

Zscaler AI Guard

概要

悪意のある行為や機密データの漏洩を防ぐガードレールによる本番環境のAIの保護

AI Guardを選ぶ理由

企業では、カスタマー エクスペリエンスの向上、従業員の生産性向上、ビジネス プロセスの合理化を目的として、AIアシスタントやAIエージェントを構築するケースが増えています。しかし、AIを本番環境に展開することにはリスクが伴います。たとえ広範なレッド チーム演習で脆弱性を特定しても、運用開始後のAIアプリは操作の標的となります。攻撃者は、プロンプト インジェクション、ジェイルブレイク、サプライ チェーンの脅威を駆使し、データ漏洩、有害な出力、望ましくない動作を引き起こそうとします。さらに、商用の生成AIアプリを使用する従業員も、データ漏洩のリスクを招きます。

Zscaler AI Guardは、ユーザー、AIアプリ、LLM (商用の主要な生成AIツールを含む)間の脅威を検知およびブロックすることで、本番環境でAIを安全に運用できるよう支援します。AIの振る舞いにガードレールを施行し、社内外のポリシーとの整合性を確保するとともに、リスク管理に必要な可視性と制御を提供します。また、AI GuardはChatGPT、Gemini、Microsoft 365 Copilotなどのアプリの使用状況を監視および管理することで、AIの安全性、信頼性、ビジネスとの整合性を維持します。



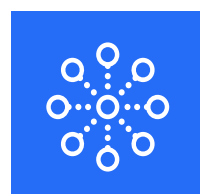
高い精度と低い誤検知: AIを活用したエンジンは、安全なコンテンツを過剰にフィルタリングすることなく、有害な入力や悪意のある入力をブロックします。重大度設定により、適切な優先順位を設定できます。



幅広い検知範囲: プロンプトと応答に適用できる18種類以上の検知機能により、幅広い攻撃パターンや脆弱性を特定できます。ChatGPTやMicrosoft Copilotなどの一般的なアプリにも対応しています。



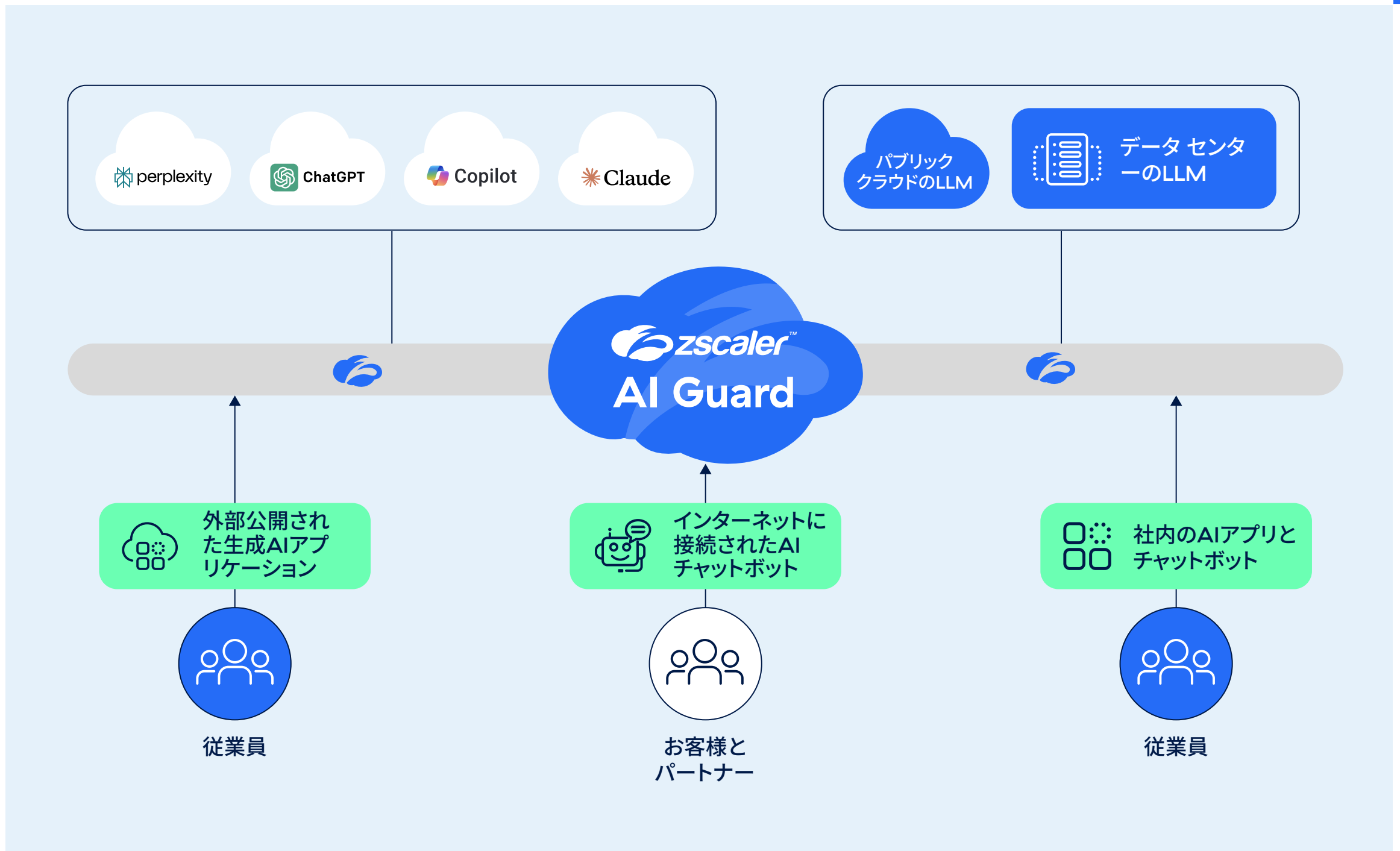
機密性の高いコンテンツの高精度の特定: 強力な保護機能により、一般的な生成AIアプリにアクセスするユーザーと、LLMとやり取りする組織のAIアプリの両方に対し、機密データの漏洩を特定し、防止します。



AIライフサイクル全体のセキュリティ: Zscaler AI Red TeamingとAI Guardはシームレスに連携することで、開発から本番運用に至るまで脆弱性を特定し、AIアプリを保護できるよう支援します。



クラウドベースのAIプラットフォームやフレームワークの活用: LLMに簡単に接続し、AWS、Azure、Google Cloud、Langchain、Palantir Webhookなどの一般的なクラウドベースのAIプラットフォームやフレームワークで活用できます。



 法律とコンプライアンスのリスク軽減

 企業の信頼と評判の維持

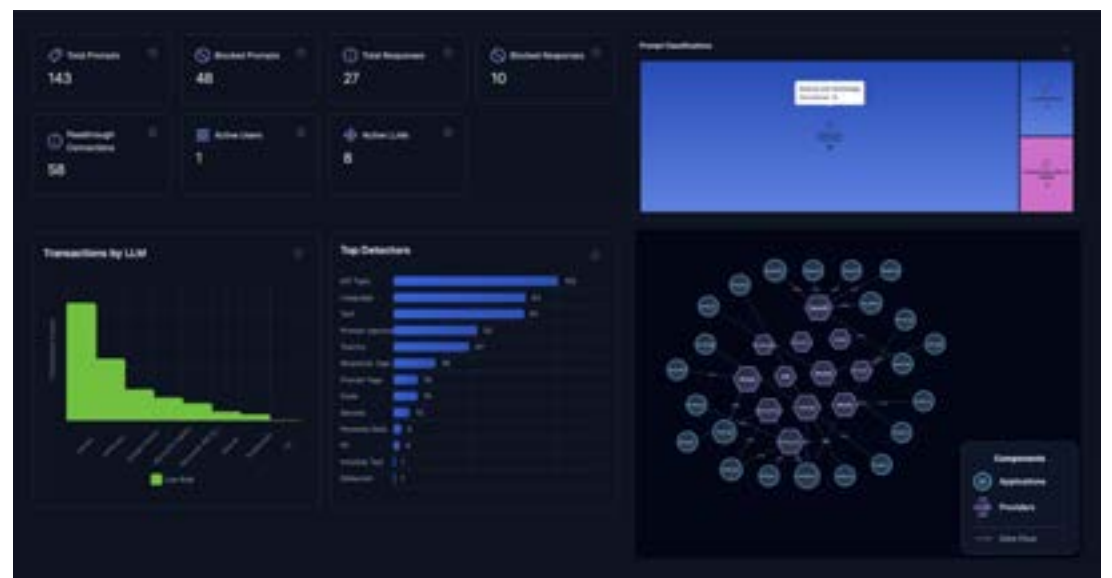
 インシデント対応の自動化

 脅威への予防的な対応

AIアプリ向けの超高速ガードレール

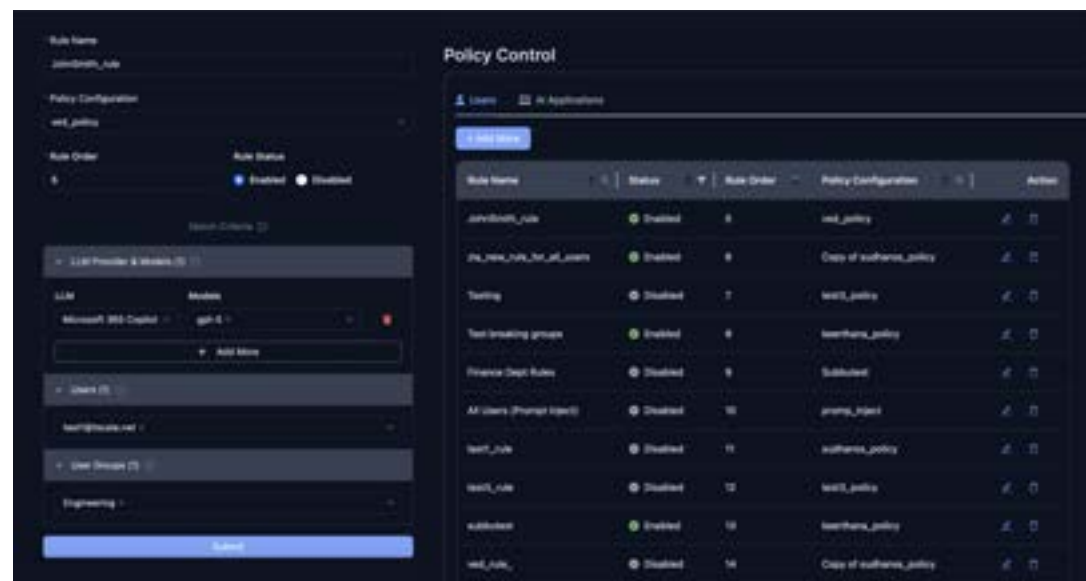
継続的な可視性とインサイトの提供

商用と組織用両方のAIアプリについて、アクセスするLLM、その使用状況、プロンプトと応答を監視し、シャドーAIを検出するとともに、ビジネスの整合性を確保します。



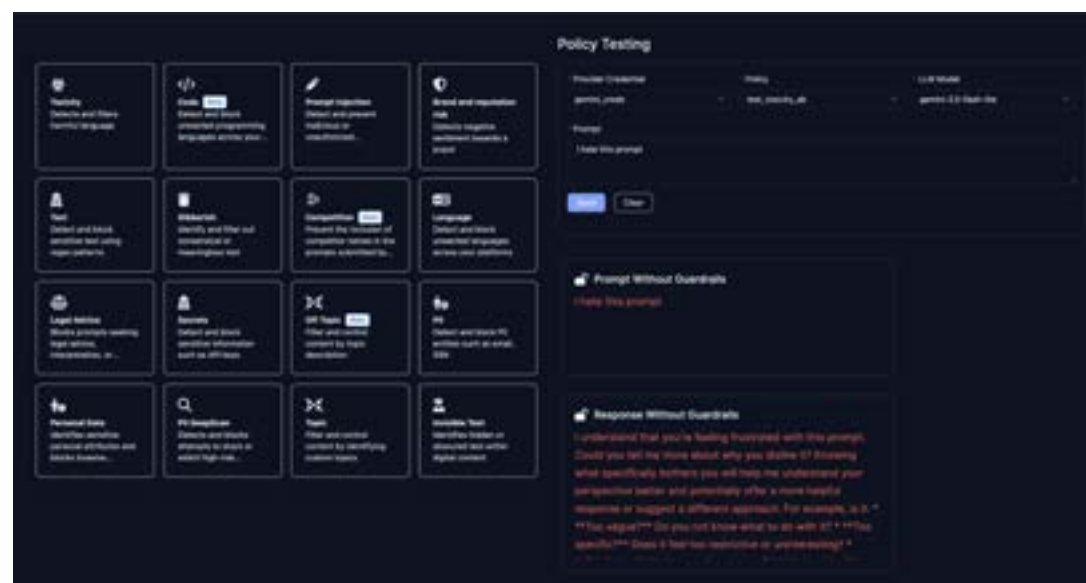
一般的なAIアプリ使用の管理

ChatGPT、Gemini、Microsoft Copilotなどの一般的なAIアプリに誰がどのようにアクセスし、使用するか制御します。特定のユーザーやユーザーグループにポリシーを作成し、適用することで、コンプライアンスを確保し、データ漏洩を防止します。



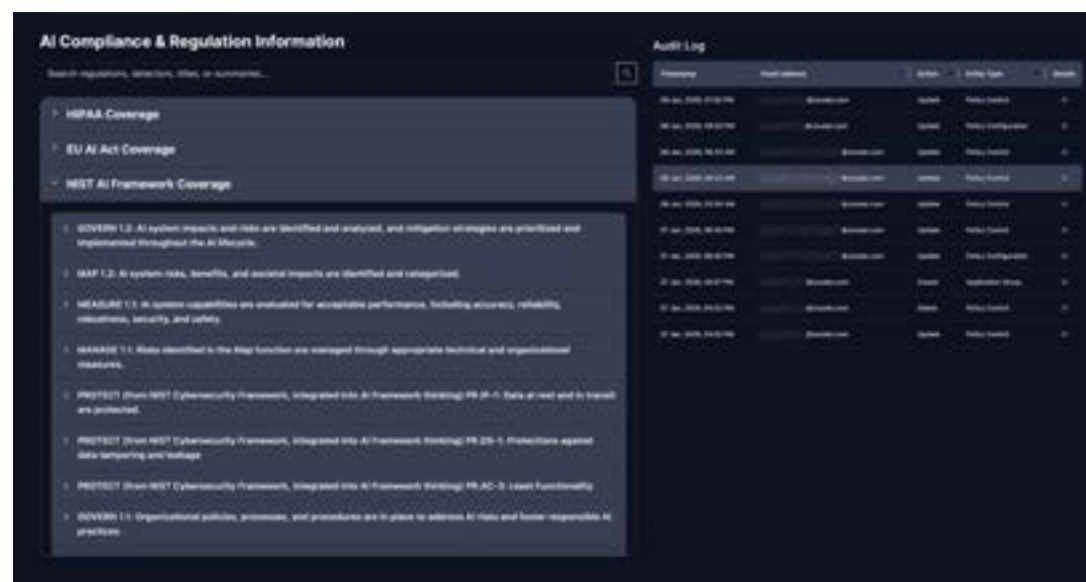
本番環境でのAIアプリの保護

プロンプトインジェクション、埋め込みコード、不適切な内容の話、有害な内容、悪意のある出力などの敵対的攻撃から組織のAIアプリを保護します。これにより、ビジネスの整合性を確保し、リスクを軽減します。AWS、Azure、Google Cloud、Langchain Agents、Palantir Webhook、AWS Boto3、Google Vertex SDKなどの一般的なクラウドベースのAIプラットフォーム、SDK、AIエージェントフレームワークとシームレスに統合します。



AI使用状況の監査およびプライバシーとコンプライアンスの確保

NIST AIフレームワークやEU AI法などの最新の標準に準拠できるように、ユーザー、アプリ、プロンプト、応答、ポリシー、操作の記録を維持します。Zscalerはプロンプトや応答を保存しません。すべての顧客データは、アクセスを保護するためにお客様の鍵によってAmazon S3バケットに保存されます。



AIアプリの確実な展開

脅威の特定とガードレールの施行により、運用中のAIアプリを保護

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をご覧ください。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。



Zero Trust
Everywhere