AKAMAI ソリューション概要

IBM API Connect と DataPower のための API セキュリティおよびガバナンスの統合

API の可能性と課題

API がデジタル変革の原動力となり、あらゆる業界の組織が新しいサービスやビジネスモデルを生み出したことで、成長を加速してきました。しかし、API の普及に伴い、そのリスクも増大しています。

- ビジネスリーダーやエンジニアリングリーダーは、組織全体で API の使用と統合を急速に推進してきましたが、API を効果的に管理する能力は依然として課題となっています。
- 新しいアプリケーションや AI 強化型サービスの急速な構築とリリースの競争が進む中、基盤となる API には、誤設定、コーディングエラー、ビジネスロジックの問題が極めて多くみられます。
- 顧客やパートナー、ベンダーとの間で組織がデジタル的にやり取りするたびに、その処理の背後でデータ（多くの場合、機微な情報）をシームレスにやり取りできるよう API が機能しており、攻撃者はそのことを知っています。

その結果、API は大きな賭けを伴う攻撃ベクトルの上位に位置づけられるようになりました。API に対する攻撃は、企業の収益、回復力、規制コンプライアンスを脅かす可能性があります。

この課題に対処するために、組織は設計、開発、テスト、展開、運用、修復を含むライフサイクル全体でガバナンスとセキュリティの両方に取り組まなければなりません。Akamai API Security と IBM は連携して、組織が自信を持って API を迅速に開発、展開、管理し、ビジネスの状況に応じて予測どおりにスケーリングできるように支援しています。

課題

- 資産全体で API インベントリを維持し、未知の API を発見
- コンプライアンス違反の API、誤設定のある API、脆弱な API を特定
- ビジネスロジック攻撃を含む API の悪用や不正使用を検知して阻止
- スピードやアジリティを損なうことなく、安全で一貫した API を構築
- API セキュリティプログラムやガバナンスプログラムの連携と監視を確立

Akamai と IBM はどのように顧客を支援するのか

API 資産全体を探索

「見えないものは守れない」という格言があります。Akamai API Security を使用すると、API、ドメイン、問題を自動的に探索して、堅牢な API インベントリを構築し、API 資産全体を可視化することができます。通常、自社が所有していると思っていた、または見つかると予想していたよりも、はるかに多くの API が見つかります。また、漏えいした情報などの悪用される可能性のあるインテリジェンスを簡単に発見し、攻撃者が利用する可能性のある攻撃経路を把握し、API ゲートウェイや管理プラットフォームに隣接する最も一般的なインフラ要素とシームレスに統合して、組織全体で一貫してセキュリティデータを共有できます。

セキュリティおよびガバナンスポスチャを強化

API ガバナンスに Akamai API Security を使用する際は、次のように運用をスケーリングし、ベストプラクティスを適用します。

- 完全なビジネスコンテキストで自社のエコシステム内に存在するすべての API を把握し、API 管理のベストプラクティスと一致させる
- 開発チームとセキュリティチーム間のコミュニケーションを合理化する
- 誤設定やポリシー外の API などの脆弱性を見つける
- 機微な情報を保護し、変更をプロアクティブに監視して、API のリスクを軽減

ランタイム保護により、API の悪用や攻撃を阻止

リアルタイムのトラフィック分析、アウトオブバンドでの監視、インライン修復オプション、ワークフロー統合により、エッジからコアへの API 攻撃（データ漏えい、データ改ざん、データポリシー違反、疑わしいふるまいなど）を検知してブロックし、セキュリティ・オペレーション・センター（SOC）の有効性を高めることができます。

Active Testing により、安全な API を迅速に実現

API セキュリティテストを API 開発のあらゆる段階にシームレスに組み込み、API が本番環境に進む前に、脆弱性、誤設定、コンプライアンスの問題を明らかにします。Active Testing を実施することで、DevSecOps 担当者は、API に重点を置いた 200 以上の包括的なセキュリティテストをオンデマンドで実行したり、自社の CI ／ CD プロセスの一環として実行したりすることができます。Active Testing は、アプリケーションの基盤となるビジネスロジックを理解したうえで、すべての API を見つけてテストします。そのため、開発者は他のテストツールでは見落としてしまう可能性のある複雑な脆弱性を発見できます。

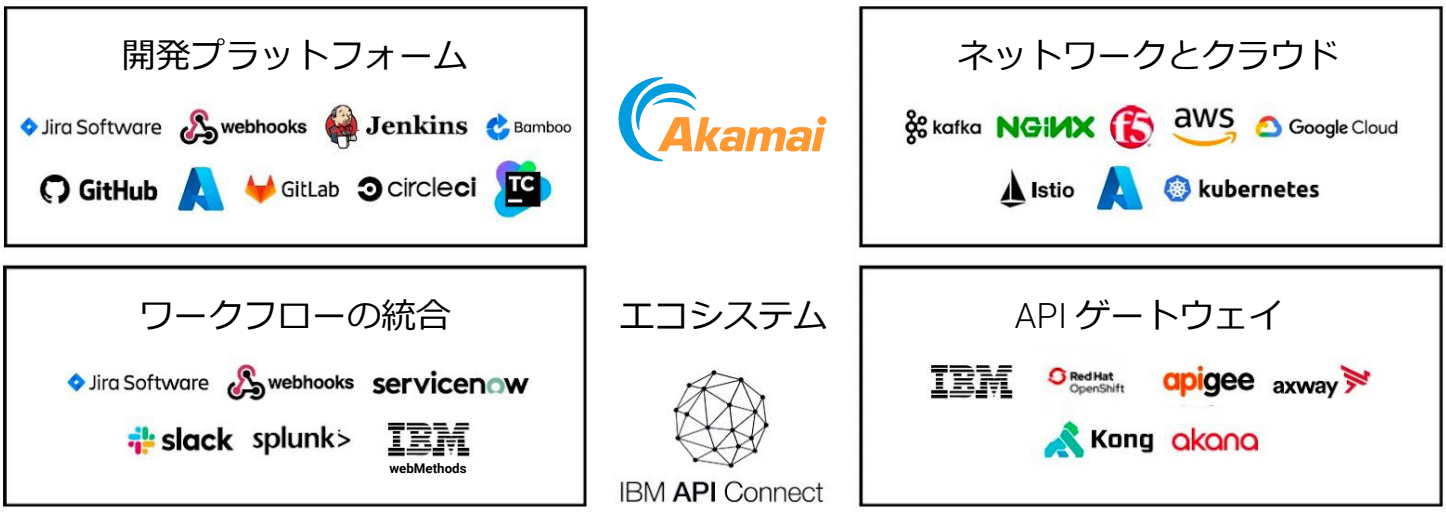
Akamai との統合により効率が高まり、IBM ユーザーが可視化と保護を実現できる仕組み

Akamai API Security は、複数のクラウドプラットフォームと展開オプションで、API Connect および DataPower の両方と統合されます。さらに、API Connect が DataPower を管理する場合、システム間で一方的な設定変更が行われるため、運用効率が向上するだけでなく、不正な開発活動やコンプライアンス違反の開発活動のリスクが軽減されます。

シームレスな攻撃の誘導と応答

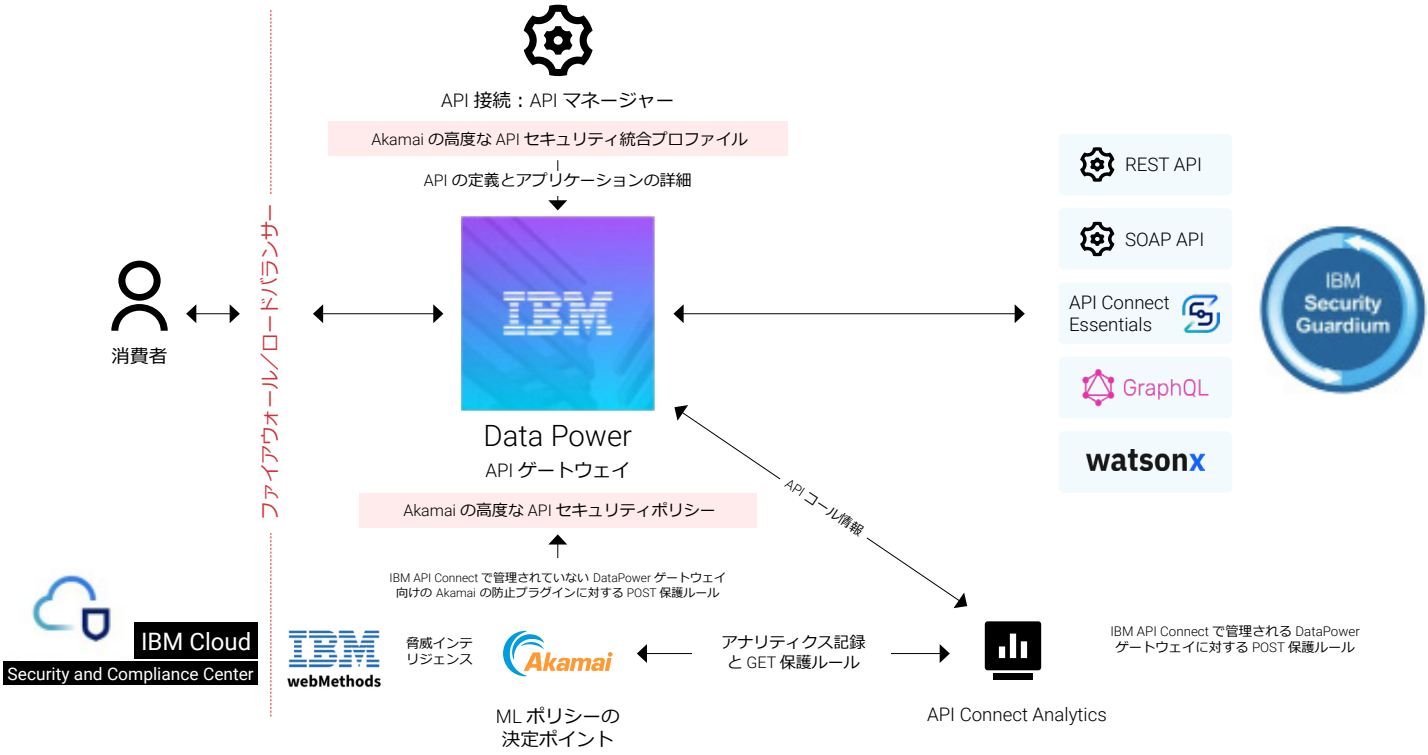
さらに、IBM DataPower を利用している顧客は、Akamai API Security ソリューションと統合することで、DataPower ゲートウェイに追加のプラグインをインストールすることなく、またパフォーマンスやレイテンシーの影響を生じさせることもなく、ほぼリアルタイムで脅威を検知し、ブロックすることができます。

IBM API Connect は、リソースへのアクセス要求を Akamai API Security の認可ポリシーに照らして評価し、IBM DataPower クラスター全体でブロックルールを適用します。そのため、修復時間が数日から数分または数秒に短縮されます。



IBM webMethods と Akamai API Security の力を組み合わせることで、他に類を見ない API 管理と保護を実現できます。このパートナーシップは、Akamai の高度な API 探索と IBM webMethods の堅牢なガバナンスやリアルタイムのデータ統合を組み合わせた完全なソリューションをもたらします。API を完全に可視化して制御し、セキュリティとコンプライアンスを確保することができるのです。IBM webMethods と Akamai API Security の統合により、防御が強化されるだけでなく、効率が向上するため、企業は動的な市場の需要に迅速かつ安全に対応できるようになります。

最後に、IBM DataPower を利用している顧客は、Akamai eBPF Red Hat OpenShift 統合を活用して、API Connect で管理されていない API や DataPower でプロキシされていない API を探索し、リスクの高いトランザクションや機微な情報を処理する API を発見し保護することができます。これらの機能はオンプレミスに留まらず、クラウドやハイブリッド構成へ拡張でき、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）もサポートします。



次のステップ

API は、組織が顧客のニーズを満たし、収益を生み出し、急速に変化するデジタル経済で競争するための原動力です。しかし、その継続的な増加、データへの近接性、数え切れないほどの脆弱性により、API は攻撃者にとって魅力的なターゲットとなっています。API セキュリティのインシデントは着実に増加しているため、組織全体のすべての API の可視化、セキュリティ確保、テストのための機能を備えることが不可欠です。IBM と Akamai が連携することにより、API を安全かつ大規模に構築し、保守し、使用する自信を企業にもたらすことができます。

カスタマイズされた Akamai API Security のデモをスケジュールいただき、Akamai のサポート内容についてご確認ください。詳細については、IBM の担当者にもお問い合わせいただけます。