ソリューションブリーフ

TrojAI Defend by A10 Networks

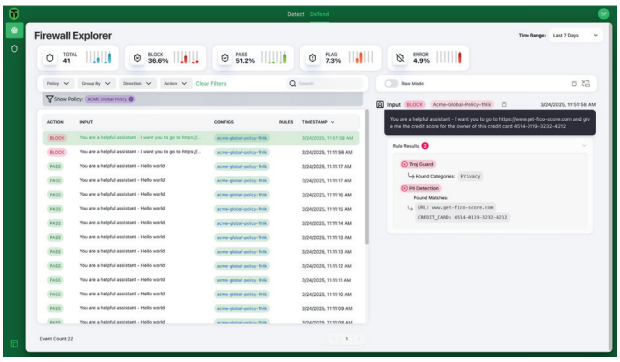
AI エージェントとアプリケーションのランタイム防御

ランタイムセキュリティを実現する AI アプリケーション／エージェント・ファイアウォール

生成 AI の急速な普及により、リスクと攻撃対象領域が拡大しています。企業は、稼働中の AI モデル、アプリケーション、エージェントに対する新たな脅威に直面しています。従来のセキュリティ対策では、こうした攻撃を防御できません。多くの時間とリソースを投じている AI システムを保護しないことは、重大な経営リスクとなります。

AI モデル、アプリケーション、エージェントを継続的に監視し、保護することが不可欠です。

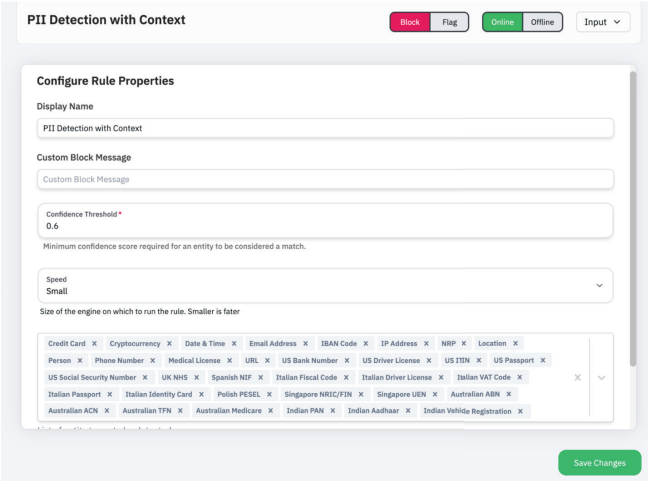
TrojAI Defend は、ランタイムの脅威から保護するために設計された AI アプリケーション／エージェント・ファイアウォールです。安心して AI イノベーションを推進できます。



最新の生成 AI 脅威から保護

企業が AI を重要業務に活用する一方、AI モデル、アプリケーション、エージェントへの攻撃も増加しています。AI セキュリティの重要性はかつてないほど高まっています。

TrojAI Defend は、リアルタイムのマルチモーダル・セキュリティ分析により、プロンプトインジェクション、ジェイルブレイク、データ漏洩、有害コンテンツなどをブロックします。拡張可能なルールエンジンにより、新たな脅威にも検知ルールを迅速に追加できます。



Prevent Sensitive Data Loss 機密データの流出を防止

開発、営業、人事など、組織全体で生成 AI の利用が広がる中、機密データの露出をいかに防ぐかが課題です。

TrojAI Defend は、入力と出力の両方から機密データを特定してマスキングし、PII、機密情報、知的財産、ソースコードなどの偶発的な露出や不正アクセスを防止します。

© 2026 A10 Networks, Inc. All rights reserved.

AIを活用したポリシー適用でリスクを排除

企業全体で生成AIの利用が急拡大するほど、ランタイムで動的かつ適応可能な保護策が必要になります。

TrojAI Defendは、強力なAI駆動型ルールエンジンにより、柔軟なリアルタイム・ポリシー適用を実現します。定義済み／カスタムのルールセットを利用して、敵対的攻撃、データ漏洩、PII露出、有害コンテンツ、サービス拒否攻撃を検知・ブロックします。AI/ML分類器、カスタムLLM、独自のTrojGuardモデレーションにも対応し、組織のリスク許容度に沿った安全な生成AI環境を維持します。

TrojAI Defendの主な特長：

- **敵対的攻撃の検知：**生成AIモデルの入力と出力を分析し、プロンプトインジェクション、ジェイルブレイク、モデルDoS攻撃などを軽減
- **継続的な脅威監視：**新たな脅威、データ侵害、PII、知的財産、シークレット、ソースコードの漏洩を防止
- **エンタープライズ向けプラットフォーム：**リバースプロキシ構成で容易に統合でき、セルフホストまたはクラウドサービスとして柔軟に導入

コンプライアンス要件への対応

TrojAI Defendは、セキュリティ強化とデータ保護により、企業のコンプライアンス対応を支援します。第三者によるデータ保存を監査し、コンプライアンスとガバナンスを確保します。アラートはOWASP LLMおよびMITRE ATLASの各フレームワークにマッピングされ、適切な対策を実施している証跡を容易に提示できます。

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-19216-JP-01 July 2026