Microsoft Azure

生成式 AI

建置您自己的 AI 應用程式指南

目錄

前言

執行摘要

生成式 AI 正在改變組織以及推動組織的人。它讓軟體更直觀且更有幫助，而提高員工工作效率和使用者滿意度。同時，生成式 AI 也帶來了一組新的挑戰和風險。

本電子書深入探究那些想要使用基礎和生成式 AI 模型建置自己的 AI 應用程式，或是想要將生成式 AI 加入其現有應用程式的人在策略上的考量事項。內容涵蓋生成式 AI 的詳細資訊，提供專為 ITDM 量身打造的指引，說明如何利用這項技術來滿足特定業務需求並達到競爭優勢。

目標讀者

本電子書是專為 IT 決策者 (ITDM) 所設計，例如在各種規模的公司 (包括獨立軟體廠商 (ISV)) 對使用基礎模型建置 AI 應用程式有興趣的技術長 (CTO) 或資訊長 (CIO)。

本電子書的閱讀時間大約為 **30-45 分鐘**。

本電子書中涵蓋的重要主題包括：

1. 了解生成式 AI

將生成式 AI 與傳統軟體方法區別，突顯其在預定輸出之外建立動態和情境相關的回應的能力。

2. 建置生成式的 AI 團隊

詳述生成式 AI 開發團隊的角色，以最佳化部署流程。

3. 利用負責任 AI 做法進行開發

了解緩解風險和支援 AI 安全、品質和合規性的工具和最佳做法。

4. 利用全方位的 AI 開發平台

選擇符合特定商務目標之生成式 AI 平台和工具的指導方針。這包括了解 **Azure AI Foundry**，這是開發、部署和管理生成式 AI 應用程式的重要工具。該平台透過模型選擇、資料整合和大規模企業級正式環境的進階工具，支援整個 AI 生命週期。

本電子書可做為導覽指南，以掌握生成式 AI 和促進可推動效率和創新的明智決策。

透過以下內容學習生成式 AI 的基礎知識
Microsoft Azure AI 基礎知識：生成式 AI。

自訂機器學習 (ML) 模型與生成式 AI 模型之間有何差別？

自訂 ML 模型

→ 專為特定用途而建

→ 您可能是模型建置者

→ 根據預先存在的資料 (過去的結果) 對未來的結果做出預測非常有幫助

生成式 AI 模型

→ 建置為「一般用途」

→ 您可能不是模型建置者

→ 當您想要從預先存在的資料中建立類似/模仿模式的新內容或資料時非常有幫助

Microsoft 提供各種課程，旨在協助資料和開發專業人員精進他們的 AI 技能。

這些課程可在我們的 AI 學習中樞找到。

比較方法：生成式 AI 支援的軟體開發與標準軟體開發的比較

相較於標準軟體開發，將生成式 AI 整合到應用程式中，在三大方面有所不同。

1. 所有權和資料控制

標準軟體開發：

在標準軟體開發中，資料控制和擁有權已清楚定義。開發人員對其資料保持完整控制權，這些資料仍然保留在自己的資料資產中。此擁有權提供直接的管理並遵守資料法規，確保安全性和隱私權，而無須涉及第三方。

生成式 AI 開發：

另一方面，生成式 AI 開發涉及較少的資料控制，因為它通常需要在自己資料資產之外傳送資料，以便與 AI 模型互動。這可能會引發安全性和法規顧慮。雖然資料仍然合法屬於開發人員，但相依於由第三方管理的外部 AI 模型和服務，在確保資料隱私權和合規性方面帶來了複雜性。

Microsoft Azure 安全性

監管行業仍然需要向風險管理和監管機構展示資料在整個開發過程中仍然保持私密。正因如此，在選擇大規模負責開發和部署生成式 AI 應用程式的平台時，安全性和合規性才如此重要。

透過 Microsoft Azure 安全性，在實體資料中心、基礎結構和作業之間獲得多層安全性。Azure 雲端是使用自訂硬體建置而成，包括整合的安全性控制及韌體元件，以及附加的防護功能來抵禦分散式拒絕服務 (DDoS) 攻擊等威脅。

了解更多有關 Azure 安全性的資訊。

2. 開發過程和問題處理

標準軟體開發：

開發人員撰寫明確的指示以解決明確的問題，從而導致可預測的一致輸出。

生成式 AI 開發：

相較之下，生成式 AI 以機率性原則操作，使用模式和背景資料來產生輸出，在相同輸入下可能有不同的輸出。這種不確定性使開發過程更為複雜，也較不可預測。它需要廣泛的測試和反覆運算，才能達到正式環境就緒的狀態。輸出的變化性往往需要特定領域專家大量參與，評估 AI 回應的相關性和準確性。

3. 評估

標準軟體開發：

開發人員使用單元測試來確定應用程式是否傳回正確的答案並如預期運作。

生成式 AI 開發：

生成式 AI 需要領域主題專家 (SME) 更深入地持續參與整個開發過程，考慮到如果多個答案輸出全都是正確答案，需要進行評估。

這些專家不僅有助於定義應用程式的範圍和規格，而且在持續評估 AI 產生的輸出以取得諸如準確性和相關性等計量方面也發揮了舉足輕重的作用。此過程的反覆性質，以及需要頻繁評估和調整，突顯了人為監督開發過程的重要性。

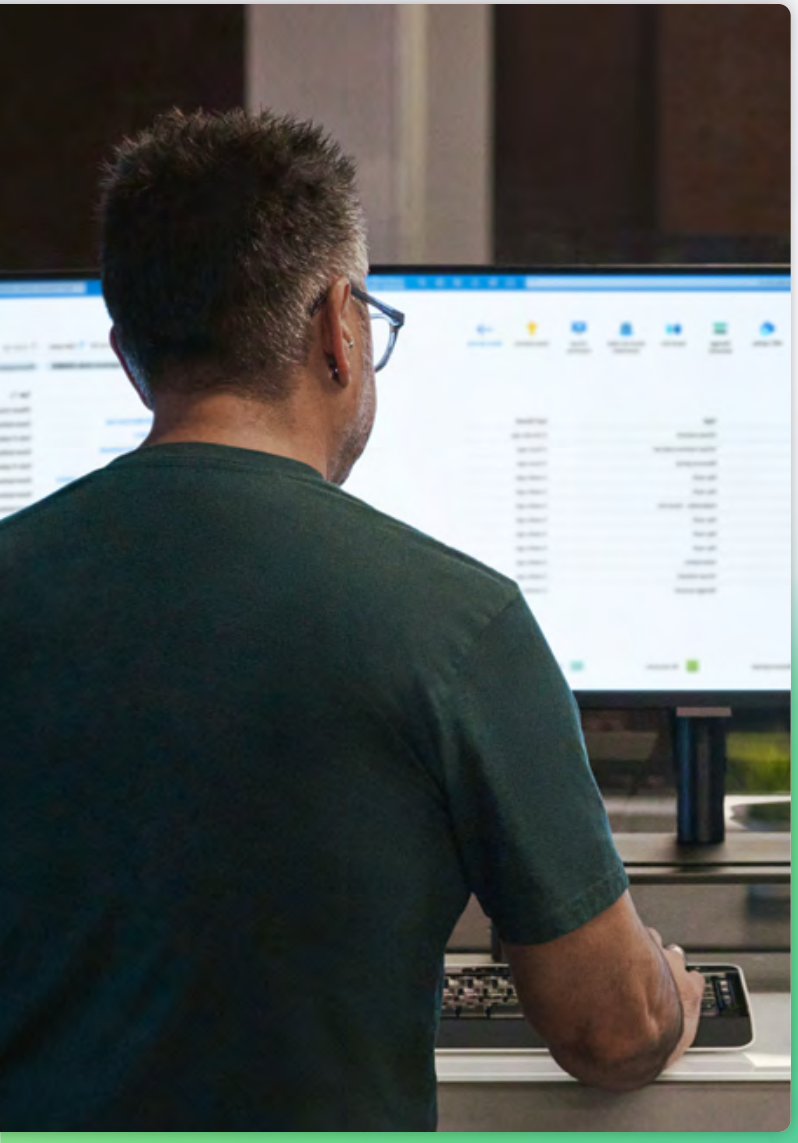
評估應用程式的其中一個方法，是由人類專家針對各個答案評分。不過，這很耗時、容易出錯，而且在大規模或正式環境中持續監視應用程式並不可行。

為了協助加快和修復此程序，Microsoft 研究人員正在開發工具，使用模型來評估其他模型的輸出，以自動化評估。

即使在這項自動化評估中，仍然需要人類專家來提供一些基本事實的答案，而這可能需要投入大量時間。

使用生成式 AI 建置的五種常見應用程式

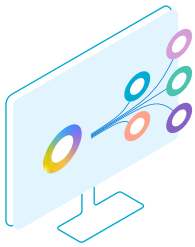
您可以從頭開始開發支援生成式 AI 的應用程式，但通常更快獲得生成式 AI 好處的方法，是將其整合到現有的應用程式中。這允許使用者以全新、更直觀的方式與應用程式互動、將協助情境化，並提供更相關的資訊。生成式 AI 也因此能橫跨整個價值鏈 (從客戶接觸到財務和營運分析) 改進應用程式。



以下是組織使用生成式 AI 所建置的五種應用程式類型。它們結合了直覺式介面、專屬知識庫的連結和企業系統：

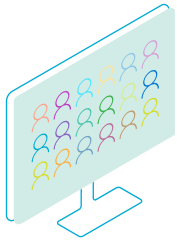
與您自己的資料聊天

許多組織在文件和網站上擁有大量專有知識。為發掘當中的價值，他們正在開發聊天應用程式，允許員工和客戶以簡單的語言查詢此資料，並得到直接的答案，而不只是來源文件的連結。生成式 AI 工具應配備內建的負責任 AI 功能，確保回應僅從內部資料衍生，以防品牌外的體驗以及透過不信任的資料來源而暴露於惡意程式碼中。如此一來，資訊就能保持安全並符合公司標準。



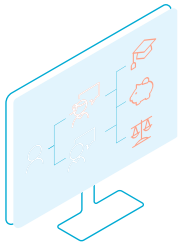
建立個人化的 AI 代理程式

軟體開發人員使用生成式 AI 將進階協助程式整合到他們的系統中，旨在減少重複性工作的單一性，並將阻礙專業注意力的干擾降至最低。這些 AI 代理程式可提供更完善的相關情境支援，針對要求者的身分識別及其查詢背景自動草擬回應，並編譯綜合的每日或每週摘要，詳述各項活動和狀態。此自動化可協助專業人員維持工作效率，而不犧牲準確性或細節。



添加超個人化

大規模為個別使用者量身打造互動。超個人化可以包括從自訂行銷訊息和根據使用者動作即時調整網站介面，到個人化產品建議，以及提高客戶參與度和滿意度。



建立客戶服務虛擬人偶

生成式 AI 和語音 AI 允許企業建立精密、多語言的品牌大使虛擬人偶，以品牌的外觀和腔調透過網站、資訊亭或智慧型手機與大眾互動。早期版本只提供了一般資訊，虛擬人偶現在則能夠進一步強化與商務系統的互動，提供特定資訊、提出明智的建議、檢查庫存，以及將品項加入電子商務購物車，使它們成為創造高價值品牌體驗一種令人興奮的新方式。

獲取見解

當重要資訊四散於不相容的系統時，分析師光是為例行報告 (例如季末績效和前景概況) 彙整資料就可能花上好幾個小時的時間。有了新的代理架構，組織現在使用生成式 AI 從多個系統提取資訊、以標準視覺效果彙整資訊，並草擬描述。由於電腦已經完成了死板的工作，如此可讓分析師將時間花在建立和增加價值上。

針對使用案例選擇合適的模型

生成式 AI 模型的數量和多樣性正在快速成長，而對可能的使用者造成混淆。以下是為應用程式選擇合適模型的一些考量事項：

模型能力

評估模型的計算能力與複雜度。這可確定其處理複雜資料集和產生細微輸出的能力。複雜工作可能需要更高的能力，而影響營運需求和相關成本。

時間效率/延遲

模型的速度至關重要，尤其是對於需要快速處理資料或立即做出決策的工作。效率不僅影響效能，也影響使用者滿意度和操作效率。

符合成本效益

分析所有相關聯的成本，包括初始設定、持續作業和維護。在模型的能力與預算之間取得平衡非常重要。

小型語言模型 (SLM)

SLM 可使用較少的參數和較少的資料量進行訓練， 您可以獲得模型的好處，該模型可以在有限的運算資源下運作，同時提高特定性。SLM 可以在本機執行 (對於受監管行業還有在延遲時間非常重要的情況中是一項優勢)，而且可以針對特定工作進行微調，並配合狹窄範圍。對於想要完成特定工作的特定行業，這可以是絕佳的選擇。例如，金融服務組織在處理索賠但希望確定要使用的確切訓練時，可以受益於 SLM。

了解更多有關 Microsoft 在 SLM 的最新進展。

微調性和擴充性

考慮針對特定資料調整模型的能力，因為對於模型和預期目的所需的擴充性和修改，這一點可能非常重要。然而，如果您的使用案例需要處理權重，則選擇開放模型比較合適。請記住，並非所有開放模型都具有許可的授權來建置商業應用程式。

LLM 授權與可用性

若要將 LLM 用於商業目的，請考慮特定模型的授權。請記住，可用性不一定都很直接了當，因為某些模型是封閉來源。

另一個可用性考量是，模型依賴於資料中心，而且不是所有模型都能在所有資料中心使用，因此在資料跨越某些邊界的限制方面帶來了挑戰。

一般性與特異性

根據您的需求廣度或特定性，在一般用途和專門模型間選擇。一般模型提供彈性，而專門模型則在特定情境中提供高效性。例如，某些模型擅長於特定工作 (像是聊天完成或摘要)，或是專為特定資料類型 (如程式碼、影像、視訊或文字) 或特定行業 (如醫療保健) 建置。

Microsoft 的生成式 AI 評估與監視計量

自動化輸出評估的計量

為了大規模進行評估，Microsoft 正在開發工具，讓 LLM 評估生成式 AI 應用程式的輸出。

論據性

以 Azure AI 內容安全為基礎的論據性

根據模型所產生的答案與來源資料資訊 (例如，在 RAG 中擷取的文件、問答或用於摘要的文件) 的一致性進行評估。評估程序會標記缺乏論據的輸出。

僅以提示為基礎的論據性

衡量模型產生的答案與來源資料資訊 (使用者定義的內容) 的符合程度。

相關性

模型產生的反應與指定問題相關且直接相關的程度。

連貫性

語言模型產生流暢、自然、類似人類語言的輸出能力。

流暢度

答案撰寫得多好以及容易理解的程度。

GPT 相似性

答案與使用者提供的基本事實有多接近，而且只有當您已提供基本事實並且使用生成式 AI 模型進行比較時才適用。

納入這些考量後，組織可以更有效地將生成式 AI 功能與策略目標保持一致。選擇和管理生成式 AI 所需的細微方法突顯了專家參與和反覆測試的重要性，確保技術不僅執行良好，而且可無縫整合到組織流程，以滿足業務需求。

關於領域 SME 和其他團隊成員角色的進一步詳細資料將在本電子書的稍後部分探討，對生成式 AI 開發之間的協作和動態特性提供更深入的見解。

建置生成式 AI 開發團隊

使用生成式 AI 進行開發需要混合方法，即標準軟體開發混合 AI 專業知識。已經出現像 AI 工程師這樣的角色，提供軟體開發與 AI 之間的這項關聯。

同時，技術和業務團隊之間也有合作關係，商務需求可推動開發。非技術企業領導者和其他關係人在確定 AI 應用程式的效用和可信度方面發揮著關鍵的作用。他們的決策對於決定是否繼續使用和投資 AI 系統至關重要。

準備您的資料進行生成式 AI 開發

組織可以有效地為生成式 AI 專案做好準備，確保資料已準備就緒。生成式 AI 乃基於資料執行，因此必須確保其品質，以便輸出更準確。

準備相關資料

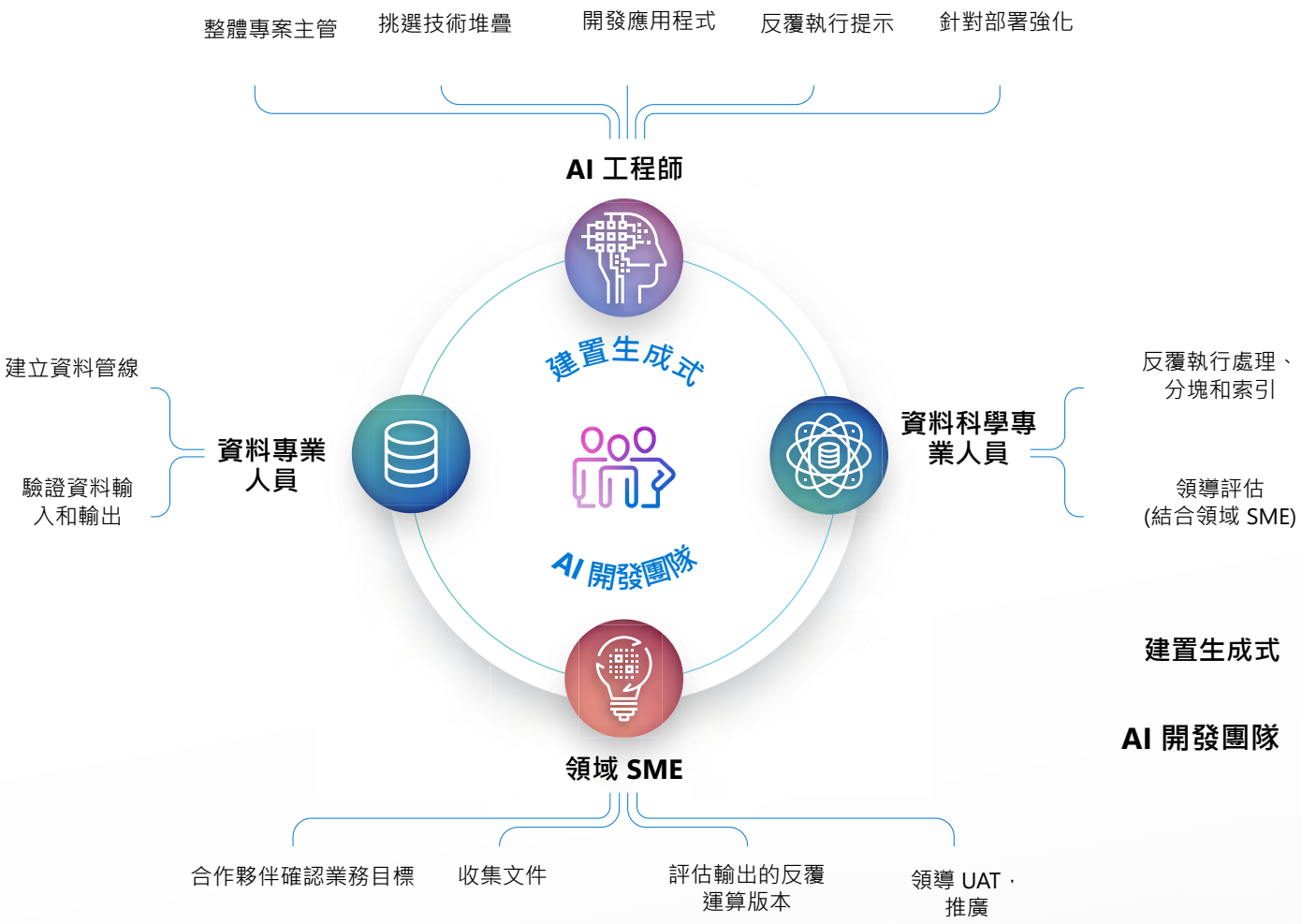
您的組織需要健全的資料基礎結構來處理大量資料和高效能的運算工作。資料必須方便存取、組織良好且安全，以促進有效的 AI 訓練和作業。

確保資料品質

清理和準備您的資料，以確保資料可信賴並適合預建的基礎模型。除了清理資料之外，也考慮資料是否正規化，以及是否消除偏差。品質至關重要，因為它會影響 AI 模型結果的精確性與可靠性。

建置生成式 AI 開發團隊

從下面的視覺效果中，我們看到 AI 工程師帶領開發團隊，而對於領域 SME 來說，可能需要投入更多時間。



AI 工程師

AI 工程師通常是核心，協調開發計劃。他們通常是經過非正式訓練以在團隊中擔任此角色的軟體開發人員。因此，AI 工程師承擔領導者和整合者雙重角色，搭起 AI 能力和業務需求之間的橋樑，而不需要深入研究資料科學 (通常是由資料科學專業人員處理)。AI 工程師也會從領域 SME 獲得資訊，並依據其測試來調整應用程式。

AI 工程師學習資源

正在尋找特定的 AI 工程師教育資源嗎？開始著手：

→ **AI 工程師認證途徑**

→ **Azure AI 基礎知識**

→ **Azure AI Foundry 簡介**

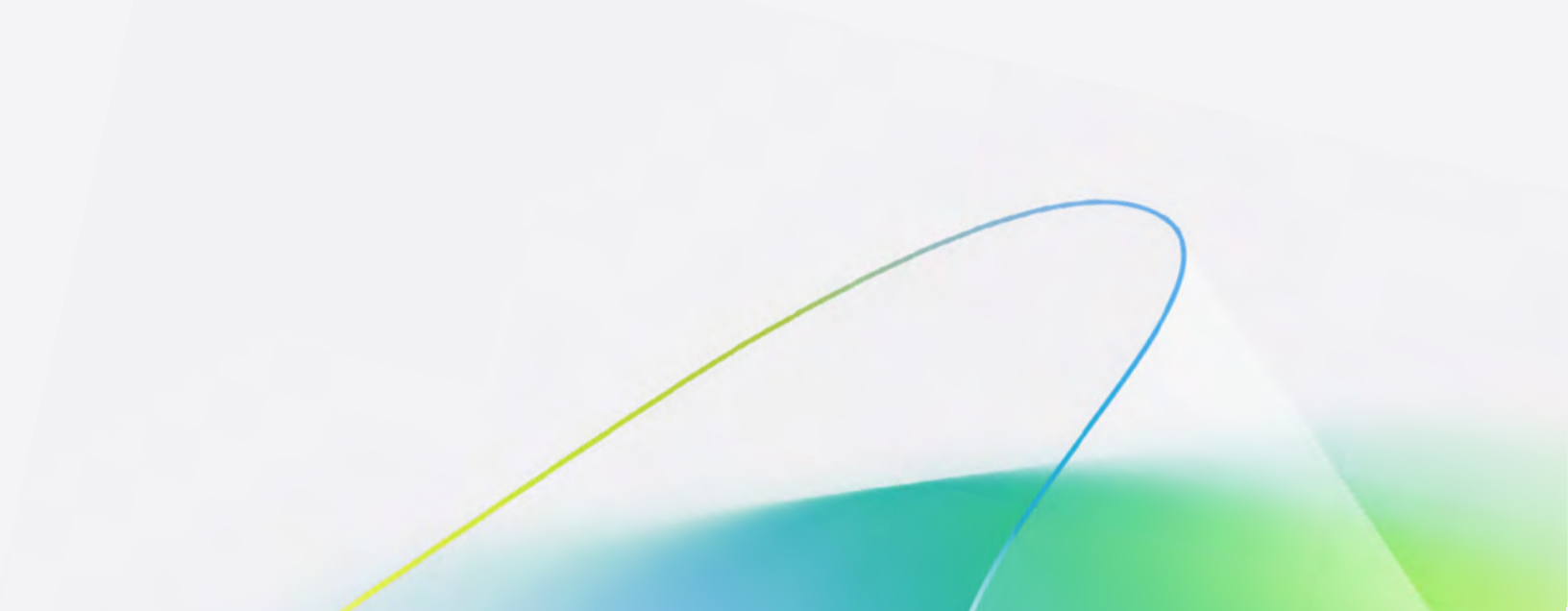
資料專業人員

使用生成式 AI 進行建置的關鍵元件，是從商務系統提取資料，並把它帶到模型。資料專業人員是建置管線並使一切以安全且有效率的方式進行的人。因此，在資料來源的細微變化方面具備專業知識對於建立高品質的生成式 AI 應用程式至關重要。資料專業人員也必須掌握複雜的資料隱私權法規，以確保所有資料收集和使用都符合法律標準。

領域 SME

領域主題專家 (SME) 與 AI 工程師密切合作，以確保準確收集資料。他們也會持續監控 AI 工程師設定的關鍵效能計量。與在標準軟體或機器學習中相比，領域 SME 在生成式 AI 開發中扮演的角色通常更重大，因為系統輸出不容易驗證。

領域 SME 承擔評估回應正確性的角色，這可能很耗時。他們的角色在銜接 AI 實作的技術和業務層面方面起著舉足輕重的作用。為了簡化其輸入，領域 SME 可以與其餘的團隊合作，建立測試提示並找出基本事實的解答。AI 工程師隨後可以使用 Microsoft 自動化評估計量來評估應用程式隨著時間的回應品質，並比較不同模型之間的績效。



資料科學家/機器學習 專業人員

並非每個生成式 AI 團隊都有資料科學家，但他們經常出現在複雜且業務關鍵的專案上。資料科學家扮演諮詢角色，負責制定正式的測試計劃和設定評估標準，以減輕部分領域 SME 的工作量。

常見的方法是檢索增強產生 (RAG)，這會將模型的推理功能與自訂資料相結合以產生回應。這包括測試各種文件分塊和註釋技術、評估檢索品質，以及跨不同提示來評估回應。

正在尋找特定的 AI 資料科學教育資源嗎？

開始著手：

→ Microsoft 認證：Azure 資料科學家助理

組織對生成式 AI 的需求不斷增加，對集中式平台以負責任的方式開發和部署這些應用程式的需求也隨之增加。這突顯了資料科學專業人員在確保以合乎道德的方式有效實施這些技術方面所扮演的角色日益重大。

Azure AI Foundry：全面性的平台

組織需要可簡化 AI 開發的工具，讓他們有更多的時間專注於大範圍的業務需求。**Azure AI Foundry** 是 Microsoft 的生成式 AI 平台，專為開發人員將 AI 開發過程民主化而設計，該平台將所需的模型、工具、服務和整合匯集在一起，開始快速且有效地開發您自己的 AI 應用程式。

87%
的組織認為 AI 將給予他們競爭優勢[1]

66%
的受訪董事表示承受加速 AI 採用的壓力[2]

中國 McDonald 利用 Azure AI 實現營運轉型、提升服務水準

他們目標為何？

中國 McDonald 需要提升他們的客戶服務、品質和營運，以配合越來越多的地點和創新的快速發展。他們需要一種方法透過擴大的數位轉型來堅持自己的品牌使命。

他們如何辦到？

在 Microsoft 支援下，中國 McDonald 設立了 AI 實驗室，允許他們預先利用大型語言模型 (LLM) 將 AI 整合到現有的作業中。

透過 AI 實驗室，AI 已經滲透到他們的整個營運，從供應鏈營運到甚至支援行銷活動，因為它會影響 AI 模型結果的精確性與可靠性。

了解更多 >

[1] Expanding AI's Impact With Organizational Learning
[2] CEO decision-making in the age of AI

Azure AI Foundry 做為開發及部署生成式 AI 應用程式的全方位平台，已成為顛覆傳統的工具，適合經驗豐富的開發人員和 AI 新手。Azure AI Foundry 具有拖曳功能、視覺化程式設計環境和預建範本，讓使用者更輕鬆地建立原型、建置和最佳化 AI 應用程式，而無需深入了解基礎演算法。

此協助工具可加速開發過程，並幫助使用者快速將其創意和商業構想轉化為完全可操作的 AI 解決方案。

Siemens 和 Microsoft 合作夥伴推動跨產業採用 AI

他們目標為何？

多國技術企業集團 Siemens需要簡化設計工程師、前線工作人員和其他團隊跨關鍵業務職能的虛擬協作。他們希望利用生成式 AI 快速產生、最佳化和偵錯複雜的自動化程式碼。

他們如何辦到？

Siemens 引進 AI 支援的助理 Siemens Industrial Copilot 後，促進了人機協作並提高了工作效率。它們也大幅縮短了模擬時間，將工作時間從數週縮短為數分鐘。維修人員現在可以使用自然語言的強大功能，獲得詳細維修指示的協助，並讓工程師能夠快速存取模擬工具。

了解更多 >

Azure AI Foundry 為使用者提供實質價值的主要功能包括：

負責任的 AI 工具和最佳做法：

Azure AI Foundry 讓開發人員能夠安全、可靠、負責任地利用 AI 進行創新和塑造未來。該全方位平台可加速開發環境就緒的代理程式，以支援企業聊天、資源開發、資料分析等。開發人員使用其受保護的資料，以協作、負責任 AI 工具和最佳做法建置自訂模型和解決方案。

API 和模型選擇：

使用者可以 API 的形式存取和部署最新模型，促進快速、無伺服器和微調的模型部署。這可以減少開發時間和資源成本，為開發人員加快上市時間，並快速為終端使用者提供最先進的 AI 功能。Assistants API 讓開發人員透過精密、類似專員的體驗來篩選資料、建議解決方案，以及使用程式碼等進階工具，將工作自動化，更輕鬆地建立自動化應用程式。

完整的 AI 工具鏈：

Azure AI Foundry 提供根據特定資料建立模型的工具，協調複雜的 AI 工作流程，並評估模型輸出的品質和安全性，確保健全的端對端管理。開發人員會發現整合和管理 AI 專案更加容易，從而提高工作效率和操作效率，同時使用者也會體驗到更可靠且更有效的 AI 應用程式。

企業級正式環境：

該平台可促進模型、流程和應用程式的可擴展部署，在安全和受治理的環境中納入持續監視和微調功能。組織可以根據需要擴展其 AI 解決方案，而不會影響安全性或效能，為開發人員提供靈活、健全的基礎結構，並確保使用者享有一致、可靠的 AI 服務。

Azure AI Foundry 平台的集中化特性提供了一個協作式開發環境，因此生成式 AI 團隊可以有效率地協同合作並保持同步。Azure AI Foundry 利用預建功能和範本，協助使用者更快地建置 AI 解決方案，終而加速解決方案開發。

透過 Azure AI Foundry 部署負責任 AI

負責任生成式 AI 是指以安全、透明和負責的方式開發和部署生成式 AI 系統。Microsoft 提供許多工具和控制項，可協助以負責任的方式部署生成式 AI。

Azure AI 服務：開發人員可以利用預建和可自訂的 API 和模型，快速建立尖端、負責的應用程式。這些服務提供詳細的透明度協助和公平性評估，例如臉部和語音，以支援客戶選擇和透明度。

負責任地使用 AI 與 Azure AI 服務

Azure AI 內容安全：開發人員可以獲得支援來偵測及減緩風險性內容，包括提示攻擊，以及產生無依據或著作權材料。開發人員可以將 Azure AI 內容安全用作為內建的安全性系統，建造更值得信賴的應用程式。

利用 Azure AI 內容安全負責任地建置 AI 應用程式

ASOS 使用 Azure AI Foundry 驚豔年輕時尚迷

他們目標為何？

隨著生成式 AI 平台的盛行，一家英國時尚和化妝品零售商 ASOS 看到了擴展其商業模式、豐富其技術基礎結構以及滿足顧客現代技術期望的機會。

他們如何辦到？

ASOS 使用 Azure OpenAI Service 和提示流程 (Azure AI Foundry 的一部分) 快速簡化其開發和測試週期，協助顧客和解決方案有效地互動。ASOS 利用內建的提示流資源幫助開發人員快速上線，從而限制對自訂程式碼的需要。

了解更多 ›

Azure AI Foundry 中的評估和監視：除了減輕有問題的輸入和輸出之外，開發人員還可以使用針對風險和安全性預建的評估和監視計量，在開發和正式環境中持續測量其緩解措施的有效性。在資料和使用者行為隨著時間而改變時，這些測量工具可協助開發人員和領域 SME 了解其應用程式的行為，並迅速在效能下降或終端使用者嘗試以超出規定的目的操作應用程式時介入。

生成式 AI 的評估與監視計量

安全性：Microsoft 使用內建的安全性控制和獨特的威脅情報，提供應用程式的多層安全性骨幹，協助識別並抵禦不斷演進的威脅。

Microsoft 安全性的一個焦點是適用於雲端的 Microsoft Defender (Microsoft 的雲端原生應用程式保護平台 (CNAPP))，該平台提供全方位的安全性，可主動緩和風險，並找出 AI 應用程式從程式碼到雲端的威脅。

了解更多有關**適用於雲端的 Microsoft Defender 的資訊**

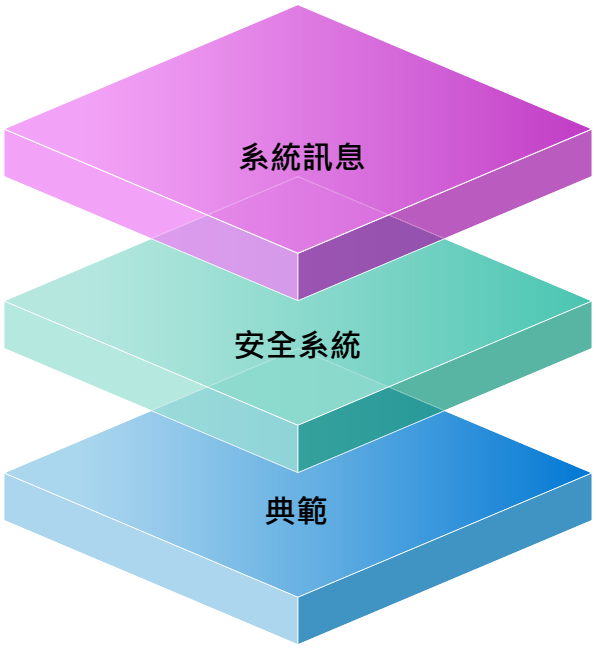
Azure AI Foundry 中的緩解措施層

使用分層式緩解計劃可協助開發人員在開發過程早期識別和修復潛在風險。以下是 Azure AI Foundry 穩健的安全機制的簡短概觀，其設計旨在保護及最佳化您的生成式 AI 部署：

系統訊息層：此層會以每個使用者提示，為模型提供隱藏的指示，讓您因而能夠引導模型的行為及擷取資料，以預設方式產生更高品質的回應。

安全系統層：此附加層超越屬於模型一部分的基本安全微調。Azure AI 內容安全透過分類模型執行提示和模型的完成，來提供這個附加層。這些模型旨在偵測並防止各種分類和嚴重性層級的有害內容輸出。

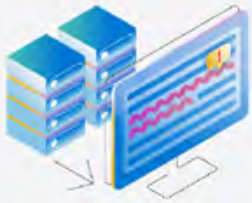
模型層：您可以使用 Azure AI Foundry 的模型目錄，探索 Azure OpenAI Service、Meta、Hugging Face 和其他模型開發人員的基準和模型卡，全都按集合和工作組織而成。



Azure AI Foundry 中的安全功能重點

Azure AI 內容篩選器

Prompt Shields：
偵測並封鎖提示注入攻擊，包括直接和間接提示攻擊。



Groundedness 偵測：
偵測模型輸出中的「幻覺」，提高 AI 產生之內容的準確性和可靠性。

可設定的有害內容篩選器：
分別以四種嚴重性等級 (安全、低、中、高) 來偵測四種類別的有害內容 (暴力、仇恨、性和自殘)，以及選擇性二進位分類器來偵測公用存放庫中的越獄風險、現有文字和程式碼。

安全系統訊息：使用 Microsoft Research 開發的系統訊息範本，引導模型的行為走向安全、負責任輸出。

安全評估：使用您自己的測試資料集或 AI 協助產生的測試資料集，評估應用程式易受越獄攻擊的漏洞和內容風險。

風險和安全性監視：了解哪些模型輸入、輸出和終端使用者正在觸發內容篩選器以訂定明智的緩解措施。

→ **系統訊息和基礎層：**這是檢索增強產生 (RAG) 的一部分。不將該模型用作為資訊來源，而是做為與查詢相關之資料來源的推理引擎。系統訊息有助於引導模型有效地使用基礎資料，並有助於引導整體行為，實現更可預測、負責的模型輸出。

→ **使用者體驗層：**在這個層級，有一系列以使用者為中心的介入、指引和最佳做法可以提供給使用者，以確保系統如預期般使用。

Azure AI Foundry 安全性功能的這些改進展示了 Microsoft 對於負責任 AI 的承諾，確保您的應用程式不僅有效，而且符合資料完整性和安全性的最高標準。

閱讀詳情：使用 Azure AI 的危害緩解策略

負責任 AI 的另一個關鍵元件是應用程式的評估和監視。我們討論了 Azure AI Foundry 提供產生品質計量的功能，但有三個涵蓋一切的主題需要考慮：

手動評估：

這是我們建議在移向自動評估之前先進行的評估形式。對於追蹤一小組優先問題的進度，這可說是一種實用的方法。

自動化評估：

另一方面，自動化評估對於大規模測量品質和安全性可能更有用，並可以取得更全面的結果。

監視：

部署在正式環境中的監視模型是生成式 AI 應用程式生命週期不可或缺的一部分。資料和消費者行為的變化可能會隨著時間改變您的應用程式效能。Azure AI Foundry 可方便您監視正式環境中的應用程式，確保持續的安全和品質。

了解更多：**生成式 AI 應用程式的評估**

開拓 AI 答案引擎 Perplexity。透過 Azure AI Foundry，AI 使輸送量加倍，並削減成本

他們目標為何？

初創公司 **Perplexity.AI** 是 Perplexity Ask 的創造者，這是一個以 AI 為基礎的革命性對話式答案引擎，它結合了大型語言模型和健全的語意搜尋引擎。為了進一步支援 Perplexity Ask，他們需要一個平台來支援更快的上市時間、為精簡員工倍增力量、擴展以支援數百萬使用者，以及以符合成本效益的價格提供安全性和可靠性。

他們如何辦到？

Perplexity.AI 使用 Azure AI Foundry，在幾個小時內開發出第一個原型。他們得以試用 Azure OpenAI Service 提供的大型語言模型，「按幾個按鍵」就能上手。整體上，這讓他們在 Azure 採用之前，並行執行兩倍之多的實驗，而能以加倍的速度重新訓練模型的新版本。

了解更多 >

整合的資料安全性和隱私權

為了確保資料安全性和隱私權，Microsoft 對客戶做出了幾項承諾。首先，Microsoft Azure 建基於安全性、隱私權、合規性。當資料儲存在 Azure 中時，您的資料仍然是您的，未經您許可，永遠不用於行銷、廣告或基礎模型訓練目的。提示和完成仍然是您的資料。

Microsoft Fabric 是 Microsoft 的整合式 AI 支援的分析平台，可協助重塑和改善存取、管理和操作資料的方式。在單一平台上，Fabric 整合資料和服務，將資料整合簡化成單一多雲端資料湖，供您的組織跨分析引擎和語言從相同資料工作。

針對與輸出內容相關的部分協力廠商智慧財產權索賠，Microsoft 有義務為客戶進行辯護。對於 Azure OpenAI Service 和任何可設定的生成式 AI 服務，客戶也必須在提供輸出內容 (索賠主體) 的供應項目中，實施 Azure OpenAI Service 文件所要求的所有緩解措施。

了解更多：推出 Microsoft Copilot 著作權承諾

此外，Azure AI Foundry 包含企業安全性設定，包括：

→ Azure 原則整合

→ 角色型存取控制 (RBAC)

→ 網路隔離和安全性

→ 資料保護和加密

→ 漏洞管理

為了在管理資料安全性和隱私權時，將這一切整合在一起，Fabric 與 Microsoft Purview 的原生整合可讓組織治理、保護及管理其整個資料資產的資料。當 Fabric 與 Purview 整合在一起時，可透過安全的資料整合來提升 AI 功能。

關鍵見解和後續步驟

隨著組織對生成式 AI 的需求增加，需要有一個集中式平台以負責且有效的方式開發和部署這些技術變得至關重要。

Azure AI Foundry 提供了一個健全的解決方案，提供的全方位平台可滿足各種程度的開發人員，包括不具資料科學專業知識的開發人員。此平台不僅提供領先提供者的完整模型目錄來簡化開發過程，還利用進階資料整合、工作流程協調流程及互動式應用程式工具支援 AI 開發的整個生命週期

開始使用 Azure AI Foundry →

- → Microsoft 認證：Azure AI 工程師助理
- → Microsoft 認證：Azure AI 基礎知識
- → 用於建置 RAG 應用程式的 GITHub 存放庫
- → Azure AI Foundry 模型目錄
- → Azure AI Foundry 概觀
- → Azure AI Foundry 簡介—訓練 | Microsoft Learn