Secure & Govern AI with Risk-Aware Context & Control

端對端 AI 資料可見性與管控能力，打造安全、負責且合規的 AI。

加速落實負責任AI
讓治理的最佳實踐跟上AI資料的使用，以推動安全將 AI且合乎道德的創新。

減少暴險
緩解AI產生的風險，例如敏感資料外洩、影子 AI (Shadow AI) 以及模型濫用 (model misuse)。

最大化 AI 投資報酬率
改善能見度與管控流程，以安全且高效地將AI規模化。

領先全球 AI 法規
確保 AI 資料實務持續符合不斷演進的隱私權與AI法。

改善稽核準備狀況與問責性 (AI Accountability)
維護具有效力的的記錄，以簡化稽核程序並展現合規性。

實現具備適應性的 AI 治理
賦予團隊共享的能見度與管控力，實現規模化的 AI治理。

> **像 BigID 這樣的工具是未來的趨勢**
> 企業應善用這類工具，將資料探索 (Data Discovery) 的流程自動化，以提供更清晰的能見度，並協助排定控管措施的優先順序。

IDC Ryan O'Leary
Future of Trust: Battling Data Discovery Confusion

The Most Comprehensive Platform for AI Data Security & Governance

專為模型、資料集與向量資料庫打造。
為您所有的 AI 資料提供無與倫比的探索、分類與控管能力。

AI 資料探索與分類
自動探索並分類橫跨雲端、地端及第三方來源的各類資料資產，包含資料集、模型、向量資料庫 (Vector DBs) 與大型語言模型 (LLMs)。

AI 風險管理與政策執行
持續評估 PII (個人識別資訊) 暴露、模型漏洞及影子 AI (Shadow AI) 等風險－並依據政策觸發告警與補救措施。

合規的 AI 治理
確保資料治理與全球法規及框架對齊，例如 GDPR、CCPA、CPRA、HIPAA 以及歐盟 AI 法案 (EU AI Act)。

AI 資料血緣(AI Lineage)與可視性
追蹤敏感資料在 AI 流程中（從資料攝取到模型推論）的流向，確保透明度與問責性。

AI 生命週期管理
自動化 AI 資料資產的保留、清理與治理，以減少攻擊面並支援資料最小化原則。

建立對AI產出結果的信任
透過確保整個生命週期中的資料品質、透明度及保障使用上合乎道德，增加 AI 輸出內容的可信度。

Why BigID Stands Apart

- **專為AI資料打造**
  專為模型、大型語言模型 (LLM)、資料集與向量資料庫的安全與治理而設計。
- **消除盲點**
  從資料攝取到模型推論，視覺化 AI 全生命週期的資料流。
- **自動化風險與政策執行**
  持續偵測 AI 產生的風險，並大規模自動化地執行補救措施。
- **統一平台，模組化管控**
  將 AI 安全、隱私與治理整合於單一平台，並具備50多種可擴充的應用程式。
- **開放且具擴充性的生態系統**
  整合您的 AI 開發環境 (AI Stack) ——包含 Hugging Face、Azure OpenAI、Vertex AI、SageMaker 等主流平台。