ZSCALER AI RED TEAMING

AIを活用した資産検出と管理

概要

LLM、ワークフロー、MCPサーバー、ガードレールなど、あらゆるAI資産を自動的に検出および保護し、包括的にポスチャーを可視化します。

AIアセット管理が必要な理由

組織でのAI技術の導入が加速するなかで、LLM、AIワークフロー、さらにはMCPサーバーやAIガードレールといったAIシステムが、かつてないスピードで部門横断的に構築および展開されています。この状況は、セキュリティ責任者にとって重大な課題をもたらします。多くの組織では、どれだけのAIコンポーネントが使用されているのか、それらがどこに展開されているのか、さらには安全に利用できるのか、また内在するセキュリティ リスクが何であるのかを把握できていません。

大企業においてその規模は驚くべきもので、数百、場合によっては数千ものAIモデルが、セキュリティ部門の把握が及ばないまま、複数の事業部門にまたがって使用されているケースも少なくありません。集中管理されたインベントリーがなければ、CISOやその部門は、リスク評価、コンプライアンスの徹底、あるいは安全でないAIコンポーネントが本番環境に導入されるのを防ぐために必要な可視性を確保できません。

ZscalerのAI Red TeamingにおけるAI資産管理は、この重大な透明性と可視性のギャップを解消します。あらゆるLLM、ワークフロー、MCPサーバー、ガードレールの検出情報を単一のAI-BOMに統合することで、Zscaler AI Red Teamingは、利用状況を正確に把握し、脆弱性を分析し、導入に適したものを判断するための明確な可視性をセキュリティ責任者に提供します。同時に、AIの透明性や説明可能性を重視するAIポリシー要件の強化にも対応します。この統合的な可視性こそが、組織規模でAIを保護するための基盤となります。

統合AIインベントリー

組織で利用されるすべてのLLM、ワークフロー、MCPサーバー、ガードレールが一元化された、信頼できる唯一の情報源です。

AI-SPMの合理化

AIの検出、セキュリティ テスト、ランタイム保護、コンプライアンス マッピングを1つのツールに統合します。

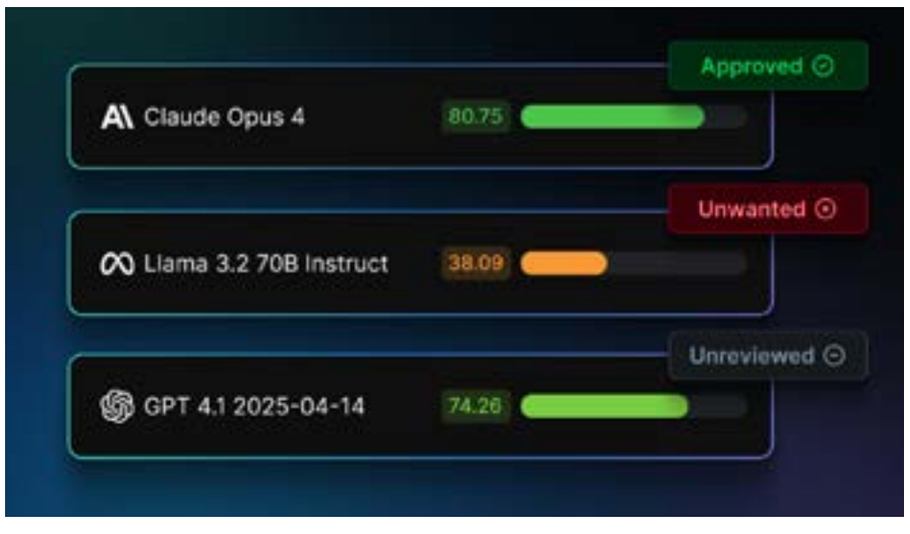
組織規模の可視性

数千に及ぶモデルやワークフローを明確に把握し、安全に導入できるものを見極めます。

統合AI-BOMによってAIスタック全体を完全に可視化

すべてのAIモデルの検出と承認

組織全体で使用または展開されているすべてのLLMを自動的に検出し、Zscaler AI Red Teamingの信頼されたベンチマークにマッピングします。セキュリティ部門は、リスクを評価し、安全性スコアを比較することで、危険なモデルを迅速に特定できます。各モデルは承認またはブロックを設定でき、CISOは組織内での利用および展開を完全に管理できます。



MCPサーバーをスキャンし、脆弱性を特定

MCPサーバーは、AIスタックにおける重要なオーケストレーション層として機能しますが、十分に監視されていないケースが少なくありません。Zscaler AI Red Teamingは、これらのMCPサーバーを自動的に検出およびスキャンし、攻撃者に悪用される可能性のある脆弱性や設定ミスを特定します。MCPの可視性を統合AI-BOMに組み込むことで、セキュリティ部門は脆弱なポイントを是正し、セキュリティを確保できます。



AIワークフローを可視化し、セキュリティ テストを実行

ソース コード リポジトリーを継続的にスキャンし、AIワークフローを検出および可視化することで、内部に含まれるすべてのエージェント、ツール、MCPサーバーを明らかにします。自動化されたリスク評価により、設定ミスや潜在的な脆弱性を特定し、AIセキュリティ部門が悪用される前にワークフローを保護し、リスク エクスポージャーを低減できるよう支援します。

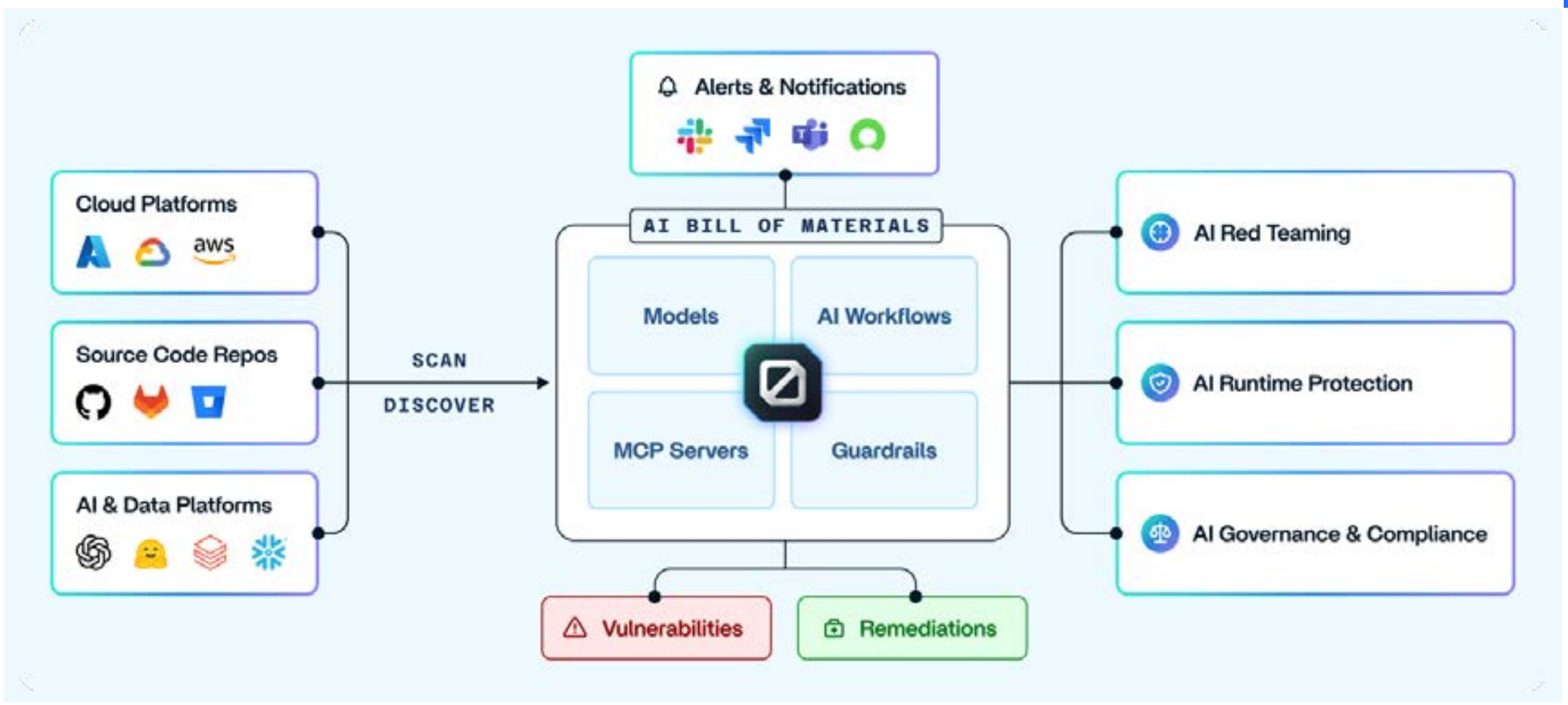


AIスタックを統合し、完全に可視化

Zscaler AI Red Teamingは、主要なクラウド プロバイダー、ソース コード リポジトリー、AI/MLプラットフォーム、データ システムと連携し、組織全体にわたってAIアセットを包括的に検出します。数千に及ぶ環境を単一のAI-BOMに統合することで、可視性の抜け漏れを排除し、セキュリティ責任者に、組織規模で求められる可視性とコンプライアンス対応力を提供します。



©2025 Zscaler, Inc. All rights reserved.



AIセキュリティ ポスチャー管理(AI SPM)

AIセキュリティ態勢の包括的な可視性と制御を実現

すべてのAIコンポーネントを単一のインベントリーに集約し、組織のAIシステムを大規模かつ安全に保護します。

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