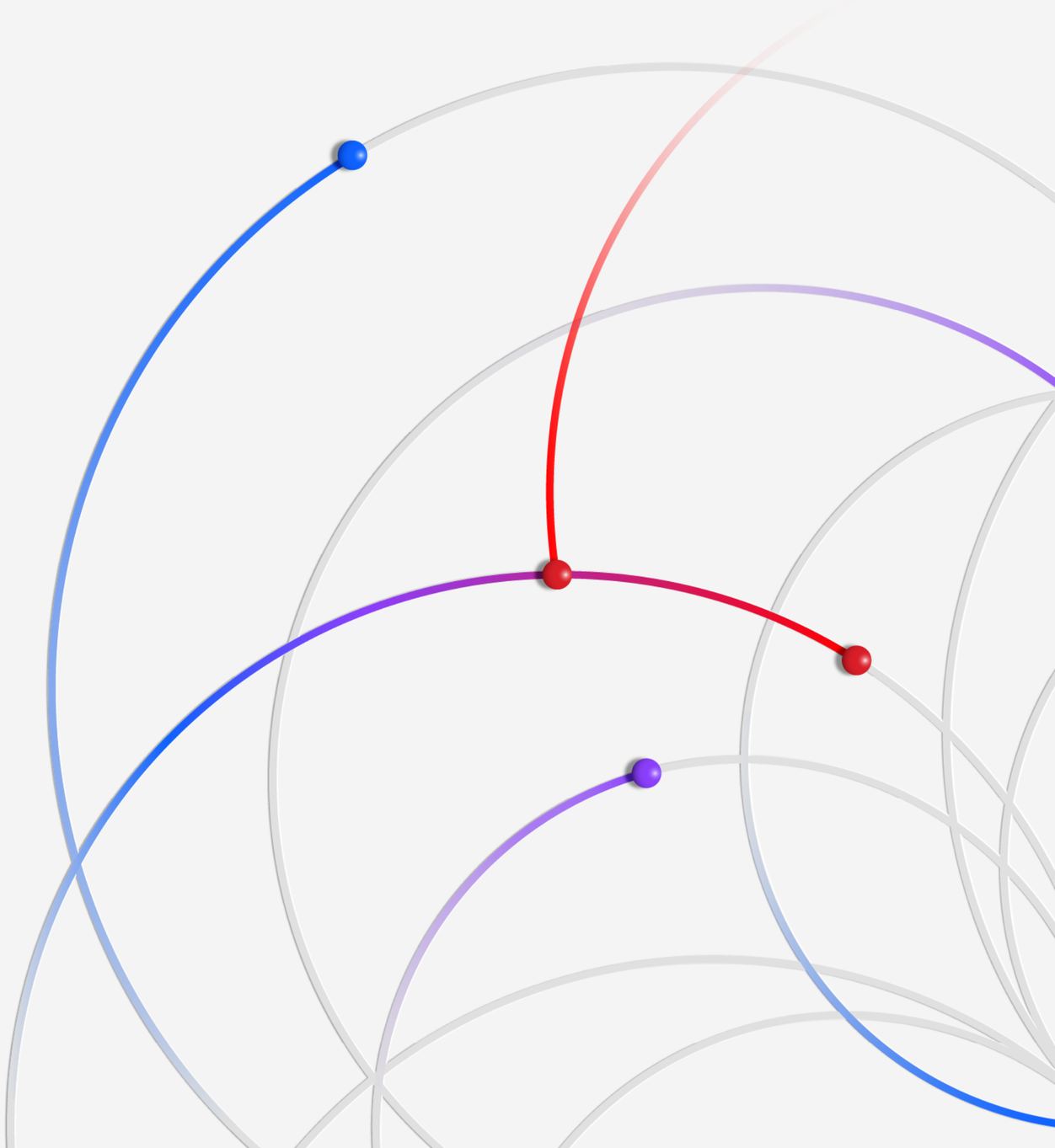
Next-Gen Data & Identity Governance Strategy

新世代資料安全與身份治理策略

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



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。

Guardium Data Protection

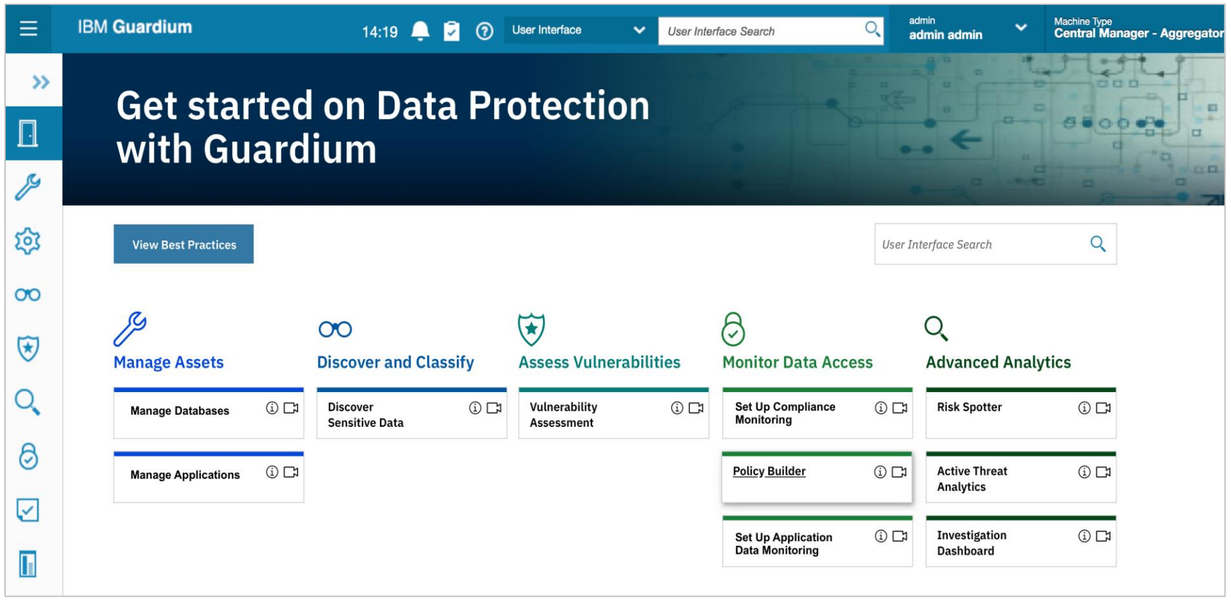
資料活動即時監視與保護的業界最佳方案

資料發掘與分類
在混合雲環境實現一致、
以資料為中心的資料安全策略

節省資料合規成本
提供不可篡改的稽核紀錄，簡化安全防護政策、工作流程與報告的合規性

完整的資料保護機制
遮蔽 (Masking)、編輯(Redaction)、隔離 (Quarantining) 或 阻斷 (Blocking) 實現資料存取機制

管理資料面臨的威脅
使用 AI 技術發現與回應內、外部的資料安全威脅。



資料稽核解決方案導入效益

67%
提升資料來源漏洞和錯誤配置的機會

50%
提升資料分類準確性

42%
減少因為資料安全問題導致的營運或稽核問題

持續 15 年獲得信賴的資料軌跡稽核解決方案

4 of 5
Top Global Healthcare Orgs

4 of 5
Top US Banks

7 of 10
Top Global Telecom companies

6 of 10
Top Global Insurance Institutions

3 of 5
Top US Retailers

4 of 5
Top Global Financial Services Orgs

資料安全策略– Monitor, Analyze, and Respond

Guardium Data Protection

資料活動即時監視與保護的業界最佳方案

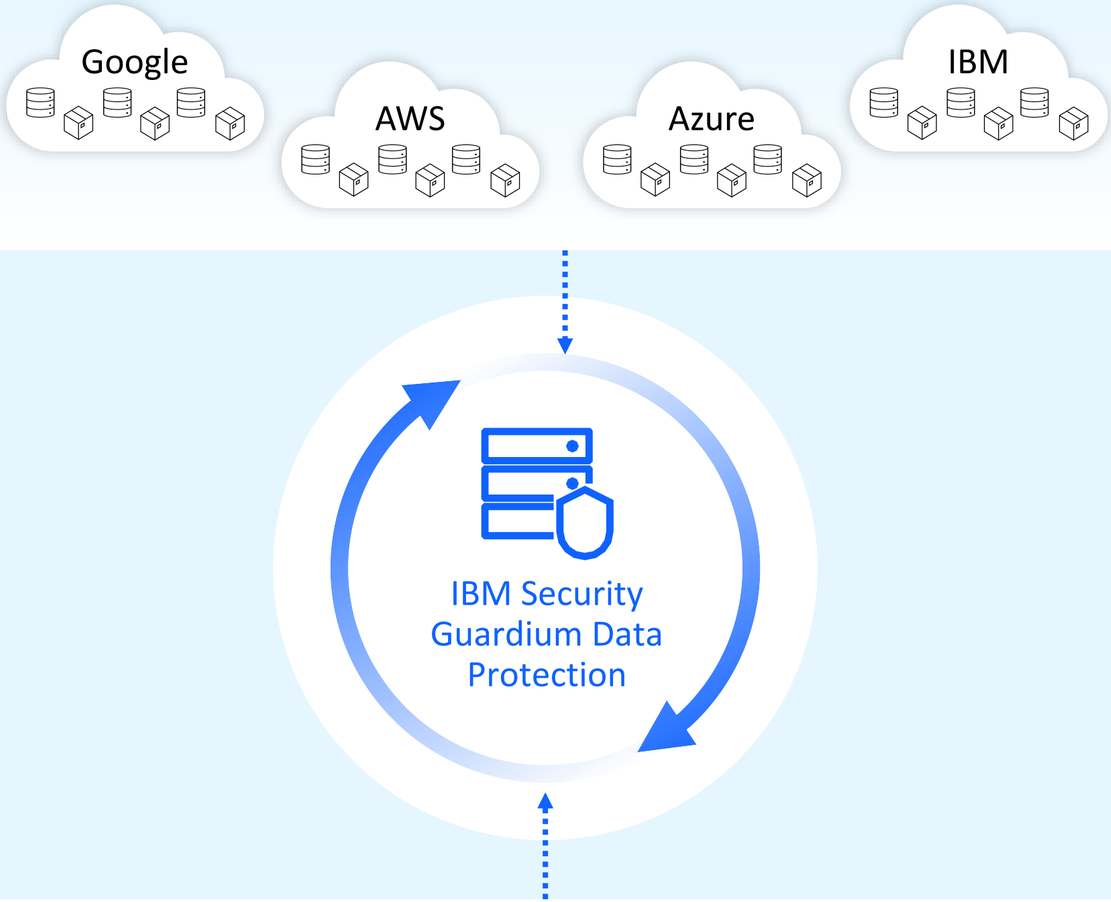
資料發掘與分類
在混合雲環境實現一致、
以資料為中心的資料安全策略

節省資料合規成本
提供不可篡改的稽核紀錄，簡化安全防護政策、工作流程與報告的合規性

完整的資料保護機制
遮蔽 (Masking)、編輯(Redaction)、隔離 (Quarantining) 或 阻斷 (Blocking) 實現資料存取機制

管理資料面臨的威脅
使用 AI 技術發現與回應內、外部的資料安全威脅。

跨雲、地環境的實現資料活動的集中化監控
Centralize visibility and control across hybrid multi-cloud environments

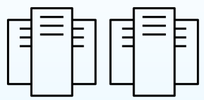


Collectors, Aggregators / Central Manager

Deployment Options

Available as virtual images
On premises, or in cloud - AWS Marketplace, Azure, Google Cloud, IBM Cloud, OCI (BYOL)

結構化資料庫
Structured data



大型主機資料監控
Mainframe

檔案與檔案系統監控
Files and file systems

敏感資料發掘分類與監管

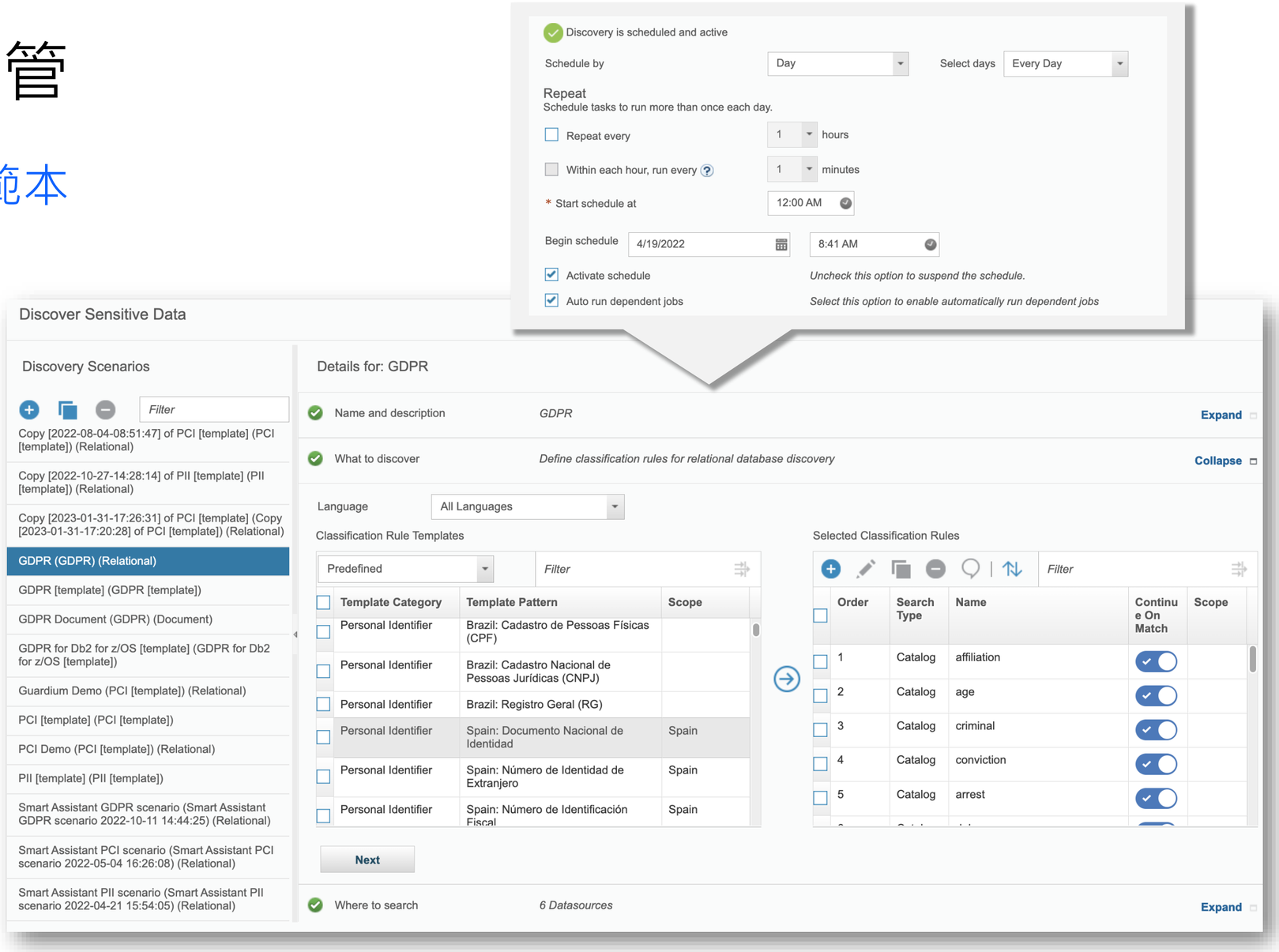
內建上百種資料發掘模式與法遵範本

混合雲資料環境 (Hybrid Cloud)
識別本地或雲端敏感數據，
例如信用卡號碼、個人財務數據或社會安全號碼

自動化監管工作流程 (Workflow)
指定發掘規則、定義對發現資料採取的操作、指定要掃描的資料來源、分派報告以及自動化資料合規流程檢查

資料庫自動發現 (Auto-Discovery)
掃描並探測伺服器是否有開放端口，以防止未知或不必要的網路連接。可依需求執行自動發現。

出於稽核需求的自動化工作流程



依照應用程式特性套用適合的資料特性與格式

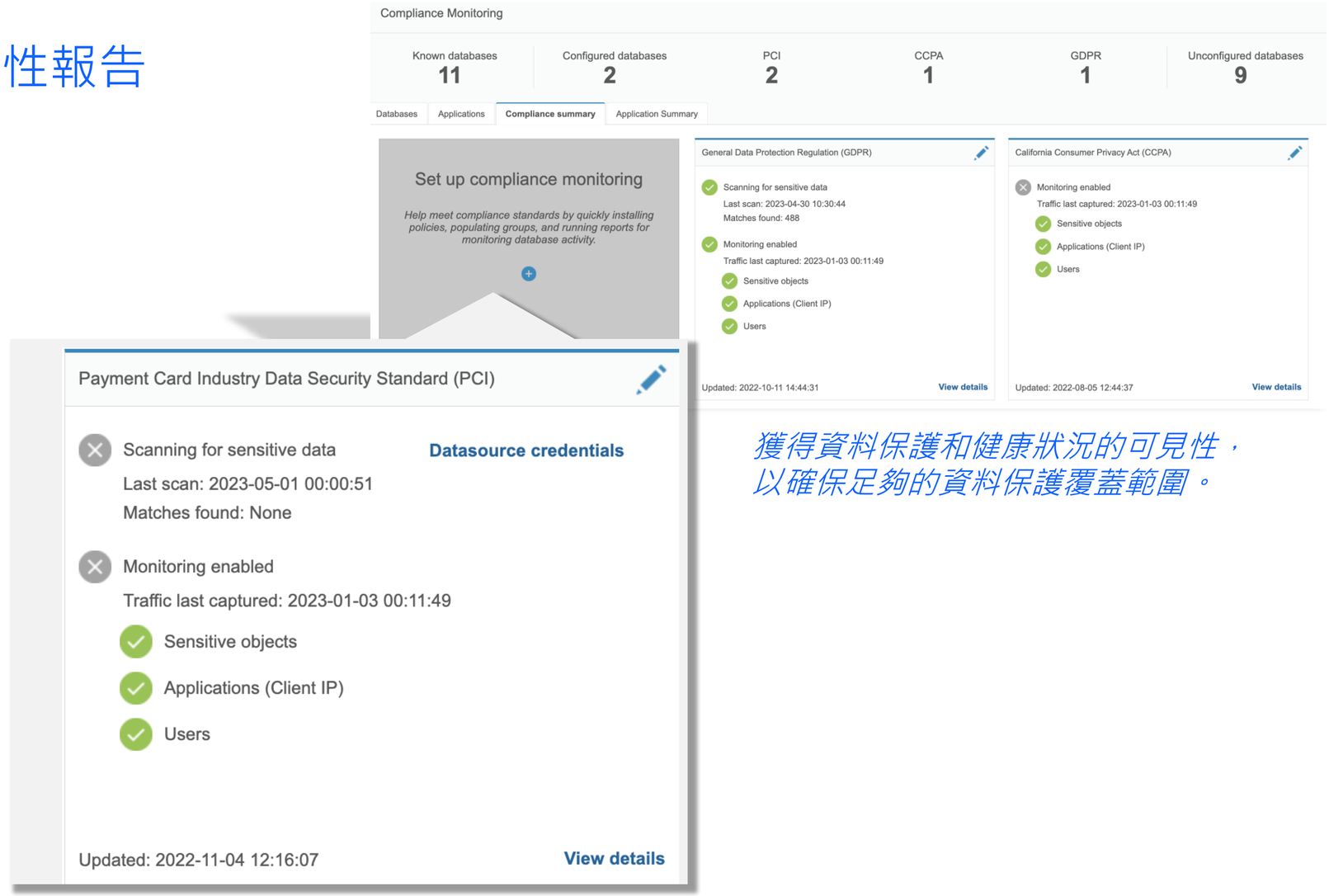
集中化資料合規狀態

建立自訂審核原則並自動化全面性報告

統一的安全政策管理 (Policy)
將組織內部政策管理統一到一個中央化的平台或系統中以便有效率地制定、部署和監控政策

確保符合職責分離 (Separation of Duties)
通過作業系統層級的代理程式監控，讓資安管理員與資料庫管理員職責區分，不同使用者僅能執行與其職責相關的操作，同時稽核紀錄儲存在無法被竄改的資料庫當中。

自動化合規組織規範 (Automation)
從單一介面追蹤所有選定法規的合規進度。設定和自動化審核流程工作流程，以便與主要利害關係人分享以供審核和簽署。



獲得資料保護和健康狀況的可見性，以確保足夠的資料保護覆蓋範圍。

快速建立新的或自訂審核策略

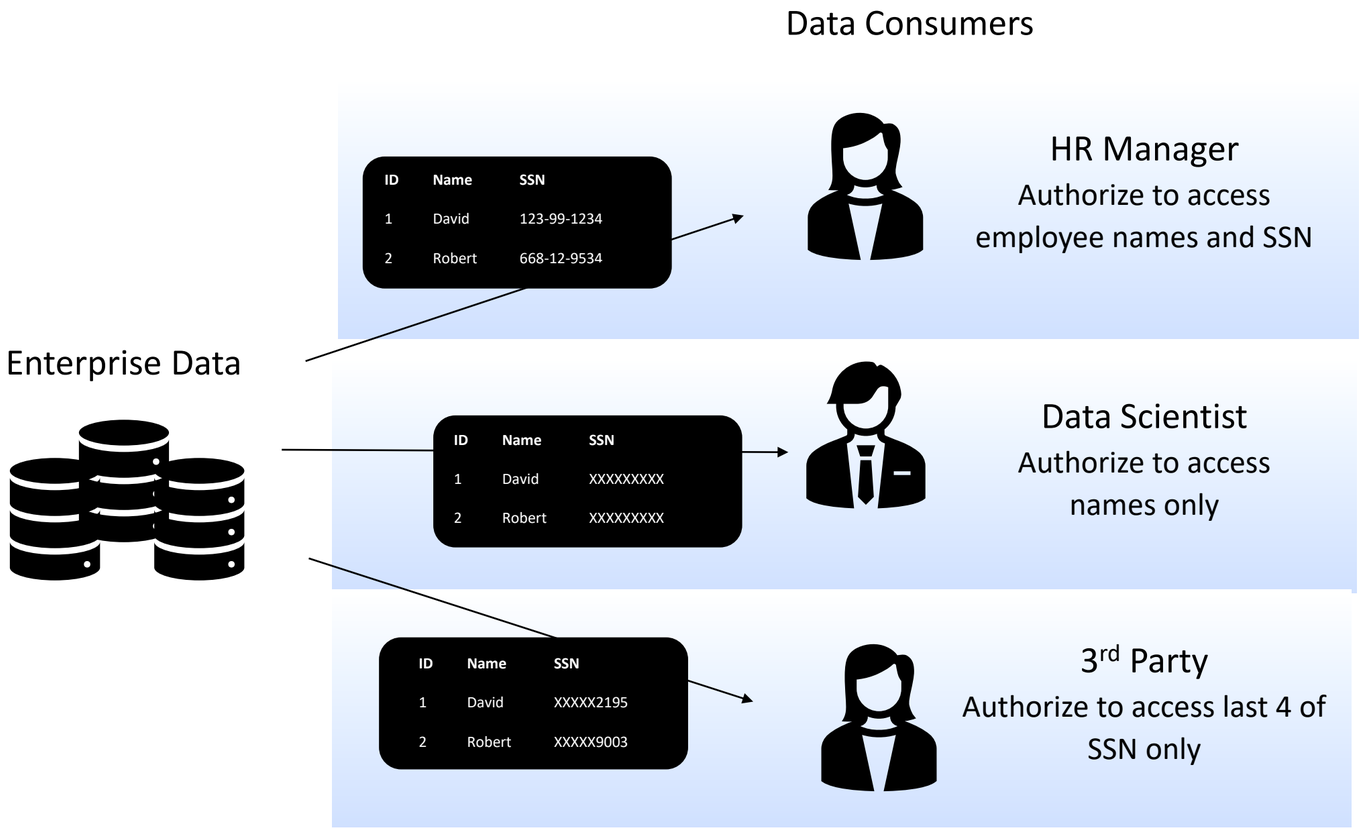
動態的資料安全保護機制

即時查看資料存取活動同時保護敏感資料

單一視角的資料活動 (Centralize Visibility)
將資料存取、使用、修改和移動的活動集中到一個平台上進行統一監控和管理提供清晰、即時的資料使用狀況

提供精細的資料層級存取控制 (Access Control)
基於規則的策略操作，以監視、記錄、報告和警告未經授權的資料存取，並適時實施即時控制，例如阻止(Block)和編輯(Redaction)。

持續性的安全政策保護 (Enforcement)
在系統中持續執行預定義的安全政策，確保資料和資源在存取與使用過程中始終符合組織的安全要求和標準。



確保適當的使用者能夠存取適當等級的細粒度資料。

資料威脅的偵測與回應

利用先進的資料安全分析技術幫助威脅優先排序，同時能根據活動狀態進行威脅調查與回應

主動式的威脅分析 (Active Threat Analytics)

每小時監測批量資料的三種不同分析視角

異常值挖掘
Outlier Mining

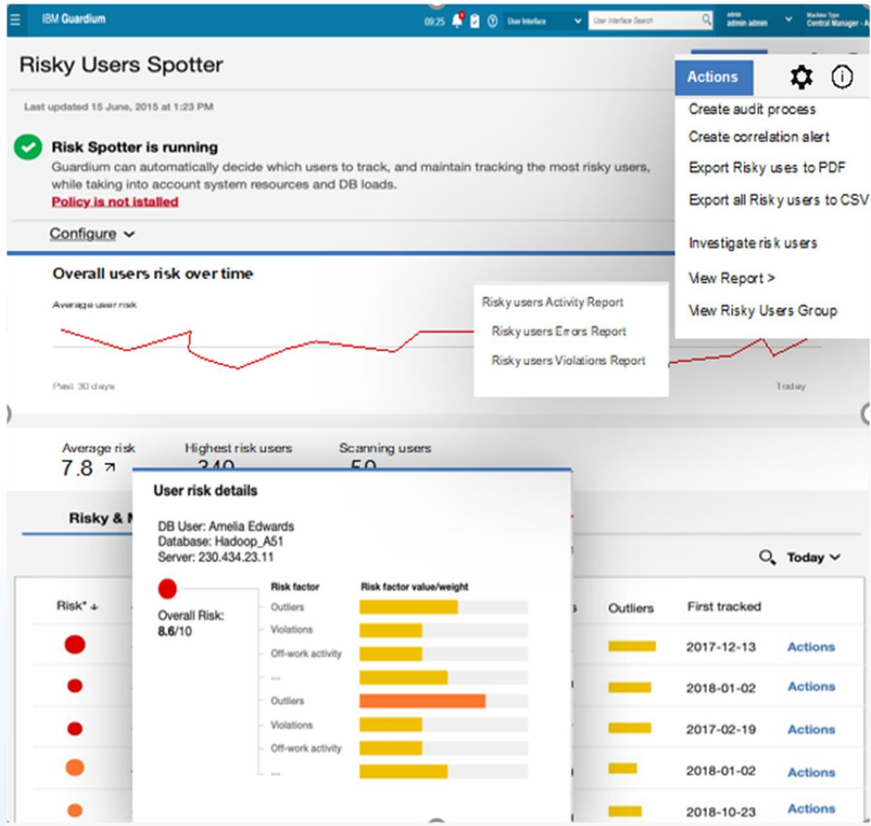
尋找行為異常的統計異常值

威脅診斷
Threat Diagnostics

尋找已知攻擊症狀的違規行為

主動發現威脅
Threat Finder

尋找具體政策違規並建立案例



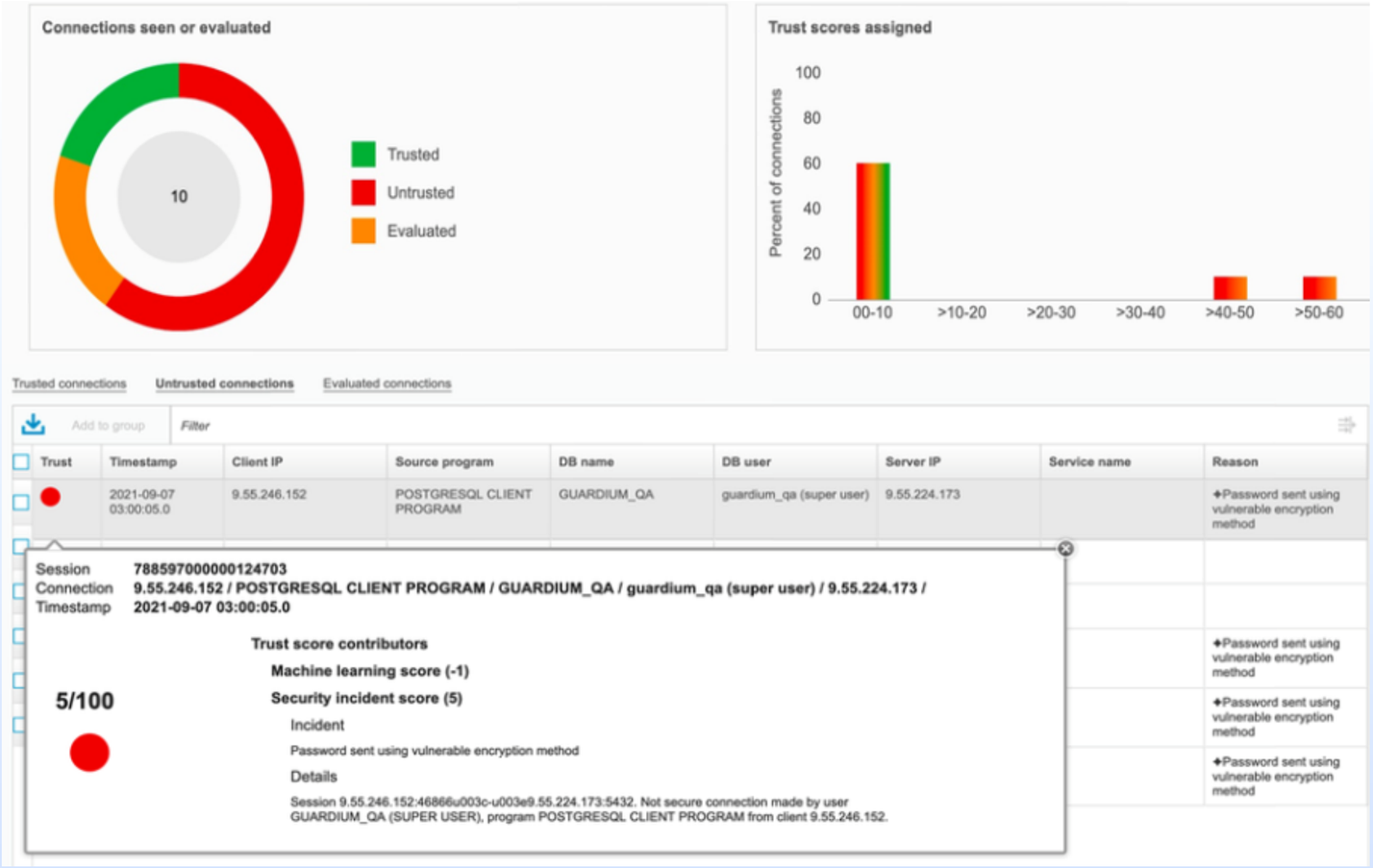
風險觀測員 Risk Spotter

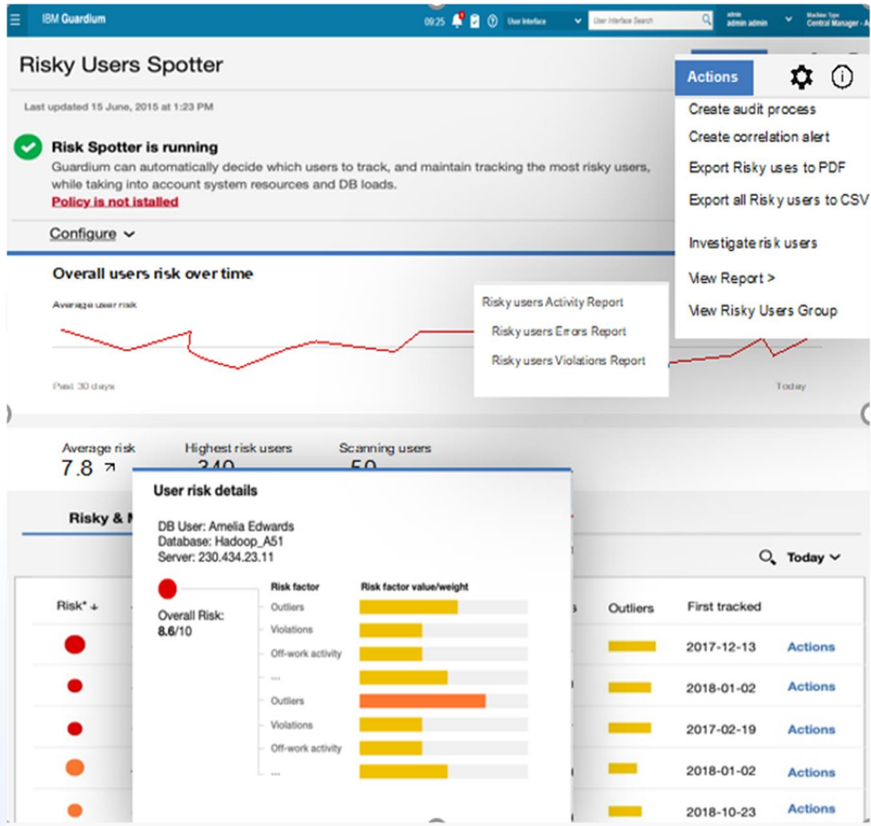
First of its kind technology

採用智慧演算法自動評估風險因子、使用者風險分析、動態採樣

資料威脅的偵測與回應

利用先進的資料安全分析技術幫助威脅優先排序，同時能根據活動狀態進行威脅調查與回應





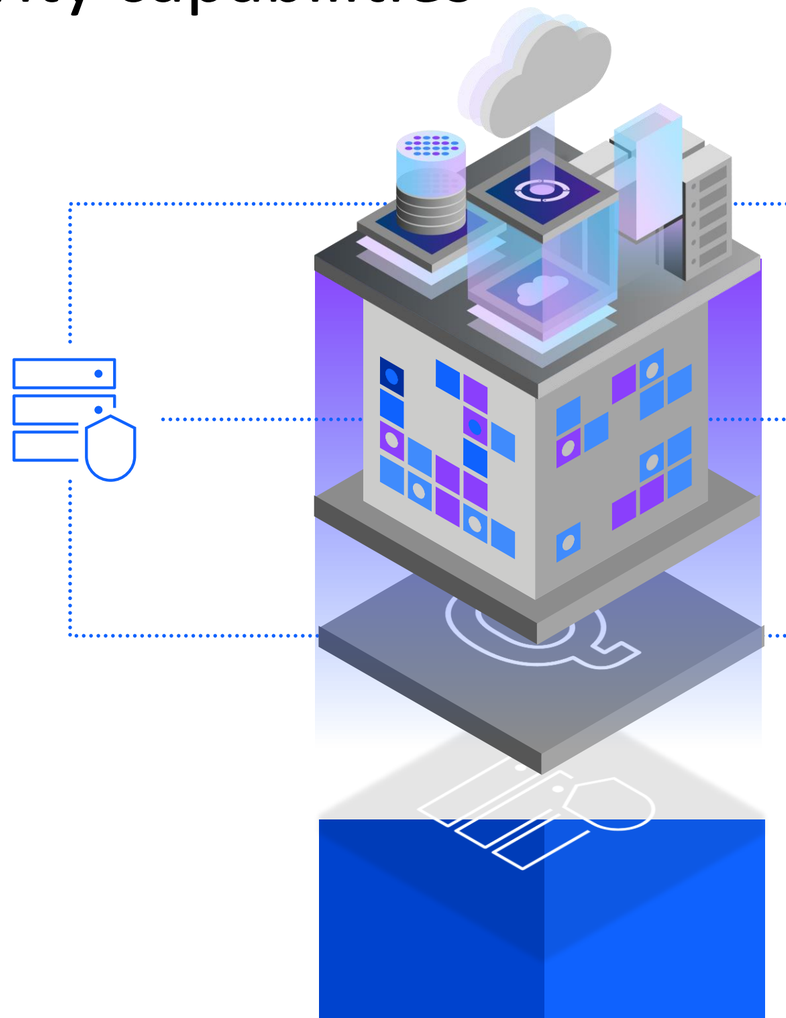
風險觀測員 Risk Spotter

First of its kind technology

採用智慧演算法自動評估風險因子、使用者風險分析、動態採樣

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**

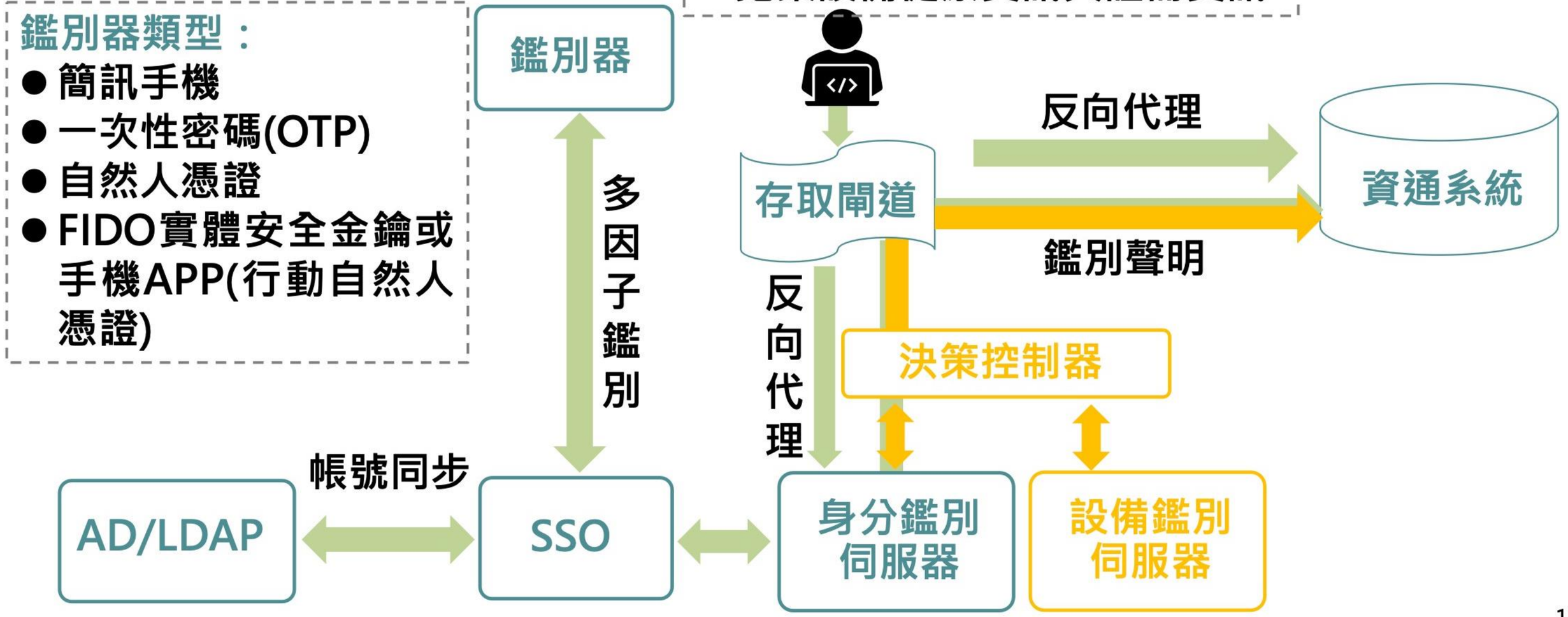
透過量子安全加密技術和金鑰管理機制保護關鍵數據。

政府零信任架構- 身分鑑別與設備鑑別

國家資通安全研究院
National Institute of Cyber Security

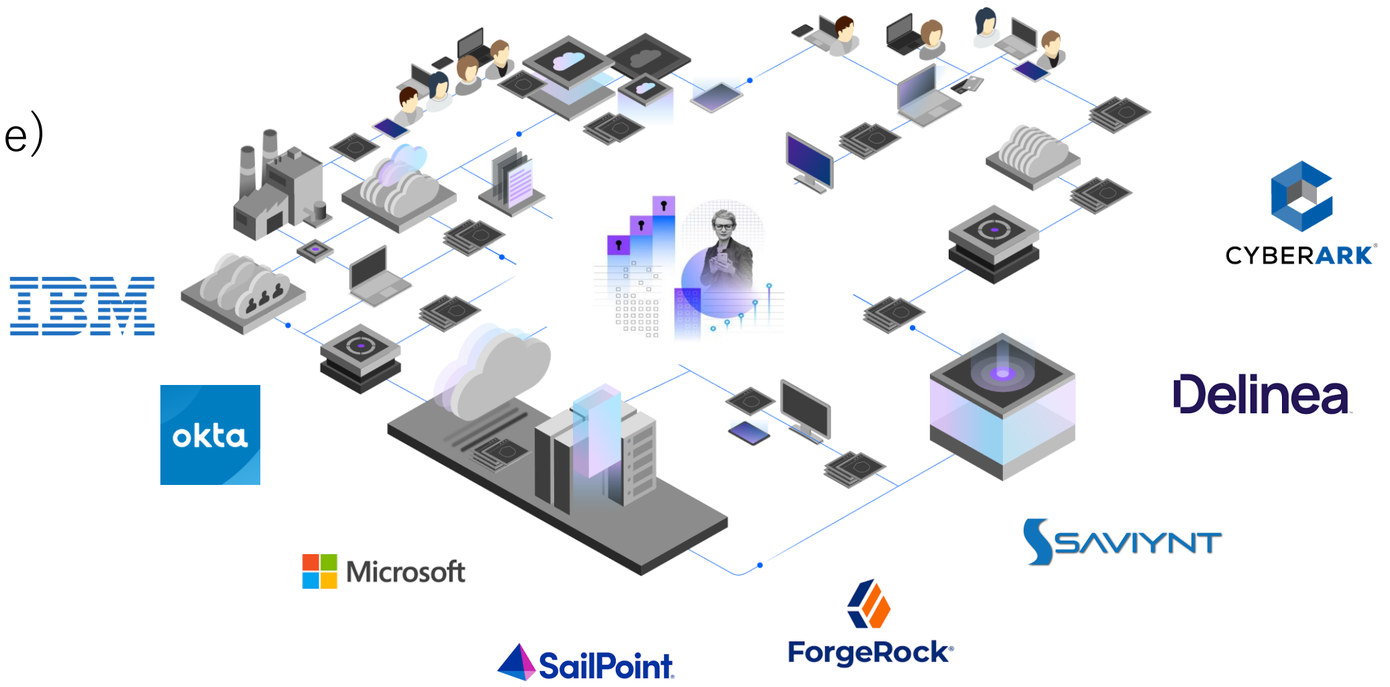
使用端設備：
- 安裝代理程式
- 蒐集設備健康資訊與註冊資訊

鑑別器類型：
- 簡訊手機
- 一次性密碼(OTP)
- 自然人憑證
- FIDO實體安全金鑰或手機APP(行動自然人憑證)



透過銜接、強化各個身份系統最大化投資成本效益
Maximize return of your current IAM investments while filling the gaps in your Identity Fabric

- 身份目錄 (Directory)
- 身份治理 (Governance)
- 存取管控 (IAM)
- 特權存取 (Privileged Access)
- 傳統應用系統群 (Legacy Apps)

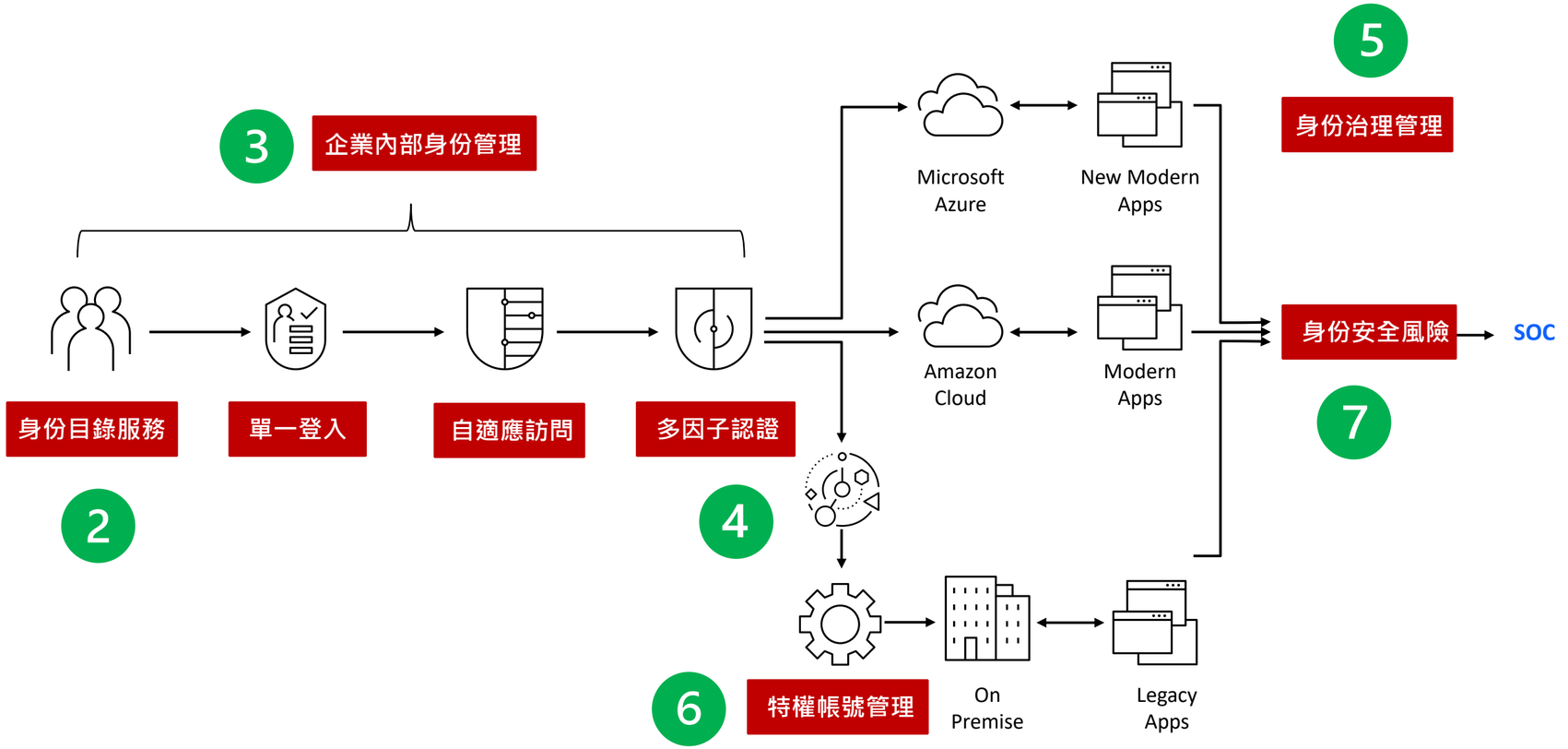


80%
的企業使用 2 個
或更多身分提供者

$1.5M
更換 IAM
解決方案的典型成本

身份織網 (Identity Fabric)

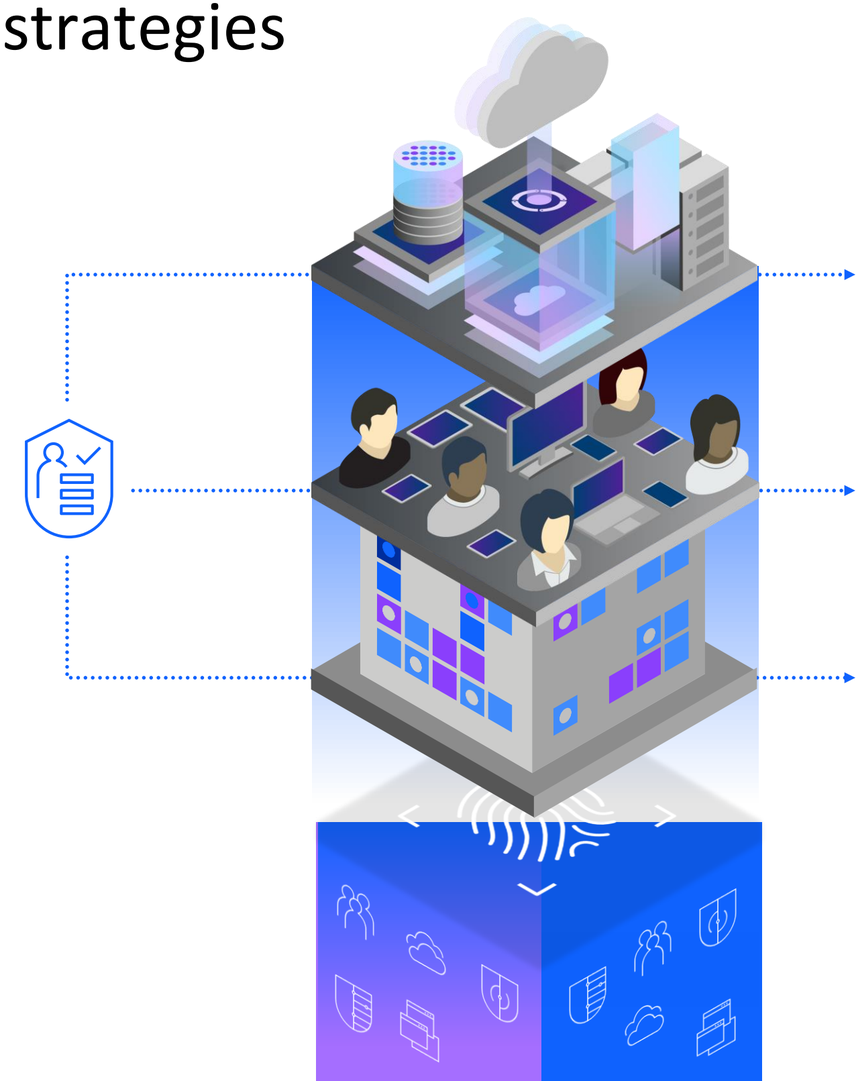
1. 整合既有身份安全工具
   (Orchestrate & Integration)
2. 集中化獨立的身份目錄
   (Consolidation)
3. 基於風險的身份認證
   (Risk-based authentication)
4. 強化傳統系統身份認證機制
   (Strength Legacy Apps)
5. 確保帳號生命週期治理
   (Governance)
6. 納管特權用戶帳號活動
   (Privileged User)
7. 身份安全風險的即時監控
   (Identity Posture)



1 身份、用戶與安全的統一性整合與自動化編排

現代化身份安全解決方案與保護策略
Modern identity security solutions and protection strategies

身份
織網
Identity
Fabric



混合雲擴增
Hybrid cloud adoption

數位轉型
Digital transformation

人工智慧
Artificial Intelligence

1 全面性的涵蓋

透過整合政策、決策和行動，提供流暢且一致的使用者體驗。

2 簡易與自動連接

採用開放標準與通用連接器，整合連接各項資訊系統，促進身份存取拓展與整合。

3 兼容強化既有工具

整合現有身份孤島並強化傳統應用程式落差，盡可能保存當前投資，同時建立有效的身份織網。

IBM Security Guardium Data Protection (GDP)

IBM 業務代表 Andy

現況需求與痛點

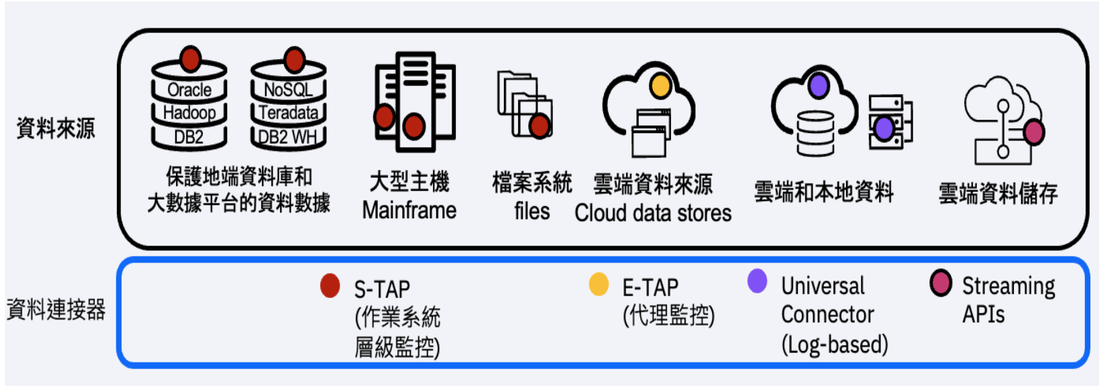
保護 (Protection) → 確保所有資料免遭未經授權的訪問
合規 (Compliance) → 使組織能遵守政府法規和行業標準

1. 相關法規與規範

- **ISO 27001** - A.9.4.4 監控敏感資料的存取與使用情況,
  A.18.1.4 定期稽核資料處理活動並生成合規性報告,
  A.9.1.2 防止未授權的資料存取
- **ISO 27001:2022 轉版** –
  A.8.11 Data masking (資料遮罩),
  A.8.12 Data leakage prevention (防範資料洩漏)
- 個人資料保護法
- 資通安全管理法 - 責任等級分級要求資料存取保護與稽核記錄管理
- 教育部資安專章檢核指標 - 內部資安稽核, ISMS相關認證
- 教育部113年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫 – 項次8.資料庫安全檢測

2. 本機資料庫稽核 (Native Auditing) 挑戰

- 資源利用率高 - 通常消耗 10% 到 12% 伺服器 CPU
- 無法實現職責分離
  - 因必須從資料庫內部設定本機審核，導致特權帳號可以繞過稽核
  - 特權帳號需要額外的活動監控，因可以逕行存取資料庫
- 資安稽核的不一致性
  - 每個資料庫系統都有獨特的記錄與稽核資料庫活動方法
  - 統一資料活動風險報告變得困難甚至不可能



產品特色

- 節省合規成本 - 使用者完整行為監控
- 防止資料外洩 - 存取規則(SQL Statement), 外洩規則(Returned Data), 異常規則 (SQL Error / Login Fail)
- 確保資料隱私 - 大量敏感性資料庫操作稽核, 存取連線
- 識別資料風險 - 異常存取與異常登入

ISAC 校園團購買一送一限時專案（優惠期限：即日起～2025/03/13止）

IBM Guardium 資料庫監控暨記錄軟體 (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