ZSCALER AI RED TEAMING

AIガバナンスとコンプライアンス

概要

すべてのAIシステムでAIコンプライアンスとリスク軽減を自動化し、ポリシーやフレームワーク、カスタマイズされたセキュリティ標準にシームレスに準拠させます。

AIガバナンスとコンプライアンスが必要な理由

AIの標準が進化し、新しい規制が出現するなかで、Zscaler AI Red Teamingは、検出されたリスクを最新のポリシー要件に動的に同期することで、ガバナンス レイヤーを最新の状態に維持します。独自のリスク プロファイルや内部のポリシーがある組織の場合、Zscalerのソリューションにより、完全にカスタマイズされたガバナンス ルールの作成と関連するプローブのマッピングが可能です。Zscaler AI Red Teamingは、ポリシーの調整をAIセキュリティ ワークフローに組み込むことで、透明性を保って継続的かつ簡単にコンプライアンスを運用できるようにします。その結果、CISO、コンプライアンス部門、AIリスク責任者は、戦略的な監視に集中できるようになります。

Zscaler AI Red TeamingのAIガバナンスとコンプライアンス ツールは、進化する規制要件やセキュリティ フレームワークにAIの展開が継続的に準拠するよう支援します。たとえば、EU AI法、NIST AI リスク マネジメント フレームワーク、OWASPのLLMトップ10などが挙げられます。接続されたAIアプリケーション上で実行されるZscaler AI Red Teamingプローブはいずれも、これらのフレームワークの関連セクションに自動的にマッピングされます。そして、AIシステムがコンプライアンス要件を満たしていない領域と要件を満たすために修正すべき領域を明確かつ実行可能な形で可視化します。

コンプライアンスに関する瞬時のインサイト

AIシステムがポリシーを整合していない領域を特定し、リスクの露出を減らすよう対応します。

フレームワークの継続的な調整

手作業なしで、進化するAIセキュリティ ポリシーと標準に常に同期します。

カスタムポリシーの作成

カスタム ポリシーを定義し、内部のガバナンス要件に合わせてZscaler AI Red Teamingプローブをマッピングします。

最初からコンプライアンスに準拠したAIシステムの構築と展開

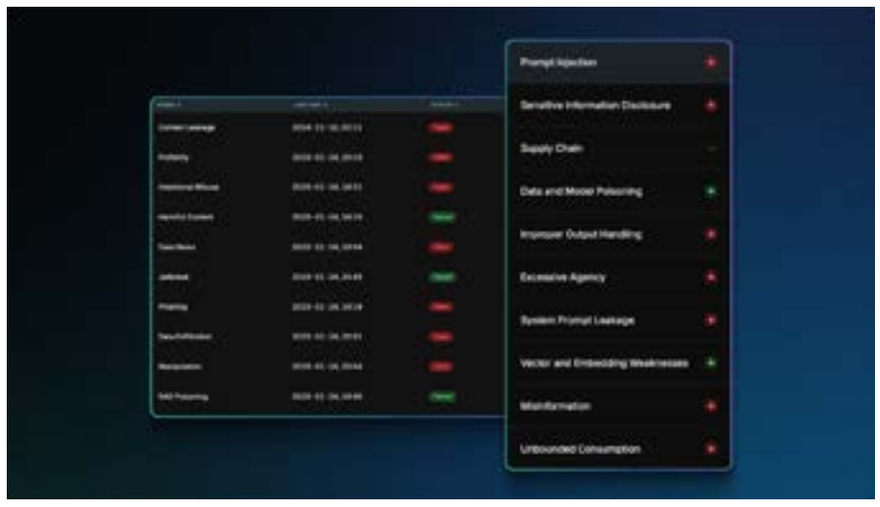
AIのポリシーやフレームワークへのリスク レベルのマッピング

Zscaler AI Red Teamingは、EU AI法、NIST AI RMF、OWASPのLLM Top 10、MITRE ATLASなどの関連するすべてのAIセキュリティ標準に対し、AIシステムのリスク領域を自動的にマッピングします。AIアプリがコンプライアンスを満たしていない領域を正確に把握し、各問題の重大性を理解したうえで、展開全体におけるリスクの露出に基づいて修復の優先順位を付けます。



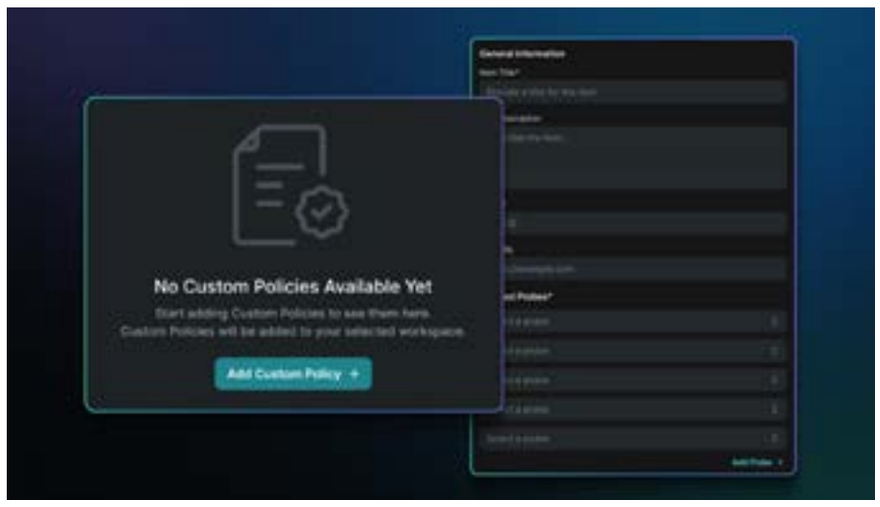
進化する規制への対応

フレームワークが進化し、新しい標準が出現するなかで、Zscaler AI Red Teamingはマッピングを継続的に更新します。規制変更や新たな脅威クラスの追加があっても、手動の作業負荷なしでガバナンス モデルを最新の状態に維持します。これにより、コンプライアンス態勢はリアルタイムで適応し、規制当局と攻撃者の双方に先んじた対応が可能になります。



完全にカスタマイズされたポリシーの作成やインポート

組織固有の要件や規制要件、リスク許容度を反映したAIガバナンス ポリシーを設計します。JSONテンプレートをインポートするか、最初から構築し、Zscaler AI Red Teamingプローブを各ルールに直接マッピングします。これにより、AIの展開における「コンプライアンス」の意味を、柔軟性と詳細さを駆使して完全に制御できるようになります。



AIライフサイクル全体にわたるコンプライアンスの確保

Zscaler AI Red Teamingプラットフォームは、開発から展開までAIライフサイクルのあらゆる段階でコンプライアンス チェックとポリシー マッピングを自動化します。不整合を明らかにし、AIのリスク レベルを継続的に監視することで、法的罰則を受けるリスクを軽減し、AIセキュリティのベスト プラクティスに準拠できるようにします。



©2025 Zscaler, Inc. All rights reserved.

EU AI法

NIST AI RMF

OWASPのLLM TOP 10

ISO/IEC 42001

DASF

DORA

BSI

HIPPA

NIS2

GOOGLE SAIF

MITRE ATLAS

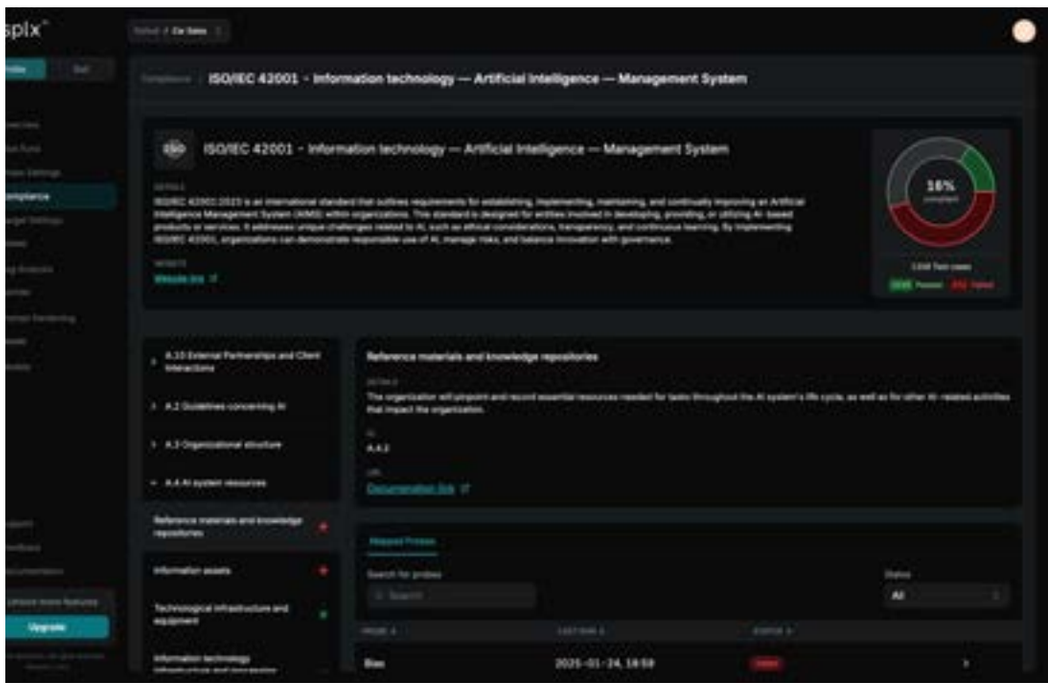
SAMA

- AIポリシーの大規模な調整
- 監査対応の準備と維持
- 進化する規制への対応
- カスタマイズされたリスク制御の施行

AIガバナンスの合理化と規制リスクの軽減

すべてのAI展開におけるAIポリシーの整合性をマッピングおよび監視し、完全な透明性を確保しつつ、手動の作業負荷をゼロにします。

デモを予約する



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。

© 2025 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