AKAMAI 製品概要

API Security

Akamai API Security により、API をビジネスロジックの悪用やデータ窃取からインテリジェントに保護

API 攻撃の進化

現在の企業は、パートナーやサプライヤー、顧客などとつながるために、日常的に API を活用しています。しかし、API を活用すると、その分、アタックサーフェスも拡大します。そこに目を付けているのが攻撃者です。API 攻撃は急速に増加および進化しており、Web アプリケーションと API の保護では検知できないケースも増えています。自社の API に関する包括的なインベントリを作成しなければ、盲点が発生し、すべての API を保護できません。

Akamai API Security をお勧めする理由

Akamai のプラットフォームにより、ライフサイクル全体（開発から運用まで）を通じて API を保護できます。API Security は、API をパートナー、サプライヤー、ユーザーに公開する組織向けに構築されており、API を探索して、リスク状況を把握し、そのふるまいを分析し、脅威が内部に潜伏することを阻止します。

API Security の重要機能

探索

多くの企業が自社の API を完全には把握していません。正確なインベントリがなければ、さまざまなセキュリティリスクにさらされます。API Security により、推測に頼ることなく、以下のことを行えます。

- 設定やタイプ（RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC、gRPC など）を問わず、すべての API を探索してインベントリを作成する
- 休眠 API、レガシー API、ゾンビ API を検知する
- 忘れられているドメイン、見落とされているドメイン、またはその他の不明なシャドードメインを特定する
- 盲点を解消し、潜在的な攻撃経路を明らかにする

テスト

アプリケーション開発はかつてないほど高速化しています。その分、セキュリティ上の脆弱性や設計上の欠陥が見落とされる可能性も高くなっています。Akamai の API セキュリティ・テスト・スイートにより、以下のことを実行できます。

- 悪性トラフィック（OWASP API Security Top 10 の脅威など）をシミュレートする 150 以上のテストを自動で実行する
- API を本番環境に展開する前に脆弱性を発見し、攻撃が成功するリスクを緩和する
- 定められたガバナンスポリシーやルールに照らして、API の仕様を確認する
- API に特化したセキュリティテストをオンデマンドで、または CI／CD パイプラインの一環として実行する

ビジネス上のメリット

探索
API のアタックサーフェスを把握できます。API のインベントリとドキュメントの更新にかかるコストを削減できます。規制要件や社内ポリシーへのコンプライアンスを強化できます。

テスト
問題を早期に発見することで、修復コストを削減できます。速度を犠牲にすることなく、コード品質を改善できます。市場投入までの時間を短縮することで、収益を拡大できます。

検知
事態を正確に把握して、なぜ問題なのか、どのような潜在的影響があるのかを明らかにし、どのように修復すべきかを決定できます。

対応
攻撃を即座に阻止することで、リスクを緩和できます。悪用される前に脆弱性を修復することで、コストを削減できます。ダウンタイムに伴う収益の喪失を削減できます。

Akamai

検知

API に設定ミスがあるだけで、サイバー攻撃に対して無防備になりかねません。侵入に成功したハッカーは、機微な情報に簡単にアクセスして窃取できてしまいます。Akamai のプラットフォームにより、以下のことを実行できます。

- インフラを自動的にスキャンして、設定ミスや隠れたリスクを把握する
- カスタムワークフローを作成して、主要関係者に脆弱性を通知する
- 機微な情報にアクセスできる API と内部ユーザーを特定する
- 検知した問題に重大度ランキングを割り当てて、修復の優先順位を設定する

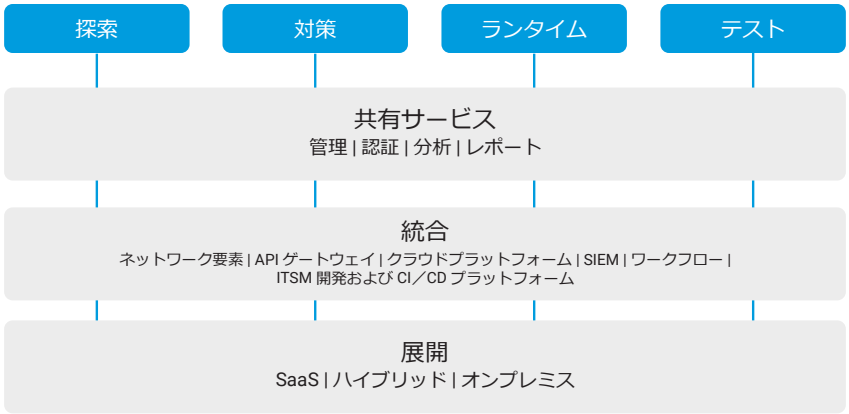
対応

あらゆる組織が攻撃を受ける可能性があります。そのため、攻撃をリアルタイムで検知してブロックできなければなりません。Akamai の人工知能／機械学習ベースの異常検知を活用して、以下のことを実行できます。

- データ改ざん／漏えい、ポリシー違反、不審なふるまい、API 攻撃を監視する
- ネットワークを変更したり、面倒なエージェントをインストールしたりせずに、API トラフィックを分析する
- 既存のワークフロー（チケット発行、セキュリティ情報およびイベント管理（SIEM）など）と統合して、セキュリティ／運用チームにアラートを通知する
- 攻撃や悪用をリアルタイムで阻止し、修復の一部または全部を自動化する

Akamai の強み：エッジで阻止

Akamai App & API Protector では、Akamai Connected Cloud を介して実行されるアプリや API に対する API 脅威を探索して緩和できます。また、API Security が突き止めた潜在的脅威が含まれるトラフィックをすべてブロックできます。Akamai の API 保護ソリューションを組み合わせて展開することで、API を包括的かつ継続的に可視化して、アプリケーション資産全体において、API セキュリティの問題を探索、監査、検知、対応できます。



API Security の仕組みについて詳しくは akamai.com/apisecurity からお問い合わせください。Akamai 担当者が直接ご説明いたします。