼上，以及禁止將資料傳輸到未受管理的應用程式。在此情境下，如果經理的手機不合規或該應用程式未受管理，這些原則可以協助防止他們存取並上傳受限的公司檔案到影子 AI 應用程式。

關鍵見解：在這兩種情況下，員工的目標都是正面的——利用 AI 提升工作效率。然而，如果沒有適當的防護措施和原則，結果可能會是負面的。這些案例說明了，若在沒有安全保障的情況下採用 AI，可能會為組織帶來新的和額外的風險。目標不是限制 AI 的使用，而是推動其應用時能夠負責任地進行。下一節將探討在評估可能提升生產力的解決方案時應考慮的核心能力，以及 Microsoft 365 E3 所具備、能協助組織設定防護措施，確保敏感資料僅在核准且安全通道中流通的功能。

透過 Microsoft 365 E3 打造安全的 AI 就緒基礎

組織是否已準備好擴展 AI？請參考以下檢查清單，了解 Microsoft 365 E3 能如何助您一臂之力。

隨著 AI 的採用加速，在擴展 AI 之前，評估貴組織的安全性態勢並識別潛在差距變得越來越重要。Microsoft 365 E3 是專為 AI 應用而設計的生產力與安全基礎，結合廣泛的身分識別、安全性、合規性與管理工具，協同運作，助您自信地擴展 AI 採用。

請參考以下檢查清單做為起點，以了解貴組織目前的狀況。如果有任何項目尚未完全導入，您的組織可能會暴露於不必要的風險之中。



落實健全的身分識別和存取權管理原則，如多重要素驗證 (MFA) 和條件式存取。

Microsoft 365 E3 包含 **Microsoft Entra ID P1**，能在雲端與內部佈署環境中強制執行健全的身分識別和存取權管理。多重身份驗證 (MFA) 和條件式存取原則等解決方案能夠驗證每一次登入，並根據使用者角色、裝置健康情況及位置等條件限制或允許存取，有助於降低未經授權存取和資料過度暴露的風險。例如，您可以將 AI 應用程式的存取權限制為只有特定員工群組能夠使用，並要求登入時啟用多因素驗證 (MFA)，以降低帳戶遭到入侵的風險。條件式存取原則還能進一步保護敏感資料，防止員工以企業憑證存取未經批准的應用程式；而共用裝置則可強制執行登出規則，以防止未經授權的工作階段使用。



啟用跨受控端點與裝置的安全協作。

Microsoft 365 E3 透過 **Intune P1**、**Defender for Endpoint P1** 及 **Windows E3** 等解決方案，提供智慧型端點安全防護。這些工具有助於管理並提升個人電腦、行動裝置和應用程式的安全性。組織可以強制執行網站篩選功能，以封鎖有風險的網站 (包括未經授權的 AI 工具)，並透過 **Windows 自動修補** 和 **Autopilot** 讓裝置持續更新安全性修補程式。這些控制措施有助於保持裝置健康、受控，並持續更新安全性修補程式，降低受攻擊面。整合式端點與裝置管理可協助組織保護工作裝置並維持應用程式合規性，無論員工使用自己的裝置或公司提供的裝置。



透過敏感度標籤及資料外洩防護原則等功能來保護資料。

Microsoft 365 E3 提供核心 **Purview** 功能 — 敏感度標籤、加密及資料外洩防護 (DLP)，以保護文件及電子郵件中的敏感資訊。標籤原則發佈後，員工可以將包含財務資料、個人資訊或智慧財產權的檔案 (例如帶有「機密」敏感度標籤) 分類，並套用加密及存取控制。DLP 原則可偵測並限制在 **Exchange Online** 及 **SharePoint Online/商務用 OneDrive** 上的未經授權分享。即使在使用 **Microsoft 365 Copilot** 時，這些防護依然持續生效：Copilot 會遵守最高敏感度標籤，並防止未具權限的使用者存取或分析受保護的內容。



掌握正在被使用的未經核准 AI 工具，並據以採取明智行動。

Microsoft 365 E3 包含 **Cloud App Discovery**，可協助您瞭解哪些 AI 應用程式 (來自雲端應用程式目錄) 正在被使用、由哪些人員使用，以及相關的風險分數，讓您能根據這些資訊決定後續措施。若判定風險過高，IT 可使用 **Defender for Endpoint P1**，限制使用者在受管理的 Windows 11 裝置上存取該網址的權限。舉例來說，如果您發現有 100 位使用者正在使用尚未經 IT 審查或核准的 AI 影像生成工具，IT 可以依據組織的安全性與合規性標準展開調查。若被認為有風險，IT 可以建議已獲授權的替代方案。這些功能能協助您緩解影子 AI 的風險，並針對 AI 的使用做出適合您組織的明智決策。



提供經核准的 AI 應用程式，例如 Microsoft 365 Copilot。

提供經授權的 AI 應用程式能帶來顯著價值，讓員工能存取符合組織安全性與合規性標準的強大且經核准的工具。例如，與其讓員工使用未經審核的 AI 影像生成器或聊天機器人，IT 部門可以提供經認可的替代方案 **Microsoft 365 Copilot** — 這些工具都經過監控、支援，並整合至公司現有原則中。**Microsoft 365 Copilot** 提供一個安全且企業級的 AI 解決方案，深度整合至 Microsoft 365 生產力套件中。**Copilot** 讓員工能更聰明地工作、自動化例行工作並產生洞察，同時尊重身分識別與資料保護原則。此方法能減少影子 IT，協助限制資料外洩，並賦予組織對 AI 使用方式的可見性與控制權。



這些能力並非孤立運作 — 它們相互強化，形成整合且多層次的防禦。身分識別、裝置與資料保護原則協同運作，協助您緩解威脅。當安全性團隊知道這些控管措施存在時，安全性能成為創新的推動者，而非阻礙。

Microsoft 365 E3 賦予您建立適當防護機制的 ability，讓您的組織能在不犧牲安全性的前提下，運用 AI 進行創新。



繼續您的 AI 採用旅程

每個組織都在探索如何讓 AI 最有效地協助實現其目標。這個承諾很吸引人，但 AI 的採用必須與強而有力的防護並行。使用 Microsoft 365 E3 時，您不必非此即彼。您將獲得一套強大的解決方案，提升您的安全性與合規性態勢，讓您能自信地擁抱 AI。

評估您的 AI 安全性整備度。



Microsoft 提供 **AI 安全性評定**³。這項[線上評估](https://security-for-ai-assessment.microsoft.com) (位於 security-for-ai-assessment.microsoft.com) 會根據您提供的資訊，提出提升 AI 安全性的建議。它可協助您根據四大關鍵支柱：**準備、發現、保護和控管**，評估您目前的 AI 安全性，並提供可行的建議。

深入了解並與 Microsoft 互動。



深入了解 Microsoft 365 E3 的功能，以及它們如何協助您自信地採用 AI。
www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab
您也可以聯繫您的 Microsoft 帳戶團隊或合作夥伴。

1. [2025 年工作趨勢指數年度報告：《前沿公司誕生之年》](#)，Microsoft, Inc.，2025 年 4 月。Microsoft 分析了來自 31 個國家、31,000 名全職受僱或自僱知識工作者的問卷調查資料。涵蓋 31 個國家的 31,000 名全職受僱或自僱知識工作者 (調查期間為 2025 年 2 月 6 日至 2025 年 3 月 24 日)、LinkedIn 勞動市場趨勢，以及數兆筆 Microsoft 365 生產力訊號。

2. [第二屆年度生成式 AI 研究：商業回報與安全性風險](#) — iSMG, Inc.，2025 年 2 月，根據對 360 多位商業及資安專業人士的調查，於 2024 年第三季進行。

3. AI 安全性評定：security-for-ai-assessment.microsoft.com/ 結果的準確性取決於輸入資料的準確性。本報告僅供參考且不保證績效或結果。這不應被視為 Microsoft 的承諾。實際結果可能因地點、購買方式及使用情況而異。Microsoft 對本報告或網站內容不作明示或默示擔保。

4. 所呈現的情境為虛構，僅供說明用途。

