API ランタイム保護の決定版ガイド

目次

はじめに

API セキュリティが不可欠な理由

顧客のニーズにいかに応えるかの競争が激化する中、組織はアプリケーション、サービス、生成 AI ツールの迅速な開発、生産、強化を迫られています。しかし、このスピードの必要性は、残念ながら隠れたリスクを生み出します。このようなイノベーションの流れの舞台裏で働く API は、その構築時に設定ミス、コーディングエラー、セキュリティ制御の欠如を生み出しがちです。そして、これらの API が本番段階に達すると、エンドユーザーだけが API とやり取りするだけでなく、攻撃者も API を侵害し、API がやり取りしているデータにどうすればアクセスできるかを常に試すようになります。

API の設定ミスや侵害は、重大なデータ漏えいの主な要因になりつつあります。しかし、デジタルエコシステム内の数千ものAPI コールを監視できている組織はほとんどありません。ランタイム API の脅威から完全に保護されている組織はさらに少なくなります。

たとえば、2021 年に、フィットネス小売企業がユーザー・アカウント・データ用の API にバグを発見し、誰でも認証なしで年齢、性別、住所、体重、誕生日などのデータをリクエストできることが判明しています。この脆弱性は幸い、セキュリティ研究者によって発見され、その会社に報告されましたが、このようなバグに気づかないまま、数週間から数か月間、悪用されることもあります。

API のセキュリティを確保するにあたっては、API ゲートウェイや Web アプリケーションファイアウォールなど、組織が通常使用している従来のツールで、基本的な保護を提供することはできます。しかし、今日のセキュリティチームは、API 攻撃の数が増え、巧妙化するにつれ、さらなるセキュリティレイヤーを追加する必要があります。そこで鍵になるのが、脆弱性、潜在的な攻撃経路、悪性のアクティビティ、API のふるまいに関する深い知見によって、既存の制御を強化することです。

組織は、次の 4 つの領域をカバーする包括的な API セキュリティソリューションによって、これらを実現することができます。

1. API 探索
2. API ポスチャ管理
3. API ランタイム保護
4. API セキュリティテスト

本書の内容

API ランタイム保護は、API が通常の処理においてリクエストを処理および管理しているときの API を保護するプロセスです。このガイドでは、API ランタイム保護の主な要件として、設定ミスや悪用を防止するための API 監視、API 攻撃防御などについて説明します。また、ランタイム防御の基礎について説明し、Akamai API Security が提供するランタイム防御機能をご紹介します。

ランタイム保護が必要な理由

API ランタイム保護は、API が稼動し、意図したエンドユーザーや攻撃者とのやり取りが可能になるライフサイクルの本番段階全体を通して、API のセキュリティを確保します。悪性の API リクエストを迅速に特定して対処できるよう組織を支援する機能を備えた、効果的なランタイム保護機能により、次のような導入後のさまざまな脅威から API を保護することができます。

- API から大量の機微な情報を引き出そうとする攻撃者
- セキュリティバグを悪用した権限昇格攻撃
- 通常のプロセスとは異なる不正な API の導入

ランタイム API の脅威をブロックするためには、API アクセス、使用状況、ふるまいなど、API ごとにどのような経緯で処理しているかを把握する必要があります。まず、API 資産の範囲を把握する必要があります。API インベントリの重要性については、『API 探索の決定版ガイド』で説明しています。完全な API インベントリがあれば、すべての API トラフィックを監視し、各 API の「典型的な」ふるまいに関する基本的な理解を得ることができるため、それに基づいて異常なふるまいを認識することができます。API ランタイム保護で検知すべきものは次のとおりです。

- データ漏えい
- データポリシー違反
- API セキュリティ攻撃
- データ改ざん
- 不審なふるまい

さらに、ランタイム保護は、API トラフィックのロギング、機微な情報へのアクセスの監視、脅威の検知、攻撃のブロックや修復を行うべきです。

API トラフィックを監視し攻撃を検知

リスクを特定するためには、API トラフィックのふるまいを観察することが不可欠です。API 資産を正確に把握せずに監視ソリューションを導入しても、可視性が制限されてしまいます。API フットプリントをインベントリ化したら、API ランタイム保護でトラフィックと API の使用状況を継続的に監視し、脆弱性と設定ミスを探す必要があります。

異常なふるまいの検知

API の通常のふるまいをベースラインとして確立することで、通常とは異なるあらゆる異常を識別することができます。過去のデータを再生することで、異常なふるまいを特定しやすくなり、攻撃者の意図を明らかにできるかもしれません。

潜在的な異常があるかどうかは、アプリケーションやネットワーク内で実行されている他のアクションとの関連でさらに踏み込んだ調査を行う必要があります。たとえば、データ要求が通常一定の規模である場合、API コールが通常の範囲を超えるデータを要求した場合は、フラグを付ける必要があります。悪性のものもあれば、そうでないものもありますが、異常な動きには綿密な検査が必要です。

データの露出の検知

所有資産の API の中には、機微な情報を送受信するものもあるでしょう。セキュリティの脆弱性により機密情報が露出することで、攻撃者は権限を昇格させたり、その他の不正なアクセス制御を設定したりできるようになります。AI と機械学習は、リアルタイムのトラフィック分析と異常検知に役立ち、データ漏えい、データ改ざん、データポリシー違反、不審なふるまい、API セキュリティ攻撃に対して状況に応じた知見を提供します。

最近ますます見られるようになってきた攻撃の 1 つに、サイバー犯罪者が有効な API キーを手に入れる、というものがあります。攻撃者が有効なキーを手に入れた場合、API の不正使用やデータ漏えいを防ぐ唯一の方法は、異常なふるまいやデータ露出を検知してブロックする能力のみです。

API セキュリティ監査

API セキュリティ監査ツールは、トラフィックをリアルタイムで監視し、攻撃やその他の悪意を警告できるものでなくてはなりません。API セキュリティ監査では、少なくとも次のことを行う必要があります。

- 攻撃者と悪性リクエストを特定するための継続的な監視を実施
- API を内部および外部から受動的にスキャンし、設定のミスや見落としがないかどうかを確認し、それが原因となって侵害や防御の弱体化が発生する可能性がないか、また悪化させる可能性がないかを確認
- API によるデータ送受信の許可／不許可を定めたポリシーを適用

API ランタイム保護は、設定ミスや既知の脆弱性を識別する API ポスチャ管理で補う必要もあります。詳細については、『API ポスチャ管理の決定版ガイド』をご覧ください。

組織の存続に不可欠なランタイム保護機能

組織が API を積極的に開発および導入している場合は、堅牢なランタイム保護を API セキュリティプログラムの一部として組み込む必要があります。ここでは、ランタイム保護ツールに何が備わっていなければならないのかについて説明します。

リアルタイムのアウトオブバンド監視

API セキュリティの監視が原因で、API トラフィックに影響したり、速度が落ちたり、レイテンシーが増えたりしてはなりません。ネットワークの変更や、面倒でインストールが困難なエージェントも必要とせず、完全にアウトオブバンドの状態で稼動できる必要があります。ランタイム保護ツールは、特定したデータソースからのトラフィックをミラーリングし、そのトラフィックデータの分析をバックグラウンドで実行し、発見したイシューをリアルタイムで警告できる必要があります。

Akamai はデフォルトでアウトオブバンドかつエージェントレスで実行されますが、必要に応じてエージェントベースの検知やインラインブロッキングのオプションを提供します。

API の異常と悪用の検知

特に API の数と API トラフィックの総量が増加し続けると、受動的なデータ収集だけでは不十分です。API アクティビティを継続的に分析して、異常なイベントを検知し、セキュリティチームと運用チームに警告する必要があります。最先端のプラットフォームツールは、AI および機械学習機能を備えており、トラフィックをリアルタイムで分析し、データ漏えい、データ改ざん、データポリシー違反、不審なふるまい、API セキュリティ攻撃に関するコンテキストに基づく知見を活用することができます。

API 攻撃の防御とリスクの解消

異常などの問題を特定し、アラートを生成した後は、一刻を争います。API を介した機微な情報の不正な移動など、API の悪用が疑われる場合は、検知して修復する必要があります。ランタイム保護は、既存のファイアウォールや API ゲートウェイとの統合を通じて API の悪用を防止するだけでなく、可能であれば自動化された修復オプションを提供する必要があります。攻撃の信頼度スコアを含む機能が搭載されているものを探します。この機能があれば、不正使用、攻撃、または侵害のシグナルが正当なものであるかどうか、さらにはエスカレーションが必要かどうかをチームが判断するのに役立ちます。

インシデント対応の統合

一般的なルールとして、ランタイム保護ツールは、組織が使用している他のセキュリティ、監視、管理ツールと簡単に統合できなければなりません。たとえば、ランタイム保護ツールには、インシデントが発生した場合に修復タスクを適切なチームに割り当てるための統合機能が必要です。設定ミス、データポリシー違反、疑わしいふるまいが検知された場合は、API ゲートウェイや SIEM システムなどの情報セキュリティエンジンに報告して、適切な認識レベルを確保する必要があります。攻撃の信頼度をスコアリングする機能が搭載されていれば、チームはノイズをフィルタリングし、API のセキュリティの真の優先順位に集中できます。

Rapyd

Rapyd は、100 か国以上で決済システムを運営している世界的な決済処理およびフィンテック企業です。API の使用状況やふるまいをきめ細かく可視化できないため、AWS クラウドで運用されている非常に複雑なグローバルシステムにおいて、公開 API や数百もの社内 API を安全に保護するための優れた方法が必要でした。Rapyd は、すべての API の詳細なインベントリを作成し、構成ミスや脆弱性を可視化し、より論理的な修復アプローチを実現するためにアラートをインテリジェントに優先順位付けする必要がありました。

Akamai API Security は、機械学習を使用してすべての API のトラフィックのベースラインを作成し、異常検知と修復を自動化する包括的な可視化とランタイム保護を備えていたため、Rapyd のニーズを満たすことができました。

お客様事例全文を読む

> 今では私たちは、最も科学的に正しい方法でリスクを評価し、自らの運命をコントロールすることができています。

– Nir Rothenberg 氏
Rapyd 社、CISO

Akamai API Security のランタイム保護

API 攻撃の発生時にその攻撃を特定して阻止できることが、コンプライアンスおよびリスク評価プログラムに不可欠です。他のセキュリティ対策が不十分な場合は、これを最後の防衛線として考えることができます。

Akamai API Security のランタイム保護モジュールには、前のセクションで説明したすべての機能が含まれています。その主な機能は、API 攻撃をリアルタイムで検知してブロックすることです。機械学習（ML）ベースの自動監視を活用してトラフィック分析を行い、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、API セキュリティ攻撃に関する、コンテキストに沿った知見を提供します。ランタイム保護は、API トラフィックの異常や潜在的な脅威を検知し、事前に選択したインシデント対応ポリシーに基づいて修復を促進します。

ランタイム保護は、WAF、API ゲートウェイ、ITSMS、SIEM、およびその他のワークフローツールと連携し、攻撃に対する総合的な防御を提供します。脅威の修復を完全に自動化することも、さまざまなレベルの手動操作を選択して可視性や制御性を高めることもできます。Akamai API Security ソリューションは、Akamai プラットフォームとネイティブに統合されているため、攻撃者の IP をエッジで直接ブロックできます。

イシューの生成

機械学習を使用して、Akamai は各 API のモデルを構築します。この通常のふるまいのベースラインは、本来アクセスできないはずのデータへのアクセス権限を個々のユーザーが取得する、Broken Object Level Authorization（BOLA）などの API ビジネスロジック攻撃を検知するために使用されます。Akamai は、API

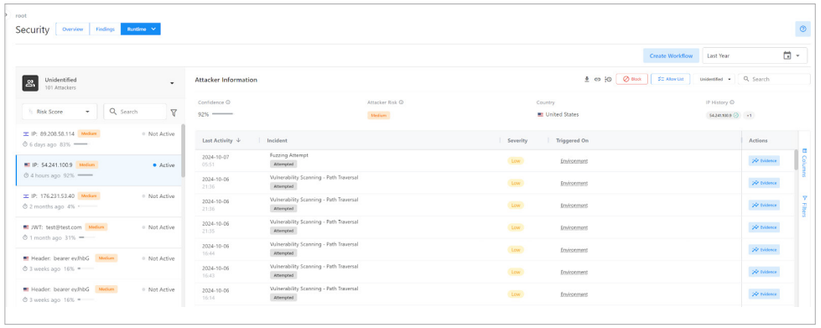
トラフィックが通常のふるまいから逸脱するたびに、リアルタイムでイシュー（issue）を生成します。イシューはアラートとよく似ており、API の異常なふるまいが検知された場合や設定ミスが見つかった場合に生成されます。イシューが生成されると、Splunk や QRadar などの SIEM にアラートが自動的に送信されます。アラートは、ServiceNow や Jira などのチケットシステムに自動的に送信することもできます。

イシューの詳細

Akamai API Security のランタイム保護モジュールによって生成されるすべてのイシューには、重大度、ステータス、OWASP API Top 10 へのマッピング、および該当する場合は攻撃者の詳細が含まれます。

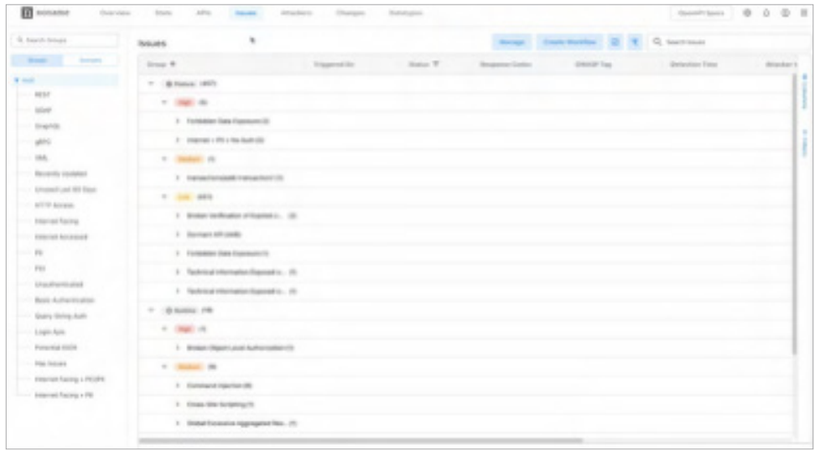
イシューの詳細ページには、イシューの説明と組織への潜在的な影響と、修復の推奨事項が記載されています。また、Akamai API Security は、各攻撃の履歴を記録しているため、攻撃者が特定の期間にどのような種類のアクションを実行したかを確認し、攻撃者に対する対策を講じることができます。

例：攻撃者の行動を可視化

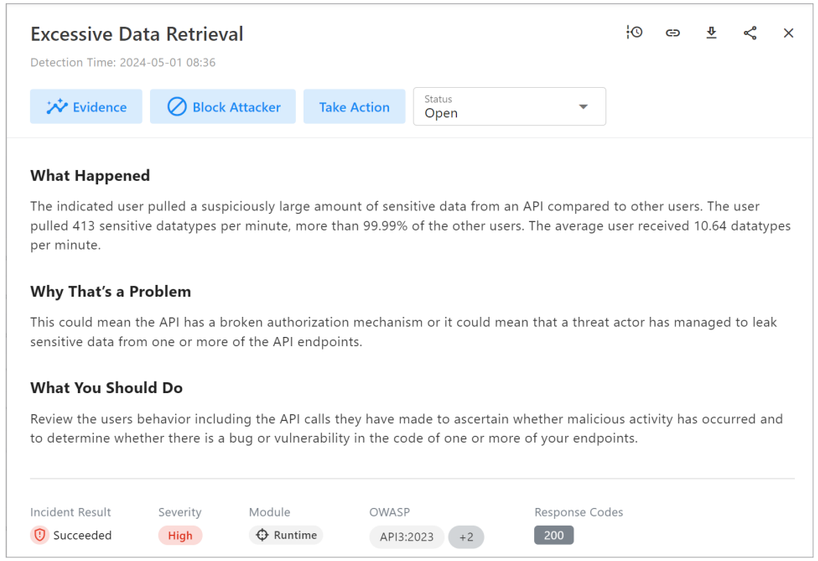


すべてのイシューには証拠が含まれます。証拠とは、イシューの早期のトリアージと修復を支援するための、イシューが生成されるまでの攻撃者セッションの詳細、API リクエストと応答のコピー（ヘッダーと本文の両方）のことです。直感的なダッシュボード、フィルタリング機能、アラート、レポート作成機能を備えた Akamai API Security ソリューションのランタイム保護モジュールは、何が起きたのか、なぜ起きたのか、何を実行すべきなのかを組織が判断するのに役立ちます。

例：証拠付きの API イシューのレポート



例：過剰なデータ取得に関する知見



ポリシーアクション

Akamai API Security は、生成されたすべてのイシューに対して半自動でポリシーアクションを実行できます。アクションには、チケットの発行、SIEM への情報の送信、サードパーティシステムへの Web フックの送信を含めることができます。また、攻撃者のブロックも含めることができます。使用可能なアクションのタイプは、Akamai プラットフォームに設定された統合のタイプによって決まります。

このソリューションには、API 攻撃と API の設定ミスを検知するための多数の事前定義済みポリシーが用意されています。Akamai API Security には、20 以上のデータタイプが事前に設定されているため、機密性の高いデータタイプが API を通過する際にそれを検知し、対策を講じるために必要なデータポリシーの作成に役立ちます。

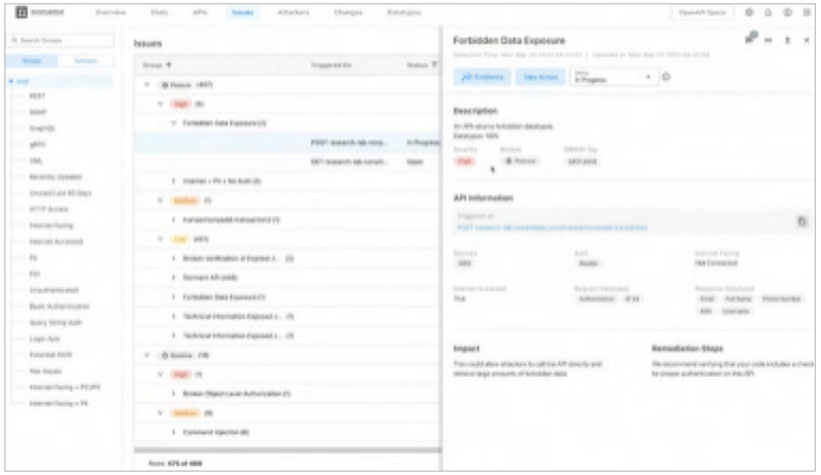
要約すると、Akamai API Security ソリューションのランタイム保護モジュールには、API 攻撃のリアルタイムの検知と防止に加えて、API の設定ミスの継続的な検知が含まれると同時に、運用と修復をシンプル化する多くの一般的なワークフローの統合も含まれているということです。

API セキュリティインシデントの詳細

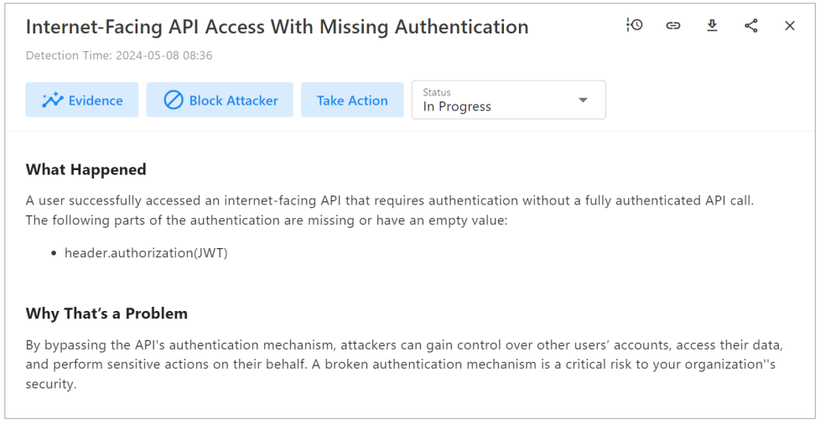
禁止されているデータの露出の例を詳しく見てみましょう。この例は、API 内部に潜むセキュリティポスチャのイシューを示しています。Akamai プラットフォームは、すべての API に関連付けられたデータのタイプと値をコンテキストに応じて認識しています。

次の図では、禁止されたデータが API によって露出しています。Akamai のプラットフォームは、送信されるデータのタイプ（この例では社会保障番号（SSN））を検知し、SSN データタイプが以前に禁止されたものとしてタグ付けされていたことを認識します。Akamai は、インターネットアクセス可能でありながら API ゲートウェイに登録されていない API など、API の外部の設定ミスを検知することもできます。

例：禁止されているデータの露出に関する知見



例：認証が欠落している API の識別



効果的な API ランタイム保護を実現するための次のステップ

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）を迅速かつスムーズにやり取りできるよう API が機能しています。API ランタイム保護の主要機能（設定ミスや悪用から防御するための API 監視、API 攻撃防御など）を実装すると、急速に増加する攻撃ベクトルから組織を保護することができます。

こちらで API セキュリティベンダーを評価して、重要なランタイム保護機能を確実に提供できるようにする方法について説明しています。

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 がどのようにお役に立てるか、ぜひご確認ください。