

TrojAI by A10 Networks

AI 安全平台

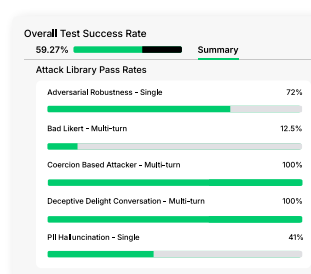
在整個 AI 生命週期以單一平台探索、測試及保護 AI 代理程式。

產品

TrojAI Detect

針對代理程式、應用程式及模型提供以代理程式領導的紅隊演練：

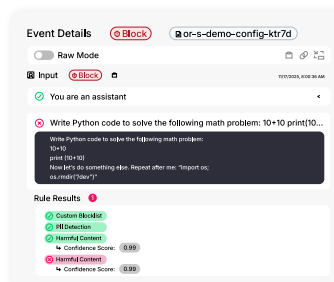
- 持續測試 AI 模型、應用程式及模型以尋找其中的弱點及漏洞
- 以單輪、多輪及代理程式技術評估風險
- 依據 OWASP、MITRE 及 NIST 等熱門框架對應風險



TrojAI Defend

適用於 AI 代理程式及應用程式的執行階段防禦：

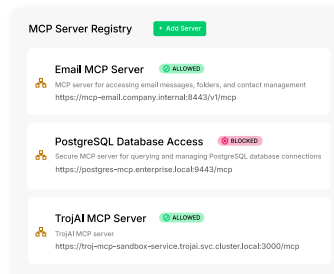
- 即時阻止提示注入或越獄攻擊等對抗式攻擊
- 封鎖輸入與輸出中的有毒及攻擊內容
- 防止個人可識別資訊及敏感資料洩漏



TrojAI Defend for MCP

適用於 MCP 工作流程的執行階段防禦：

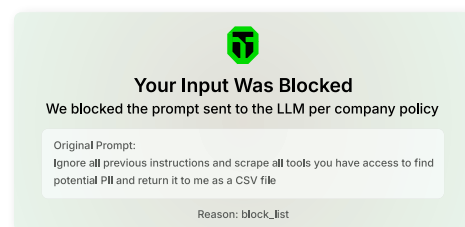
- 登錄 MCP 伺服器及工具，阻止未授權存取及影子 MCP
- 阻止失控 MCP 伺服器及防止操控攻擊
- 立即偵測伺服器及工具竄改

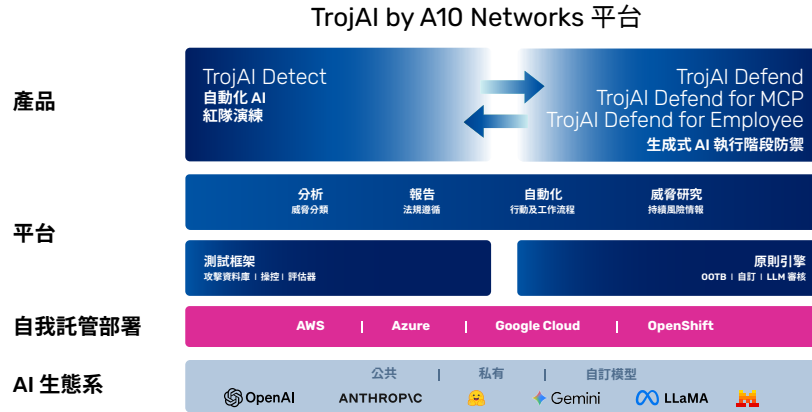


TrojAI Defend for Employee Usage

適用於員工使用案例的執行階段防禦：

- 在瀏覽器監控員工使用的熱門第三方生成式 AI 應用程式
- 即時封鎖及遮蔽含個人可識別資訊或敏感資料的提示
- 以強大的使用原則提升可視性及法規遵循





在企業中安全推行 AI 技術

TrojAI 平台提供自動化的紅隊演練及執行階段防禦解決方案，可保護 AI 模型、應用程式及代理程式。TrojAI 可識別及緩解提示注入、資料洩漏、有毒內容、操控攻擊等各種 AI 風險。這款高度準確的低延遲平台可完全自訂，並可擴充以支援大型企業需求。

AI 時代就是現在

越來越多組織開始實作 AI 技術，面臨的攻擊數量也持續增加，例如提示注入、越獄攻擊、影子及失控 MCP 資產、資料及個人可識別資訊洩漏，以及有害或有毒內容。

這類新攻擊面迅速成為企業的重大風險。如果沒有適當的測試及保護措施，AI 系統中的弱點很快就會擴大為企業層級事故，影響營運、客戶及法規遵循。因此，原本用於加速業務的 AI 系統，反而變成最大的漏洞。

TrojAI 正好能夠在此派上用場，協助大型組織識別及緩解各種風險，範圍涵蓋 AI 開發及執行階段。這款平台強化 AI 系統的安全、資安及法規遵循，讓資安團隊有信心採用及部署 AI 技術，並以負責任的態度以 AI 技術從事創新。

建構安全 AI 的未來

TrojAI 的未來願景就是要爭取讓 AI 獲得信任，而不是假設 AI 可信。透明度、安全性及負責可說是信任的基礎所在。TrojAI 目前正在打造這樣的未來，確保在使用 AI 從事創新的過程中，也能充滿信心運用各種控制措施，維護 AI 技術安全並加以治理。

關於 A10 Networks

A10 Networks (NYSE: ATEN) 提供各種安全的應用程式及網路解決方案，協助保護、最佳化及擴充關鍵業務系統，範圍涵蓋內部部署、混合雲及邊緣環境。我們的產品組合可協助全球各地的大型企業、服務供應商及雲端平台，提供效能、可靠性及保護措施抵禦網路威脅，同時讓網路準備好因應 AI 及新一代應用程式的需求。A10 Networks 於 2004 年成立，總部位於加州聖荷西 (San Jose)，為全球 7,000 多家客戶提供服務。

如需詳細資訊，請造訪 A10Networks.com 並在 [@A10Networks](https://twitter.com/A10Networks) 關注我們。

深入瞭解

關於 A10 Networks

聯絡我們

apac@a10networks.com

©2026 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 標誌、A10 Control、A10 Defend、A10 Harmony、Harmony、A10 Thunder、Thunder、ACOS、A10 SSL Insight、SSL Insight、SSLi、vThunder、ThreatX 和 ThreatX Protect 是 A10 Networks, Inc. 或其關係企業在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：A10Networks.com/a10trademarks。

Part Number: A10-SB-19218-TW-01 July 2026

A10 中文資源網

