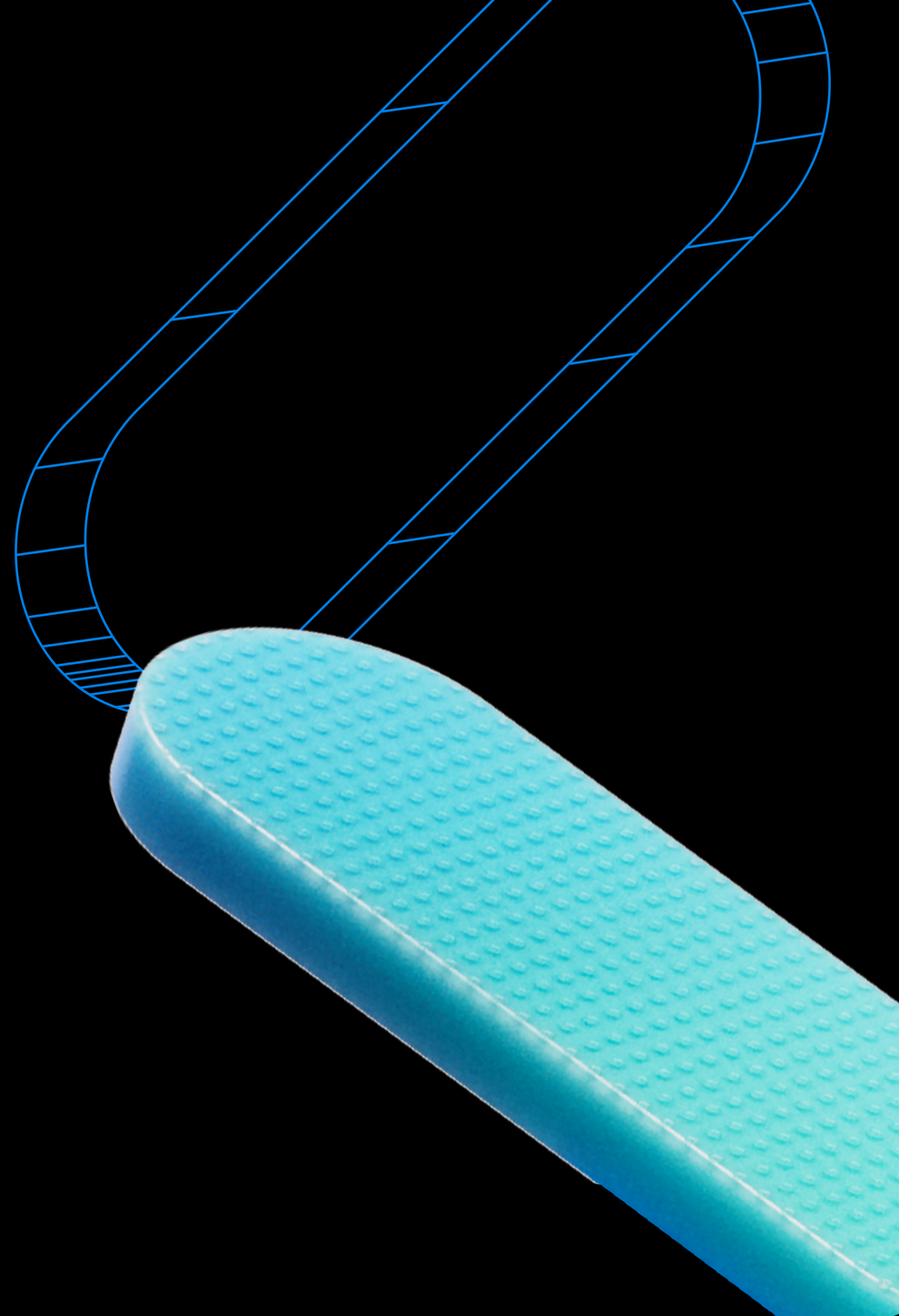
Microsoft Azure

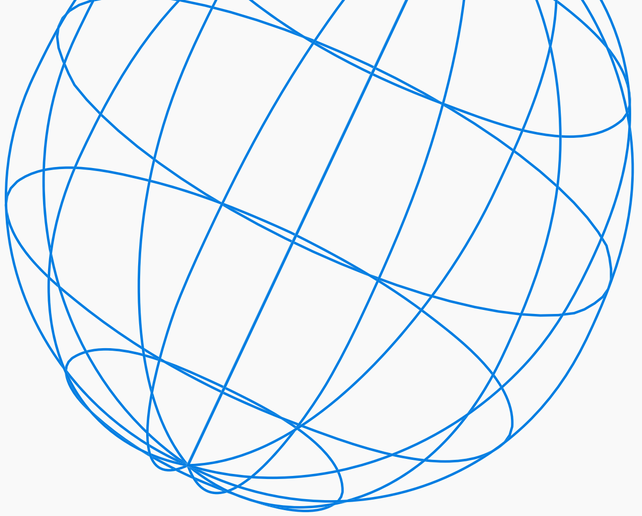
雲端與 AI 安全性的前 11 大要素

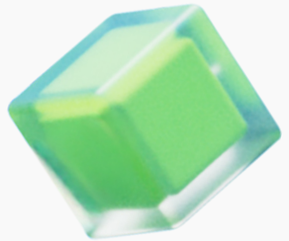
專為技術領導者設計的多層式安全性指南，
以及 Azure 如何一應俱全



前沿基礎

目錄





概觀

專為 AI 時代設計的雲端安全性

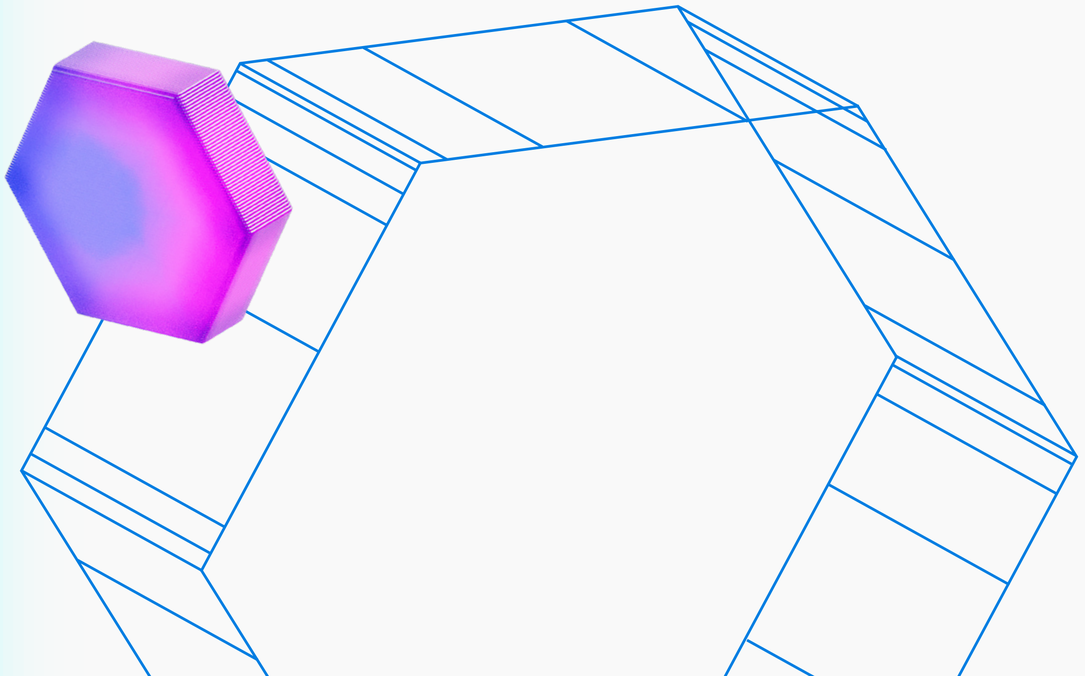
當您選擇信任雲端平台與服務時，您將受益於提供者內建的防護機制與韌性。您可以在此基礎上做出安全的選擇來保護您的應用程式、資料和身分識別，做為您與雲端提供者共同承擔責任的一部分。

Microsoft Azure 經過獨特設計，可保護您雲端堆疊的每一層，包括硬體、資料、程式碼及 AI 工作負載。保護您的應用程式、資料與身分識別，意味著遵循共同責任模式，同時享有內建的防護措施，涵蓋機密運算、威脅偵測、AI 治理及合規自動化。這種全面且安全的雲端運算方法在業界獨樹一幟，使 Azure 成為各種規模企業值得信賴的雲端。

本指南概述了與雲端提供者合作時最重要的安全性要素。您將了解為何業界領先的保護、治理與信任，使 Azure 成為您雲端工作負載的最佳平台。

第一要素

縱深防禦基礎結構安全性



運算、網路與資料平台在有內建的平台加密、隔離與區隔功能下，應該具備預設安全性。

要確保工作負載安全，必須在雲端基礎結構的每一層都內建安全性。Azure 建置於此縱深防禦模式的基礎上。保護層已到位，包括實體安全、網路區隔、身分識別管理、加密、監控及威脅偵測。即使其中一層被破壞，其他層仍會保護系統。例如：

- 運算服務可受益於 Hypervisor 層級的隔離、安全開機，以及作業系統強化。
- 內建的 DDoS 防護功能有助於保護所有 Azure 服務。
- 平台服務的網路邊界防禦屬於標準措施。
- 每種儲存體類型預設都會加密以保護資料機密。

縱深防禦已建構於您所使用的 Azure 資料服務、分析和應用平台中。此外，Azure 生態系統透過企業級安全性解決方案 (如適用於雲端的 Microsoft Defender) 擴展內建防護，用於態勢管理、威脅偵測與回應。

近期的進展，例如預測防護和快速攻擊阻斷，展現了 Azure 基礎結構安全性如何提供主動防護，協助您的組織事先掌握不斷演變的威脅。結果是為可調整、AI 就緒的應用程式和資料建立統一、受控管的基礎。

Microsoft 的嵌入式安全性與合規性

3.5 萬

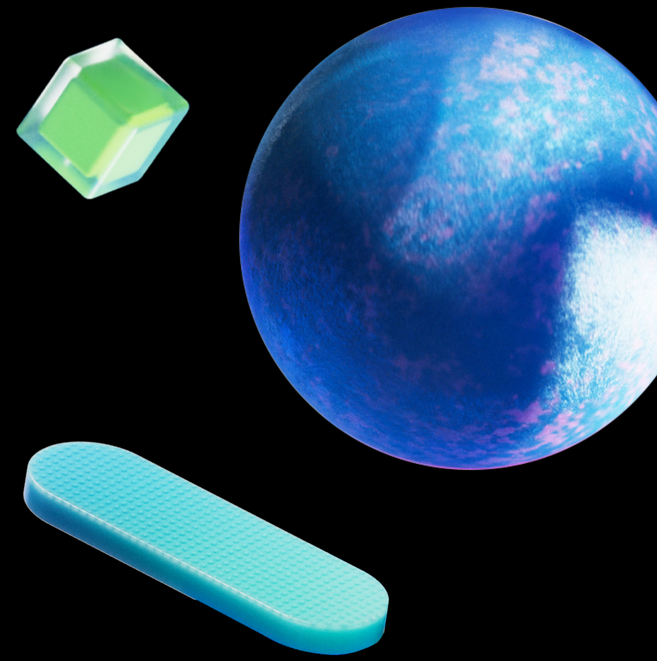
在 Microsoft 指派參與安全性計劃的全職工程師

1.5 萬

具備安全性專業知識的合作夥伴

100 多

合規性認證，包括超過 50 項針對全球地區與國家的認證



FDB Vela 透過 Azure 保障電子處方的安全，並針對 1,500% 的容量成長進行擴展

醫療科技創新者 FDB Vela 管理個人健康資訊，成為駭客的主要目標。為了強化其電子處方網路的安全性，該公司採用了 Azure。現在，它能夠符合嚴格的合規性和效能要求，同時擴展以處理每天 15,000 份處方，甚至每小時可多達 10,000 份處方。

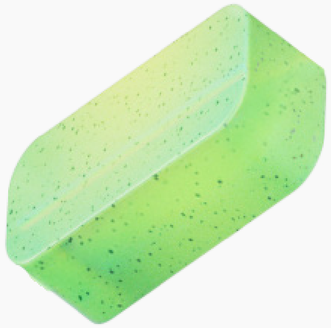
「我們決定採用 Azure，原因不僅是可擴縮性。這是為了找到一個雲端平台，能夠提供滿足我們隱私權需求和法規要求所需的安全性功能，並且還有我們可以信賴的客戶支援。」

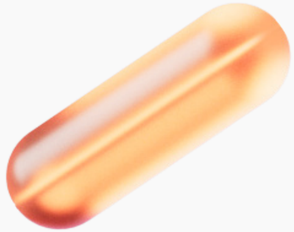
Sean Taylor，
FDB Vela 研發總監

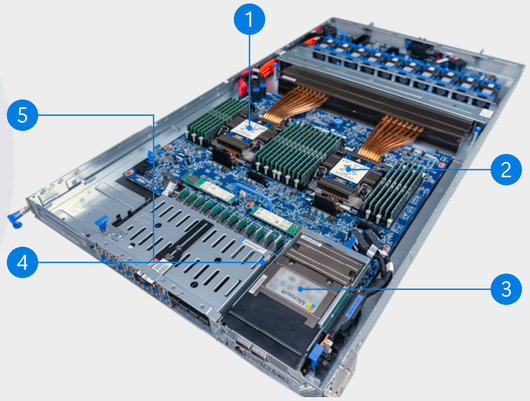
閱讀完整案例

第二要素

晶片信任根







硬體信任根是所有高階安全性控制的基礎。

以硬體為基礎的信任必須鞏固軟體防禦。即使是最優秀的程式碼，硬體漏洞也可能使其暴露於遭竄改的風險之中。雲端提供者必須能夠證明每台伺服器和晶片的真實性與完整性，並在沒有額外費用的情況下提供這項保證。

在 Azure 上，端對端的完整性與認證從晶片開始。Azure Boost 透過隔離虛擬機器 (VM) 硬體中的控制平面與資料平面來降低風險。

此外，Azure 整合 HSM 自訂安全性晶片在 Azure 伺服器中提供 FIPS 140-3 第三級加密金鑰保護，為信任與雲端韌性樹立新標竿。機密運算進一步透過以硬體為基礎的受信任執行環境 (TEE) 保護使用中的資料。

這些創新將硬體層級的保護從資料中心延伸到您的工作負載，無需您的團隊額外設定或操作。

信任根要點

1. **機密運算**將信任根延伸至資料使用期間。
2. **Caliptra** 將開放原始碼信任根嵌入晶片中。
3. **Azure Boost** 及其資料處理單元 (DPU) 可大規模提供節能的效能，現已可搭配第 7 系列 Azure 虛擬機器使用。
4. **Datacenter Secure Control Module (DC-SCM)** 整合了安全管理控制器與平台信任根。
5. **Azure 整合式 HSM** 的加密金鑰保護為敏感資料與合規性需求提供卓越的保障，且不增加額外複雜度。

第三要素

在安全且可交互操作的平台上打造 AI

AI Agent 和工作負載需要內建的可檢視性、防護措施與安全性，以實現跨環境一致的機群管理。

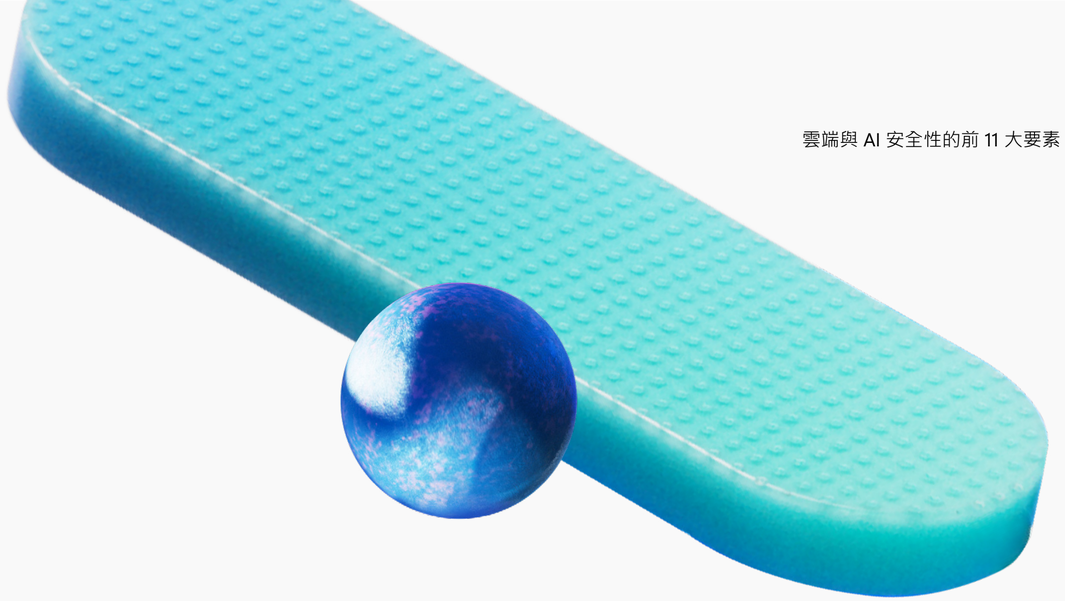
隨著 AI 的採用加速及更多 AI Agent 的部署，營運複雜度與風險也隨之增加。分散且通用的技術堆疊，配備不一致的防護措施與獨立工具，造成盲點與治理缺口。您的團隊需要對代理程式行為與譜系有一個相連的視角，並具備強制原則與可稽核性，以便在問題擴散前偵測到。

值得信賴的 AI 始於 Microsoft Foundry，這個統一的平台可用於建立、觀察、控制、保障和管理您的 AI 應用程式和代理程式組合。Foundry 控制平台為團隊提供代理程式、模型與工具的單一視野。他們可以在同一位置上建置並執行受信任的 AI Agent，並在整個代理程式生命週期中進行監控和強制原則。

Foundry 也能無縫連接 Microsoft Fabric，提供安全的資料存取與分析。這項整合對於代理型 AI 情境至關重要，因為敏感資料與快速處理需要強大的安全性與治理。

關鍵要點

- 機群管理需要對所有代理程式具備可見度。Foundry 控制平面提供您一個集中管理 AI 機群的地方，從建置到生產。
- 代理程式身分識別是標準化治理、驗證與授權的第一步。透過與 Microsoft Entra 整合，Fabric 提供您組織內部署及使用的所有 Microsoft 及第三方代理的完整清單。
- 端對端可檢視性幫助團隊在日益複雜的環境中維持控制、問責與韌性。Foundry 提供即時可見度、監控、診斷與追蹤，涵蓋 AI 管線、代理程式與應用程式，並透過 OpenTelemetry 深入洞察代理程式的行為、效能與互動。
- 原生 Microsoft 安全性功能，例如適用於雲端的 Microsoft Defender 對模型和代理程式的保護，能讓您在整個生命週期中建置時即具備身分識別、威脅偵測與合規性。Foundry 也與 Palo Alto Networks 和 Zenity 等合作夥伴整合，為您的團隊提供更多安全性與原則執行的選擇。
- 內建治理整合有助於簡化 AI 合規性，同時不影響開發速度。Foundry 與關鍵治理平台 (包括 Microsoft Purview、Credo AI 及 Saidot) 的整合，能協助您落實 AI 原則、符合法規要求，並持續展現合規性。



第四要素

主動的身分識別和存取安全性

安全的雲端基礎控制誰能存取什麼，並確保每個身分識別都經過驗證與保護。

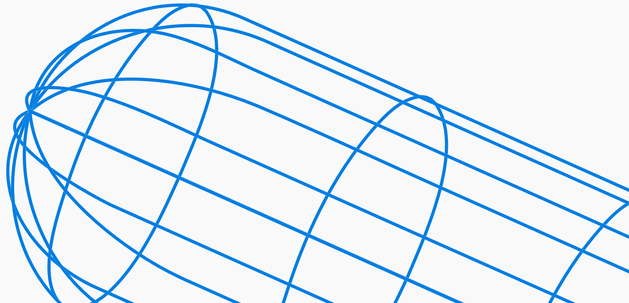
身分識別是在當今由 AI 支援的多雲端世界中，強制存取一致、降低風險並簡化合規性的控制平面。隨著您新增員工、承包商、合作夥伴、客戶，以及最重要的機器、服務和 AI 身分識別時，您必須確保合適的實體適時獲得適當的存取權。非受控身分識別與過多權限是組織面臨的最大風險之一，因為每個使用者、代理程式與應用程式都可能成為潛在的入口。

Microsoft 連續第九年被評為 Gartner Magic Quadrant 存取管理的領導者。[1] Microsoft Entra 將身識別和存取權管理嵌入到您雲端環境的每一層。集中控管、調適型原則及跨平台深度整合，幫助您在不減緩創新速度的前提下保護雲端資源。

例如，Microsoft Entra 的身份識別與網路存取產品支援安全性預設值，協助保護您的組織免受身分識別相關攻擊。Azure 也包含一套完整的服務、工具與參考架構，協助您的組織建立並維護高度安全且營運效率高的環境。

關鍵要點

- 將身分識別設為您的主要控制平面，並集中於 Microsoft Entra。首先，清查您的工作負載身分識別。以更安全的驗證方式取代密碼、認證、憑證和金鑰，例如 Azure 資源的受控識別，或其他環境中等同的雲端原生身分識別選項。
- 對所有應用程式 (包括私有及舊有應用程式) 實作多重要素驗證。優先採用防網路釣魚的驗證方式，例如通行金鑰，這被公認為目前最安全的選擇。
- 在 Microsoft Entra 中實作最低權限和即時存取，並結合以風險為基礎的條件式存取原則，以增強安全性。使用持續存取評估來改善即時存取檢查，而條件式存取中的權杖保護或 Microsoft Entra 網際網路存取，則能加強抵抗權杖遭竊。



[1] Microsoft 連續九年被評為 Gartner® Magic Quadrant™ 存取管理的領導者 - Microsoft 安全性部落格文章 - 2025 年 11 月 21 日 -

第五要素

安全的開發人員工作流程

開發人員必須將安全性內建於每一個體驗中，從程式碼到雲端都應用零信任原則。

領先組織正推行左移，亦即在軟體開發生命週期的起始階段嵌入安全性。左移實務能及早發現漏洞，執行安全的編碼標準，並自動化合規。隨著這些實務趨於成熟，其範疇從開發延伸至營運，進而形成 DevSecOps。使用整合型 DevSecOps 防護的團隊能更有效率地在安全性任務上協作，並更快速地修復威脅，有助於顯著降低入侵的風險。

Microsoft 正在引領這一轉變，將 GitHub Advanced Security 中以開發人員為優先的應用程式安全性與適用於雲端的 Defender 的執行階段保護相結合，並透過代理型修復加以強化。您的開發團隊不僅能獲得偵測漏洞的協助，也能排定風險的優先順序，讓他們能專注於最重要的事情。與適用於雲端的 Defender 整合有助您在部署後強制原則並保護工作負載。這些工具可共同打造安全的 DevSecOps 管線，將開發人員見解與雲端防禦相銜接。

加快行動[2]

- **修正 50% 的警示**
  透過 GitHub Copilot Autofix 修正提取請求中的警示
- **平均修復時間縮短 70%**
- **修復 68% 的警示**
  使用 GitHub Advanced Security 中的安全性活動

[2] GitHub 內部資料。

落實零信任

Microsoft 採用零信任原則來設計所有產品與服務，包括 Azure：絕不相信，一律驗證。無論在網路內部或外部，每位使用者、裝置與服務都必須進行驗證。

零信任確保所有對 Azure 資源的請求都經過驗證與授權，並僅授予最低必要的存取權。網路流量會持續受到監控，以便在威脅影響應用程式之前偵測並阻擋這些威脅。所有資料，無論是儲存或傳輸中，預設皆會加密。適用於雲端的 Defender 提供持續監控與威脅偵測，而 AI 驅動的監控能學習正常運作模式，並即時識別異常。

關鍵要點

- **互聯生態系統效率。**GitHub Advanced Security 與 Azure DevOps 的原生整合有助於及早揭露程式碼漏洞，而 Azure 原則和適用於雲端的 Defender 則在所有部署中套用並強制安全性控制。
- **整合工具提升開發人員速度。**團隊能配合安全設計原則，使用 GitHub Copilot、Visual Studio Code 及 Azure DevOps 進行安全協作，在無摩擦下建置、測試及部署軟體。
- **程式碼到雲端的安全性。**使用適用於雲端的 Defender 有助於保護多雲端與混合環境中的雲端應用程式。

第六要素

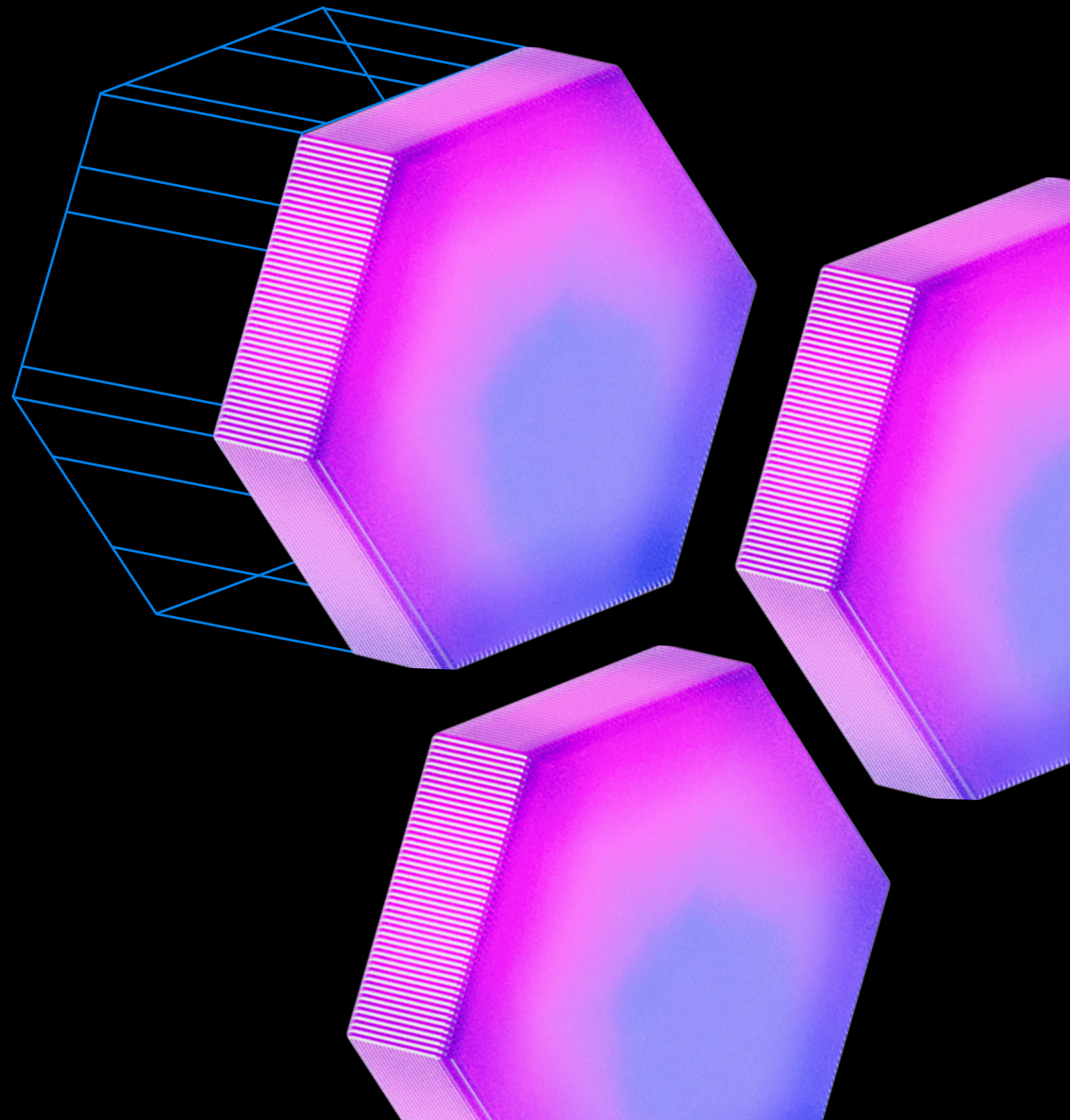
橫跨您的資料資產的全面保護

現代雲端資料庫應具備安全設計、針對 AI 進行最佳化，並整合全平台的保護。

AI 驅動的解決方案依賴無縫的資料存取，但分散的資料庫與舊有系統往往成為障礙。統一您的資料資產能減少孤島與盲點，讓您能在混合與多雲端環境中套用一致的原則與控管。

Microsoft 提供完整的 SQL、NoSQL 及專門資料庫組合，您可以在 Azure 虛擬機器上執行、做為完全受管理的服務使用，並部署於混合與多雲端情境中。例如，當您選擇完全受管理的 Azure 資料庫服務時，您的應用程式和 AI 解決方案可以利用零觸控復原、單位數毫秒延遲及進階向量搜尋等功能。您可以提升 SQL、NoSQL、PostgreSQL 和 MySQL 的效能，並且與自我管理的環境相比，可將擁有權總成本降低高達 58%。[3]

無論您選擇哪一種 Azure 資料庫，都能享有企業級的安全性功能。此外，與適用於雲端的 Defender 的整合可提供先進的威脅防護，偵測可疑行為並提供可行的修復措施，讓您的管理員能迅速調查並緩解警示。



[3] Analyzing the Economic Benefits of Microsoft Azure SQL Managed Instance，TechTarget，2025 年 3 月。

關鍵要點

- 集中管理資料庫使用者的身分識別與權限，能夠更方便且安全地存取資源。使用 Microsoft Entra，您可以在同一地方管理資料庫使用者和群組，然後將這些 Entra 身分識別對應到資料庫角色，以便取得資料庫內權限。
- 列層級安全性可讓您根據使用者的身分識別、角色或工作階段內容，強制細緻的逐列存取規則。它內建於 Azure SQL Database 和適用於 PostgreSQL 的 Azure 資料庫，在多租用戶和 SaaS 應用程式中，以及需要依使用者或組織分割敏感資料的情境下，特別實用。
- 對待用和傳輸中的資料進行加密。Azure 資料庫支援傳輸層安全性 (TLS) 加密，保護用戶端與伺服器間傳輸的資料，免受中間人攻擊等威脅。透明資料加密 (TDE) 可協助防止未經授權或離線存取原始檔案或備份中的待用資料。
- Always Encrypted 是一項 Azure SQL 功能，旨在保護像信用卡號碼這類敏感的欄層級資料。資料在資料庫引擎內永遠不會以未加密形式出現，即使是像資料庫管理員這樣的高權限使用者也無法看到未加密的資料，這有助於保護伺服器上待用和使用中資料。

KPMG 在安全且可調整的轉型基礎上創新

KPMG 正在重塑工作方式，將 AI 置於其稽核、稅務及諮詢服務的核心。為了加速創新，公司賦權讓 28 萬名專業人士打造自己的 AI Agent，並擴展智慧解決方案。初步結果很正面。代理程式有助於簡化持續的合規性任務和新員工的入職流程。

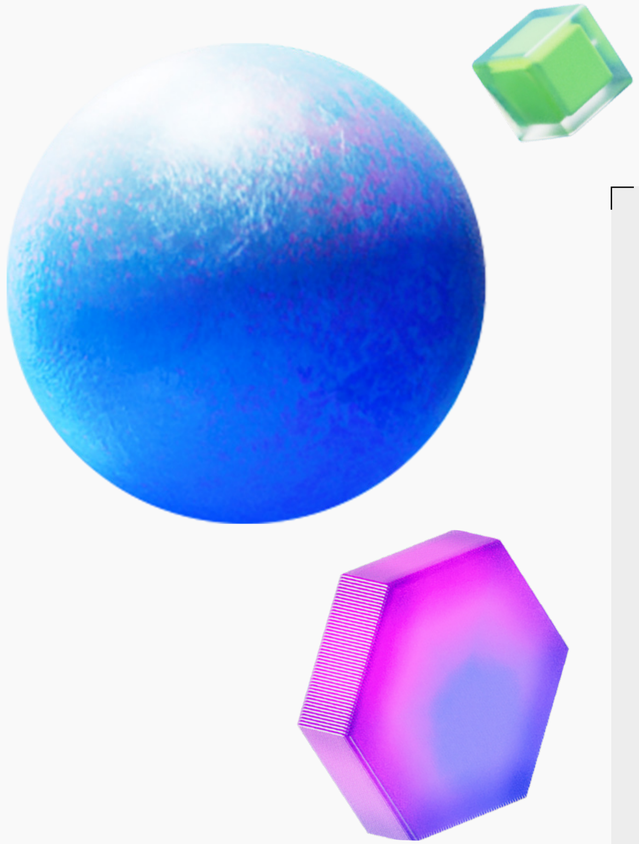
「我們正在創造一個智慧前沿，一種受規範且可調整的工作方式，由代理程式在背後自主運作。這就是未來，而我們正與 Microsoft 一起邁向未來。」

Cherie Gartner，
KPMG Microsoft 全球首席合夥人

閱讀完整案例

第七要素

統合資料治理和保護



整合資料安全性、治理、合規性與隱私權，有助於降低風險與複雜性。

隨著組織擴展雲端應用、採用 AI 並支持遠端工作，資料已成為成長的引擎，同時也是風險的來源。在混合與多雲端環境中，保護與治理這些資料變得更加複雜。然而，透過統一的安全性、治理與隱私權方法，您可以恢復對全企業可見度與控制權。在最近一項研究中，組織透過實作微調資料外洩防護 (DLP) 原則，並提升跨雲端、裝置與應用程式的敏感資料可見度，成功將資料外洩的風險降低了 30%。[4]

像 Microsoft Purview 這樣的解決方案體現了這種現代的一體化方法。透過整合資料安全性、治理、合規性與隱私權功能，Microsoft Purview 使您能持續擴展雲端與 AI 計畫。無論您的敏感資料是存留在資料庫、檔案系統、SaaS 應用程式或 AI 平台中，Microsoft Purview 都能確保您的團隊能夠快速找到正確的資料、信任它，並迅速取得受控管的存取權。

關鍵要點

- 在資料的整個生命週期及整個資料資產範疇內，保護並防止資料遺失。Microsoft Purview 提供一套協調式資料安全性解決方案，包括資訊保護、資料外洩防護、內部風險管理，以及資料安全性態勢管理。
- 無縫且全面地控管資料。在 Microsoft Purview 中提供現代資料治理解決方案，具備全面可見度、資料可信度及負責任的創新，您可以定義資料擁有權、套用原則、確保高資料品質，並衡量業務成果。
- 簡化合規性並遵守法規要求。Microsoft Purview 結合了安全性稽核、通訊合規性、電子文件探索及記錄管理，協助您的組織降低合規性風險並滿足法規要求。

[4] The Total Economic Impact™ Of Microsoft Purview，委託 Forrester Consulting 進行的研究，2025 年 8 月。

第八要素

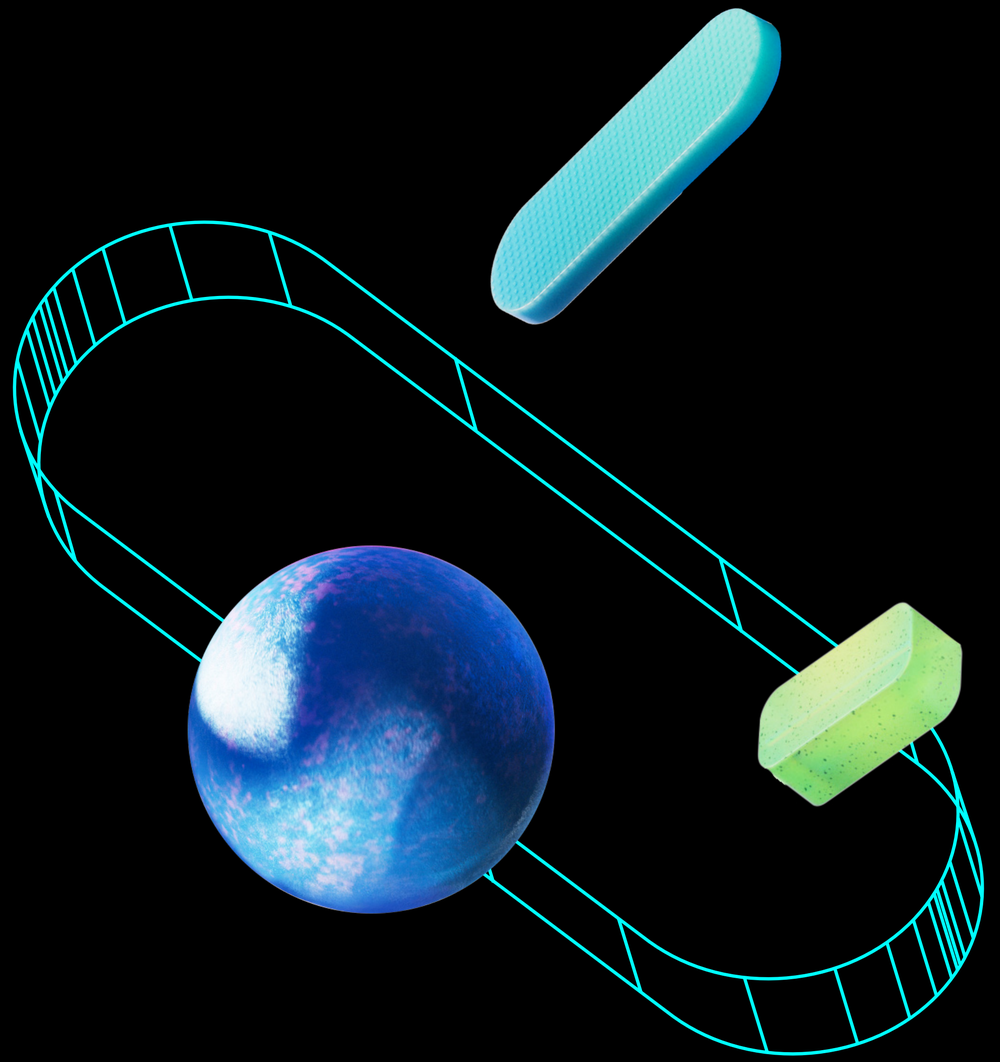
經壓力測試的元件

為了降低潛在風險，雲端提供者必須在其硬體、軟體及服務供應鏈中實施透明且有效的風險管理。

選擇雲端提供者意味著信任其整個供應鏈，包括用於建置與操作資料中心的硬體、軟體和服務。提供者對其廠商管理、認證及安全性管控應保持透明。當透明度內建於基礎結構與軟體開發生命週期時，您可以確信每個元件都是真實、未遭入侵，且以符合道德的方式由負責任的合作夥伴取得。

Azure 安全性與韌性架構 (ASRA) 在雲端基礎結構及更廣泛的供應鏈中嵌入安全性與韌性。每個伺服器元件在部署前都經過嚴格測試。所有開放原始碼及第三方軟體都經過嚴格審核，以防止隱藏風險。透過供應商管理辦法及永續性稽核，確保向負責任合作夥伴的採購符合道德標準。

這些實務超越全球標準，反映數十年最佳做法，幫助您達成法規遵循要求，並在安全且具韌性的雲端上運作。



第九要素

先進的實體防護措施

安全性從根本層面做起，搭配強大的實體防護措施，包括資料中心的受控存取、監控以及環境防護。

每一項更高層級的控制都取決於底層基礎結構的完整性。當伺服器、備份和硬體的實體安全性獲得保障時，您可以信任加密、身分識別管理和網路保護如預期般運作。

Microsoft 資料中心在多層式安全防護方面堪比金融業設施，配備生物辨識掃描器、控制系統及安全檢查點，有效防止未經授權的存取。持續監控與即時監督可保護營運，並使資料中心符合最全面的國際標準。

Fairwater：全球首個全球規模 AI 超級工廠

永續性是全球最強大的 AI 資料中心的設計核心理念，該資料中心位於威斯康辛州芒特普萊森特並由 Microsoft 投資 70 億美元建造而成。該地採用 Fairwater 資料中心設計，運用單一平面網路，能整合數十萬顆最新的 Nvidia GB200 與 GB300 GPU，打造出一部龐大的超級電腦。

做為一項技術里程碑，該資料中心擁有足夠的光纖電纜可繞地球四周，但其年用水量卻相當適度，約等於一般餐廳每年的用水量。下一個 Fairwater 場址位於喬治亞州亞特蘭大。

閱讀完整案例

第十要素

與資安公司合作

廠商必須投入持續改進、威脅情報及復原力計畫，以協助雙方共同應對不斷演變的風險。

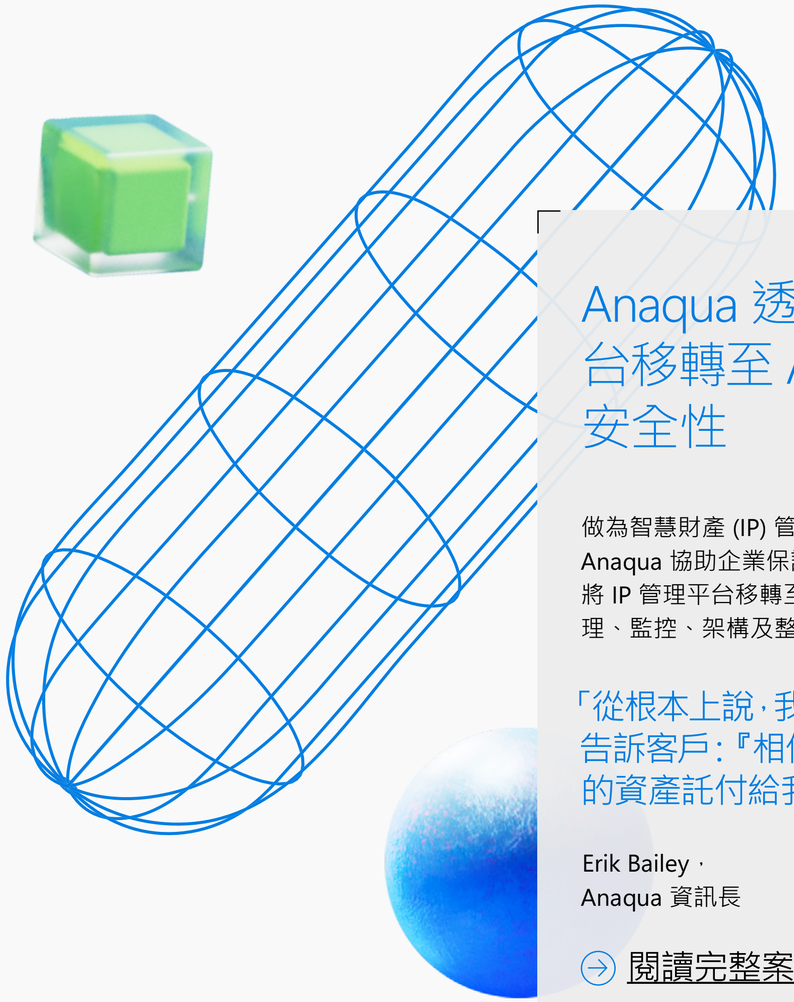
安全性環境不斷變化，而新技術帶來強化防禦的機會。只有致力於大規模持續改進的提供者，才能提供您所需的主動防護，保障您的工作負載安全且合規。

Azure 是 Microsoft 安全未來倡議 (SFI) 的重要組成部分，這是公司歷史上最大規模的網路安全性工程專案。超過 35,000 名工程師致力於嵌入安全設計、預設啟用安全機制，並以安全作業做為後盾。這些做法有助於降低您在 Azure 上的暴露風險，減輕團隊的營運負擔，為他們提供一個將大規模安全性視為首要任務的雲端平台。

Microsoft 引領全球網路安全性

100 兆
每天處理的安全性訊號數

10,000
安全性和威脅情報專家



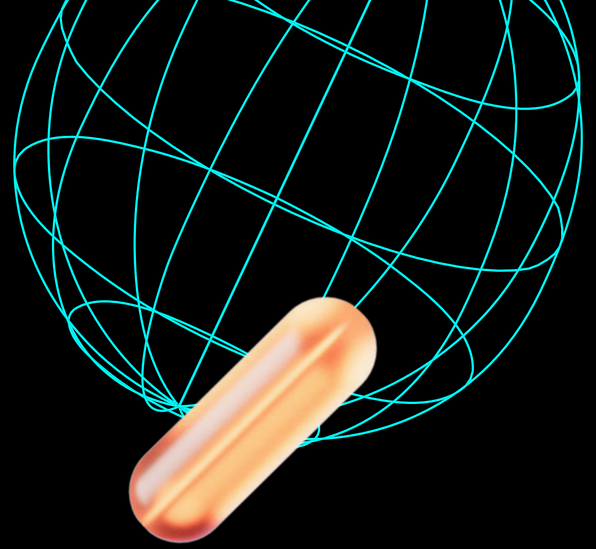
Anaqua 透過將其 IP 平台移轉至 Azure 來強化安全性

做為智慧財產 (IP) 管理解決方案的市場領導者，Anaqua 協助企業保護其最有價值的資產。透過將 IP 管理平台移轉至 Azure，公司提升了端點管理、監控、架構及整體安全性。

「從根本上說，我們是在銷售安全性，告訴客戶：『相信我們，將您最有價值的資產託付給我們。』」

Erik Bailey，
Anaqua 資訊長

閱讀完整案例



第十一要素

以防範為核心

主動安全性是指在問題成為事故之前，識別漏洞並緩解風險。

整合式安全性解決方案能提供全面的可鹼度與更強健的防禦力，不像各自為政的點式工具容易造成防護漏洞。適用於雲端的 Defender 提供整合的威脅情報，幫助您在問題影響企業之前加以預防。其多層式防護橫跨從晶片到雲端，提供超過 450 項自動化建議與即時偵測，適用於混合及多雲端環境。

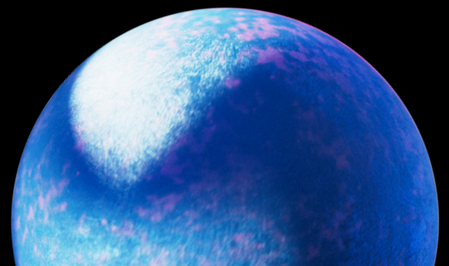
Microsoft 是唯一同時提供公有雲和開發人員平台的領先提供者，並且還提供雲端原生應用程式保護平台 (CNAPP)。適用於雲端的 Defender 提供整合式 CNAPP 檢視，能夠關聯端點、身分識別與應用程式之間的訊號。您將獲得雲端儲存體、資料庫及生成式 AI 工作負載的深度防護，並且修復更快速、盲點更少，以及在雲端規模下更安全的創新。

關鍵要點

- 預防為先。內建並原生整合的安全性控制能夠揭示優先處理的風險，並提供自動化建議，讓您能夠及早採取行動。
- 無需整合多個工具，即可全面掌握雲端資源的可見度與態勢管理。
- 更快地回應。即時偵測與生成式 AI 支援的修復，幫助團隊專注於重要問題，縮短修正時間。
- 減少手動作業開支。無代理程式機器掃描有助於防護各種環境中的漏洞、錯誤設定、惡意程式碼、機密資訊以及敏感資料洩漏。

適用於雲端的 Microsoft Defender

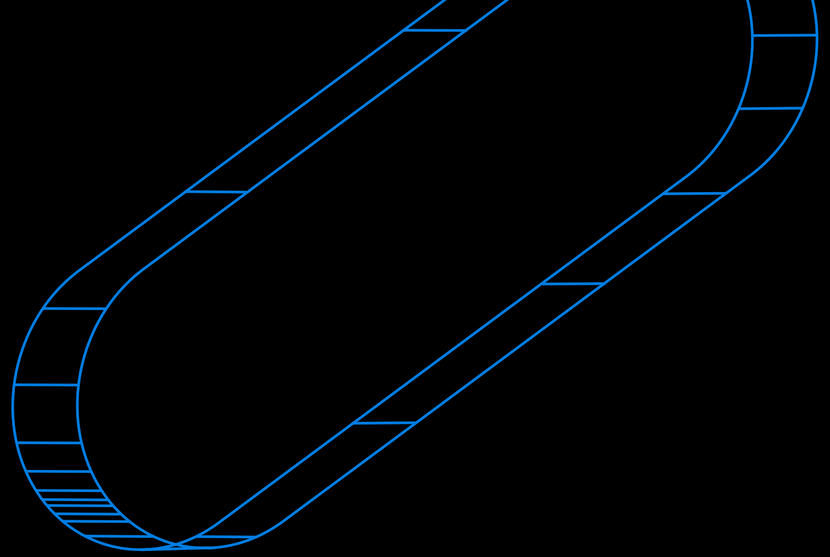
- 修復威脅的速度加快 30%
- 高達 117% 的 3 年投資報酬率[5]
- 免費試用 30 天



[5] The Total Economic Impact™ Of Microsoft Defender for Cloud，委託 Forrester Consulting 進行的研究，2025 年 1 月。

向前邁進

經實證的雲端安全性藍圖



Azure 的多層式安全性為您的每個工作負載提供預設的保護保證，並以全球最大的安全投資做為後盾，並受到專家指導的支持。

在此基礎上，您的團隊需要合適的指導和技能。Microsoft 提供免費資源，為您的團隊提供結構化指引、安全性軌跡，以及雲端就緒的登陸區域，協助設計並維護符合您的業務目標及業界標準的安全環境。

如需存取經實證的安全雲端採用藍圖，請參閱 Azure 基礎元件、 Microsoft 雲端採用架構及 Azure Well-Architected Framework。這些資訊會持續更新，以反映最新的資訊、技術和法規遵循要求，協助您在瞬息萬變的環境中支持靈活且安全的成長與合規性。

安全地移轉和現代化，以加速 AI 創新。

- 了解如何在雲端旅程的每個階段保護您的環境：保障轉移的安全：應對移轉和現代化中的安全性挑戰
- 了解如何透過整合防護，在雲端與混合環境中強化您的安全性態勢：整合雲端安全性：適用於雲端的 Microsoft Defender
- 透過資金、專家指導及解決方案加速器啟動現代化工作：探索 Azure Accelerate