IBM Security Guardium Data Protection 資料與合規性稽核安全保護解決方案

蔡睿誠 Mark Tsai, CISSP
臺灣 IBM 資訊安全技術顧問
mark.tsai@ibm.com

IBM **Security**

《資料外洩的平均成本》
教育產業 **education industry**

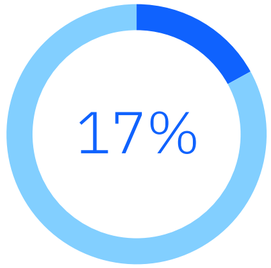
USD 3.50M

15th highest cost
在 17 研究產業中

33% lower than
4.88M USD
global average

4% lower
compared
to 2023

Key statistics

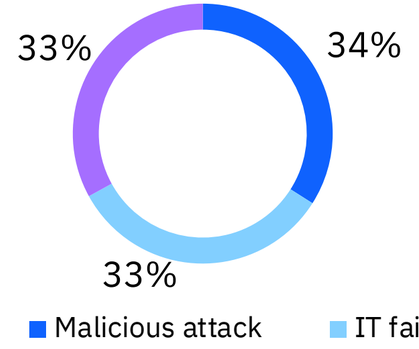


廣泛使用安全人工智慧和自動化的教育組織的百分比%

USD 1.9M

與不使用安全人工智慧和自動化相比，
廣泛使用安全人工智慧和自動化可節省成本

Root causes of a data breach



Global highlights

Top 3 initial attack vectors

USD 375M

洩漏超過 5000 萬筆記錄的平均總成本

USD 4.91M

勒索軟體相關違規事件的平均成本

Time to identify and contain

USD 248K

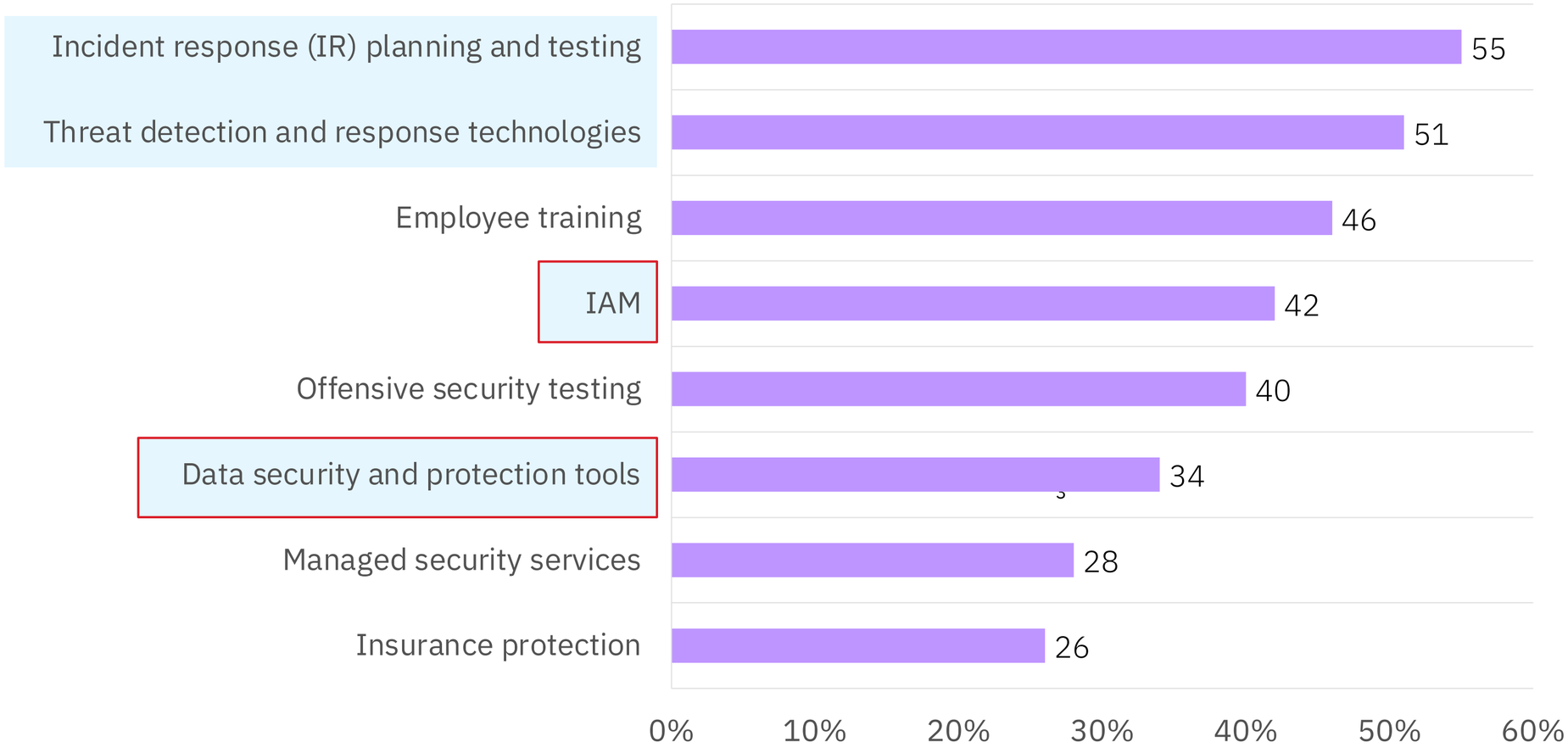
使用事件回應 (IR) 團隊和測試與不使用 IR 團隊或測試相比平均節省的成本

USD 223K

透過支援混合環境和使用者體驗的身份和存取管理 (IAM) 策略節省平均成本

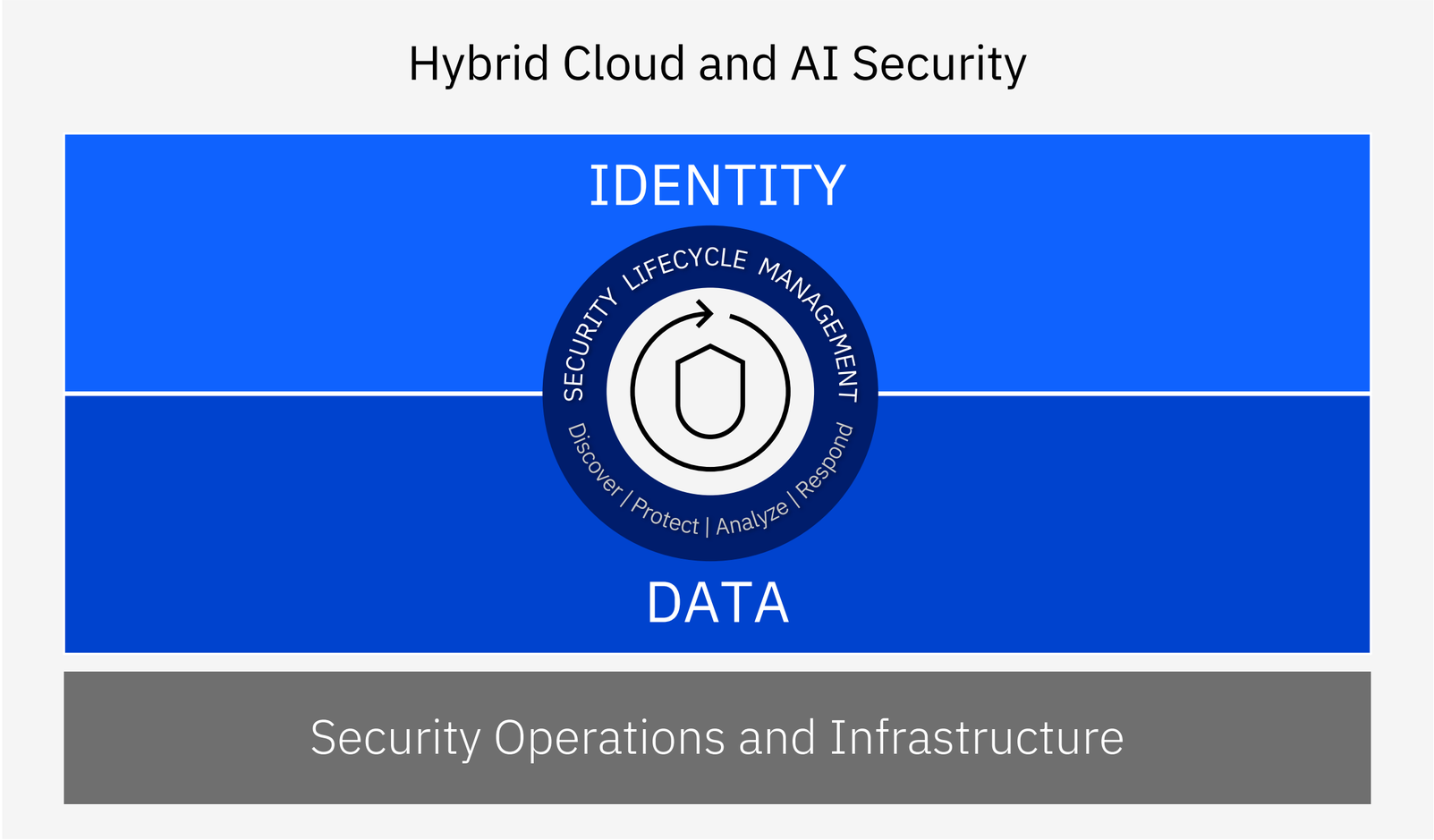
資料外洩事件後主要資訊安全投資項目
The top security investment categories following a data breach

- 從 2023 年到 2024 年，投資增幅最大的 3 個領域是**威脅偵測和回應** (13%)、**身分和存取管理或** IAM (10%) **以及資料安全** (9%)。
- 與 2023 年相比，2024 年安全服務託管投資下降了 3 個百分點，員工安全意識與技能培訓持平。



© 2024 IBM Corporation

混合雲與 AI 安全策略
Secure hybrid cloud and AI



快速的業務與科技發展，導致關鍵數據暴露在風險當中

從傳統的資料保護機制，必須持續拓展到雲端安全到人工智慧安全，以及未來的量子時代的資料保護

科技創新擴大了資料威寫層面與風險途徑 (Threat Surface)

To simplify data protection in the future, a shift from point products to a data security platform is happening

資料合規挑戰 (Compliance)

滿足合規性需要，需花費大量時間準備稽核資料以及多方的稽核團體；同時未來 AI 使用與量子安全威脅也帶來新的監管。

資料暴露風險 (Exposure)

雲端和 GenAI 導致的資料儲存、權限管控，以及傳統資料保護的機制將失效；而量子運算的到來，也將既有傳統加密措施遭到破譯，從而導致「現在搜集、未來解密」的資料暴露風險。

人工智慧風險 (AI risks)

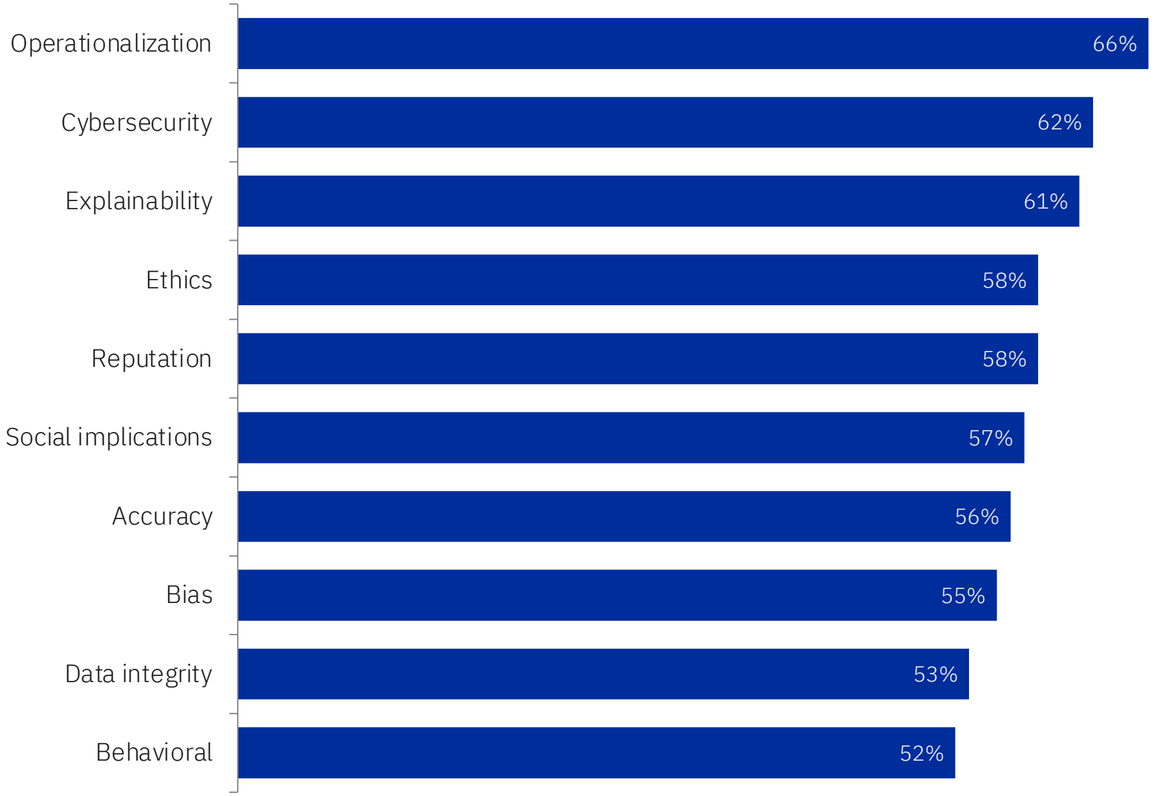
Gen AI 的到來，創造新的攻擊威脅 – 即訓練的資料、模型與應用，都必須具有資料安全管理、模型監管與輸出規範等合理控管機制。

安全風險狀態 (Security posture)

如何解決一系列資料安全風險，包含像是影子資料、影子人工智慧到傳統加密資料被揭露與不當使用的問題。

Gen AI 帶來新的安全威脅

風險種類 (Type of risk)



代表意涵 (What it means?)

責任歸屬：增加法律責任

資訊安全：引入新的漏洞

可解釋性：答案未指明資料來源

道德 AI：與社會價值衝突的結果

聲譽：損害企業品牌認知

社會影響：傳播錯誤訊息

精准度：將不正確資訊斷言為事實

偏見：有偏見或優惠的提議

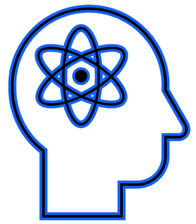
完整性：來源資料不可信

蓄意：欺騙和操縱人

Source: IBM Institute for Business Value. 2023 IBM IBV Generative AI CEO Pulse

Comments from a Gartner Security Panel Discussion

"AI security is a data problem"



Why?: Organizations are limiting the adoption of AI and LLM's until data is properly secured. **Data is the new security edge.**

如何防護 AI pipeline 過程的風險性？

Attackers will target

資料收集和處理

被集中存放用來參與模型訓練的各式敏感資料

Data being centralized

模型開發和訓練

新的安全漏洞會從採用外部模型透過 API 傳入

Vulnerabilities

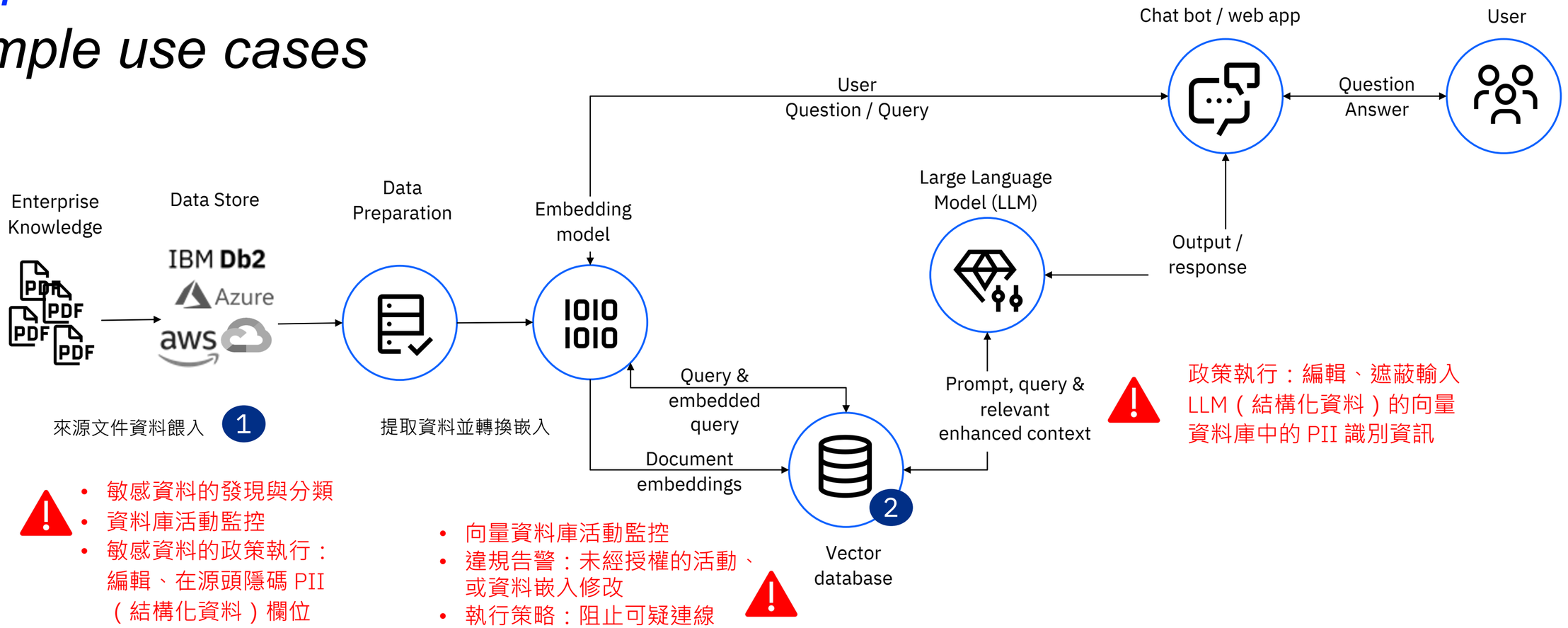
模型推理和實際使用

透過推理攻擊來操縱或劫持模型運作行為

Inferencing attacks

AI Pipeline 資料安全保護情境

Example use cases

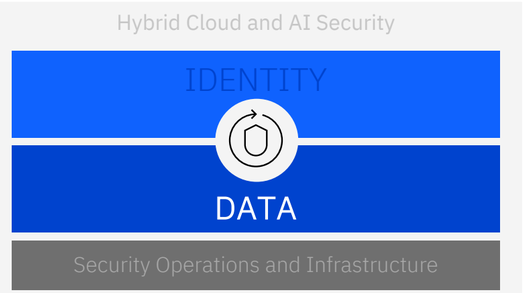


1 從資料來源即開始保護 (Protect data at the source)

保護敏感資料、監控資料庫和資料來源活動、強制正確使用用於訓練 AI 模型的資料、滿足合規性

2 從資料使用過程持續保護 (Protect data in use)

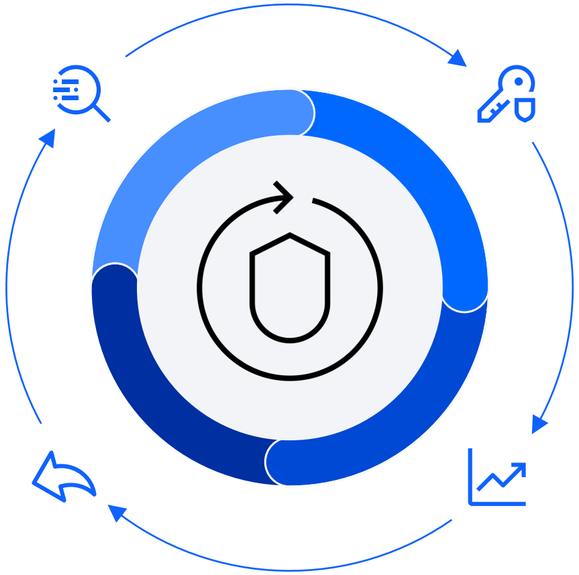
保護和監控向量資料庫與過程活動的資料合規性



提升資料安全，保障業務轉型
Streamline data security to protect business transformation

發掘 (Discover)

– 資料發現與分類 (Discovery & Classification)
– 模型和加密機制 (Model & Algorithms)
– 發現關鍵漏洞 (Vulnerabilities)



保護 (Protect)

– 透過加密和金鑰管理保護數據 (Encryption)
– 集中定義和執行合規政策 (Security Policy)
– 持續監控數據暴露 (Continuously Monitor)

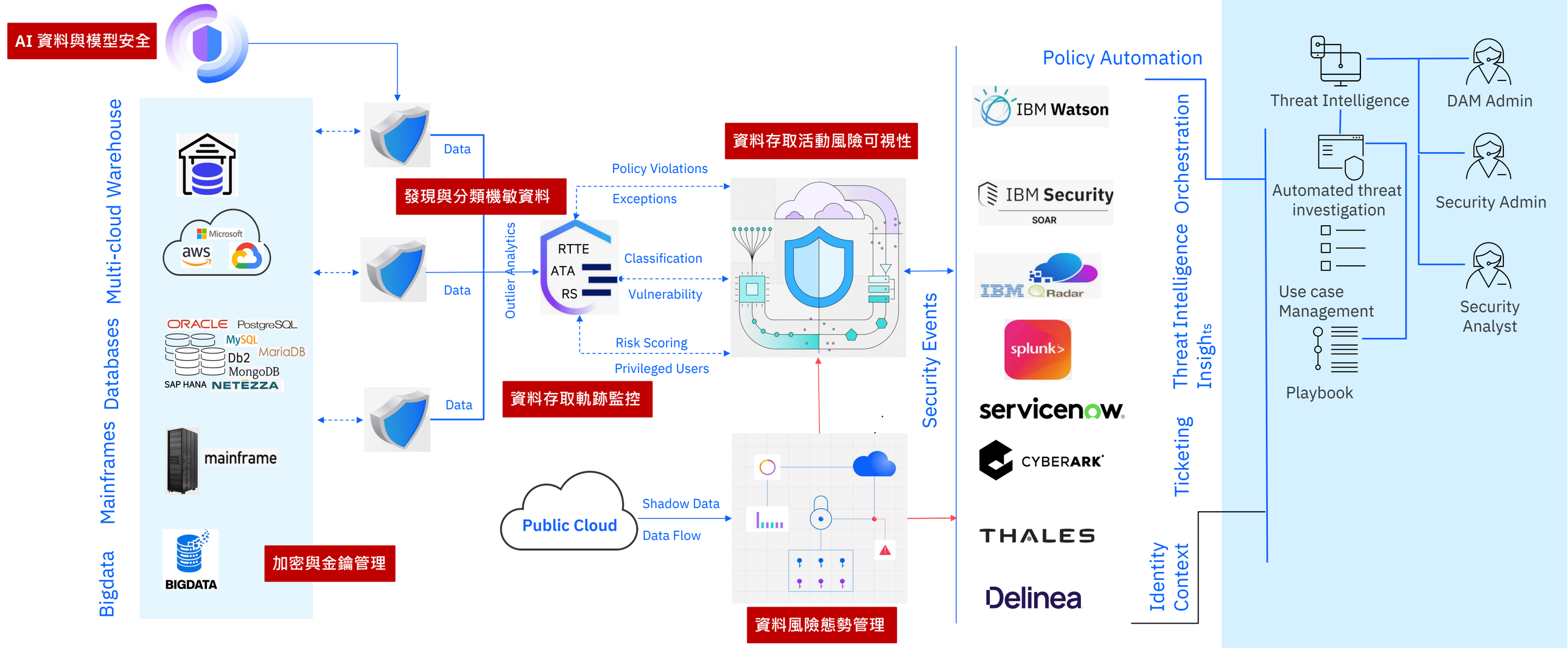
回應 (Respond)

– 按威脅程度修復風險 (Remediation)
– 強化 SOC 調查顆粒度 (Enrichment)
– 流程系統整合 (Integration)

分析 (Analyze)

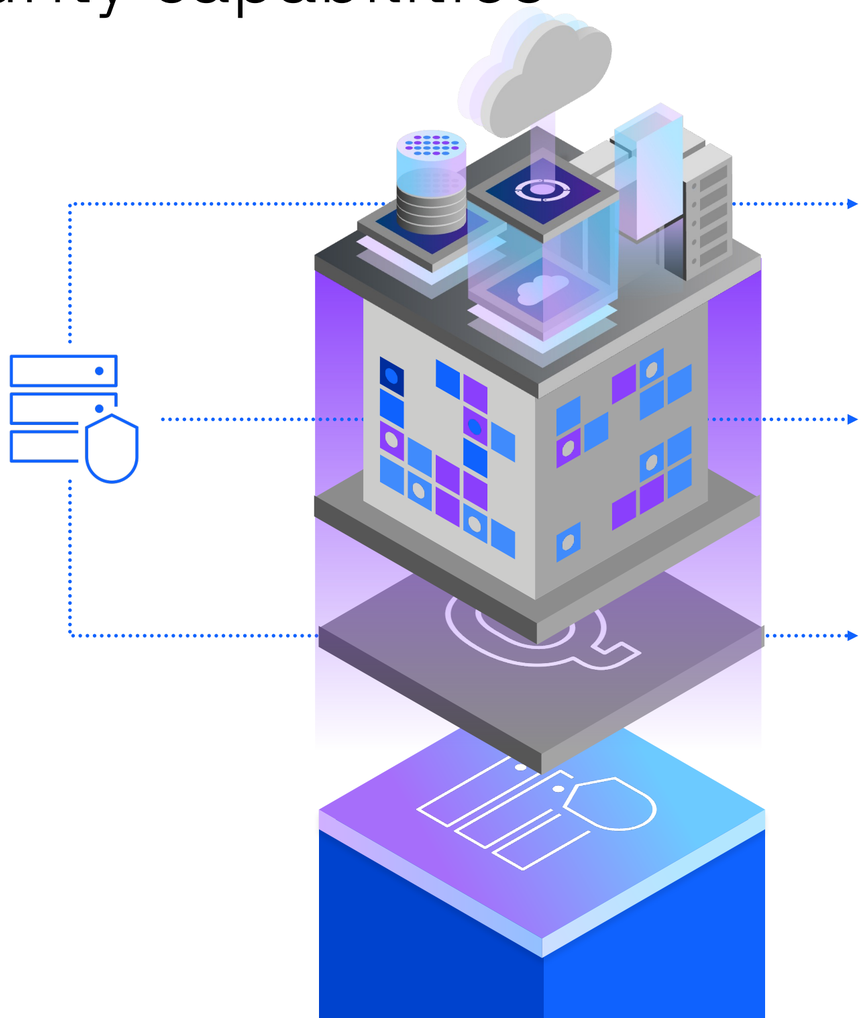
– 按威脅程度排序風險和漏洞 (Prioritized risk)
– 視覺化資料移動途徑 (Data flow)
– 自動化稽核合規流程 (Automated workflow)

企業環境資料活動的典型場景 .....Big picture story



強化資料安全確保業務持續營運與創新
Secure business innovation with robust data security capabilities

資料
安全
Data
Security



混合雲擴增
Hybrid cloud adoption

Gen AI 潮流
Generative AI proliferation

量子運算的到來
Rise of quantum computing

1 **資料活動監控與合規性**

提供可擴展方式滿足敏感資料存取活動監控，同時滿足各式現有與未來法規遵循

2 **資料與 AI 安全狀態管控**

視覺化混合雲和本地環境的影子資料和 AI 訓練威脅風險程度

3 **資料風險偵測與回應**

採用人工智慧輔助的資料安全機制監控資料存取活動以偵測異常行為，同時強化 SOC 調查顆粒度。

4 **密碼演算法與金鑰管控**

透過量子安全加密技術和金鑰管理機制保護關鍵數據。

ISAC校園團購買一送一限時專案

優惠期限：即日起～2024/12/13止

IBM Guardium 資料庫監控暨記錄軟體 基礎組合(1 database) 兩套(永久授權)

內含**IBM Guardium professional service** 一式

- IBM Guardium 工具安裝
- IBM Collector 主機建置設定
- Guardium基本教育訓練一日

IBM 業務代表：Andy
電話：0921-860752
Email: andy.zhuang@ibm.com

IBM顧問

活動問券(可兌換贈品)

*主辦單位保留內容修改異動之權利