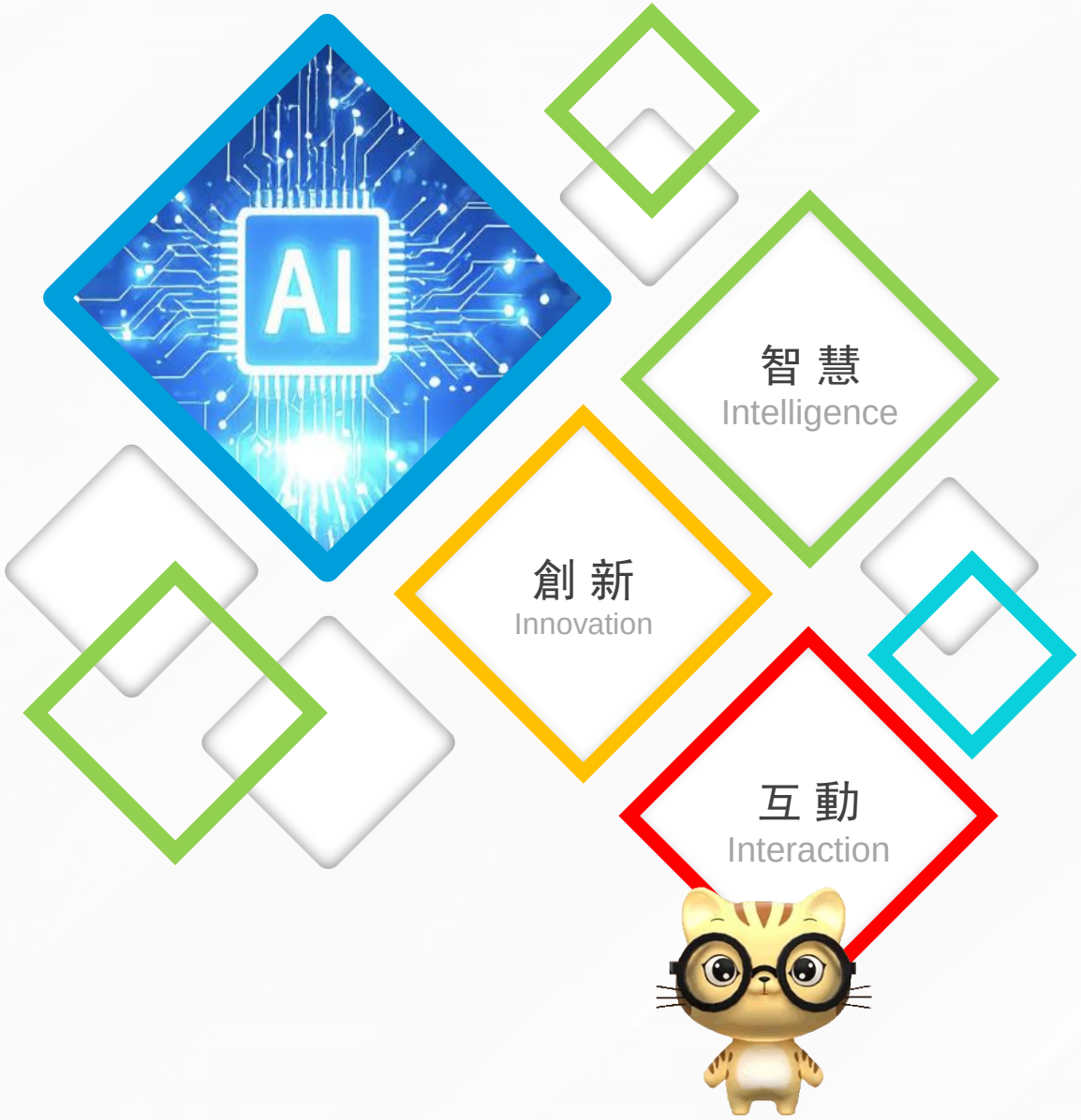
AI校務知識中台
主權資料應用

黃繹呈 Eason Huang
Ai3 co. 導入顧問

2026.04.24



Agenda

高等教育Top 10 issue

資料治理讓「AI 走向數據」

主權資料的雲地架構選擇

知識中台核心的應用案例

2026 EDUCAUSE Top 10 IT資訊議題

1. 協作式網絡安全

Collaborative Cybersecurity

2. AI 的人性化

The Human Edge of AI

3. 營運與財務洞察的數據分析

Data Analytics for Operational and Financial Insights

4. 打造全校性的數據中心文化

Building a Data-Centric Culture Across the Institution

5. 知識管理助力安全 AI

Knowledge Management for Safer AI

6. 新技術的審慎評估方法

Measured Approaches to New Technologies

7. 未來職場的技術素養

Technology Literacy for the Future Workforce

8. 從被動應對轉為預主動決策

From Reactive to Proactive

9. AI 驅動的效率與成長

AI-Enabled Efficiencies and Growth

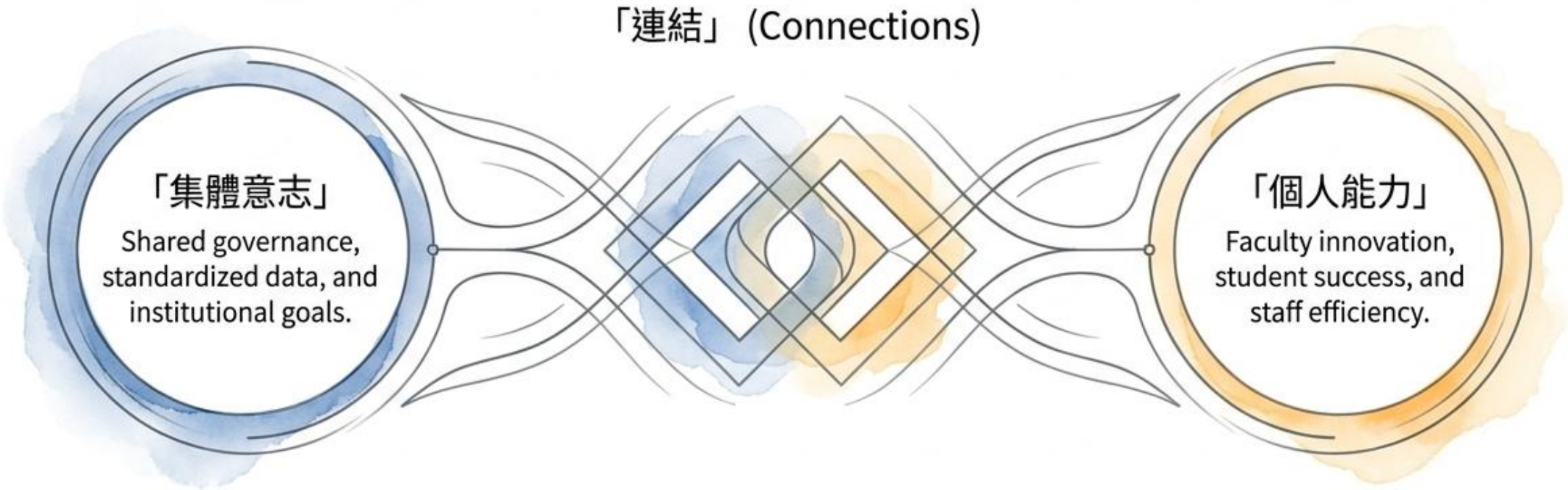
10. 決策者的數據技能與素養

Decision-Maker Data Skills and Literacy

The Voice of the Higher Education Technology Community
EDUCAUSE REVIEW

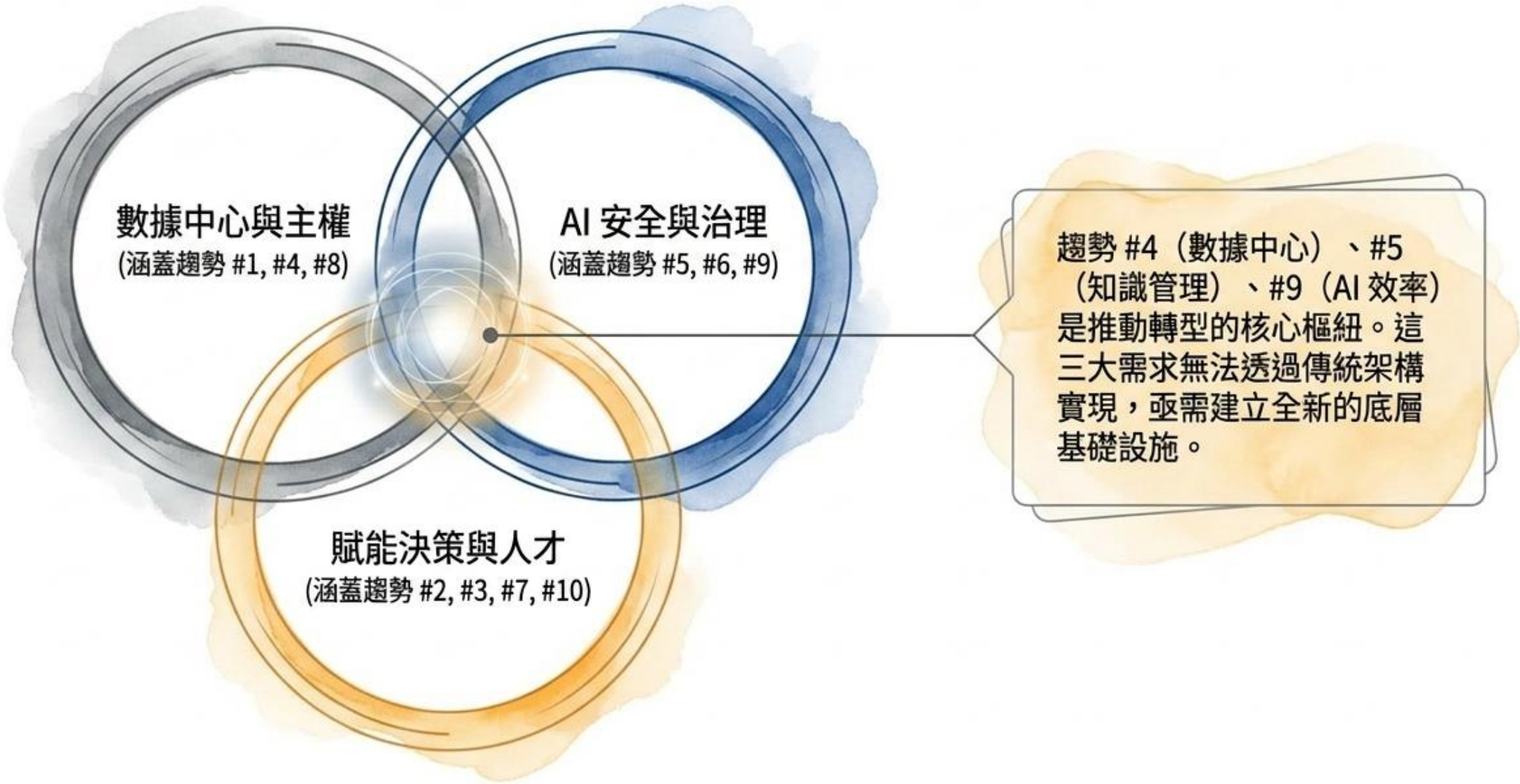
2026 EDUCAUSE Top 10: Making Connections

高教挑戰的解方：凝聚集體意志與賦能個人能力

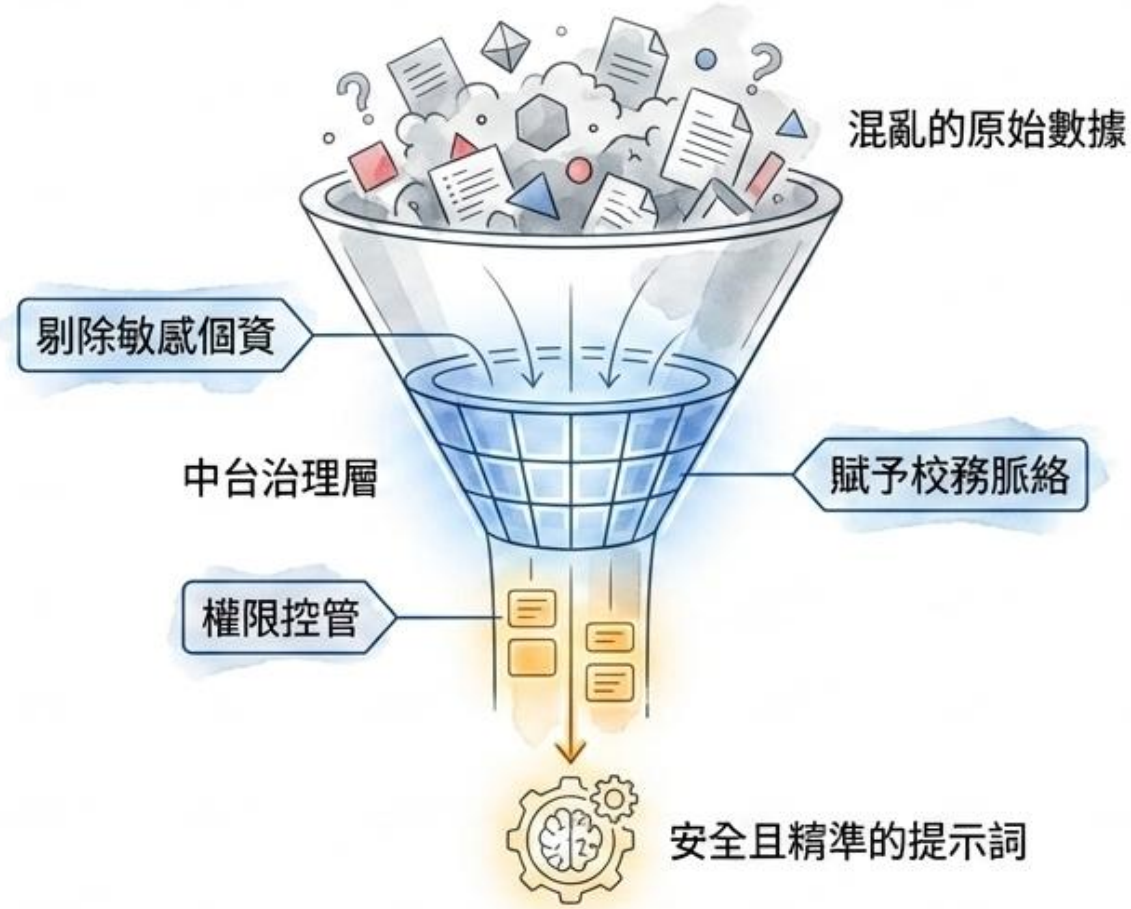


- EDUCAUSE 2026 核心精神指出：面對預算緊縮與技術顛覆，單點式的科技導入已經失效。
- 未來的韌性建立在「人與人」、「數據與系統」的深度連結。唯有打破孤島，才能在動盪的世代中前行。

2026 關鍵趨勢的戰略收斂：三大核心支柱

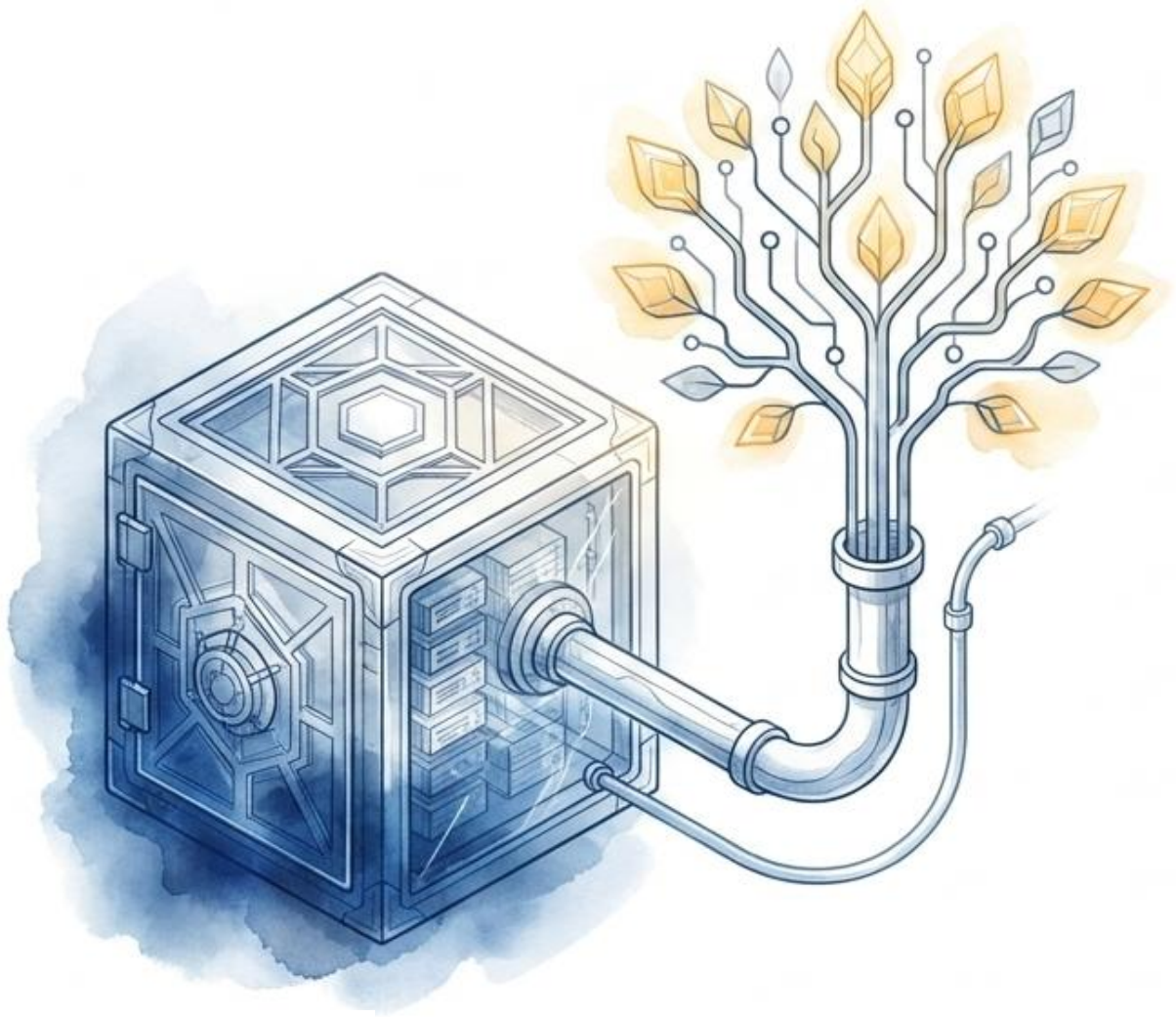


透過知識管理過濾風險，確保 AI 安全輸出 (趨勢 #5)



沒有優質的知識管理，就沒有企業級的 AI 安全。中台扮演資料守門員的角色，確保校園 AI 既懂學校的歷史與脈絡，又不會逾越隱私紅線。

掌握主權資料，奠定全校數據文化與資安聯防 (趨勢 #1, #4)



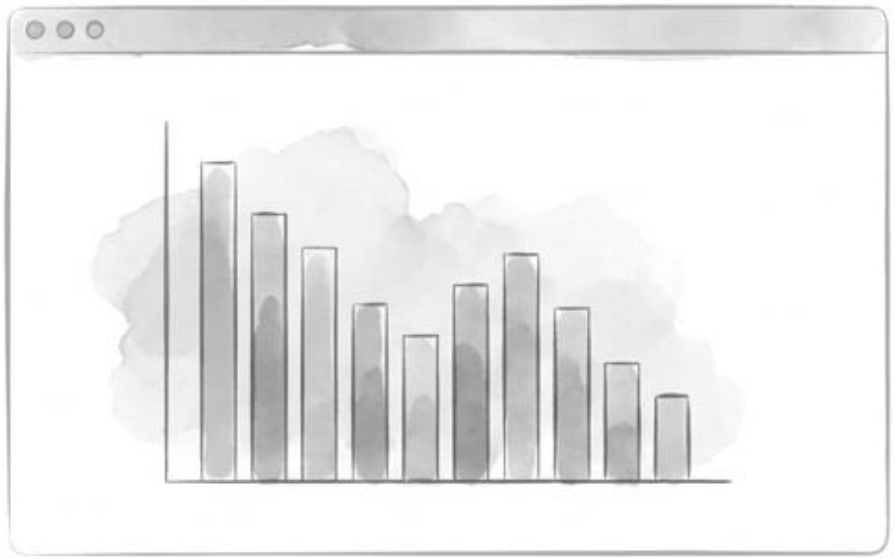
主權資料 (Sovereign Data) 的戰略意義：
將數據的所有權與脈絡牢牢掌握在校方手中，而非分散於外部 SaaS 廠商。

協作式網絡安全：
集中治理的數據中台能大幅降低攻擊點，實現真正的校園資安聯防。

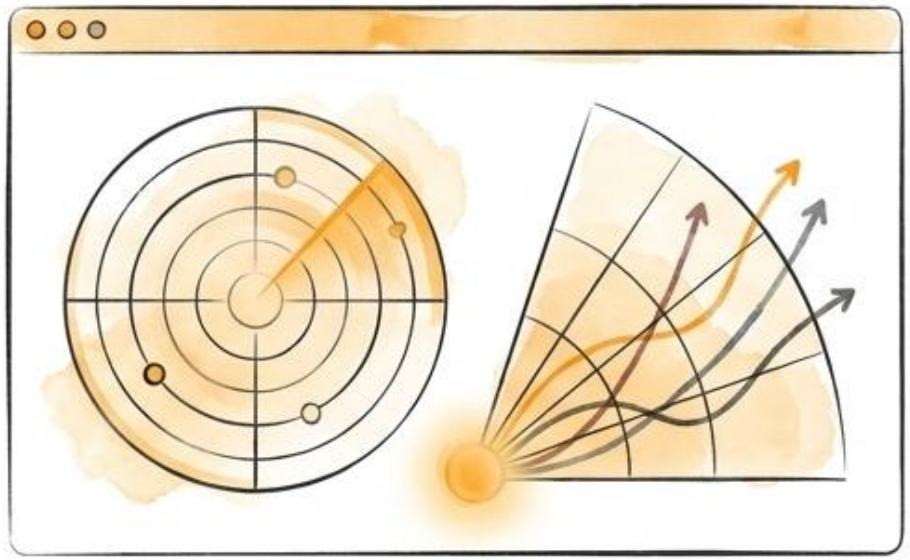
數據中心文化：
當資料安全無虞且易於存取，數據將不再只是 IT 部門的專利，而是全校教職員共有的戰略資產。

從後視鏡到雷達：由被動應對轉向主動預測 (趨勢 #8)

歷史報表 (Rear-view mirror)



情境模擬與預測 (Radar/Headlights)



- 面對招生與財務的雙重挑戰，學校不能再蒙眼飛行。
- 知識中台提供高品質的主權資料，讓校務研究 (IR) 從單純的「描述過去」，進化為「預測未來與情境模擬」，大幅提升大學的敏捷性。

將複雜數據轉化為高階主管的決策武器 (趨勢 #3, #10)

沒有數據識讀能力，資料毫無價值。

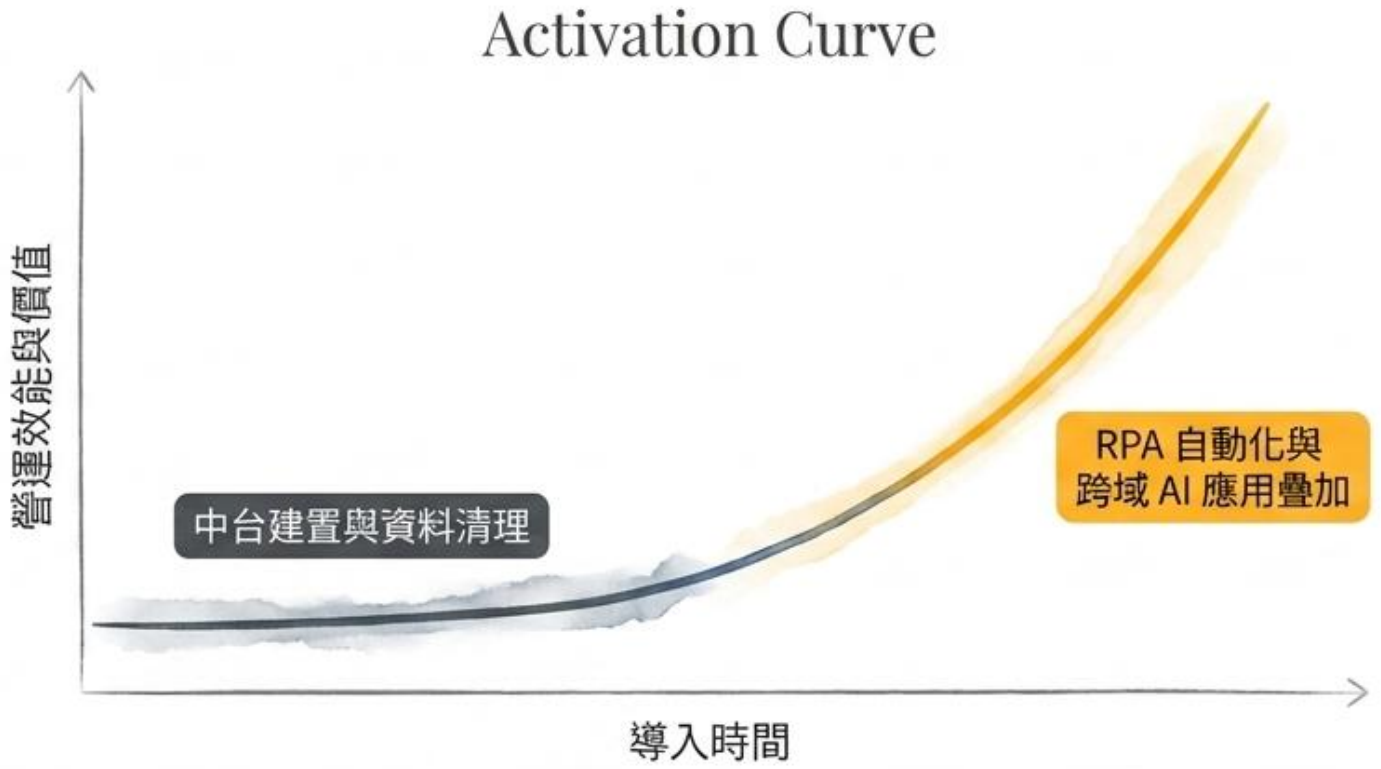
知識中台肩負繁重的數據清理工作，為決策者提供最直觀的財務與營運洞察。讓主管無需成為 IT 專家，也能精準解讀數據，制定攸關存亡的資源分配策略。

打造安全的校園 AI 沙盒，培育未來職場人才 (趨勢 #2, #7)

科技素養與就業準備：
2026 年的職場高度依賴 AI 技能。

安全的實踐場域：
透過中台治理，校園系統本身即成為師生最安全的 AI 實驗室。讓師生能在受保護的環境中，培養批判性思維與真實世界的數位素養，賦能未來。

審慎評估技術投資：短期建置換取指數型回報 (趨勢 #6)



拒絕「頭痛醫頭」的短期 SaaS 採購陷阱。

雖然初期需要投入時間梳理基礎架構，但隨著中台穩固，後續開發的每一個 AI 應用與自動化流程，都將帶來邊際成本遞減、效益呈指數型成長的長遠回報。

重新定義校園架構：傳統孤島 vs. 知識中台

評估維度	傳統離散式 IT 架構	AI 知識中台架構
資料所有權	依賴外部廠商，資料四散	校方 100% 掌握主權資料
AI 導入風險	影子 IT 氾濫，具洩密風險	集中治理，無幻覺與資安疑慮
決策速度	耗時的跨部門資料索取	即時、跨域的視覺化洞察
投資回報	購買單一工具，效益無法累積	底層建置一次，上層應用無限延伸

資料治理讓「AI 走向數據」

在傳統架構中，習慣「數據走向應用」，將資料匯入各種服務應用。但在 AI 時代，數據量大且極度敏感，將使搬遷成本與風險指數級增長。

發展可信任AI智慧決策應用

異質資料來源 | 資料收容治理 | 集中化知識/決策中心 | Multi-AI agent

MES
HIS
ERP
CRM/CDP
POS
SCM

整合數據

結構/非結構

ORACLE Microsoft SQL Server TERADATA
MySQL mongoDB MariaDB PostgreSQL

Database / Storage

Relational Graph Blockchain Text XML JSON

Multi-Dimensional OLTP Data Warehouse Data Lake Machine Learning Real-Time Analytics

ORACLE AI Database 26ai

資料治理 AI{Fusion} 萃取高品質訓練資料

Business intelligence

Knowledge Platform

開發治理 Qbi GPT 符合AIMS之管理開發平台

行銷互動
客戶服務
人資助理
成長教練
個案管理
特助幕僚

AI治理 Qbi Agents 滿足多元領域應用之AI代理人服務

互動資料匯流

持續強化回饋

客戶服務AI應用發展平台

領域應用

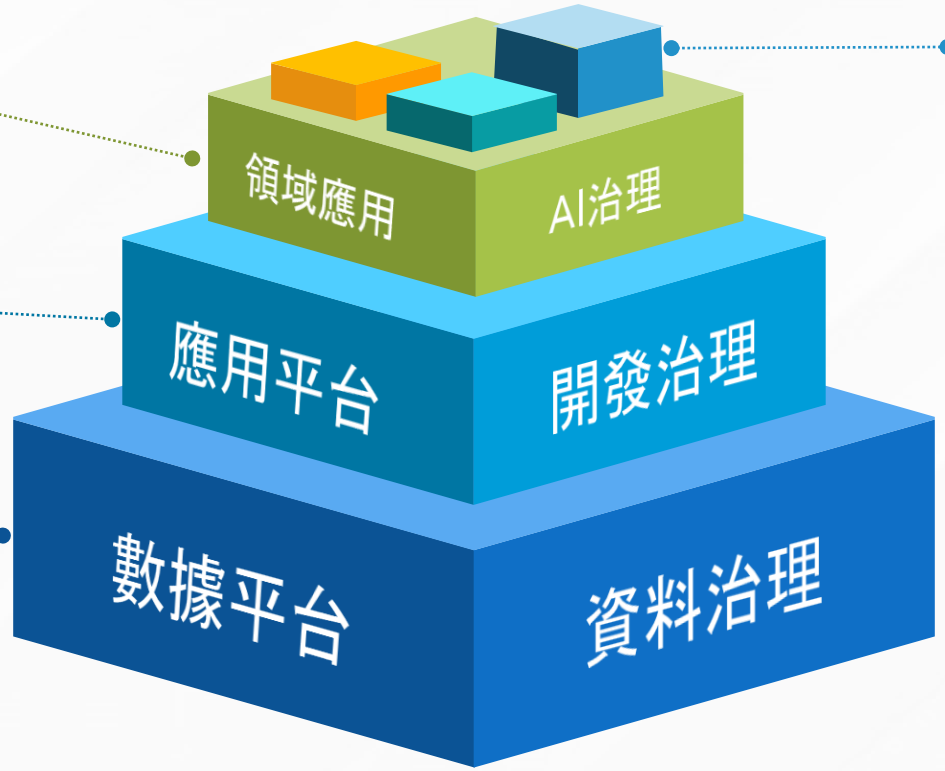
各領域應用,
互動AI、服務AI、效率AI

AI、CRM、KM

AI Agent應用發展平台

民眾數據+政務知識

結構化資料 / 非結構化資料



AI應用領域

智慧政府、智慧醫療、行銷科技、
金融科技、政府與公共服務等...

政府與公共服務

1988普發現金
中華民國法務部
行政院人事行政總處
1999市民專線(新北、桃園、台中、台南、高雄)
台灣自來水1910
台灣中油
台灣電力公司
台灣高鐵

以客戶服務互動為例：設計領域全方位AI智慧應用

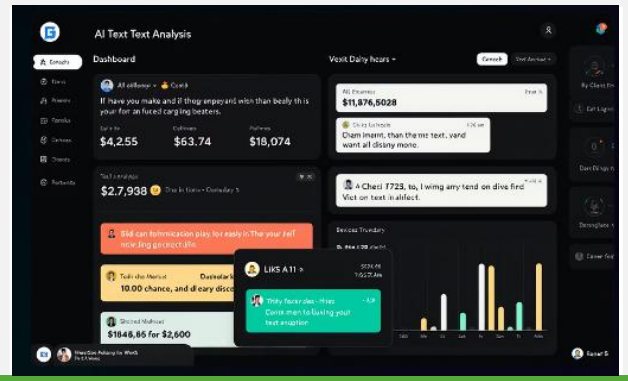
Interaction AI

智慧語音與機器人

QbiBot GPT　QbiBot GPT+　QbiBot Agent

1. AI機器人
2. AI服務機器人、AI行銷機器人
3. 語音導航AI客服
4. 智能語音核身
5. AI電銷 & AI電訪
6. AI Agent AI助理

Service AI



AI客服

QbiCRM GPT

1. QbiCRM 語音/文字客服
2. 通話分析助理
3. 自動服務摘要、活動代碼、
4. 客戶特徵
5. 智慧對話資訊登錄與引導
6. AI質檢-個人質檢、場景質檢

Workforce AI

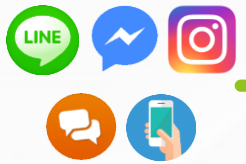
知識中台、人力輔助與訓練類

QbiCRM GPT

1. QbiCRM 知識中台
2. Qbi助理 AI助手
3. AI Mentor 培訓師
4. 瑕疵檢測、預修保養
5. 產品配方
6. 員工作業整合

每個企業都需要AI賦能

智慧民眾經營中心



QbiBot Agent

1 AI 服務機器人

API 系統查詢

資訊服務系統

1 AI 行銷機器人

產品知識

服務知識

6 員工助理

單位同仁

知識對話

問題諮詢

客服作業平台

真人客服中心

2 AI知識中台，企業CRM

對練培訓

5 人員培訓師

知識貢獻

通報陳情、自動派工

二線問題處理

3 對話分析助理

4 質檢管理師

顧客

FAX

QbiCRM GPT

AI機器人
應對顧客服務、行銷、辦理

知識中台/企業CRM
輔助客服人員及員工助理

對話分析助理
服務要項、通話摘要、發現商機

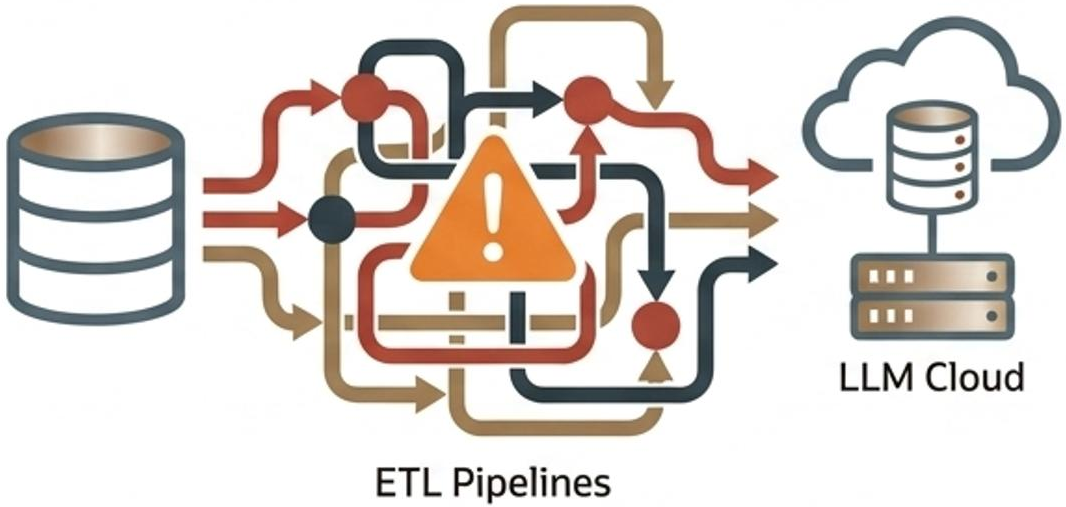
質檢管理師
服務品質檢驗，發現異常

人員培訓師
知識培訓、機器對練

員工助理(Qbi助理)
經驗傳承、人機協作、完成作業

架構升級：僅需維護單一資料庫

傳統架構 (Move Data to AI)



需建置繁瑣 ETL 管道，資料重複儲存。
痛點：同步延遲、資安斷點、合規風險飆升。

Bring AI to the Data

機器學習與大語言模型整合於資料庫內執行。
價值主張：零資料搬運 = 零延遲 + 零外洩風險。

主權資料的雲地架構選擇

根據「資料敏感度」與「使用流量頻率」動態調整的混合架構

非機敏、大流量的任務：公開課程檢索、校園導覽

核心機敏資料： 學生輔導紀錄、未公開的研究成果

APPLICATIONS

MODELS

INFRASTRUCTURE

CHIPS

ENERGY

CHATBOTS

DIGITAL BIOLOGY

ROBOTAXI

ENTERPRISE AI AGENTS

SCIENCE

ROBOTICS

MANUFACTURING

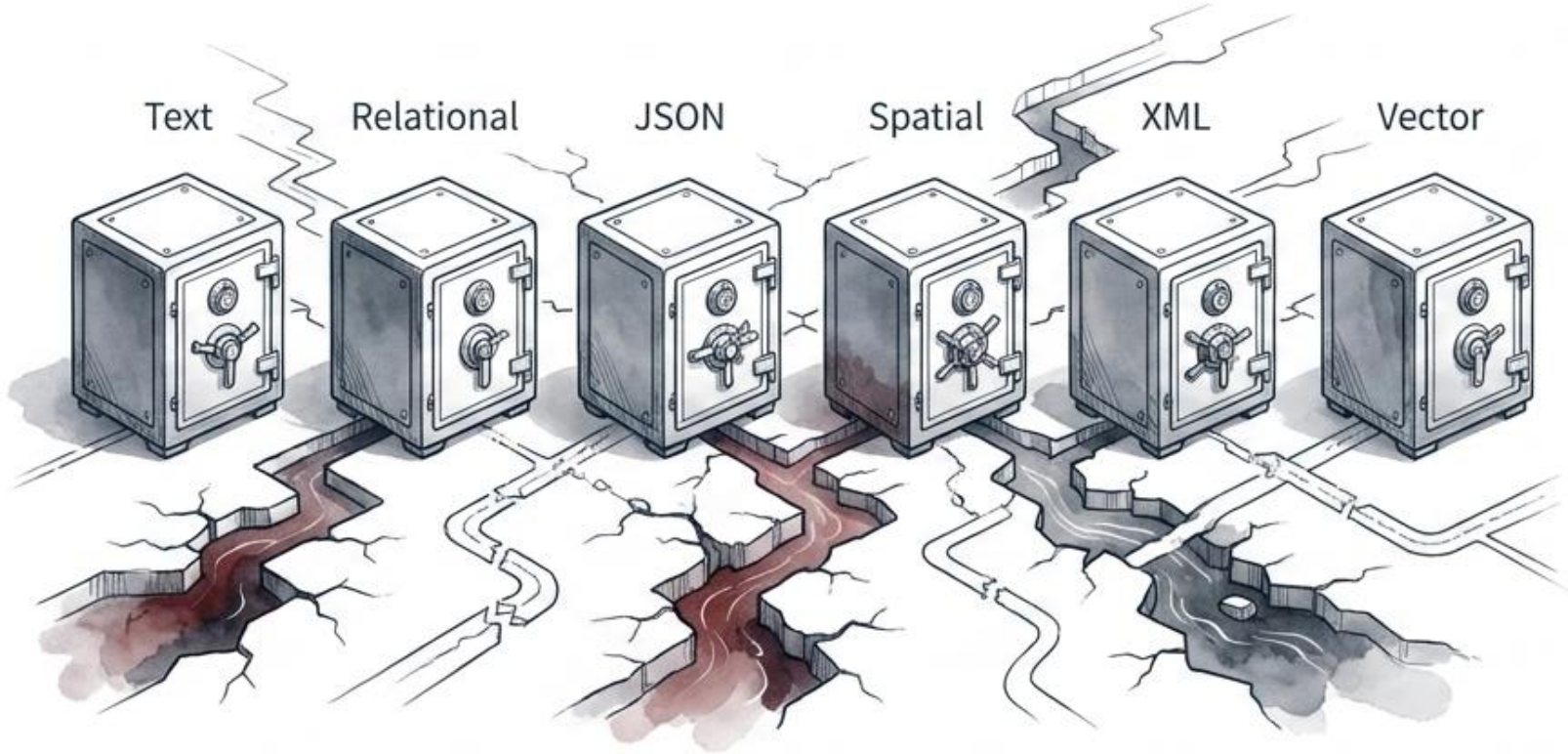
AI CODER

LLM | VLM | VLA | MMLLM | GPT

DM | GNN | MOE | SSM | LBM

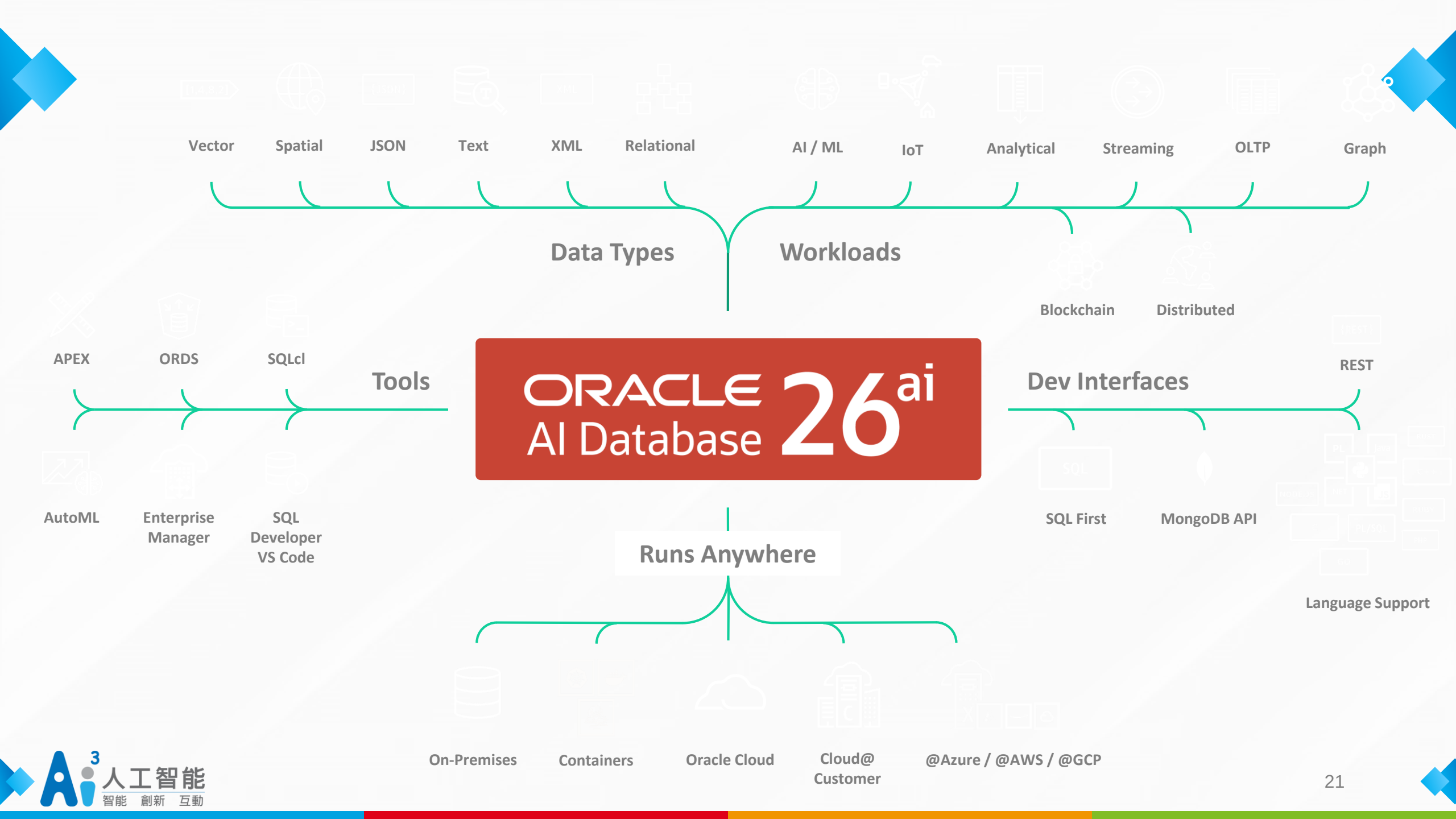
AI FACTORIES

現代數據挑戰：打破資料格式的孤島

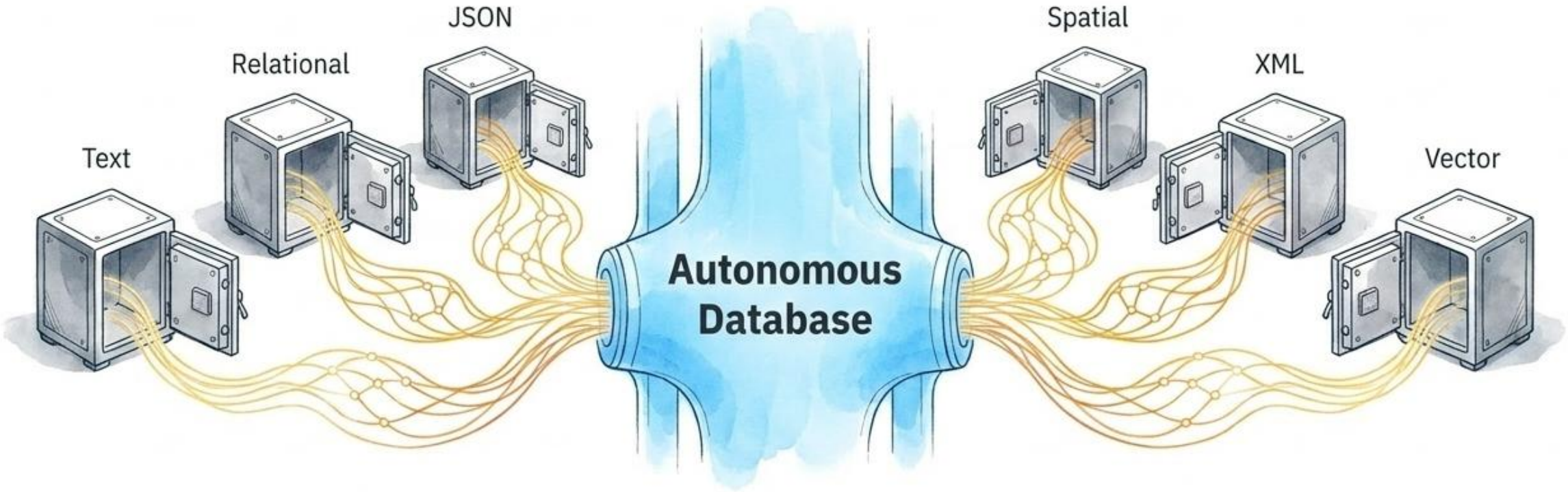


現狀的困境

當資料庫因格式不同而各自為政時，即使引入最先進的 AI 模型，也無法跨域調用完整上下文，嚴重削弱 AI 的分析與自動化能力。


Vector
Spatial
JSON
Text
XML
Relational
AI / ML
IoT
Analytical
Streaming
OLTP
Graph
Data Types
Workloads
Blockchain
Distributed
APEX
ORDS
SQLcl
Tools
ORACLE AI Database 26ai
Dev Interfaces
REST
AutoML
Enterprise Manager
SQL Developer VS Code
SQL First
MongoDB API
Language Support
Runs Anywhere
On-Premises
Containers
Oracle Cloud
Cloud@ Customer
@Azure / @AWS / @GCP

單一引擎的極致融合：化孤島為數據中台



將零散的 Text、Relational, JSON, Spatial, XML, Vector
統一轉化為可被高效調用的企業資產，奠定 AI 應用的基石。

賦能開發者：建立靈活的創新生態

靈活的語言與 API

- MongoDB API
- REST
- SQL First

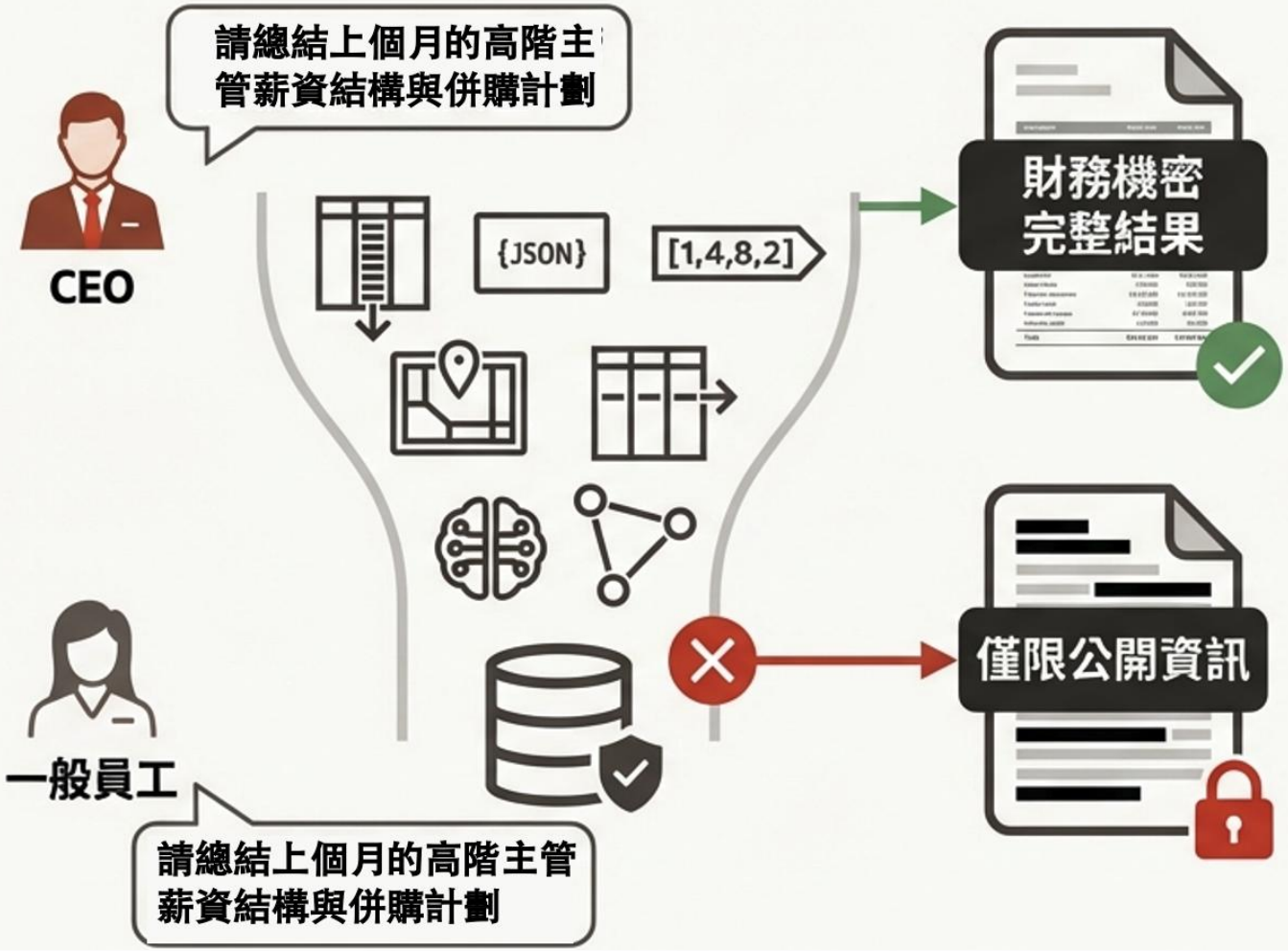
全方位的開發工具鏈

- APEX
- ORDS
- SQL Developer
- VS Code
- AutoML
- SQLcl
- Enterprise Manager

透過高度整合的介面，加速企業從資料到 AI 應用的開發週期。

防禦機制一：具備安全感知的向量搜尋 (Security-Aware Vector Search)

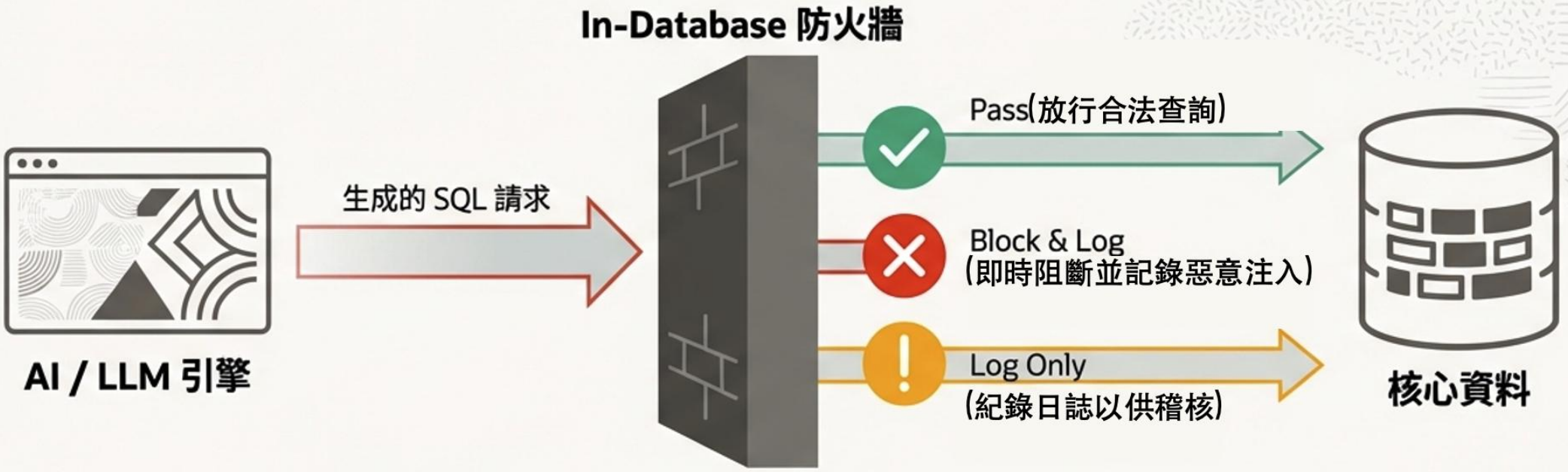
業界唯一：檢索增強生成 (RAG) 完全繼承資料庫既有權限。沒權限看，AI 就查不到。



- ✓ **無縫整合VPD與RLS：** AI向量查詢 (AI Vector Search) 自動套用Virtual Private Database (VPD)與Row-Level Security (RLS)策略。
- ✓ **動態權限識別：** 無論使用者是透過應用程式、SQL還是自然語言(Select AI)進行查詢，系統皆能精準識別其角色與授權範圍。
- ✓ **零信任RAG管道：** 在SQL內完成向量生成、檢索與LLM提示組合，確保所有的資料邏輯與安全控管都在單一、受保護的位置執行。

防禦機制二：內建於核心的 AI 專屬 SQL 防火牆 (SQL Firewall)

即時防禦 LLM 幻覺與惡意 Prompt 所帶來的新型態注入攻擊。



無法被繞過的底層防禦

- 不同於容易被攻破的中介層防火牆，Oracle SQL Firewall 深植於資料庫核心，監控所有連線路徑。

阻斷為授權行為

- 自動學習合規的SQL模式與連線特徵，一但偵測到異常、未經授權的SQL或資料隱碼攻擊，立即啟動防禦。

彈性處置機制

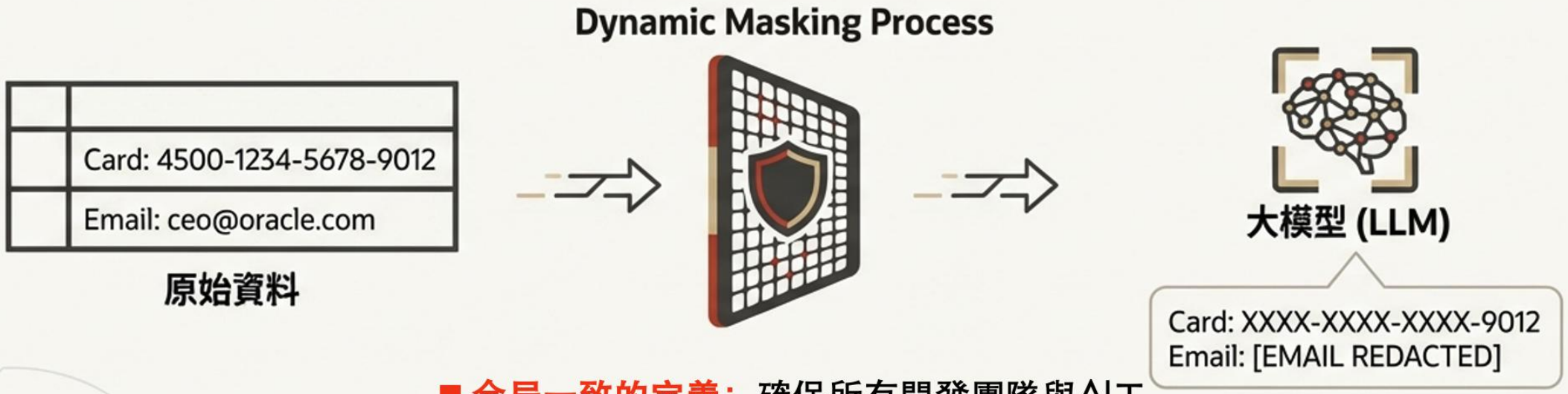
- [✓] Pass
- [✗] Block & Log
- [!] Log Only

防禦機制三：即時動態的資料遮罩與去識別化 (Data Redaction)

在提供給LLM之前過濾敏感資料，確保AI應用的絕對合規。

■ **資料域與註釋標記 (Data Domains and Annotations)**：直接在資料庫內對Email、信用卡號、個人身份資料(PII)進行語意標記。

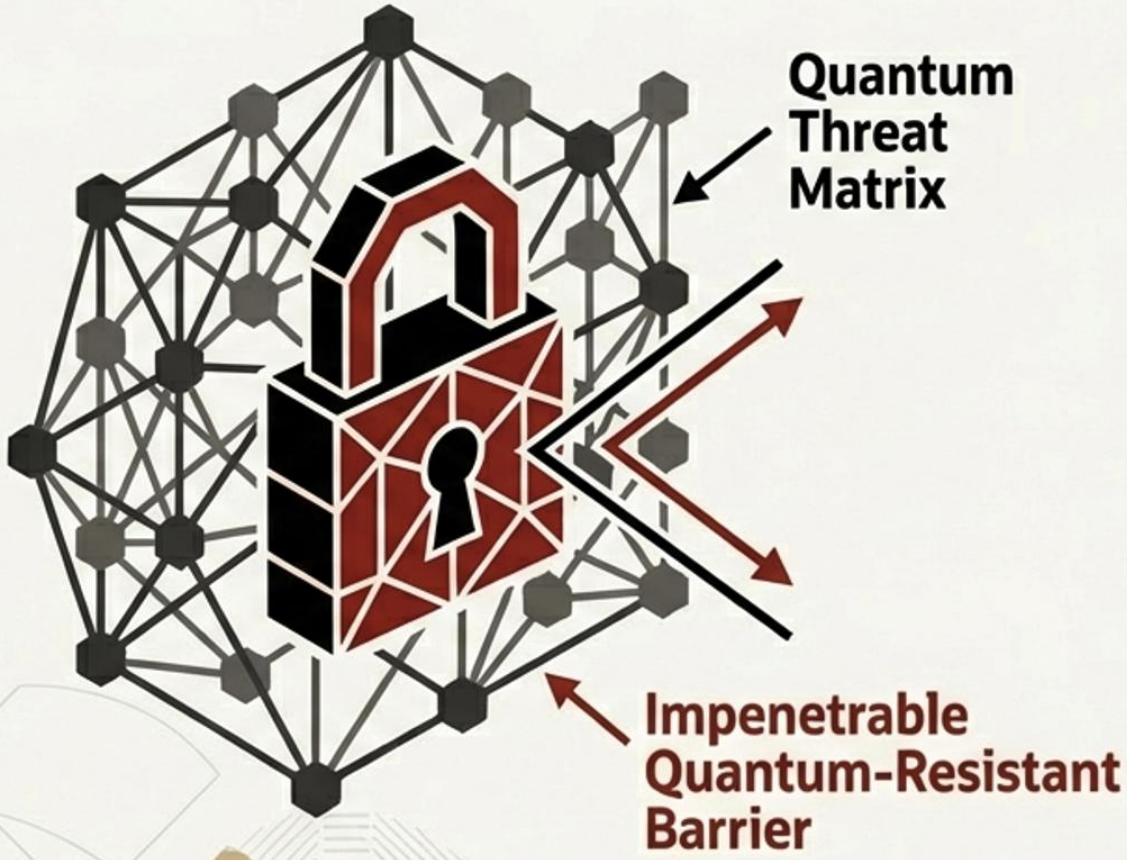
■ **動態遮蔽 (Dynamic Masking)**：在RAG檢索過程中，即時且動態地遮蔽PII與敏感字串。



■ **全局一致的定義**：確保所有開發團隊與AI工具對敏感資料的理解與處理方式完全一致，加速安全的AI應用程式開發。

防禦機制四：超前部署的抗量子加密 (Quantum-Resistant Cryptography)

抵禦未來的「先竊取，後解密（Harvest Now, Decrypt Later）」威脅。



- **採用 NIST 核准標準**：領先業界導入如 ML-KEM 等美國國家標準暨技術研究院 (NIST) 核准的抗量子演算法。
- **全方位加密保護**：針對傳輸中 (In-flight) 與儲存中 (At-rest) 的敏感資料進行深度加密。
- **未來防禦就緒**：在量子電腦具備破解現有傳統加密技術的能力之前，提前為企業的無形資料資產建立堅不可摧的防護罩。

防禦機制五：確保資料主權的彈性部署與隔離 (Deployment Choice)

將企業級防火牆與硬體隔離帶入您的機房，滿足最嚴格的法規駐留要求。

雲端技術落地機房

✓ 透過Exadata Cloud@Customer，在企業實體防火牆的保護下安全交付Oracle AI Database的完整功能。

專屬區域 (Dedicated Region)

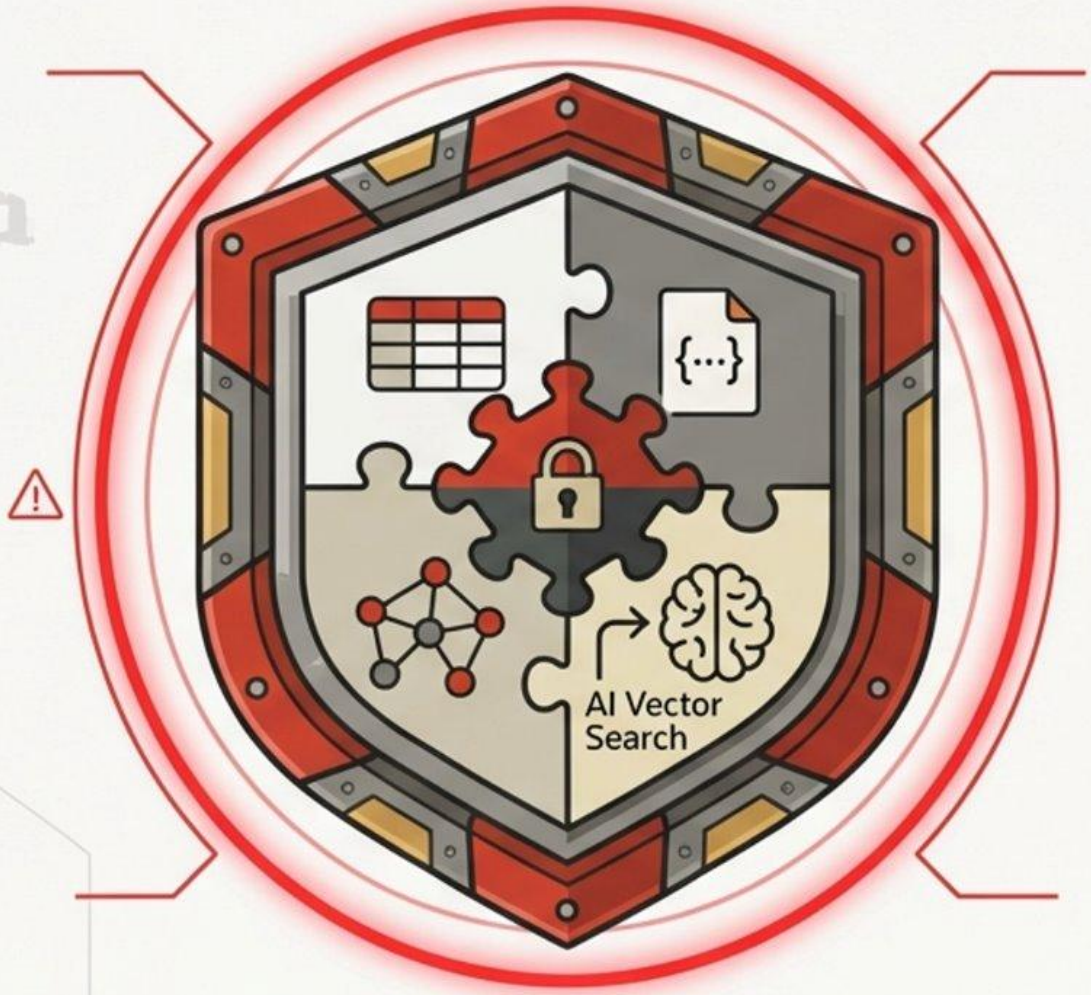
✓ 爲金融與政府等高度監管行業提供完全隔離的雲端基礎設施，確保資料絕對的主權與掌控力。

多雲策略 (Multicloud)

✓ 透過Oracle Database@X等方案，在您選擇的雲端環境中安全執行高效能的AI資料庫服務。

架構典範轉移：就地 AI 運算 (Bring AI to the Data)

從根本上消除傳輸風險，Oracle Database 26ai讓AI靠近資料，而非將資料送往AI。



原生安全的融合式資料庫 (Converged Database)：

- ✓ **數據絕對不離境**：AI與機器學習模型直接在資料庫內執行，無需整合多個第三方解決方案。
- ✓ **私有AI運行環境**：透過Private AI Services Container載入與執行AI模型，確保原始數據無需與外部服務商共享。
- ✓ **單一安全模型** (One Common Security Model)：所有的資料型態(關聯式、JSON、向量) 均受同一套嚴密的企業級資安網保護。

資安防禦轉化為真實的商業投資報酬率 (ROI)

安全的融合式資料庫不僅降低風險，更能大幅削減隱性成本，加速創新步伐。

1

66%↑

DBA團隊效率提升：消除管理多個外部向量資料庫與第三方整合工具的繁瑣作業。

2

48%↑

IT基礎架構團隊效率提升：減少資料搬遷的頻寬浪費與沈重的系統維護成本。

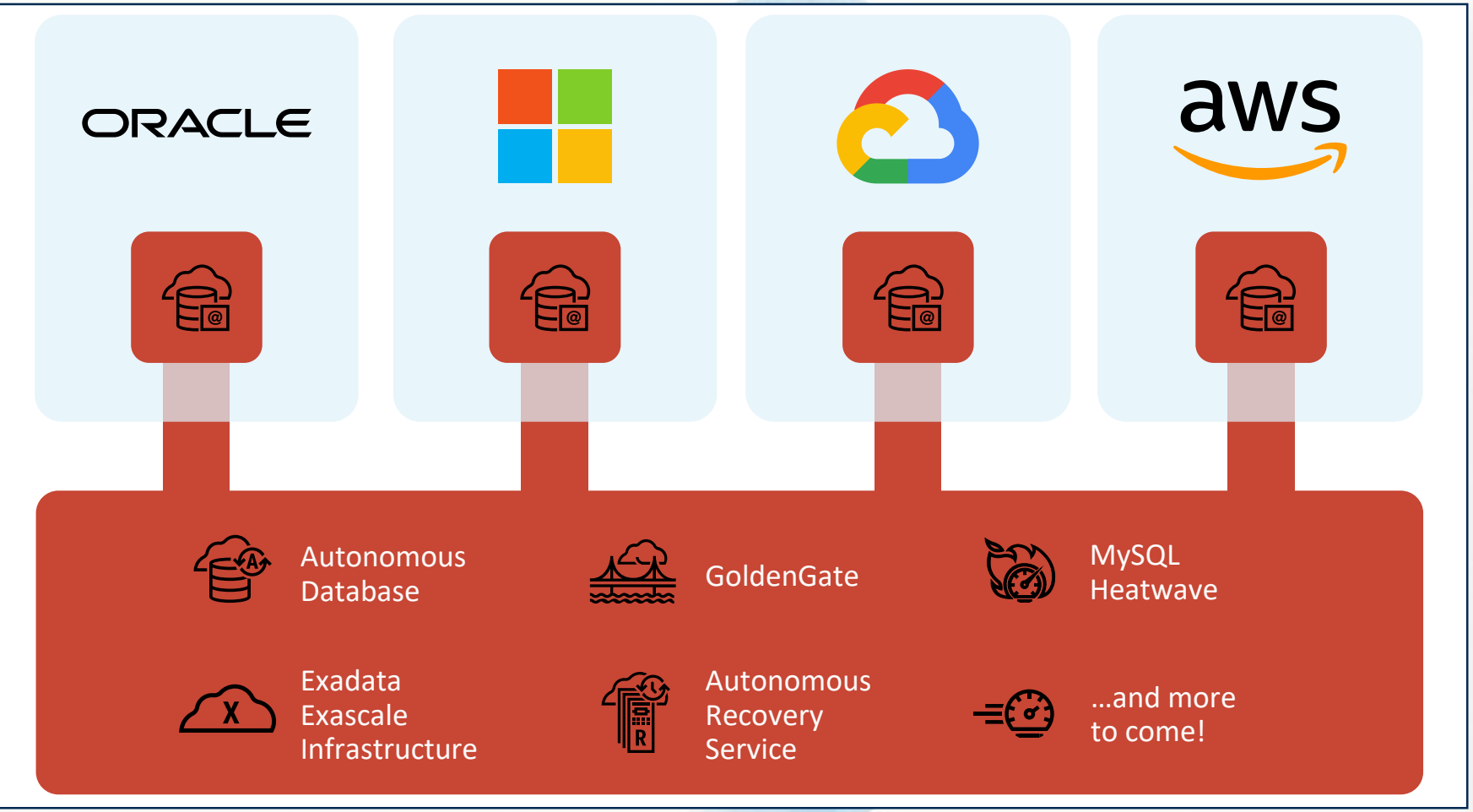
3

436%↑

三年投資報酬率（ROI）：根據IDC商業價值報告，Autonomous AI Database為企業帶來顯著的營運效益與最低的總擁有成本（TCO）。

掌握主權：無所不在的雲端部署 (Runs Anywhere)

Oracle is in all clouds



Same Database.
Same Features.
Same Pricing.

確保企業在任何環境下皆能靈活擴展，不被單一基礎設施綁架。

OCI 提供出色的性價比 (The TCO Proof)

Year 5 Consumption

- 620K OCPUs
- 30 PB Object storage
- 120 PB SSD Storage
- 30 PB NW Egress

面對高達 163%~253% 的成本差異，選擇正確的底層架構，意味著企業能釋放數十億美元的創新動能。

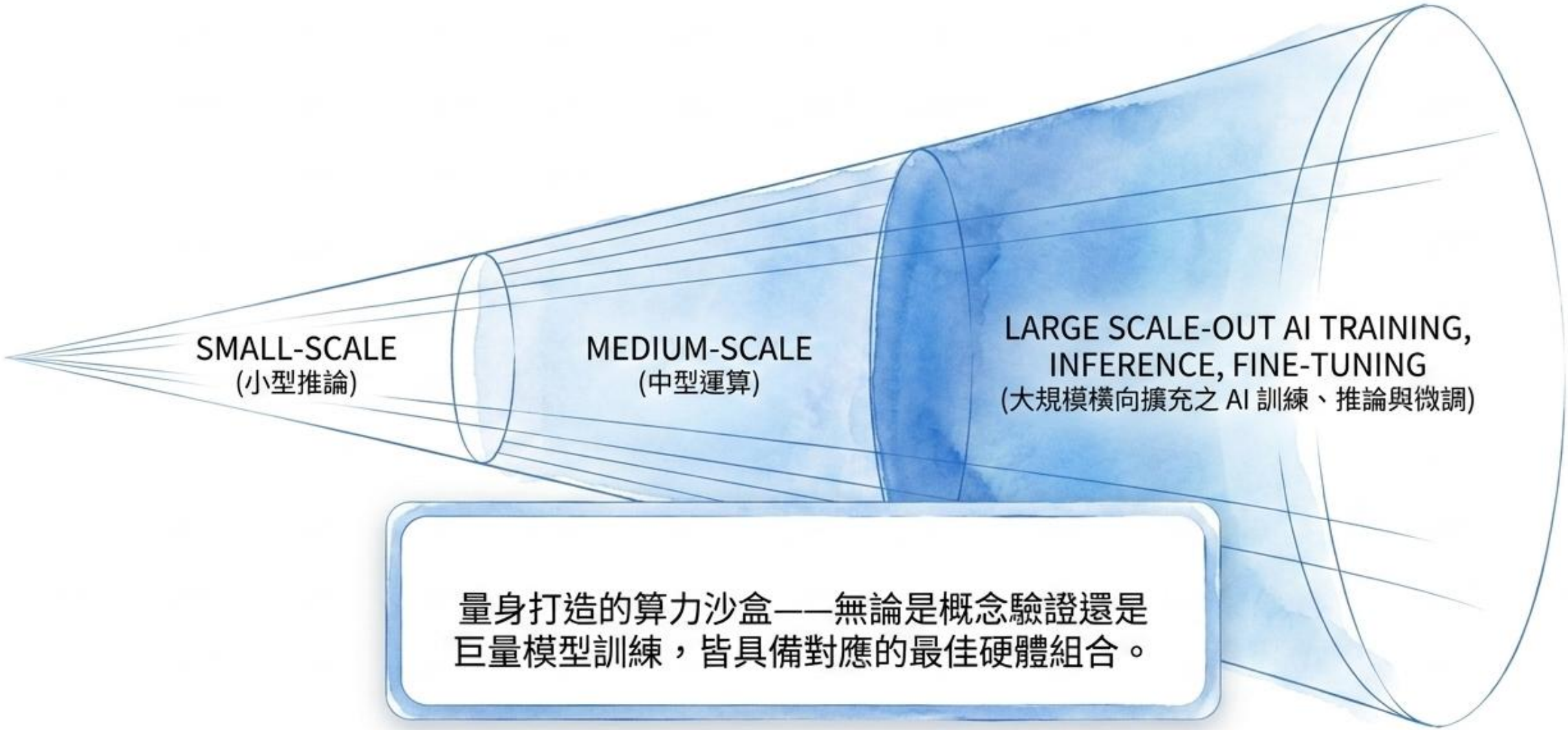
全球佈局：具備強大韌性的雲端網路

200+ live and planned regions

滿足不同層級的資料主權與合規需求：

- ✓ Commercial
- ✓ Government
- ✓ EU Sovereign
- ✓ Dedicated Region
- ✓ Oracle Alloy

邁向 AI 時代：滿足所有需求的 AI 基礎設施



敏捷擴展：中小型訓練與推論算力配置

中型算力 (Medium-Scale)

- Bare metal
  GPU.A100-v2.8
- VM
  GPU.MI300X.8

最高支援 400 Gb/sec Front-end network 與 640 GB GPU memory

小型推論 (Small-Scale)

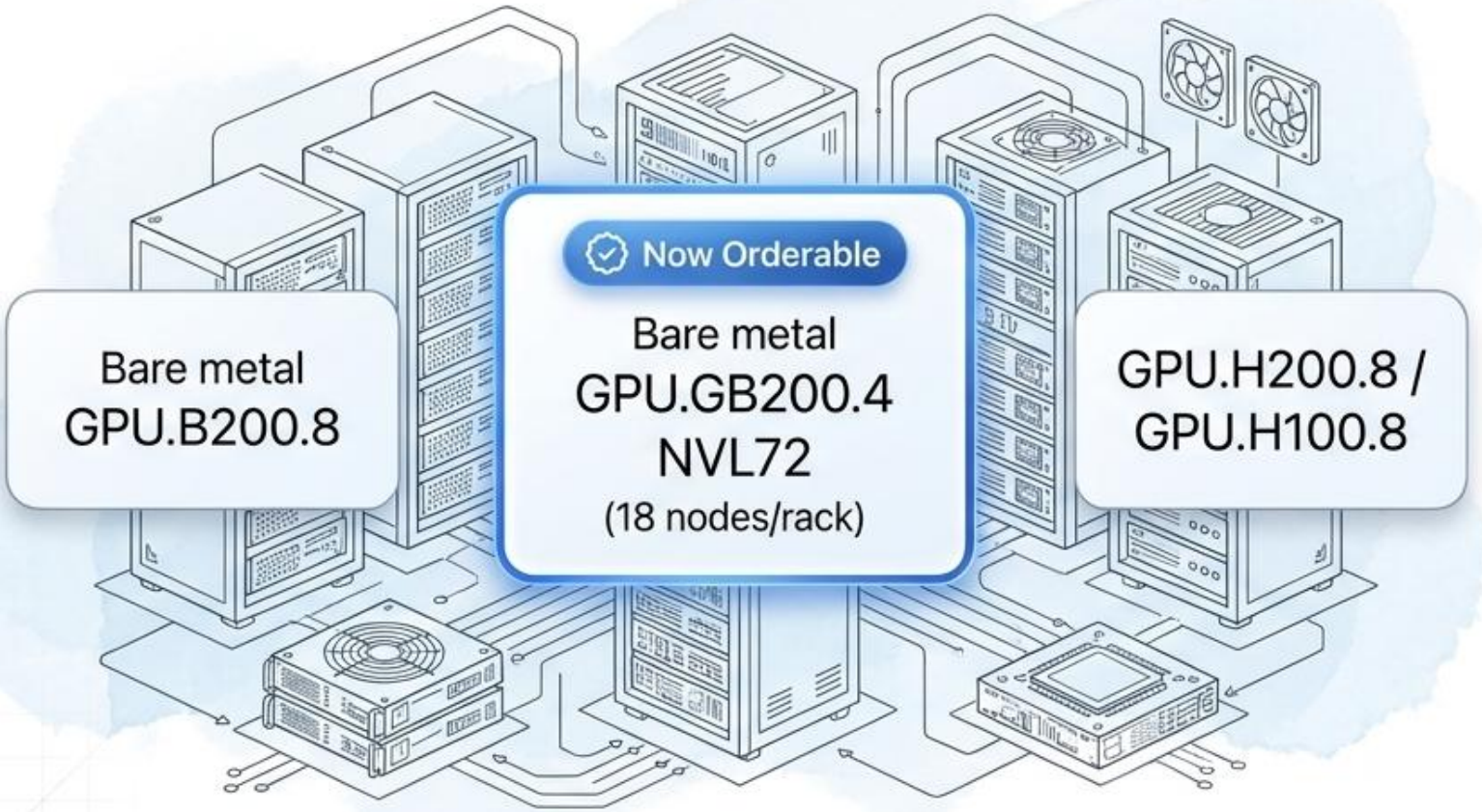
- Bare metal
  GPU.L40S.4
- VM
  GPU.A100.1
  (1 x A100 80GB)

1 x H100 80GB

(註明：OCI 同時支援前代 NVIDIA P100 與 V100 GPU)

提供高度彈性的虛擬機 (VM) 與裸機 (Bare Metal) 選擇，精準對接不同的營運成本與效能需求。

頂級算力：專為大規模 AI 訓練打造 (Large-Scale AI)



1,536 GB
GPU Memory

30.7 TB
Local NVMe

100 Gb/sec
Front-end Network

突破硬體極限，以超低延遲網路串聯裸機節點，為新一代生成式 AI 提供不妥協的運算力。

知識中台核心的應用案例

以知識中台為核心，打造全域 AI 應用生態
校務 AI 的成功不在於做了多少個 AI agent，而在於有沒有一個「單一事實來源」。可被管理維護並成為正循環。

AI智慧應用選擇 - 痛點優先的決策邏輯

解題第一步：從現況的痛點出發

01 現況評估與痛點辨識
分析流程瓶頸、資源浪費，量化痛點影響。

02 業務影響評估
評估潛在提升，聚焦高價值問題。

03 決策鏈
技術是否能帶來獨特優勢？

04 是否適合用AI解？
確保技術適合且可行，避免為AI而AI。

AI智慧應用選擇 - AI解題的核心心法

先有服務思維，再找科技實現

服務思維先行

聚焦痛點

始終從用戶需求和業務痛點出發。

價值導向

確保AI應用能創造真實、可量化的價值。

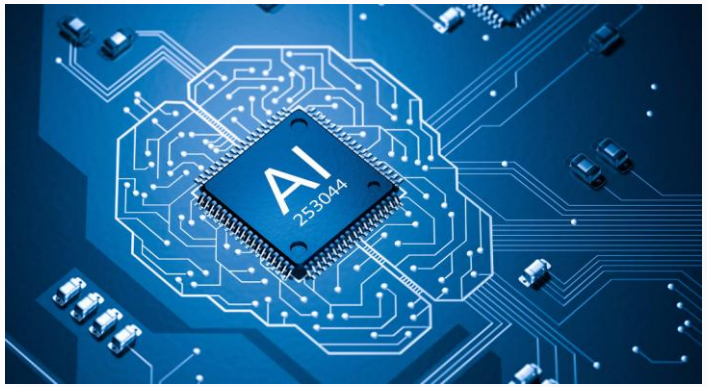
科技精準賦能

AI是工具

將AI視為解決「點」問題的強大工具。

策略性應用

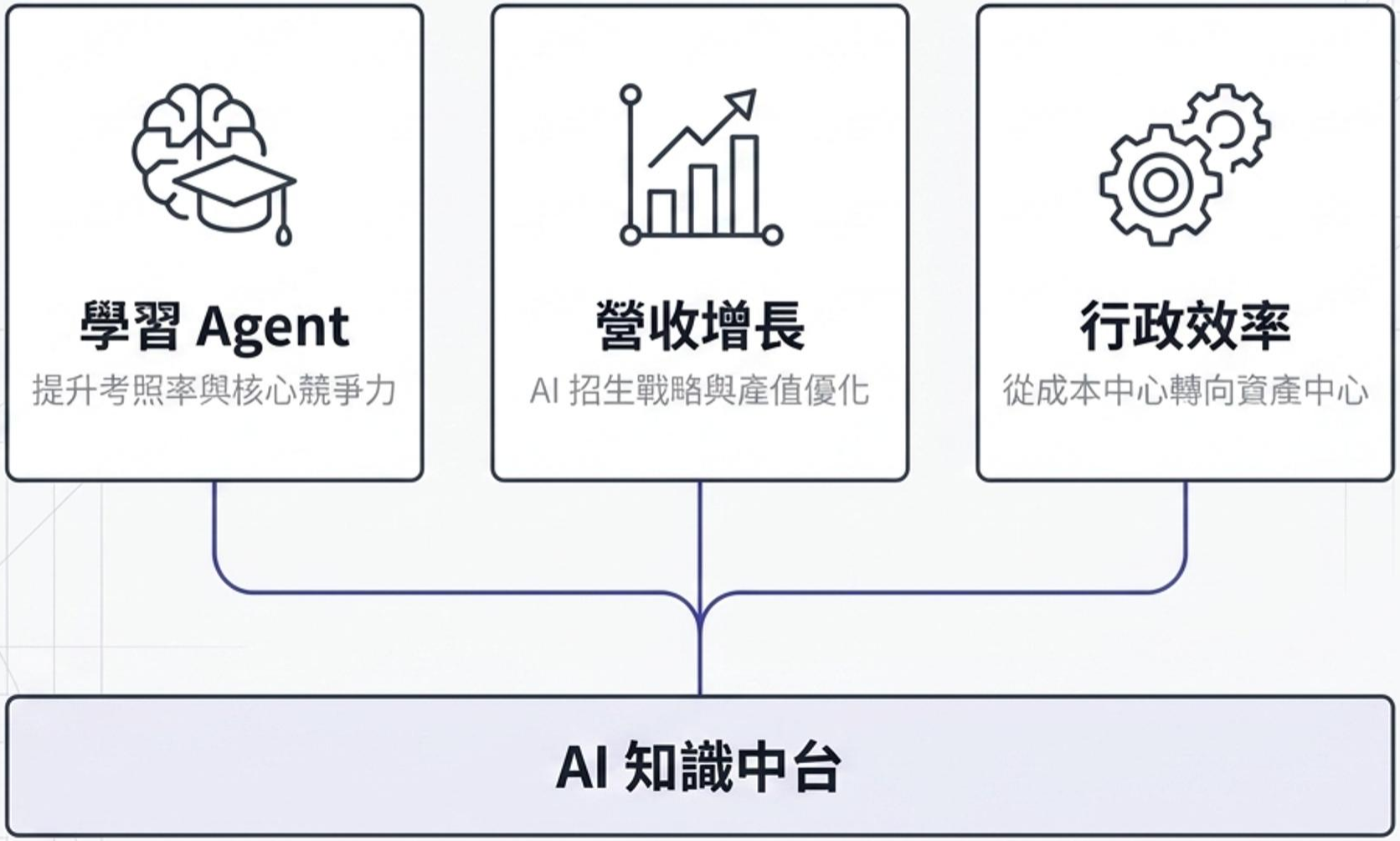
避免盲目追逐技術，精準選擇AI介入時機。



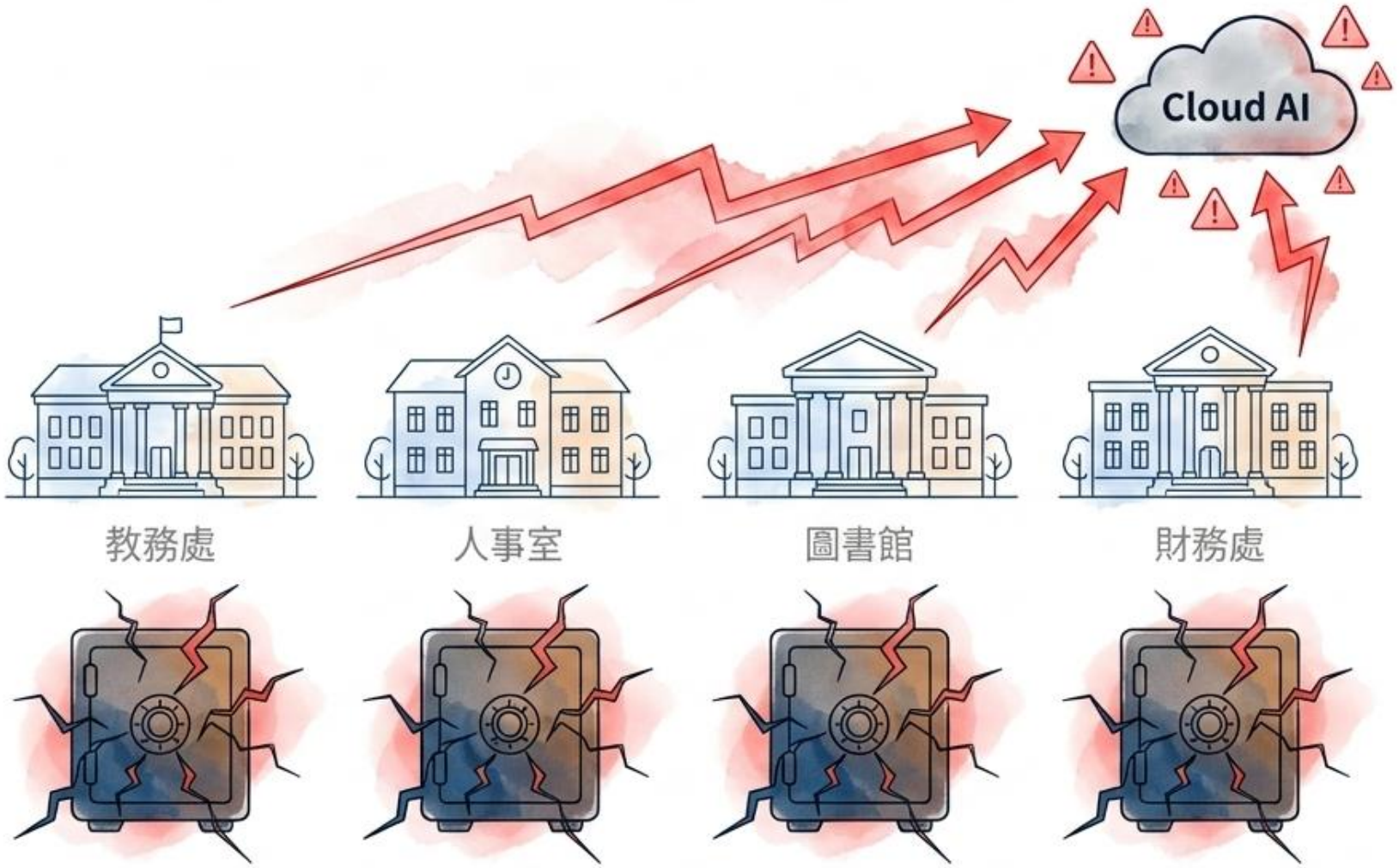
立即行動 - 從小而美開始

從一個小痛點開始，設計一個AI試點。建立度量與學習機制，讓AI驅動的成長飛輪轉動起來。

智慧校園的三大戰略支柱



資訊孤島是阻礙 AI 效能與數據價值的最大痛點



現狀的困境：

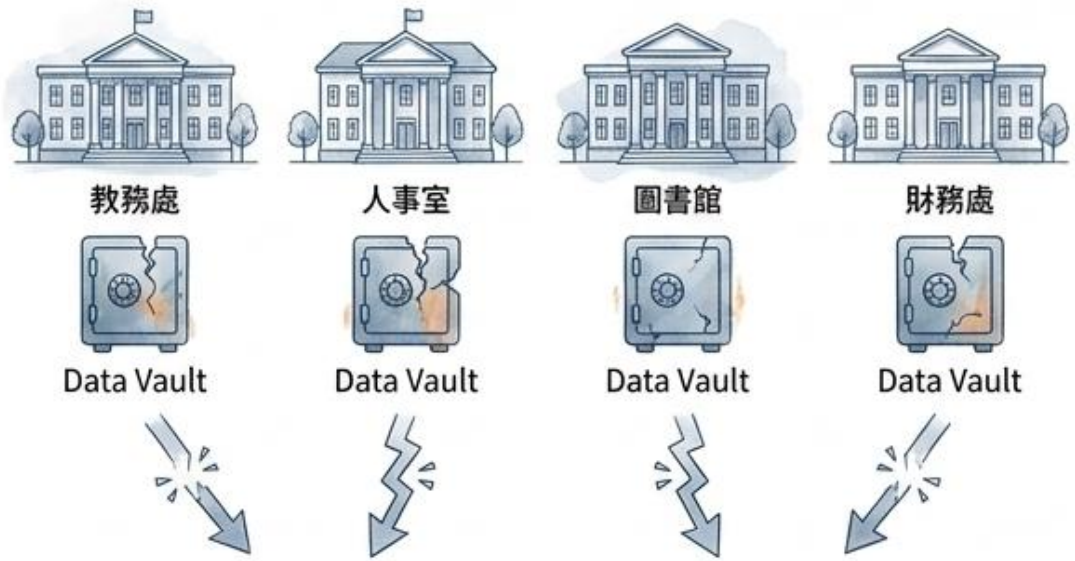
當各處室的數據格式不一、各自為政時，即使引入最先進的 AI 模型，也無法發揮跨域流程自動化（趨勢 #9）的效益。

潛在風險：

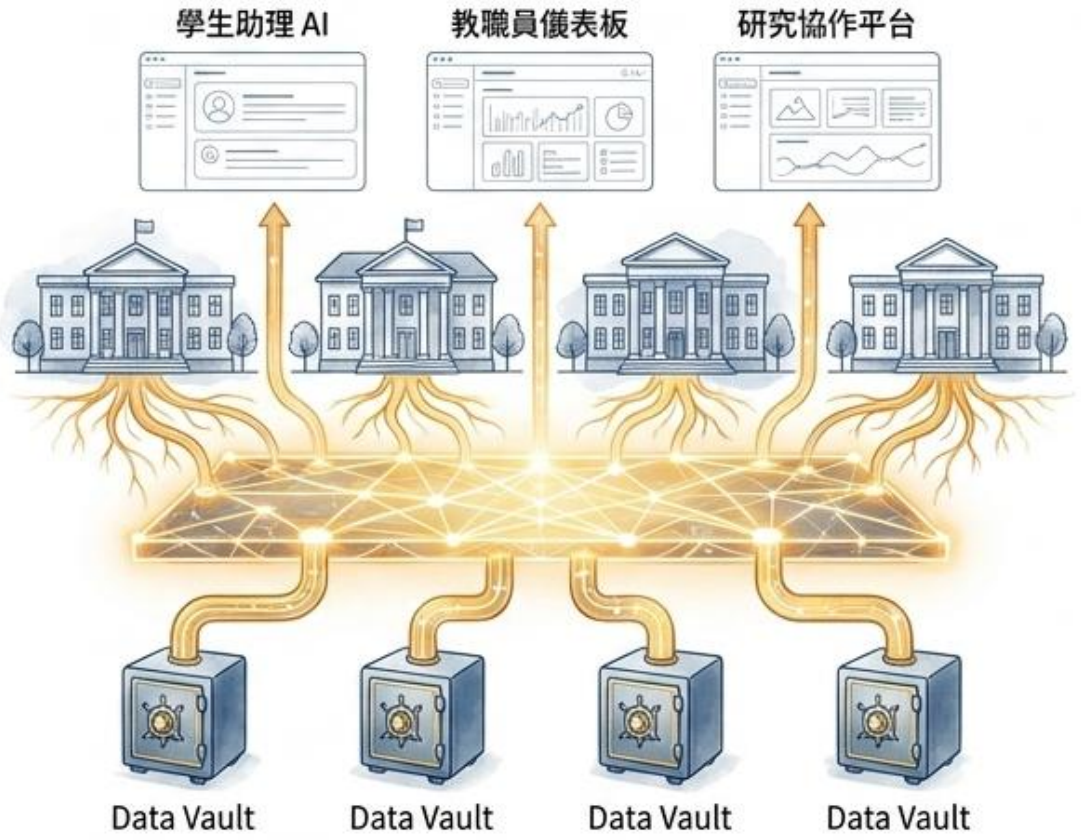
破碎的資料基礎會導致 AI 產生幻覺 (Hallucinations)，甚至引發隱私外洩。

AI 校務知識中台：化孤島為神經網路的關鍵解方

Traditional Silos



Knowledge Middle Platform



定義知識中台：介於底層原始數據與前端應用之間的**「智慧連結層」**。

核心功能：統整全校資料、制定統一的**安全規則**與**權限**，將零散的數據轉化為可被 AI 安全調用的**「校務知識」**。

智慧校園AI知識中台 - 賦能師生

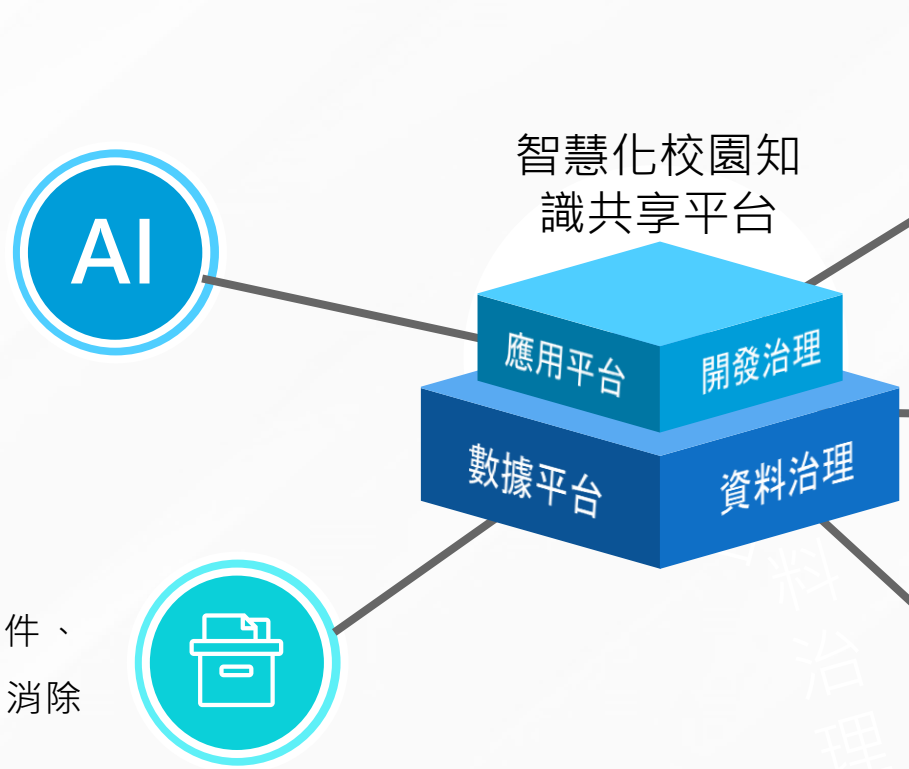
透過 AI 助理與工作流程的整合，實現校園知識的即時共享與自動化管理，讓課綱文件即時轉化為可運用的知識資產。

AI 智慧搜尋

結合語意搜尋與自然語言問答，快速定位跨系所資訊，協助決策並加速知識流通。

集中化知識中心

統一儲存校園公開/行政文件、SOP，打造單一資料入口，消除資訊孤島。



工作流程再設計

提升執行效率並減少人為錯誤。

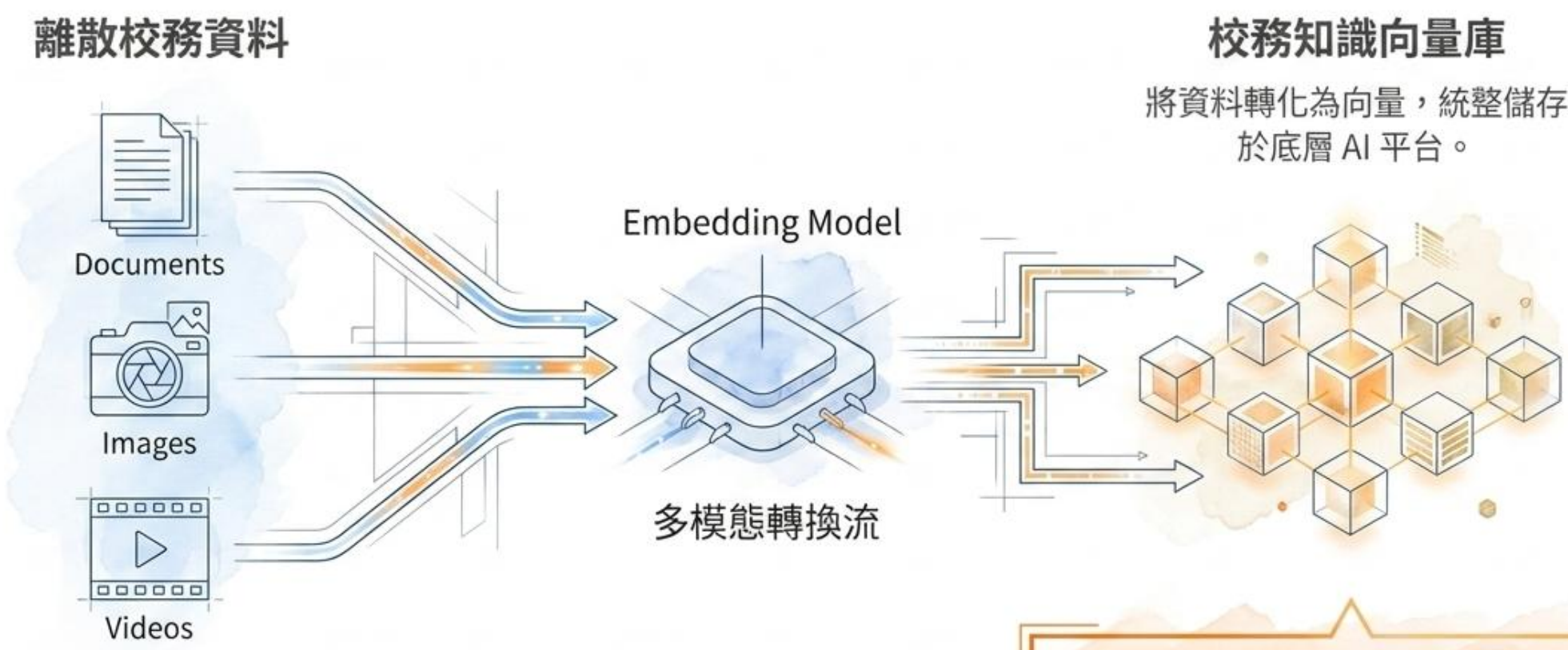
AI應用發展

應用流程發展工具，以單一事實來源設計不同情境Agent。

權限與安全控管

依角色分級存取，兼顧資訊共享與機密保護，確保資料安全與合規。

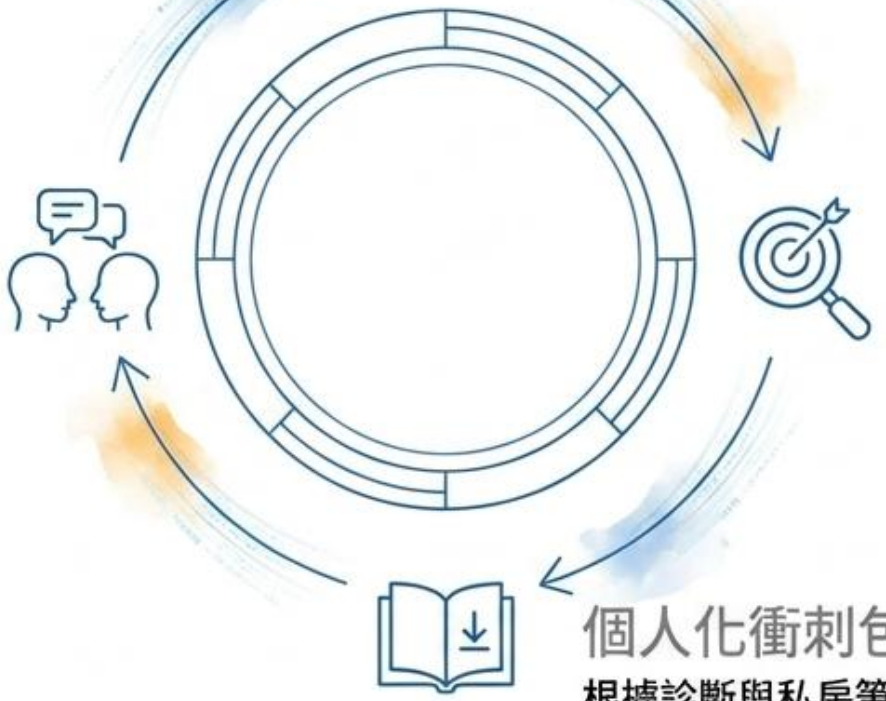
打破資料型態限制：多模態 AI Vector Search



校園中擁有極度多樣化的非結構化資料，
包含文字法規、教學影片、校園活動影像等。

讓師生用自然語意的方式精準搜尋，
大幅提升知識流通效率！

釋放靜態知識價值：動態陪練員機制



練習與上傳

學生完成模擬卷並上傳系統。

精準弱點診斷

AI 不只批改，更標註關聯核心（例如：精準對應《行政法》第15條與過去課程概念）。

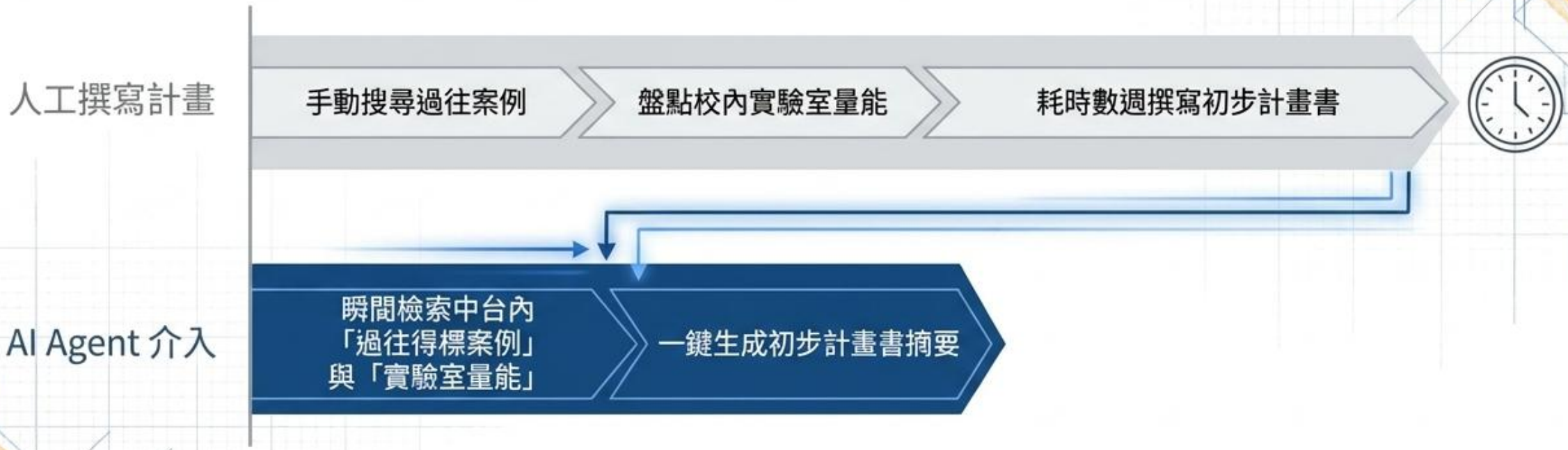
個人化衝刺包

根據診斷與私房筆記，一鍵生成專屬考前精華。

AI 模擬口試

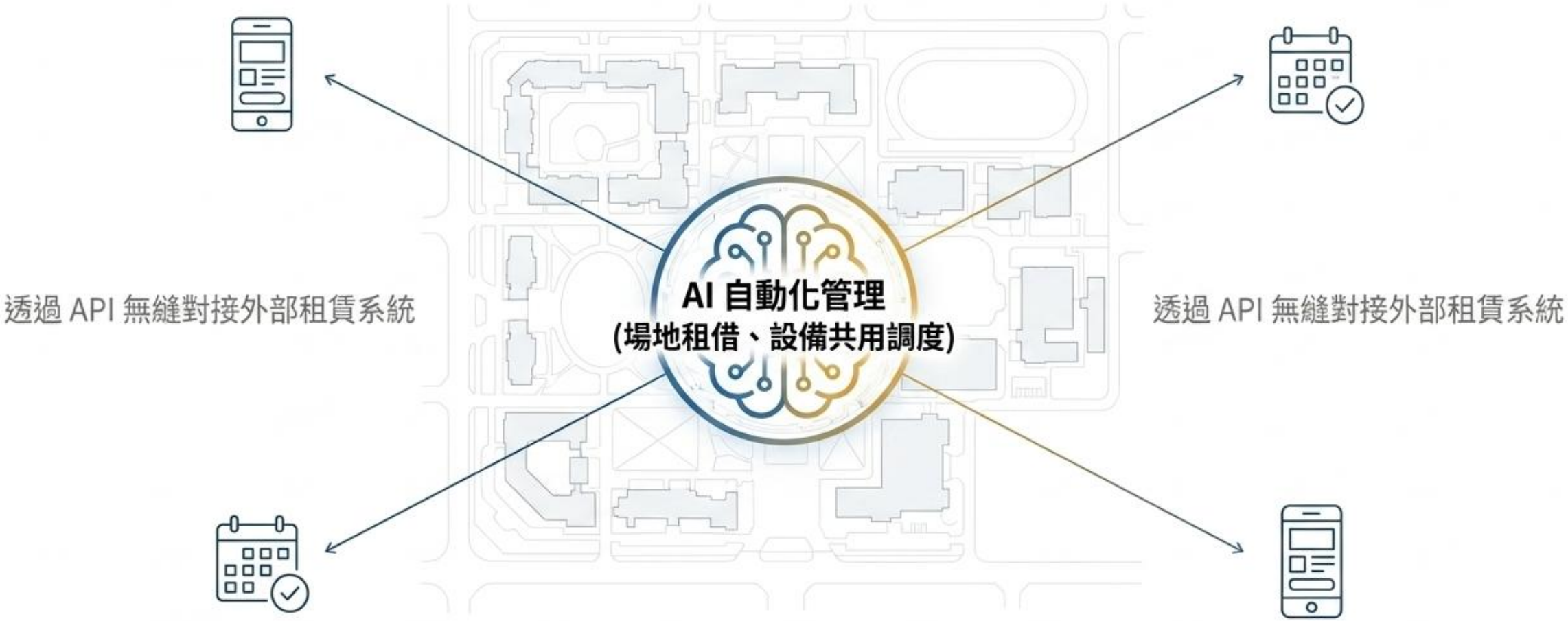
針對工程專案或諮商心理師等需求，提取專業問題進行壓力測試與改進建議。

工作流程自動化：產學標案助手



大幅降低申請門檻，顯著提升學校爭取政府與企業外部研究經費（產學收入）的成功率與頻次。

營收戰略再進化：校園空間與實體資產活化



釋放並極大化閒置空間與設備的變現能力，讓校園實體資產在非營運時段也能自動創造收益。

資訊服務與校園AI運用推廣的機會

1. 協作式網絡安全
2. AI 的人性化
3. 營運與財務洞察的數據分析
4. 打造全校性的數據中心文化
5. 知識管理助力安全 AI
6. 新技術的審慎評估方法
7. 未來職場的技術素養
8. 從被動應對轉為預主動決策
9. AI 驅動的效率與成長
10. 決策者的數據技能與素養

Executive Memo

1. 您正承受**推動 AI 創新與防範校務資料外洩**的雙重壓力。
2. 透過 AI 知識中台架構，**無須重構既有系統或冒險搬運敏感資料**，讓 AI 直接在您最信任的防護網內運行。
3. 掌握雲地架構的黃金配比，您獲得的不只是最低的整體擁有成本 (TCO)，而是一套**立即可用、驅動招生成長與行政效率的企業級 AI 基礎設施**。

啟動校園 AI 革命，建立無可取代的數據主權。

實現主權、安全、智能的未來高教藍圖

建立 AI 校務知識中台，絕非單純的 IT 升級，而是攸關高高等教育存續的底層重構。

整合路徑已然清晰：從掌握主權資料出發，透過知識管理確保 AI 安全，最終實現凝聚集體意志、賦能個人能力的 2026 願景。

啟動您的智慧校園藍圖

從現在開始，盤點校園內的「主權資料」。

打造專屬 AI 知識中台，讓沉睡的數據成為驅動未來的最強引擎。