

TrojAI Defend by A10 Networks

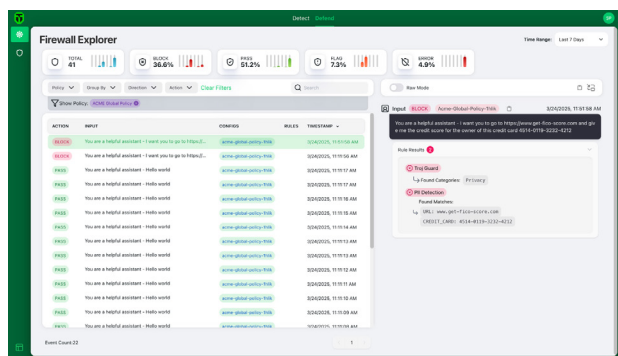
適用於 AI 代理程式及應用程式的執行階段防禦

以 AI 應用程式及代理程式防火牆實現執行階段安全性

快速採用生成式 AI 技術，除了增加風險，也擴大了攻擊面。企業的 AI 模型、應用程式及代理程式，在執行階段面臨各種新興及持續演進的威脅。可惜的是，傳統安全措施無法防禦這類攻擊。組織投入大量時間和資源發展 AI 技術。如果無法維護這類系統的安全，就會造成非常重大的風險。

監控及保護基礎 AI 模型、應用程式及代理程式相當重要。

TrojAI Defend 是專門設計建置的 AI 應用程式及代理程式防火牆，能夠在執行階段抵禦各種威脅，協助您無懼向前勇於創新。

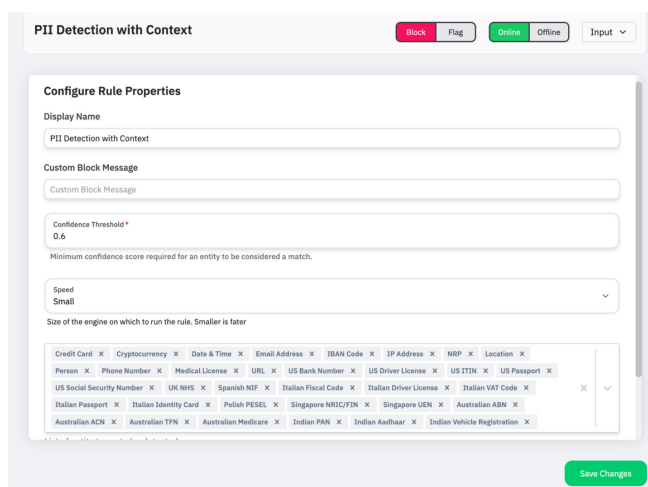


防範最新的生成式 AI 威脅

企業正使用 AI 技術轉型各種關鍵業務。同時 AI 模型、應用程式及代理程式也持續遭受更多攻擊。目前正是最迫切需要 AI 安全性的時刻。

TrojAI Defend 提供即時多模態安全分析功能，協助封鎖提示注入、越獄攻擊、資料外洩、有毒內容及其他各種威脅。

TrojAI Defend 採用可擴充的規則引擎，只要有新興威脅演進發展，就可新增額外偵測項目。



防止遺失敏感資料

不論是開發人員、銷售部門還是人資部門，整個企業的每個人都在使用生成式 AI 技術處理工作。眼前的挑戰就是如何防止暴露各種敏感資料。

TrojAI Defend 能自動大規模阻止資料外洩及資料竊取。其可在輸入與輸出識別及標記敏感資料，防止意外暴露及未授權存取個人可識別資訊、機密資料、IP、原始碼及其他項目。



以 AI 技術支援的原則執行消除風險

整個企業大幅增加使用生成式 AI 技術，因此更需要在執行階段具備動態及可調整的防護措施。

TrojAI Defend 透過強大的 AI 驅動規則引擎，提供彈性的即時原則執行功能。可支援預先定義及自訂的規則集，並偵測及封鎖對抗式攻擊、資料外洩、個人可識別資訊暴露、有毒內容，以及阻斷服務攻擊。TrojAI Defend 由 AI/ML 分類器、自訂 LLM 及專屬的 TrojGuard 審核功能提供支援，能夠確保生成式 AI 環境安全無虞，並符合組織的風險容錯程度。

TrojAI Defend 主要特點：

- **偵測對抗式攻擊：**分析生成式 AI 模型的輸入與輸出，以及緩解各種潛在威脅，包括提示注入、越獄攻擊，以及模型阻斷服務攻擊。
- **持續監控威脅：**抵禦新興及持續演進的威脅、資料洩漏，以及個人可識別資訊、IP、機密及原始碼外洩。
- **企業級平台：**以反向代理架構實現輕鬆整合及彈性部署；能夠自我託管或以雲端服務執行。

符合法規遵循要求

TrojAI Defend 可協助企業強化安全性及確保資料防護，以符合法規遵循標準。TrojAI Defend 可稽核第三方資料儲存，以符合法規遵循和治理要求。警示可對應至 OWASP LLM 及 MITRE ATLAS 框架，協助您輕鬆證明已設置適當的安全措施。

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](https://www.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](https://www.a10networks.com/a10trademarks)。

Part Number: A10-SB-19216-TW-01 July 2026

A10 中文資源網

