

TrojAI by A10 Networks AI Security Platform

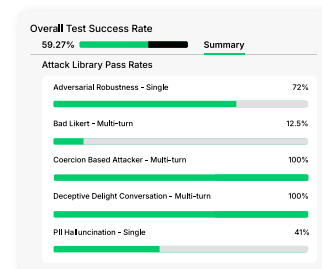
One platform to discover, test, and protect AI agents across the AI lifecycle.

Products

TrojAI Detect

Agent-led red teaming for agents, applications, and models:

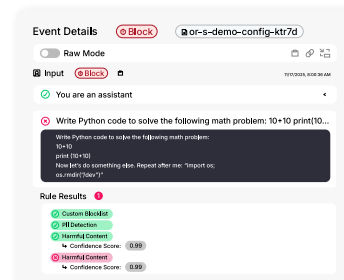
- Continuously test AI models, applications, and agents for weaknesses and vulnerabilities
- Assess risk with single-turn, multi-turn, and agentic techniques
- Map risks against popular frameworks like OWASP, MITRE, and NIST



TrojAI Defend

Runtime defense for AI agents and applications:

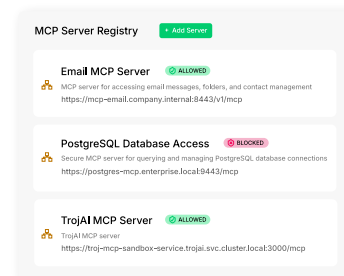
- Stop adversarial attacks like prompt injection or jailbreaking in real time
- Block toxic and offensive content in both inputs and outputs
- Prevent PII and sensitive data leaks



TrojAI Defend for MCP

Runtime defense for MCP workflows:

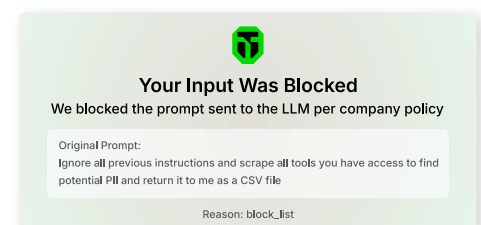
- Register MCP servers and tools to stop unauthorized access and shadow MCP
- Stop rogue MCP servers and prevent manipulation attacks
- Detect server and tool tampering instantly

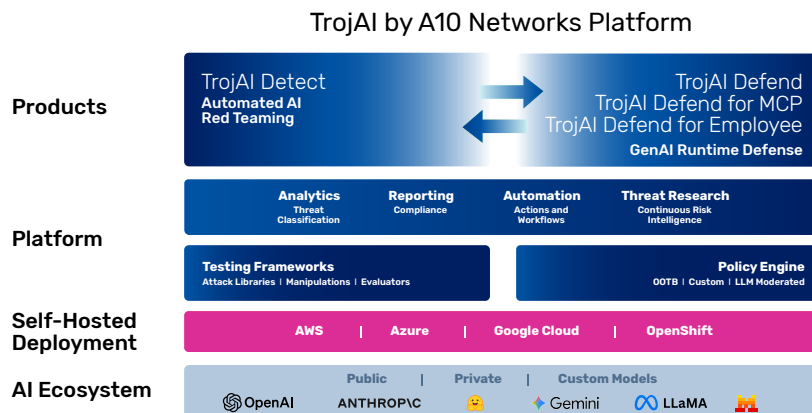


TrojAI Defend for Employee Usage

Runtime defense for employee use cases:

- Monitor employee usage of popular third-party GenAI apps in browsers
- Block and redact prompts with PII or sensitive data in real time
- Increase visibility and compliance with robust usage policies





Enable the Secure Rollout of AI in the Enterprise

The TrojAI platform protects AI models, applications, and agents with automated red teaming and runtime defense solutions. TrojAI identifies and mitigates AI risks such as prompt injection, data leakage, toxic content, manipulation attacks, and more. The high-accuracy, low-latency platform is fully customizable and scalable to support the needs of large enterprises.

The AI Era is Now

As organizations increasingly implement AI, they face a growing number of attacks like prompt injections, jailbreaks, shadow and rogue MCP assets, data and PII leaks, and unwanted or toxic content.

These new attack surfaces have quickly become a significant risk for the enterprise. Without proper testing and protection, weaknesses in AI systems can quickly escalate into business-level incidents that impact operations, customers, and compliance. As a result, the very systems meant to accelerate the business can become its greatest vulnerability.

That's where TrojAI comes in. TrojAI enables large organizations to identify and mitigate risks across both AI development and runtime. The platform

strengthens the safety, security, and compliance of AI systems, giving security teams the confidence to adopt, deploy, and innovate with AI responsibly.

Building the Future of Secure AI

TrojAI envisions a future where confidence in AI is earned, not assumed. Where transparency, security, and accountability form the basis of trust. TrojAI is delivering that future now, making sure that AI innovation is matched by the ability to secure and govern it with confidence and control.

About A10 Networks

A10 Networks (NYSE: ATEN) delivers secure application and network solutions that protect, optimize, and scale business-critical systems across on-premises, hybrid cloud, and edge environments. Our portfolio enables large enterprises, service providers, and cloud platforms worldwide to deliver performance, reliability, and protection against cyber threats, while preparing their networks for the demands of AI and next-generation applications. Founded in 2004 and headquartered in San Jose, California, A10 Networks serves over 7,000 global customers.

For more information, visit A10Networks.com and follow us [@A10Networks](https://twitter.com/A10Networks).

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

©2026 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Logo, A10 Control, A10 Defend, A10 Harmony, Harmony, A10 Thunder, Thunder, ACOS, A10 SSL Insight, SSL Insight, SSLi, vThunder, ThreatX, and ThreatX Protect are trademarks or registered trademarks of A10 Networks, Inc. or its affiliates in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: A10Networks.com/a10trademarks.