AWSで稼働するAIアプリ向けのゼロトラスト セキュリティ

課題

メリットがある一方、アクセスとセキュリ ティの面で新たな課題を引き起こすAI

企業は、よりよい意思決定、成長の加速、効率性の向上のためにAIアプリは欠かせないと考えています。しかし、エージェント型AIを含むAIアプリには、可視性やアクセス、セキュリティにおいて、重大な課題があります。

2026年版 Zscaler ThreatLabz AIセキュリティ レポートに より、企業におけるAI/MLトランザクションが前年比で83%増加し、3,400以上ものAIアプリが利用可能であることが明らかになりました。こうしたトラフィックは金融/保険業および製造業において最も多く発生しています。しかし、データ漏洩、 不正アクセス、コンプライアンスへの懸念により、トランザク ションの39%がブロックされています。

Zscalerのソリューション

あらゆる場所でのAI利用を保護する、実績のあるゼロトラスト プラットフォーム

Zscalerを利用することで、組織は、機密データの漏洩を防ぎながら、パブリックおよびプライベートのAIアプリとのやり取りを可視化し、制御できるようになります。Zscaler Zero Trust Exchange™は、あらゆる場所のすべてのユーザー、アプリケーション、ワークロードに対して、ゼロトラストのアクセスとセキュリティを提供するクラウド ネイティブ プラットフォームです。

さらに、堅牢なダッシュボード、プロンプトと応答の可視化、および強力な情報漏洩防止制御により、データの安全性とユーザーの生産性が維持されます。Zscalerは、従来のVPNやファイアウォールに伴うセキュリティの脆弱性、パフォーマンスの遅さ、コストや複雑さといった問題も解消します。

メリット

Zscalerは、10年以上にわたってゼロトラストのリーダー[1]であり、AWS AIコンピテンシー パートナー(エージェント型AIアプリケーション カテゴリー)として、世界中の数千のAWS顧客を保護しています。

きめ細かな可視化

AIアプリや部門別の使用状況を自動的に検出し、ユーザーのプロンプトと応答を可視化します。ダッシュボードには、さまざまな傾向や機密データの取引状況などが表示されます。

機密データを保護

AIを活用したデータ検出により、エンドポイント、インライン、パブリック クラウドのすべてで、機密データを特定します。AIアプリに送信される機密データをブロックし、設定ミスや脆弱性を特定して、リスクを修復します。

ゼロトラスト アクセス

ユーザーによるAIアプリへのアクセスを管理し、一貫したポリシーを適用します。これに基づき、直接アクセスの許可、ブロック、警告、または カット、ペースト、ダウンロードを防止するブラウザー分離を使用したアクセス許可を決定します。

Amazon Bedrockの保護

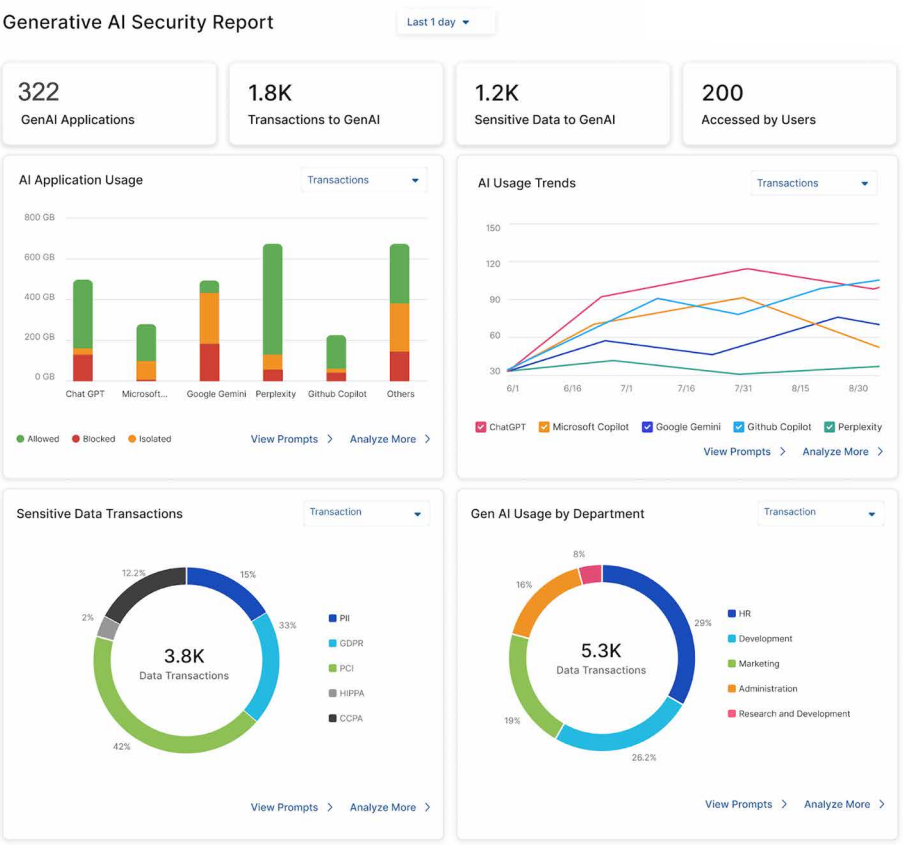
Zscaler AI-SPMは、AI環境におけるAIの導入状況、トレーニング データ、設定、および潜在的な不正使用を監視し、セキュリティおよびコンプライアンスのリスクを軽減します。

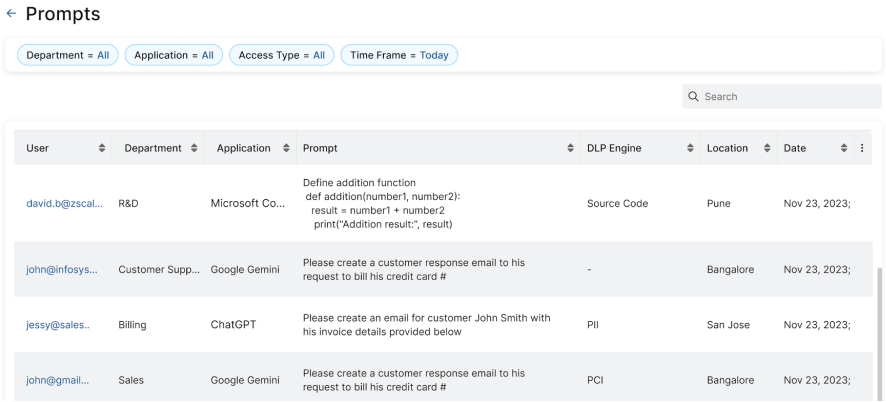
[1]Gartner® セキュリティ サービス エッジ(SSE)のMagic Quadrant™

Zscaler Zero Trust

Zscaler Zero Trust Exchangeは、世界最大のインライン セキュリティ クラウドです。ほとんどのAWSリージョンに対応する、グローバルな160か所以上のPoPを活用することで、ユーザー、デバイス、アプリケーション、ワークロード間の安全な接続を確立します。

詳細な可視性と制御





AWS AIアプリの保護

Amazon Bedrock

Amazon SageMaker

Amazon Q

「セキュリティ部門は、Zscaler DLPにより、シャドー生成AIアプリの利用状況をきめ細かく可視化し、ユーザーが入力したプロンプトまで把握できます。AIアプリの利用が企業ポリシーに準拠しない場合は、リアルタイムでDLPによるブロックとアプリケーション アイソレーションを施行し、リスクを未然に防ぎます」。

Debashis Singh氏
Persistent、CIO

詳細はZscalerのAI向けセキュリティ、Zscaler AI-SPMおよびZscaler for AWSをご覧ください。

zscaler™ | Act fast. Stay secure.™

Zscalerについて
Zscaler (NASDAQ: ZS)は、ゼロトラスト セキュリティの先駆者であり、世界的なリーダーです。世界中の大企業や重要インフラ機関、政府機関がZscalerを採用し、ユーザー、拠点、アプリケーション、データ、デバイスを保護しつつ、デジタル トランスフォーメーションを加速させています。Zscaler Zero Trust Exchange™プラットフォームは世界160か所以上のデータセンターに分散され、高度なAIを活用して、毎日数十億件のサイバー脅威やポリシー違反を防ぎ、コストや複雑さを軽減しながら、現代企業の生産性向上を支援します。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™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、Zscaler Digital Experience™、ZDX™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