Akamai

ホワイトペーパー

API 検知および応答における 10 の重要な機能

API セキュリティ戦略を進化させる

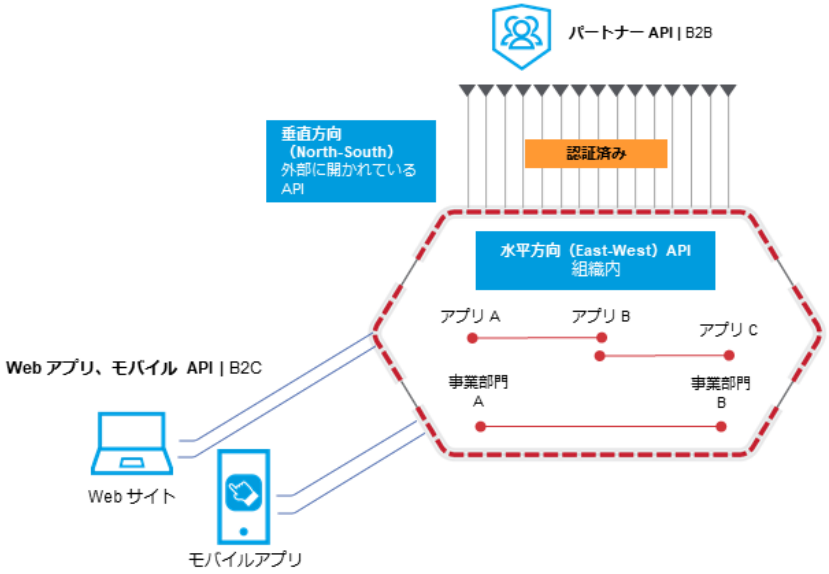
はじめに

API はイノベーションの推進に欠かせない重要な構成要素であり、この変革の中心にあるのが企業間取引（B2B）と企業対消費者（B2C）のアプリケーションです。つまり、重要であり機密性が高い場合が多い、マイクロサービス間の内部コミュニケーションとクライアントやパートナーとの外部コミュニケーションを保護することが不可欠であるということです。現在では、ほとんどの組織が、長期的なビジネスの成功には健全なアプリケーションセキュリティ戦略が必要であることを認識しており、Web アプリケーションおよび API 保護（WAAP）プラットフォーム、クラウドセキュリティ機能および製品、セキュリティ・テスト・ツールなどのセキュリティテクノロジーを使用して、アプリケーション・セキュリティ・リスクを低減しています。重要なのは、WAAP を回避して組織内の API を標的とする攻撃が、どのように進化してきたかを認識することです。このような脅威に備えて、API セキュリティ戦略をどのように調整するかを検討する時ではないでしょうか。

API セキュリティ戦略における API 検知と対応の位置づけ

過去数年間で、組織は Web アプリケーションインターフェースよりも多くの API チャネルを作成してきました。これらの API に含まれるコア・ビジネス・データとビジネスロジックの量は、増大の一途をたどっています。API は、より多くのユースケースを可能にし、変化を促進し、さらに機微な情報を運び、たくさんのユーザーに開かれているため、ビジネスのあり方を大きく変えました。

自社の API 環境の状況



API は普及が進んでいるため、ほとんどのセキュリティ製品カテゴリーは何らかの形で API をサポートしていますが、API は別の資産クラスであり、一部のコンプライアンスフレームワークでは別の資産として表示されることさえあります。WAAP プラットフォームのような旧式のセキュリティ製品に API 脅威防御機能を追加しても、API 資産がもたらす新たな課題には対処できません。セキュリティ組織は、API を独立した資産クラスとして扱い、API を徹底的に保護するために不可欠な機能を認定する必要があります。

それでは、まず、新たな脅威に対応するために API 保護がどのように変化してきたかという、基本的なことから説明します。これまでは、組織が API の完全なインベントリと堅牢な WAAP を持っていれば、大体の API 脅威は回避できました。現在の攻撃は、WAAP を回避するように設計された方法を使い、組織内やそのパートナー組織内の API を標的にしています。

たとえば、API の悪用の中には、API 認証情報を付与された顧客やパートナーが、許可されていない方法でそれを使用することを選択したことに起因するものがあります。また、一見正当な API 認証情報や、セキュリティトークンを乗っ取るという方法もあります。その他の攻撃ベクトルとして、API クライアントの実装に潜む脆弱性があります。攻撃者がこの脆弱性を利用して、従来のセキュリティツールでは検知できない方法で API を悪用する可能性があります。

幸いなことに、新たな脅威から API を保護するために不可欠な機能（特に検知と対応）は、すでに組織で十分に利用可能なレベルに達しています。以降のページでは、変化し続ける API 脅威の状況に対して、これらのプラットフォームが効果を発揮するために不可欠な機能について、丁寧に説明しています。

不可欠な機能 #1
プラットフォームを選ばない保護

一般に、API サービスは組織内のさまざまなグループによって実装されるものであり、多くの場合、多様なプラットフォームやテクノロジーを組み合わせて使用します。たとえば、ある API はオンプレミスで実装され、別の API はパブリッククラウドで実行されます。また、中間的なテクノロジー、たとえばリバースプロキシ、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）、コンテンツ・デリバリー・ネットワーク（CDN）などが使用されている場合もあり、これらが API の可視化を複雑にしています。

これらの各テクノロジーからの API アクティビティデータにアクセスする機能が不可欠です。プラットフォームを選ばない API 脅威防御アプローチを用いれば、実装の詳細や使用しているインフラを問わず、組織は常に、API アクティビティ全体を把握することができます。保護対象としては、次のものがあります。

- すべての部門、買収した企業、環境
- 認可された API とシャドー API（API ゲートウェイ利用の有無を問わない）
- 垂直方向 API だけでなく、パブリック API、パートナー API、社内水平方向 API を含む、拡張された可視性

API 脅威防御プラットフォームの可視性をできるだけ広く確保することで、外部からの攻撃者によるリスクだけでなく、インサイダーの脅威やパートナー組織による API の悪用からも組織を守ることができます。

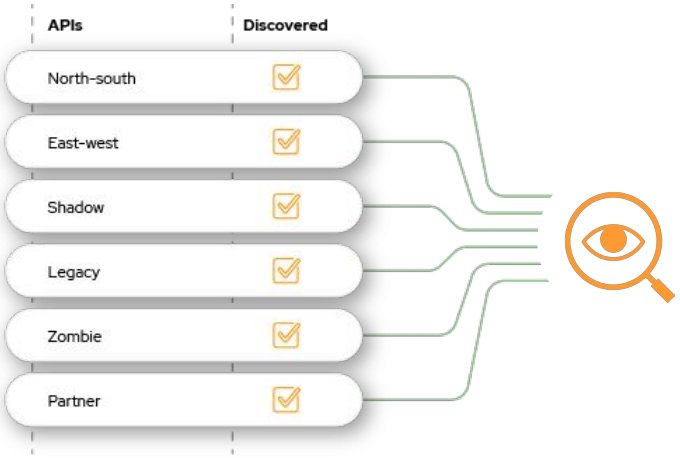
不可欠な機能 #2
継続的な API の探索と対策管理

組織全体で使用されているすべての API の包括的で継続的に更新されるインベントリは、あらゆる API セキュリティ戦略の重要な基盤となります。この理由は単純で、組織が自社の環境に何があるのか把握していなければ、それを保護することはできないからです。多くの API セキュリティ製品が、何らかのレベルの API 探索を実行できるとうたっていますが、あくまでオンデマンドや日次ベースの運用に限定されています。自社のプラットフォームの API 探索機能で以下の作業を実行できるか確認することが重要です。

- 一度しか使用されなかった API の探索を含め、24 時間体制で API を自動的かつ継続的に探索（オンデマンドや日次ベース程度の探索では不十分）。
- さまざまなテクノロジーやインフラであらゆる API を探索
- 新しく展開された API を探索し、十分に文書化された API と比較することで、シャドー API を特定
- 各 API サービスとエンドポイントのリスクスコアリングを実行
- OWASP API Top 10 に概説されているような、既知の API 脆弱性のインスタンスを検知

可視性の向上

API インベントリを見失うことがなくなる



不可欠な機能 #3
API のふるまいを可視化する

実際の API のふるまい（API コール）を表示し可視化する機能は、API セキュリティプラットフォームの基本的な機能です。この機能は、API がどのように使用または悪用されているかをセキュリティチーム、開発チーム、運用チームの主要関係者が確認して理解できるようにするために必要です。これにより、チーム間でコミュニケーションを取り、ケースを調査することができます。具体的な可視化機能としては、以下のようなものがあります。

- **調査:** どのアラートにも、アラートに対する特定のトリガーを識別するために、コールごとに元の API アクティビティを調査する機能が含まれている必要があります。
- **脅威ハンティング：** 履歴データは、すべての API アクティビティを確認し、特定のアラート範囲を超えた時間枠とコールに対してクエリーを実行する機能を含め、少なくとも継続して 30 日間のビューに拡張する必要があります。この機能は、コンプライアンスにも役立ちます。
- **データの忠実性と充実性：** すべての API コールについて、誰がどのような操作をしたのか、どのレコードにアクセスまたは操作したのか、どのようなヘッダーやパラメーターが使われたのか、などを把握できなければなりません。
- **データプライバシー：** データの忠実性は重要ですが、機微な情報をそのまま保存することはできません。トークン化は、機微な情報を保存することなくデータの豊かさを維持するために必要です。
- **タイムラインの視覚化：** アクティビティのシーケンスを前後に簡単に移動できるビューをユーザーに提供する必要があります。

ふるまい分析による脅威検知：

不可欠な機能 #4
複数のユーザーエンティティの追跡

エンティティを理解し、関連する API アクティビティを確認できれば、どのような使用や悪用に対してもコンテキストを得ることができます。したがって、API 保護プラットフォームがこれらのエンティティを個別に追跡できる高度な機能を備えていることが重要です。あるカテゴリーのユーザーにとっては正常な活動が、別のカテゴリーでは悪用の兆候となる可能性があるため、こうしたコンテキストは非常に重要です。タイムライン上で各エンティティのアクティビティを表示する機能は、重要な可視性とコンテキストに基づく理解を提供します。以下に例を示します。

API アクティビティ	参加者	エンティティ	ビジネスプロセス エンティティ
例	社内ユーザー、B2B パートナー、社外ユーザー	IP アドレス、API トークン、業者 ID、セッション ID、テナント ID	支払い ID、請求書 ID

不可欠な機能 #5
B2B および水平方向 API カバレッジ

API 利用で最も増えているのは、社内向けと社外向けの B2B ユースケースです。API セキュリティは、垂直方向（外向き）と水平方向（内向き）の両方のインスタンスを含めた、B2B のマシン間 API をカバーしなければなりません。

B2C Web アプリケーションは WAAP と WAF プラットフォームによって保護されますが、最も機密性の高いタイプの API アクティビティ、たとえば水平方向の内部 API や、B2B API を通じてパートナーに公開される独自のアプリケーション機能などは、WAAP を通した場合でも侵害される可能性があります。

通常、B2B パートナー API でいったん認証されたユーザーは、安全であるとみなされ、それ以上の監視は行われません。これが、多くの組織の API セキュリティ体制に深刻なギャップを生じさせています。API アクティビティと広範な脅威の全体像を把握するために、組織はすべてのユースケースに対して効果的な可視性、可観測性、監視性を提供するアプローチを採用する必要があります。

不可欠な機能 #6
ふるまい分析と検知

巧妙な API の脅威を検知することは、個々の API コール、もっと言えば、個々のセッションを分析するだけでは不可能です。API を検知し対応するためには、ふるまいのコンテキストを深く理解し、学習することが必要です。API のふるまいに異常があるかどうか、つまり侵害されている可能性があるかどうかを見極めるには、API の使用状況を長期にわたって分析する必要があります。ふるまい分析の技術は、ベースラインとなる通常のユーザーのふるまいを決定し、そのふるまいを継続的に監視して異常を検知するものです。

このレベルの分析を標準的なエンタープライズの API アクティビティに対して実行するために必要なストレージとコンピューティングリソースは、スケールに制約があるオンプレミスの API セキュリティツールで提供することは現実的ではありません。EDR ソリューションと XDR ソリューションによって、有意義なふるまい分析を行うには SaaS（Software as a Service）に基づくアーキテクチャが必要であることが示されました。クラウドのパワーとスケールは、長期にわたるデータの保存を可能にすると同時に、正常なユーザーの経時的なふるまいを特定する分析を可能にすることで、干し草の山から 1 本の針を見つけ出すような精度で悪用を検知することができます。SaaS アプローチには他にも、より迅速でシンプルな実装、API 使用量の増加に伴うスケーラビリティと柔軟性の向上といった利点があります。

不可欠な機能 #7
コンテキストに沿った有意義なアラート

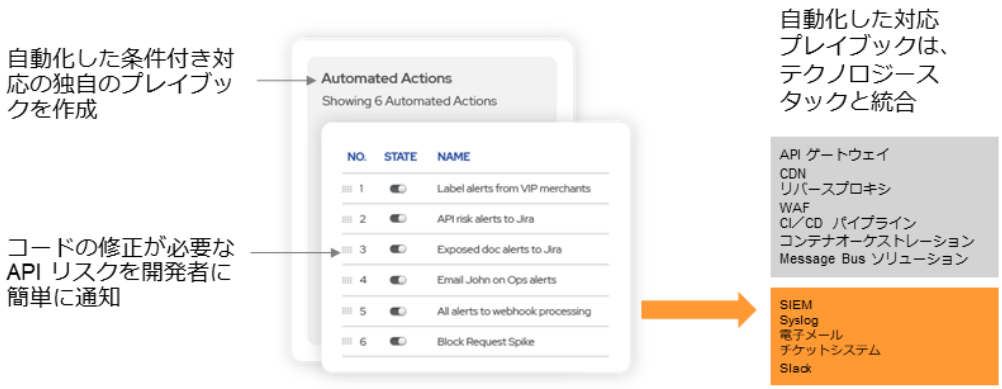
組織がすべての API アクティビティとスケールでのふるまい分析を可視化できるようになれば、API アクティビティに関するアラートは、はるかに有意義なものになります。組織は、セキュリティモニタリングのアプローチをより抽象化させ、あらゆる攻撃手法を予測する必要がなくなります。正常なふるまいをベースライン化し、異常を検知するようにすれば、パターンやシグネチャでは検知できないことが多い API の悪用も検知できるようになります。さらに、攻撃を巻き戻してアラート前に何が起こったかを確認できるため、API 資産の使用と悪用に関する貴重な知見を得ることもできます。

不可欠な機能 #8
カスタマイズされた自動応答

従来のインライン API アプローチでも自動化されたアクションを実行して疑わしい API 攻撃をブロックすることができますが、それには、組織が攻撃を特定できなければなりません。API 上のふるまい分析および異常検知は、はるかに大きなビジネスコンテキストに基づいて時間をかけて実行されるため、検知が深まるにつれ、異常が表面化します。これにより、自動化およびカスタマイズされた幅広い対応が可能となり、高い精度で実行することができます。例としては次のものがあります。

- サポートされている API ゲートウェイおよび CDN エッジフィルターでトラフィックをブロックまたはスロットリングする
- セキュリティおよびビジネス関係者に電子メールで通知する
- 開発者に対してチケットを作成する
- Webhook をトリガーする

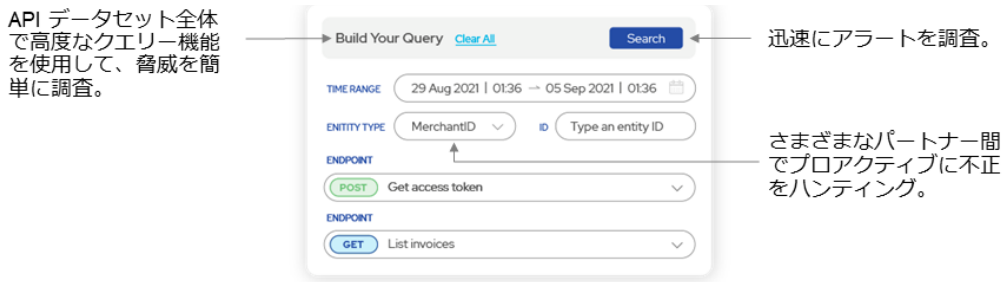
ユーザーのビジネスプロセスに合わせてカスタマイズ可能



不可欠な機能 #9
予防的調査と脅威ハンティング

多くの組織には、アクティブなセキュリティインシデントが発生するまで待ってから行動できるほどの余裕はありません。それよりも効果的なアプローチは、望ましくない状況を特定し、それを積極的に探し出すことです。たとえば、予防的な脅威ハンティングを通して、ある API で悪用を検知したアラートが、別の API で同じふるまいをしていることを特定できるかもしれません。このため、API 脅威防御プラットフォームには、アクティブなインシデントに対応して生成されるアラート以外にも、特定のタイプのふるまいを検索する機能を含める必要があります。脅威ハンティング機能は、API アクティビティデータに潜む悪用を探し出すために、履歴データにアクセスする必要があります。データの内容を充実させてコンテキストを提供することをしない単発リクエストソリューションでは、首尾一貫したストーリーとしてまとめることができません。脅威の探索と調査は、履歴データを基礎として成り立っています。

調査や脅威を簡単に発見する力



不可欠な機能 #10
観測可能なデータレイク

堅牢な API セキュリティ戦略のすべての機能において、長期にわたって API を保護する上で鍵となるのはコンテキストです。脅威を観察し、潜在的な脆弱性を特定し、攻撃時にトラブルシューティングを行うために十分なコンテキストを維持する最善の方法は、すべての API のふるまいをログに記録し、このアクティビティのバックログを保持することです。これは、API セキュリティソリューションとデータレイクを関連付けることで実現できます。戦略に必要な過去の詳細情報を最も多く提供するデータレイクを見つけてください。基本的なリクエストデータを機械学習モデルにフィードすることも可能ですが、リクエストパラメーターのような詳細があれば、組織は将来の脅威や攻撃から保護できる方法で、履歴データに基づいて実際に行動することができます。

#1 プラットフォームを選ばない保護	API 脅威防御プラットフォームの可視性を可能な限り広く確保することが、脅威や悪用から組織を守ることにつながります。
#2 継続的な API の探索と対策管理	組織全体で使用されているすべての API のインベントリを包括的かつ継続的に更新することは極めて重要です。組織は自分の環境の中に存在すると知らないものを保護することはできないからです。
#3 API のふるまいを可視化する	可視性は、API がどのように使用または悪用されているかをセキュリティチーム、開発チーム、運用チームの主要関係者が確認して理解し、チーム間でコミュニケーションを取り、ケースを調査できるようにするために必要です。
#4 複数のユーザーエンティティの追跡	エンティティを理解し、関連する API アクティビティを確認できれば、どのような使用や悪用に対してもコンテキストを得ることができます。したがって、API 保護プラットフォームがエンティティを個別に追跡できる高度な機能を備えていることが重要です。
#5 B2B および水平方向 API カバレッジ	API アクティビティと広範な脅威の全体像を把握するために、組織はすべてのユースケースに対して効果的な可視性、可観測性、監視性を提供するアプローチを採用する必要があります。
#6 ふるまい分析と検知	API のふるまいに異常があるかどうか、つまり侵害されている可能性があるかどうかを見極めるには、API の使用状況を長期にわたって分析する必要があります。ふるまい分析の技術は、ベースラインとなる通常のユーザーのふるまいを決定し、そのふるまいを継続的に監視して異常を検知するものです。
#7 コンテキストに沿った有意義なアラート	組織がすべての API アクティビティとスケールでのふるまい分析を可視化できるようになれば、API アクティビティに関するアラートは、はるかに有意義なものになります。組織は、セキュリティモニタリングのアプローチをより抽象化させ、あらゆる攻撃手法を予測する必要がなくなります。

#8 カスタマイズされた自動応答	API 上のふるまい分析および異常検知は、はるかに大きなビジネスコンテキストに基づいて時間をかけて実行されるため、検知が深まるにつれ、異常が表面化します。これにより、自動化およびカスタマイズされた幅広い対応が可能となり、高い精度で実行することができます。
#9 予防的調査と脅威ハンティング	多くの組織には、アクティブなセキュリティインシデントが発生するまで待ってから行動できるほどの余裕はありません。それよりも効果的なアプローチは、望ましくない状況を特定し、それを積極的に探し出すことです。
#10 観測可能なデータレイク	脅威を観察し、潜在的な脆弱性を特定し、攻撃時にトラブルシューティングを行うために十分なコンテキストを維持する最善の方法は、すべての API のふるまいをログに記録し、このアクティビティのバックログを保持することです。これは、ユーザーの API セキュリティプラットフォームとデータレイクを関連付けることで実現できます。

この記事が参考になったとお考えの場合は、次のステップとして Akamai の API Security ソリューションをご検討ください。トップレベルの堅牢さを誇る、API セキュリティ戦略を構築していただけます。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 12 月。