Zscaler AI Securityの概要

概要

AIセキュリティのメリット

AI資産とリスクの可視化
シャドーAIや高リスクのアプリから、AIモデルやパイプラインに至るまで、自社のAIエコシステム全体を検出し、可視化します。

AIの脆弱性を特定
継続的かつ自動化されたテストにより、AIシステムの脆弱性やリスクをレッドチームにより検証します。

AIアクセスの保護
インライン型AIガードレールを活用し、脅威対策、情報漏洩防止、安全な利用の確保をリアルタイムで実施します。

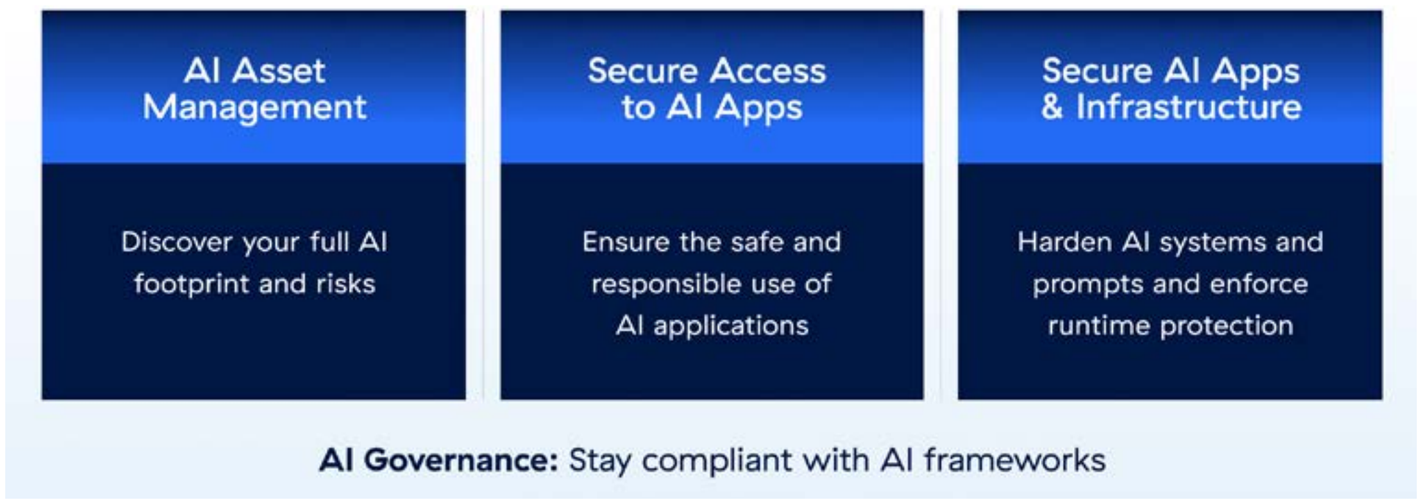
AIコンプライアンスのガバナンス
AIフレームワークを活用してAIフットプリントと展開を管理し、リスクコンプライアンスを維持します。

ZscalerによるエンドツーエンドのAIセキュリティ

Zscalerは、AIの持つ変革力を組織が最大限に活用できるよう支援するとともに、関連するリスクを適切に管理するためのAI活用型ソリューションを提供します。

リスクの高いAI利用の特定から、安全な開発の確保、さらに高度なインライン防御による機密性の高いビルドの保護まで、幅広い機能を備えています。

Zscalerは、安全なAIイノベーションという概念を再定義します。AIの潜在能力を安全に活用し、リスクを恐れない成長をZscalerが後押しします。



AIセキュリティにZscalerが選ばれる理由

AIライフサイクル全般にわたって保護
発見から導入まで、AIセキュリティを包括的に提供

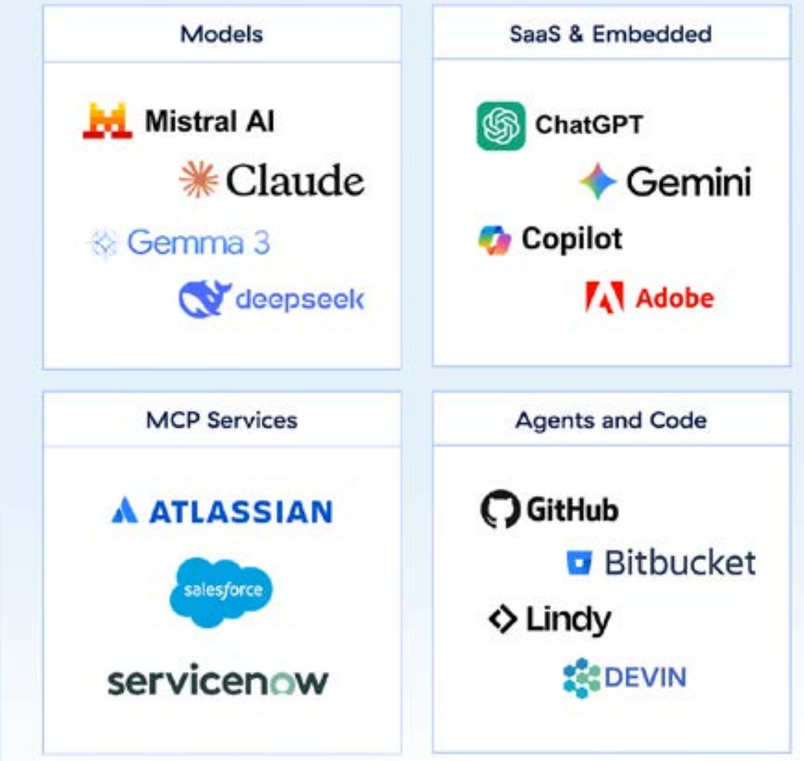
統合プラットフォーム
AIセキュリティをゼロトラストと統合した実績あるプラットフォーム

実績あるパートナー
お客様の成功と変革を支援してきた豊富な専門知識

AI SPMによる資産の可視化

急速に進化する現在のAI環境において、組織のAIフットプリントを把握することは容易ではありません。シャドーAI、モデル、サービス、MCPサーバー、パイプラインに対する十分な可視性がなければ、組織がリスクを効果的に検知し対応することは困難になります。

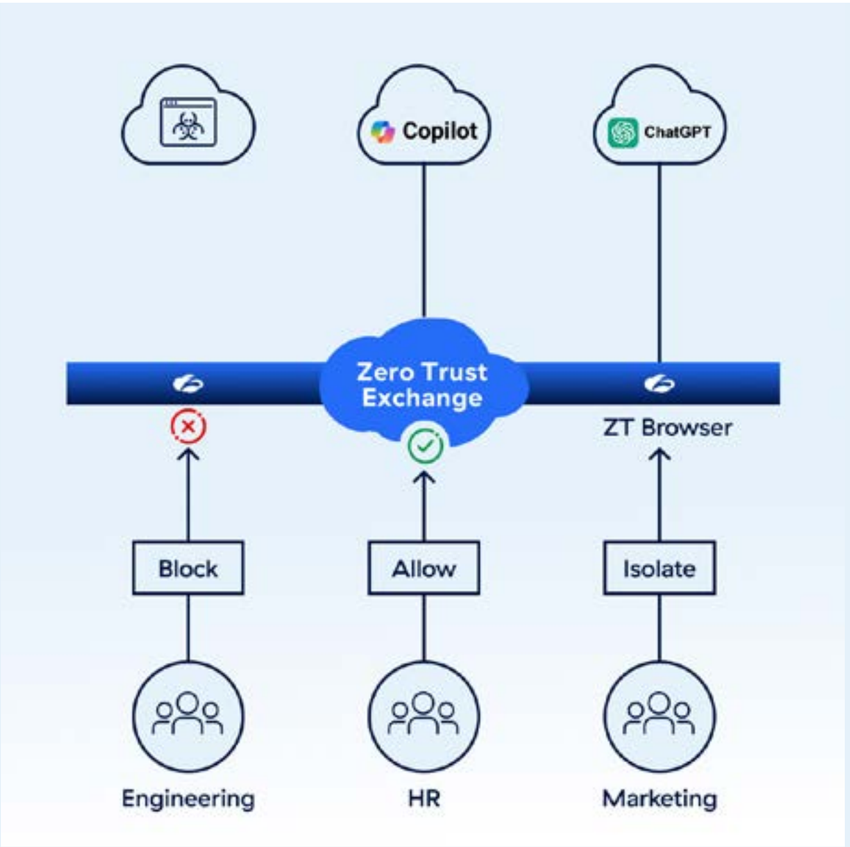
ZscalerのAI SPMを活用することで、組織はAIエコシステム全体を包括的に可視化できます。生成AIアプリ、LLM、モデル、MCPサーバー、パイプラインにわたる利用状況を把握し、データやビジネスを危険にさらす可能性のある高リスクの露出箇所や脆弱性を特定することが可能です。



AIアクセス セキュリティ

生成AI SaaSアプリケーションへのアクセス制御とセキュリティ確保は、ますます難しくなっています。シャドーAIの無秩序な拡大や、情報漏洩およびコンプライアンス違反利用のリスクが高まるなかで、組織にはこれらの脅威に対処する効果的な解決策が求められています。

ZscalerのAI Access Securityを活用すれば、AIアプリケーションの安全でコンプライアンスに準拠した責任ある利用を徹底できます。きめ細かいアクセス制御を適用し、どのユーザーやアプリがAIツールを利用できるかを管理します。さらに、DLP保護や分離技術を活用してプロンプト経由での情報漏洩を防止し、コンテンツ モデレーションを適用することで、組織の利用規定への準拠を確保します。



©2026 Zscaler, Inc. All rights reserved.

自動レッド チーミングによる検証

AIシステムの脆弱性検証は、多くの場合、複雑で時間のかかるプロセスです。専任のレッド チーム リソースを持たない組織にとって、徹底した評価を実施することはほぼ不可能に思えることがあります。

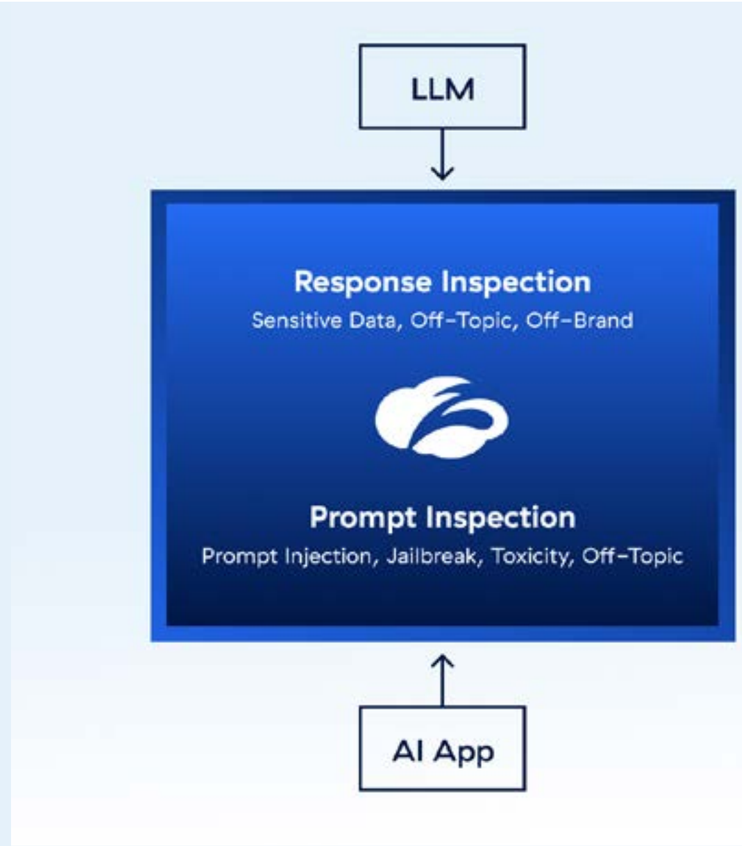
Zscalerの自動的かつ継続的なレッド チーミングは、革新的な自動レッド チーミング エンジンにより、こうした課題に対応します。25種類以上の事前定義プローブに加え、完全なカスタム プローブやデータセットのアップロードにも対応しており、SPLXは、組織の特定のドメイン、規制環境、ユース ケースに合わせてテスト シナリオを柔軟に設定できるようにします。



AI Guardによるインライン保護

LLMは、脅威や情報漏洩の新たな攻撃ベクトルとして急速に悪用され始めています。これらの通信に対して高パフォーマンスなインライン検査を実施できなければ、組織はデータ露出やAIシステムの侵害、悪意のある攻撃に対して脆弱な状態に置かれます。

ZscalerのAI Guardを活用すれば、AIプロンプトや操作に対する高性能なインライン検査を実現できます。プロンプト インジェクションやジェイルブレイクといったリスクの高い脅威を検知し、機密情報の漏洩を防止するとともに、コンテンツ モデレーションを通じて安全な利用と利用規定の順守を徹底します。インライン検査の分野で確立した実績と知見を活かし、Zscalerは重要なAIトラフィックを確実に保護します。

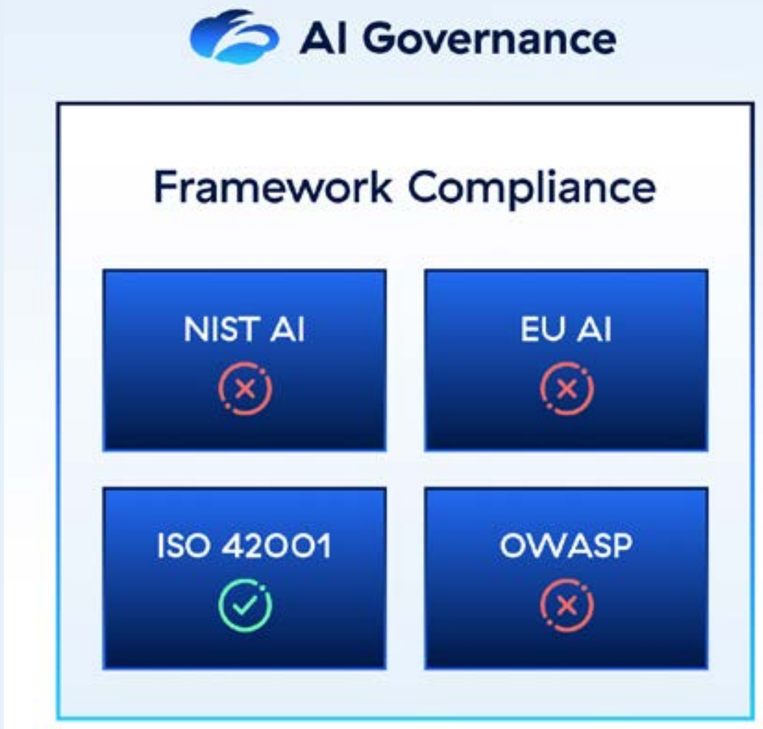


©2026 Zscaler, Inc. All rights reserved.

AI SPMによるAIガバナンス

組織が大規模にAIを導入するなかで、AIシステムのコンプライアンス確保とガバナンスの維持はますます複雑化しています。ポリシー順守状況やAIフレームワークに対する適切な監督がなければ、組織は法律、財務、評判上のリスクにさらされる可能性があります。

ZscalerのAIガバナンス アプローチを活用すれば、コンプライアンス監視を自動化し、レポーティング プロセスを効率化できます。AIシステムが社内ポリシーや規制基準に準拠しているかを継続的に監視するとともに、監査対応や各種要件を満たすためのエビデンスを提供します。AI利用がガバナンス フレームワークに沿って適切に運用されるよう支援し、組織のリスク低減と健全な事業運営を実現します。



Zscalerについて

Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータ センターに分散されたSSEベースのZero Trust Exchange™は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

© 2026 Zscaler, Inc. All rights reserved. Zscaler™および**zscaler.com/jp/legal/trademarks**に記載されたその他の商標は、米国および/または各国のZscaler, Inc.における(i)登録商標またはサービス マーク、または(ii)商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

Zero Trust Everywhere