Zscaler AI Security Posture Management で AI の安全な導入を加速

概要

AI リソースやデータの保護における課題

IDC は、2028 年までに AI アプリケーション、AI インフラ、AI サービスへの投資額が全世界で 6,320 億ドルに達し、年平均成長率 (CAGR) が 29% を記録すると予測しています。この急激な増加により、今後 3 年以内に AI 関連のコストがパブリック クラウド全体の支出の 40% を占めると見られています。多くの組織が、拡張性、専用インフラ (GPU、TPU)、プラットフォーム (Amazon Bedrock、AI Foundry、Google Vertex AI など) を活用し、パブリック クラウド (Azure、AWSAzure、Google Cloud など) に生成 AI モデルを展開しています。このように急速に導入が進む AI ですが、サイバー犯罪者にとっても価値の高いターゲットとなっています。脅威アクターは設定ミスのある AI インフラを悪用することで、モデルの改ざんや機密データの窃取を試みています。新たなリスクと既存のリスクの両方を軽減するには、AI システムを予防的に保護することが不可欠です。

AI モデルは機密性の高いデータを扱うことが多く、そのセキュリティの責任は完全に組織が負うことになります。クラウド サービス プロバイダー (CSP) の責任共有モデルと同様に、組織はトレーニングと推論に使用される AI リソースやデータを適切に保護する必要があります。

LLM アプリケーションの OWASP Top 10 では、クラウド内の AI 資産を保護するために対処すべき重大なリスクとして以下が挙げられています。

- **データ ポイズニング：**トレーニング データの改ざんや細工を行うことで脆弱性やバックドア、バイアス (偏り) を仕込み、モデルの完全性とセキュリティを脅かします。
- **プロンプト インジェクション：**機密データを抽出するように設計された悪意のあるプロンプトを注入します。
- **サプライ チェーンの悪用：**トレーニング データ、ML モデル、展開プラットフォームを侵害し、偏った結果やセキュリティ侵害、システム全体の障害を引き起こします。
- **データ漏洩：**過剰な権限や不適切なアクセス ガバナンス フレームワークによって、データが漏洩します。
- **モデルの悪用：**過剰な自律性を持つ AI は、意図しないセキュリティ リスクにつながる可能性があります。これを防ぐには、AI のアクセス レベルを制限し、ユーザー権限を厳密に管理する必要があります。
- **モデルの窃取：**大規模言語モデル (LLM) への不正アクセスによって、財務損失、信用の失墜、専有データや機密データの漏洩が発生する可能性があります。

Zscaler AI Security Posture Management (AI-SPM)

Zscaler AI-SPM は、パブリック クラウドにおける生成 AI (GenAI) ワークロードの保護に重点を置き、データの漏洩、誤用、モデル ガバナンスなど、AI 特有のリスクに対応します。Zscaler AI Data Protection プラットフォームの一部として、既存のデータ セキュリティ ポスチャー管理 (DSPM) ソリューションと統合されており、AI モデル、機密性の高い推論データ、モデルの展開状況、リスクの相関関係までを包括的に可視化します。また、モデルの構成、データフロー、システム間のやり取りを監視することで、従来のツールでは見落とされがちなセキュリティとコンプライアンスのリスクを特定します。

Zscaler AI-SPM で組織を保護する方法

Zscaler AI-SPM は、AI のリスクを効率的かつ簡単に管理できるソリューションを提供します。AI の責任者やセキュリティ部門は、AI サービス、リスク分析、優先順位付けと関連付けがなされたリスクの修復を一元的に把握することで、AI の潜在的なリスクを排除しつつ、組織のコンプライアンスを維持しながら部門間の連携を強化できます。AI が進化し続ける現代においても、Zscaler は組織が革新性と安全性を両立できるよう強力にサポートします。

Zscaler AI-SPM は、以下を可能にします。

- **環境全体でセキュリティの監視を一元化し、組織全体にわたって AI の展開を保護します。**
- **不正な AI の利用を検出し、許可されていない展開によるデータ漏洩やコンプライアンス違反を防止します。**
- **データの取り込みから展開まで、AI ライフサイクルのすべてのフェーズを監視し、AI 運用の死角が生まれないようにします。**
- **データの誤用、モデルの脆弱性、敵対的攻撃など AI 特有のリスクを予防的に特定し、軽減します。**
- **AI ガバナンスとロールベースのアクセス制御を監査および施行することで、世界的な規制 (GDPR、CCPA など) の順守を簡素化します。**

機能とメリット

AI モデルの包括的な検出

管理型、半管理型、あるいは非管理型の AI モデルが増えるにつれ、それらの管理はますます複雑化しています。Zscaler AI-SPM は、AI の展開を詳細に可視化することで監視を効率化し、以下を可能にします。

- **モデルのスプロール化の制御:** AI モデル、オープン ソース モデル、仮想マシンに展開されたモデルのインベントリーを維持し、シャドー AI を排除します。
- **不正使用の防止：** モデルの使用状況を追跡および制御することで、組織の AI フットプリントを完全に可視化し、未承認または不適切なアプリケーションを特定してブロックします。また、AI リソースにアクセスできるユーザーとその権限も明確に可視化します。
- **ガバナンスの強化：** 新しいモデルが展開されるとリアルタイム アラートを送信し、必要な制御がすべて実装されているかどうかを確認します。

機密データの保護

AI モデルは、膨大なデータセットを基にトレーニングされますが、その中には個人を特定できる情報 (PII) や企業秘密などの機密データや規制対象情報が含まれることがあります。そのため、これらの AI モデルは、不注意による漏洩や敵対的攻撃に対して特に脆弱です。Zscaler AI-SPM は、AI モデルが使用する機密データを監視および保護し、以下を可能にします。

- **トレーニング データの検出と分類：** 自動データ検出と AI による分類を活用することで、正確なトレーニング データ セットを構築し、過剰な共有を防止します。
- **AI トレーニング データの保護：** 展開前に機密データによってモデルのトレーニングと微調整が行われないようにすることで、データ ポイズニングを特定して防止します。

- **RAG と推論データ フローの監視：**データ取得 (RAG) に使用されるデータ セットとデータ フローに関するインサイトを提供し、データ取得がデータへのアクセスにどのような影響を与えるかを可視化します。

- **モデルとのやり取りの分析：**プロンプトと出力のログを確認することで、モデルの誤用を検出し、データ漏洩の潜在的なリスクを軽減します。

- **AI を悪用した攻撃経路の可視化：**脆弱性、設定ミス、権限間の関連性をマッピングすることで、隠れた攻撃経路を明らかにし、リスクをより効果的に軽減します。

リスク評価

適切な構成を確保し、AI ワークロードの脆弱性を管理しながら、AI リソースへのアクセスを制御することが重要です。AI のデータ パイプライン、トレーニング環境、展開インフラにおける設定ミスやアクセス制御の弱点は、セキュリティとコンプライアンスの重大なリスクをもたらす可能性があります。Zscaler AI-SPM は、包括的なリスク評価、スキャン、実用的なインサイトを提供することで、AI セキュリティ態勢を強化し、以下を可能にします。

- **リスクの特定：**Zscaler DSPM の組み込みルールとコンテキストに基づくインサイトを活用することで、エンドツーエンドの AI 展開を評価し、アプリケーション、データ、パイプライン全体の脆弱性を明らかにします。

- **リスクの優先順位付け：**AI セキュリティに関する問題に優先順位を付け、そのキューを直感的なダッシュボードに表示することで、担当部門が最も重要な問題に集中できるようにします。

- **モデル アクセス ガバナンスの強化：**展開された AI モデルと、それに関連するコンピューティング、データ、アプリケーションなどのリソースへのアクセス状況を可視化します。

- **権限の最適化：**過剰なアクセス権限を特定し、修正します。RAG を含む内部での AI 展開によって過剰なデータ共有が発生するのを防ぎ、機密データへの不正アクセスのリスクを最小化します。

- **リスクの軽減：**RAG と微調整のアーキテクチャーに関する AI アプリケーションの知識をマッピングすることで、機密データの漏洩を制御し、最新の規制を順守します。

- **脅威エクスポージャーの防止：**LLM の OWASP Top 10 に該当する脆弱性について AI モデルを詳細にスキャンし、特定されたセキュリティ上の問題に迅速に対処するための修復の推奨事項を取得します。

- **AI 使用の管理：**運用、規制、評判のリスクに対して AI システムを評価します。

Zscaler AI Security Posture Management は、AI モデル、トレーニング データ、AI サービスにわたる継続的な可視化と予防的なリスク軽減を通じて、AI 展開を加速させます。包括的なセキュリティ対策により、組織は機密データを保護し、コンプライアンスを確保しながら、安全かつ確実に AI の導入と活用を拡大できます。

Zscaler AI-SPM の詳細については、Zscaler の専任の担当者によるデモを依頼してください。

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。

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

Zero Trust Everywhere