

AI Security Platform

AI 安全平台

- 跨「人員、AI 代理、資料與模型」的統一活動控管
- 涵蓋自建系統、SaaS、嵌入式應用與端點(Endpoint)



產品總覽

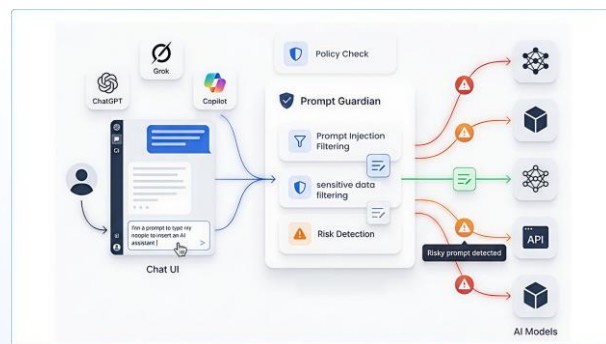
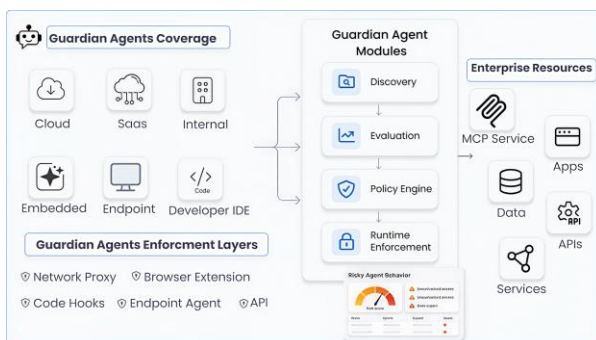
Pragatix 是一套 AI 安全平台，提供涵蓋人員與 AI 代理(Agent) 互動的端到端防護與 AI 使用可視性。透過代理 (proxy)、瀏覽器擴充套件與 API 整合，Pragatix 能即時在雲端與端點環境中，對自建代理(Agent) 與第三方 AI 服務執行政策控管。平台可實現 AI 代理(Agent) 的監控與控管，同時確保資料隱私與 AI 主權，並針對提示詞 (prompt) 與行為進行治理，亦可評估企業內部 AI 應用中所使用模型的風險。

關鍵能力

代理護欄 (Guardian Agent)

管理企業中自主 AI Agent 及其行為

- ✓ 探索與可視性 (Discovery & Visibility) : 盤點所有 Agent，包括工作流程、擁有者與相依關係
- ✓ 監控與可追蹤性 (Monitoring & Traceability) : 追蹤所有行為並保留完整稽核軌跡
- ✓ 身分與存取控管 (Identity & Access Control) : 管理權限、工具與系統存取
- ✓ 行為與異常偵測 (Behavior & Anomaly Detection) : 確保行為符合預期並偵測濫用
- ✓ 執行階段行為控管 (Runtime Action Enforcement) : 即時阻擋、修正與動態調整



提示詞護欄 (Prompt Guardian)

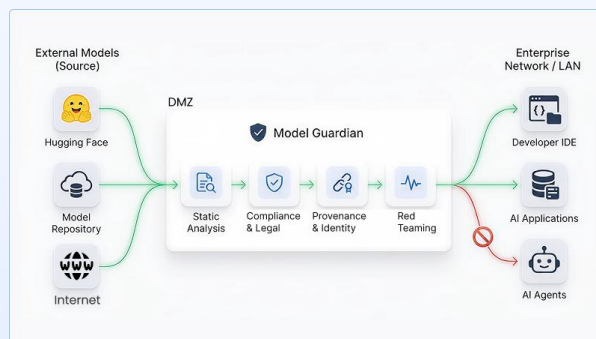
控管使用者與 Agent 如何與 AI 系統互動

- ✓ Shadow AI 使用探索: 識別並管理未授權的 AI 工具
- ✓ 提示詞檢測與防護 (Prompt Inspection & Protection) : 防止提示詞注入攻擊 (Prompt Injection) 與資料外洩
- ✓ 風險導向控管 (Risk-Based Enforcement) : 依情境套用使用政策
- ✓ 使用可視性與稽核 (Usage Visibility & Audit) : 監控並記錄所有互動

模型護欄 (Model Guardian)

評估並保護企業中使用的 AI 模型

- ✓ 風險與信任評估 (Risk & Trust Assessment) : 在模型正式使用前進行評估
- ✓ 弱點測試與紅隊演練 (Vulnerability Testing & Red Teaming) : 識別越獄行為、弱點與濫用風險
- ✓ 治理與法規遵循 (Governance & Compliance) : 審核並控管模型使用



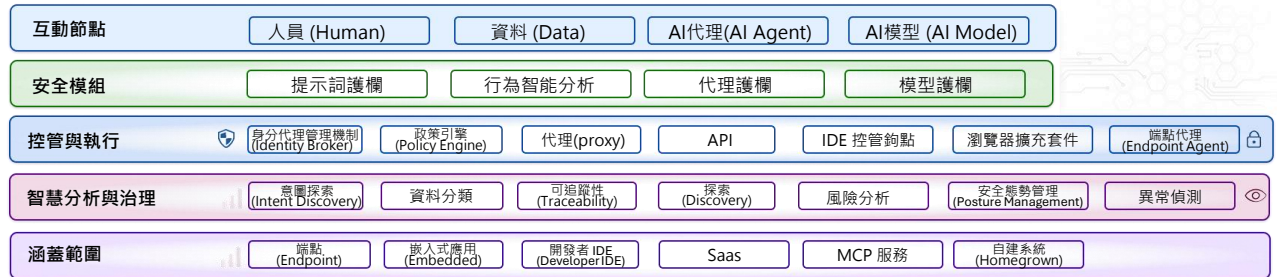


資安意識 (Security Awareness)

掌握每一次 AI 互動：誰、做了什麼、何時發生，以及風險程度

- 人員風險 (Human Risk) : 識別員工與 AI 聊天服務及 代理(Agent) 的高風險互動
- AI 代理風險 (AI Agent Risk) : 偵測並控管 AI 代理(Agent) 可執行的行為
- 情境式訓練 (In-context Training) : 即時提供情境化的資安意識指引

AI 安全平台層級架構



彈性部署

- ☒ SaaS
- ☒ 本地部署(On-premises)
- ☒ 私有雲
- ☒ 隔離環境 (Air Gapped)

從可視化到實際控管

Most Risky AI Agent Behavior (Risk Score)

AI Agent	Connected Tool	Risk Score	Activity Type
ChatGPT	Gmail	9.3	Unauthorized
Copilot	Salesforce	9.3	Exporting data
Claude	Asana	8.7	Delete tasks
Cursor	GitHub	8.5	Code changes
AI Agent	AWS Console	8.0	Infrastructure
ChatGPT	Google Drive	8.5	Data extraction

了解更多 Pragatix 解決方案

私有 AI 套件 (Private AI Suite)

本地 AI 能力 - [Click here](#)

導入智慧 (Adoption Intelligence)

衡量 AI 以提升生產力- [Click here](#)



在不限制創新的情況下，實現安全的 AI 導入
立即免費試用 [AI Security Suite](#). [Click Here](#)



AGAT

info@agatsoftware.com

LinkedIn

+972-2-579-9123

Facebook

www.agatsoftware.com

YouTube

相關產品資訊 · 敬請洽詢台灣地區代理商：
商丞科技股份有限公司 | 電話：(02) 2914-8001