

TrendAI Vision One

AI 風險治理平台

全面可視化 · 持續掃描 · 自主式資安營運

您企業的 AI 正在高速擴張——
您的安全治理，**跟上了嗎？**

企業 AI 化浪潮下的**三大治理挑戰**

01 AI 盲區

員工私下使用 ChatGPT、Claude 等外部生成式 AI，企業無從掌握資料流向，敏感資訊隨時外洩。

02 模型漏洞

自建或採用的 AI 模型存在 Prompt Injection、資料投毒等風險，傳統資安工具無法識別 AI 特定攻擊向量。

03 合規壓力

ISO 27001、GDPR、個資法要求完整事件軌跡與稽核報告，手動整理耗時且容易出現缺口。

唯一整合 AI 風險可視化 · 模型掃描 · 合規報告的企業資安平台

TrendAI Vision One 是趨勢科技（Trend Micro）推出的一款以 AI 驅動的企業級網路資安平台。將 AI 安全治理從被動應急轉化為策略性風險管理，讓企業在擁抱 AI 創新的同時，確保合規與資料安全。



降低
70%
的網路資安成本



減少
99.6%
的日常警報數量



縮短
65%
的攻擊滯留時間



降低
92%
的資安風險

立即聯繫羽昇國際，提升企業的雲端安全韌性！



TrendAI Vision One 是一個易於部署的 AI 驅動平台，能將資安從被動應對轉為策略性風險管理，保護企業、營運基礎架構以及資料，防範 AI 驅動的攻擊。圖片來源：趨勢科技（Trend Micro）

三大核心能力 × 全方位 AI 風險治理

01 AI 風險可視化中心

- ✓ 統一儀表板掌握全企業 AI 使用行為
- ✓ 即時偵測員工存取外部生成式 AI 的異常行為
- ✓ 透過 AI-SPM 持續監控 AI 應用的安全狀態
- ✓ 整合 XDR 資料湖，提供攻擊路徑預測分析

02 AI 模型漏洞持續掃描

- ✓ AI Scanner 持續分析模型檔案、資料集與執行期提示
- ✓ 主動偵測 Prompt Injection、資料投毒等 OWASP LLM Top 10 威脅
- ✓ AI Guardrails 雙向內容防護，攔截惡意輸入與敏感輸出
- ✓ 支援 AWS、Azure、GCP 多雲環境無代理程式部署

03 自動化合規治理報告

- ✓ AI Security Blueprint 建立可稽核的 AI 治理基準
- ✓ Risk Insights 自動生成完整攻擊鏈報告
- ✓ 一鍵輸出 ISO 27001、GDPR、個資法稽核所需事件軌跡
- ✓ 整合 Apigee 存取紀錄，提供完整阻斷證據

Zero Trust Secure Access

延伸零信任原則至生成式 AI 工具，實現精細化存取政策管控。透過 ZTNA 管控員工與外部 AI 模型的互動，防止敏感資料外洩與影子 IT 風險，所有存取行為完整記錄、即時可視。

歡迎聯繫羽昇國際體驗 TrendAI Vision One 企業網路資安平台

專為 AI 打造，準備迎接未來



羽昇國際
WingWill Int'l Co., Ltd.

企業雲端領航員，一站式整合服務

羽昇國際為零壹科技子公司，為雲端整合專家，專注於雲端應用市場，致力為各產業推動 IT 現代化，規劃最適切的雲端戰略，提供海內外客戶進行跨國多雲、混合雲、雲地整合以及資訊安全管理服務。



聯絡我們