

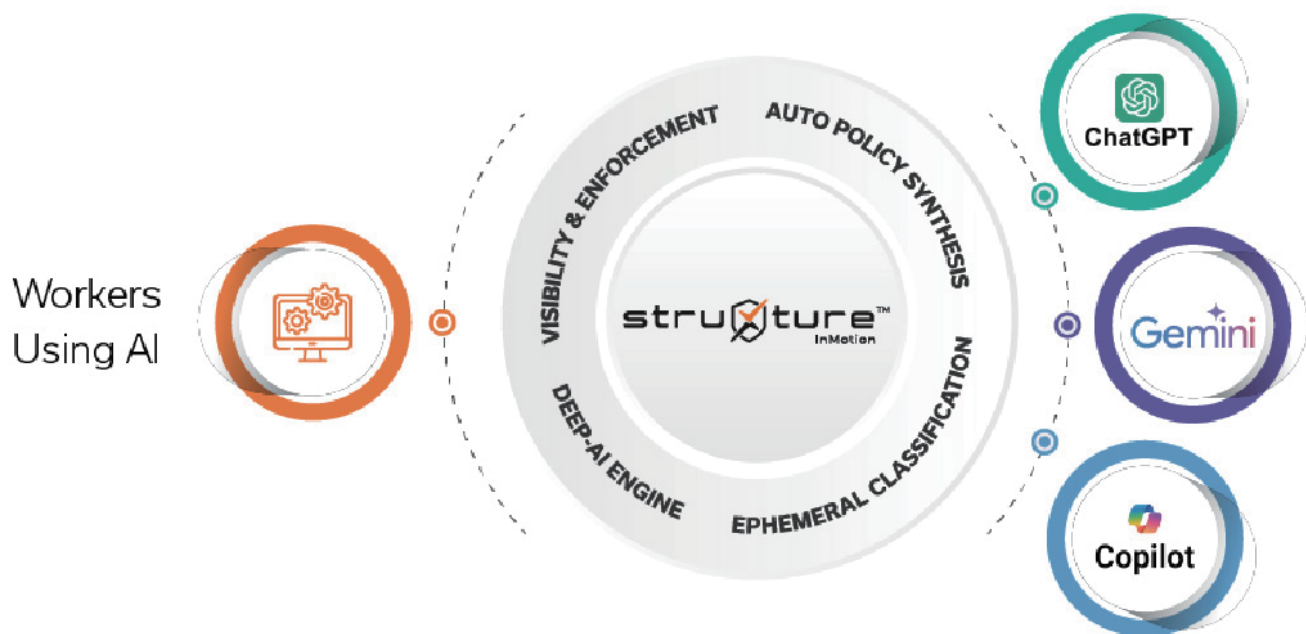
Deep-AI的資料外洩防護(DLP)方案

保護您的關鍵業務資料

struXture™ InMotion 是新一代資料外洩防護 (DLP) 解決方案，透過自動化機制，全面防範機敏資料被惡意竊取或非預期外洩。無論是地端 (On-Premises) 或雲端 (Cloud) 環境，struXture™ InMotion 的 Deep-AI 引擎皆能彌補傳統 DLP 解決方案的不足，簡化資料防護的部署與管理，提供更高效、更智能的資料安全性。

AI驅動的整合式資料安全

struXture™ 專為 AI 時代而打造，提供即時 DLP 防護，兼具智能分析、敏捷性與業務所需的高效能。不僅符合現代企業的資料安全需求，還能滿足資安團隊對技術強度的高標準要求。



struXture™ 功能特色



即時資料分類

AI 自動識別與分類資料，適用於動態工作負載，如 AI 生成內容與海量資料分析。



自動策略生成

AI 自動建立存取策略，降低誤判與管理成本，確保資料安全。



掌控非結構化資料

強化可視性與存取控管，有效防範文件、程式碼、設計圖等機敏資訊外洩。



高效能擴展

支援各類型資料處理，適用於大規模環境，提升使用體驗與安全性。



即時啟用防護

開箱即用，簡化策略設定，快速完成端點裝置與存取規則管理。



角色導向存取控管

動態調整存取權限，確保只有授權人員可存取機敏資料。



雲端資料保護

自動偵測並阻擋未授權的雲端資料傳輸，確保 SaaS 與儲存伺服器安全。



AI 動態防護

AI 自動學習業務邏輯，提升資料識別能力，防範 AI 生成內容洩漏機敏資訊。

AI驅動的DLP防護 全面守護企業機敏資料安全

保護您的關鍵業務資料

- 機密資料外洩風險：公司擁有大量機密設計文件、原始碼、產品規格等資訊，需確保這些智慧財產被未授權存取或外洩。
- 合規與法規要求：需符合合約及法律規範，確保合作夥伴的智慧財產受到嚴格保護，避免法律風險。
- APT 高度威脅：由於產業特性，公司成為進階持續性威脅（APT）的主要目標，需要更強的資料外洩防護機制。
- 傳統 DLP 方案失效：過去使用的 DLP 方案無法有效偵測並防範內部或惡意資料外洩，造成重大損失。

導入方案

struXture™ 透過 AI 自動識別、分類，並即時監控資料流向，大幅降低外洩風險：

- AI 自動分類與標籤：無需手動設定，減少人為疏失及惡意行為的風險。
- 智能合規偵測：即時識別合規問題，確保資料傳輸符合企業與法規要求。
- 即時資料監控與分析：提供詳細的異常行為報告，確保機密資訊安全存取。

達成效益

- 智慧財產安全提升：精準識別與管控機密資料，防止未授權存取與外洩。
- 合規與風險管理：即時偵測異常資料流動，降低罰款與法律風險。
- 降低營運成本：無須手動標記與管理，減少維護與合規成本。
- 即時預警與應對：AI 自動分類 + 即時策略執行，防止意外與惡意資料外洩。

