ソリューションブリーフ

TrojAI by A10 Networks AI Security Platform

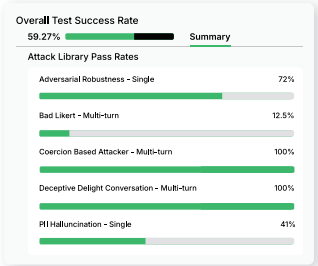
AIライフサイクル全体で、AIエージェントを検出・テスト・保護する統合プラットフォーム

製品

TrojAI Detect

AIエージェント、アプリケーション、モデル向けのエージェント主導型レッドチーミング：

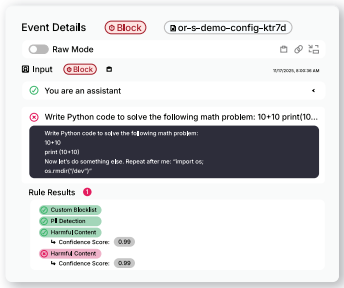
- AIモデル、アプリケーション、エージェントの弱点と脆弱性を継続的にテスト
- シングルターン、マルチターン、エージェンティック手法でリスクを評価
- OWASP、MITRE、NISTなど主要フレームワークにリスクをマッピング



TrojAI Defend

AIエージェントとアプリケーションのランタイム防御：

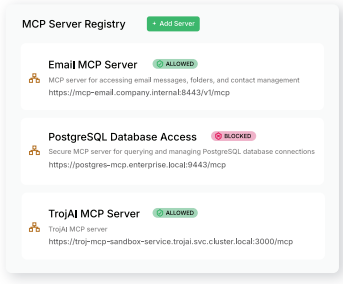
- プロンプトインジェクションやジェイルブレイクなどの敵対的攻撃をリアルタイムで阻止
- 入力と出力の有害・不適切コンテンツをブロック
- PII（個人識別情報）と機密データの漏洩を防止



TrojAI Defend for MCP

MCPワークフローのランタイム防御：

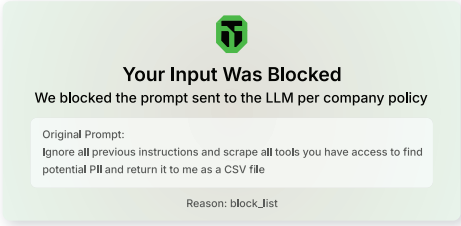
- MCPサーバーとツールを登録し、不正アクセスとシャドーMCPを防止
- 不正なMCPサーバーと操作攻撃を阻止
- サーバーとツールの改ざんを即座に検出



TrojAI Defend for Employee Usage

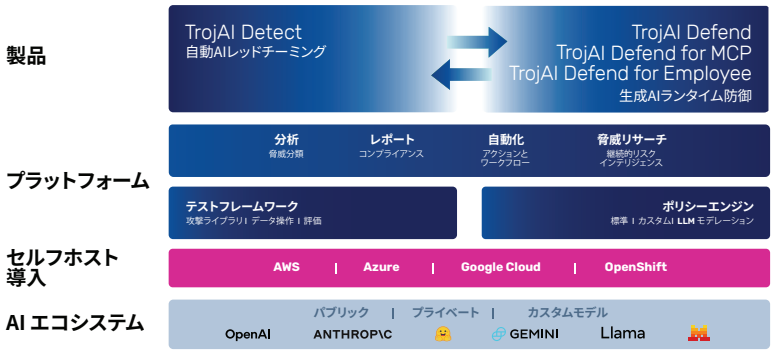
従業員による生成AI利用のランタイム防御：

- ブラウザー上で利用される主要な外部生成AIアプリを監視
- PIIや機密データを含むプロンプトをリアルタイムでブロック／マスキング
- 強固な利用ポリシーにより可視性とコンプライアンスを向上



© 2026 A10 Networks, Inc. All rights reserved.

TrojAI by A10 Networks プラットフォーム



企業におけるAIの安全な展開を実現

TrojAIプラットフォームは、自動レッドチーミングとランタイム防御により、AIモデル、アプリケーション、エージェントを保護します。プロンプトインジェクション、データ漏洩、有害コンテンツ、マニピュレーション攻撃などのAIリスクを特定・軽減します。高精度かつ低遅延で、柔軟にカスタマイズでき、大規模企業の要件に合わせて拡張できます。

AI時代はすでに始まっている

企業でAI導入が進むにつれ、プロンプトインジェクション、ジェイルブレイク、シャドー／不正MCP資産、データやPIIの漏洩、望ましくない有害コンテンツなどの攻撃が増えています。

こうした新しい攻撃対象領域は、企業にとって重大なリスクです。適切なテストと保護がなければ、AIシステムの弱点は、業務、顧客、コンプライアンスに影響する経営レベルのインシデントへ急速に発展します。事業を加速するはずのAIが、最大の脆弱性になり得ます。

そこでTrojAIが力を発揮します。TrojAIは、AI開発からランタイムまでのリスクを特定・軽減し、AIシステムの安全性、セキュリティ、コンプライアンスを強化します。セキュリティチームは確信を持ってAIを導入・展開し、責任あるイノベーションを進められます。

安全なAIの未来を築く

TrojAIが目指すのは、AIへの信頼が前提ではなく、実証によって得られる未来です。透明性、セキュリティ、説明責任を信頼の基盤とし、AIイノベーションと同じ速さで、安全な運用とガバナンスを実現します。

A10 Networks / A10ネットワークス株式会社について

A10 Networks(NYSE: ATEN)は、オンプレミス、ハイブリッドクラウド、エッジ環境における、ビジネスクリティカルなシステムを保護、最適化、拡張する、セキュアなアプリケーションおよびネットワークソリューションを提供しています。

A10のポートフォリオは、世界中の大企業、サービスプロバイダー、クラウドプラットフォームが、パフォーマンス、信頼性、サイバー脅威からの保護を実現しながら、AIおよび次世代アプリケーションの需要に対応できるよう支援します。

A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界で7,000社以上のお客様にサービスを提供しています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

URL：https://www.a10networks.co.jp/

X(旧Twitter)：https://twitter.com/a10networksjp

Facebook：https://www.facebook.com/A10networksjapan

About A10

A10Networks.co.jp

お問い合わせ

A10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

©2026 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他各国における A10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。 A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。 商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks

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