AKAMAI ソリューション概要

Akamai API Security を活用した API 資産管理

組織がますますクラウド中心になり、デジタル化しているなかで、API の範囲、規模、価値が拡大しています。また、API は急速に増大するリスクをもたらしています。

無防備な API や設定ミスのある API が蔓延しており、そのような API は侵害されやすく、保護されていないだけでなく、極めて脆弱な「シャドウ API」のように、認識されておらず、管理されていないことが多くあります。このような API の急増により、エンタープライズ全体のすべての API を特定してインベントリを作成することが困難になっています。

Akamai API Security は、組織が必要な可視性を獲得できるように、社内ユーザーと社外ユーザーの両方のための API を自動で分類し、インベントリを作成します。

包括的なインベントリを構築するためのインプットとして、Akamai API Security ソリューションは、API ゲートウェイ、Web アプリケーションファイアウォール（WAF）、パブリック・クラウド・サービス、ネットワークトラフィック、API ドキュメントなど、さまざまなソースを使用します。これにより、API の変更が追跡され、最新バージョンが API ライブラリに反映されるようになります。

Akamai API Security ソリューション

Akamai API Security は 4 つの統合モジュールで構成され、API 資産管理とエンドツーエンドのセキュリティを実現します。

探索
内から外、外から内の両方の API と関連リスクを特定し、インベントリを作成します

対策
脆弱性や誤設定を明らかにして、迅速に修復し、コンプライアンスを確立します

ランタイム
機械学習を活用したリアルタイムのトラフィック分析により、API 攻撃を検知し、ブロックします

テスト
開発ライフサイクルにおいて脆弱性を見つけ、修復します

利点

API カタログ
API を公開するシステム、サービス、アプリケーションを特定し、詳細に分類

クエリーカタログ
ユースケースや規制フレームワークに合わせて API インベントリを検索および管理

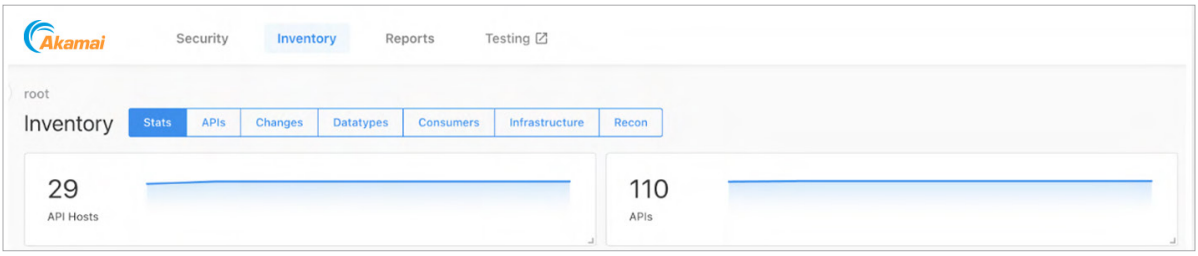
API 標準
OpenAPI 仕様ファイルとリンティングルールのファイルをアップロード、表示、分析

API の再利用
新しい API をコーディングするのではなく、必要なタスクを実行する既存の API を特定

資産管理の出発点は、探索モジュールです。環境内のトラフィックソースを分析することで、このソリューションは組織が使用している API の数を明らかにし、さまざまなフレームワークに基づいて API を自動的に分類します。

API カタログ

Akamai API Security は、既存の API の包括的なカタログを作成します。このカタログは、それらの API を公開するシステム、サービス、アプリケーションを特定し、個々の API を詳細に分類します。

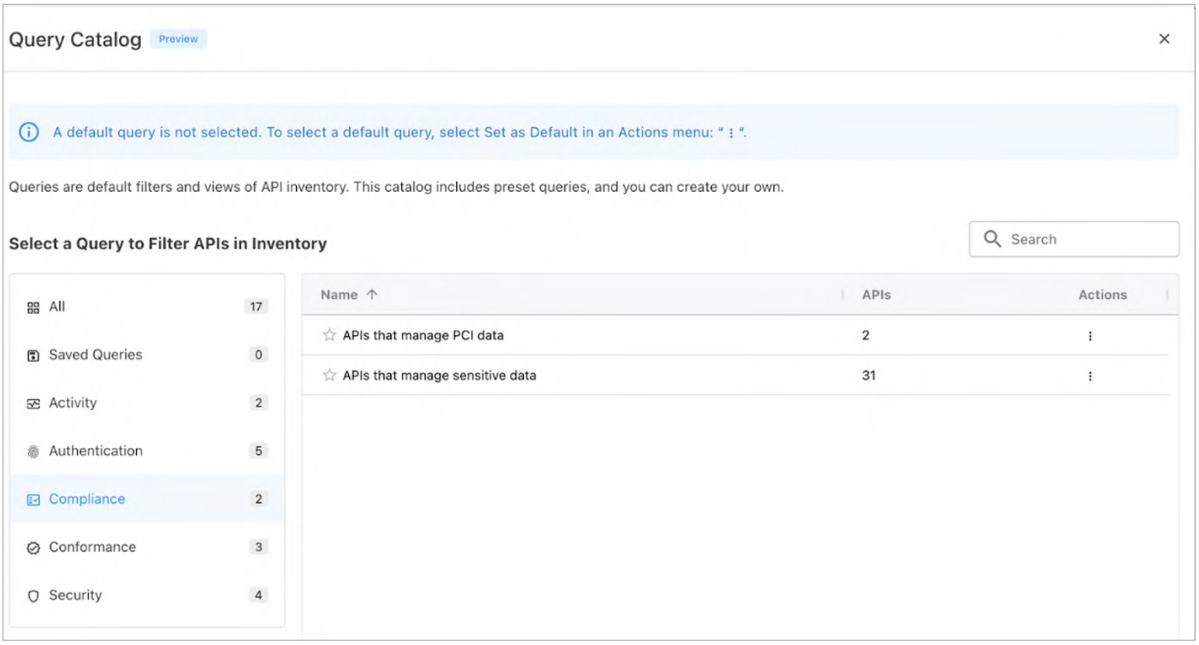


Akamai API Security は、API に加えられたすべての変更を追跡し、ユーザーがそれらの変更に基づいて最新のドキュメントを OpenAPI 仕様ファイルとしてエクスポートできるようにします。また、新しい API がユーザーの環境に追加された場合、ユーザーに通知できます。

さらに、Akamai API Security に組み込まれている管理 API を使用して API ライブラリから情報を抽出し、一元化された API CMDB（設定管理データベース）を作成できます。

クエリーカタログ

Akamai API Security にはクエリーカタログが組み込まれているため、特定のユースケースや規制フレームワークに応じて簡単にインベントリの検索と管理を行えます。



各 API について、このシステムは以下の情報を提供します。

- API の所有者、タイプ、コールフロー
- 処理されるデータのタイプ
- サポート対象の認証方法
- API のソースと場所
- 検知された API が API の仕様／ドキュメントに合致しているかどうか
- API の背後にあるインフラ
- API の依存関係を示す完全なネットワークグラフ

API 標準の活用

このソリューションでは、独自の OpenAPI 仕様ファイルやリンティングルールのファイルをアップロード、表示、分析することもできます。リンティングとは、API が技術的に正しいものであり、API ガイドラインの形式で文書化されることの多い一連の追加制約に準拠していることを確認するプロセスです。Akamai は、開発者が API を作成、文書化、維持できるようにするオープンソースツールである Spectral のデフォルトのリンティングルールを組み込んでいます。さらに、次の 3 つの形式の仕様ファイルをアップロードできます。

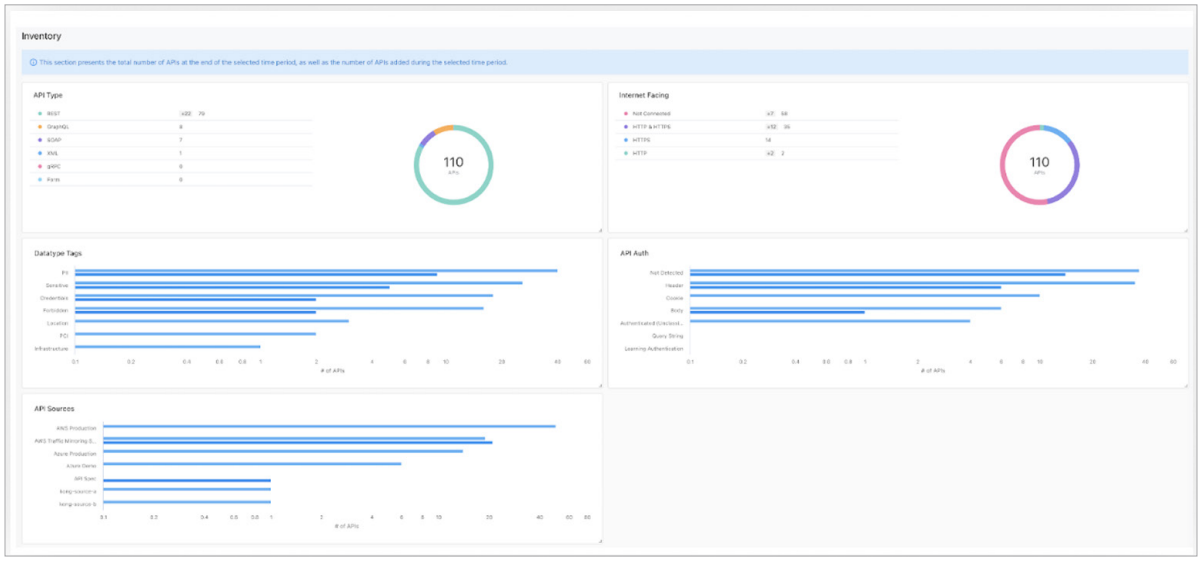
- RESTful API Modeling Language
- Web Services Description Language
- Web Application Description Language

これにより、既存の API 標準を活用したり、独自の API 標準を定めて環境に適用したりすることができます。これらの標準は、Banking Industry Architecture Network に基づいた金融サービス業界向けの標準的なオープンバンキング API など、業界固有のものにすることができます。

さらに、Akamai の API Security ソリューションは標準からの逸脱を検知し、この種の検知に対処するための修正ポリシーを定めることができます。また、このシステムは、仕様ファイルから API を検知してインポートし、実際のネットワークトラフィックと比較します。Akamai API Security を再設定することで、単純なドメイン名情報に基づいて外部 API の検知とインポートを行うこともできます。

API の再利用の促進

検索やナビゲートのしやすい包括的な API ライブラリがあれば、開発者は新しい API をゼロからコーディングするのではなく、必要なタスクを実行する既存の API を見つけることができます。開発者やセキュリティ専門家などのために自社の環境における可視性のギャップを抑える際には、API のインベントリとカタログを使用することで、API の再利用を容易に促進できます。



詳細はこちら

API は、組織が顧客へのサービス、収益の創出、効率的な事業運営を行えるようにするための重要な要素です。しかし、その継続的な増加、機微な情報への近接性、セキュリティ制御の欠如により、API は今日の攻撃者にとって魅力的なターゲットとなっています。探索、体制管理、ランタイム保護、セキュリティテストの機能を提供する包括的な API セキュリティソリューションを使用することで、組織は API 攻撃のリスクを軽減し、セキュリティを確保できます。

Akamai API Security が組織にどのように役立つのかについて、詳細をご覧ください。