Akamai

ホワイトペーパー

API 検知と対応に不可欠な 11 の機能

API セキュリティ戦略の進化

はじめに

API は、組織が顧客のために構築するもの、社内で使用するもの、ベンダーやサプライヤーが利用できるものなど、すべてのアプリケーションにおいて不可欠な役割を果たします。API の役割は、テクノロジー間で情報（多くの場合、機微な情報）を交換することです。API はアプリケーション内だけでなく、クラウド移行、生成 AI ツール、デジタル・サプライ・チェーンの至るところに存在します。

課題は、API が組織のアタックサーフェスの中でも顕著になっていることです。

企業がイノベーションを急いでいるため、API は多くの場合急いで開発され、十分にテストされず、誤設定があったりセキュリティ制御が欠如していたりする状態で運用環境にリリースされます。さらに、このような API が集まって無秩序に拡大し、セキュリティチームは自社の API 資産の大部分を可視化できなくなっています。そして、適切な可視性がなければ、組織は次のような事態に陥ります。

1. 機微な情報、インターネット、攻撃者に野放し状態でさらされたまま忘れられ、管理されていない API を検知できない
2. そのため、API のリスクを評価できない（たとえば、完全な API インベントリを備え、どの API が機微な情報を返すかを把握している企業はわずか 27% であり、2023 年の 40% から低下している）
3. 最終的に、API 中心の脆弱性だらけのアタックサーフェスが発生し、攻撃者に頻繁に（多くの場合は容易に）悪用される

組織は最近まで、API の管理や保護のベースラインを把握するために一般的に使用されるツールに依存している状態に満足していました。しかし、過去 12 か月間に API セキュリティインシデントに見舞われた組織の割合は 84% であり（2023 年の 78% から増加）、何かを変える必要があります。

API 攻撃の数と巧妙さが増している今こそ、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）、Web アプリケーションおよび API 保護（WAAP）プラットフォームなどのツールに新たな保護レイヤーを追加することを検討するときです。

新しいレイヤーは、組織の環境内のすべての API とそのリスクをより明確に可視化するものでなければなりません。それには、次のような管理されていない API の大部分が含まれます。

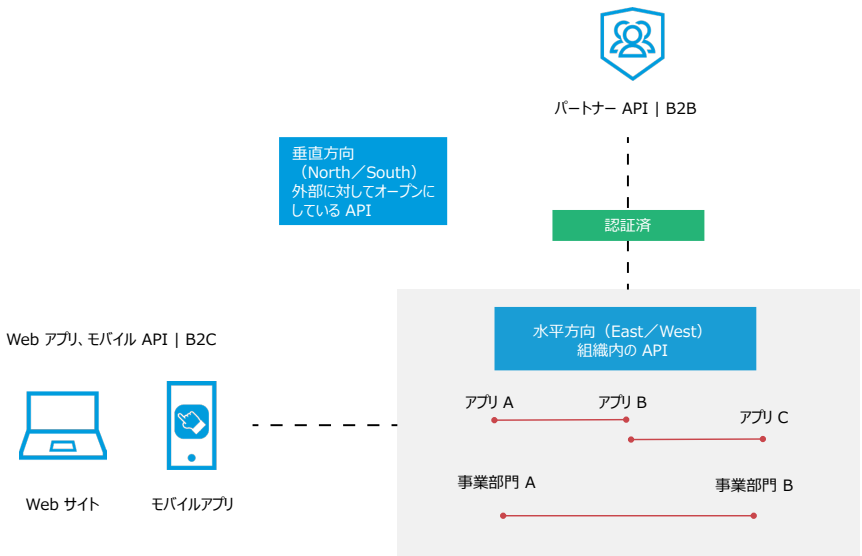
- 廃止されるべきだったがアクティブなままのゾンビ API
- 文書化されておらず、排除するか正式なガバナンスプロセスに組み込む必要のあるシャドー API

組織にはさらに、OWASP Top 10 API セキュリティリスクに詳述されているすべての脅威を含め、API の悪用や API 攻撃を検知して対処するためのより高度な機能が必要です。また、API のライフサイクル全体を通して脆弱性を見つけて修正することに目を向けると、企業は初期開発段階から本番環境まで、厳格なリアルタイムの API セキュリティテストを導入する必要があります。

これは、問題が発生するたびに新しいツールを積み重ねていくということなのでしょうか。いいえ、違います。例えると、オーケストラに適任の奏者を揃え、適切なタイミングで適切な音を奏でるようにする、そして奏者同士で正確に連携することに似ています。

API 保護スタックに新しいレイヤーを追加する方法を考える際には、セキュリティチームが他の脅威に適用している多層防御アプローチを検討します。たとえば、ランサムウェア攻撃の影響を検知、防止、緩和するための厳格な制御の展開です。組織は API についてこのように考える必要があります。

このホワイトペーパーでは、API の脅威の検知と対応に重点を置き、API セキュリティ戦略に組み込むことができる 11 の重要な機能について説明します。



コンテキストが鍵
API セキュリティ戦略における API 脅威検知と対応の位置づけ

おそらく誰もが目の当たりにしてきたとおり、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伝送し、たくさんのユーザーに開かれることにより、ビジネスのあり方を大きく変えました。組織が Web アプリケーションインターフェースよりも多くの API チャネルを作成したことは驚くべきことではありません。また、このように増え続ける API に組み込まれる基幹ビジネスデータやビジネスロジックの量が増加しているため、リスクが増大しています。

セキュリティチームがすでに保護している無数のテクノロジー（アプリケーションなど）に API が普及していることを考慮すると、ほとんどのカテゴリーのセキュリティ製品は API を何らかの形でサポートしています。しかし、API とアプリケーションは同じではなく、一部のコンプライアンスフレームワークでは異なる資産に見える場合もあります。既存のアプリケーションセキュリティ製品などに、個別の API 脅威保護機能を追加するだけでは不十分です。一般的に、ほとんどの組織は API を十分に重視していません。今日のセキュリティチームは、API を明確なリスク属性のある個別の資産クラスとみなし、すべての API を大規模にとらえてセキュリティを確保するための重要な機能を探す必要があります。

以前は、API インベントリを持っていて API 管理および保護のためのベースラインツールがあれば、組織は、既知の一般的な API 攻撃を防止することができました。残念なことに、今日では多くの攻撃者が、企業のようにイノベーションを起こし、継続的な改善にも同様に取り組んでいます。

- 悪意のあるアクターは、API の防御のためにほとんどの組織が利用していることが明らかになっているツールを回避するよう、論理的に戦略を進化させています。
- ほとんどの企業の AI 利用方法と同様に、攻撃者は常に生成 AI 機能の支援を受けて、限られた人間の能力を増強しています。
- 攻撃者はますます、API 保護に優先的に取り組んでいない可能性のある B2B パートナーなど、企業の API 接続デジタル・サプライ・チェーン内の脆弱なつながりを探すようになっています。

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。脅威アクター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、急速に進化する攻撃手法から API を保護するために不可欠な機能は、組織で十分に利用可能なレベルに達しています。以降では、API 自体と API が交換するデータを攻撃から保護するための対策を講じる際にチームが最初に確保すべき 11 の重要な機能について、詳しく説明します。

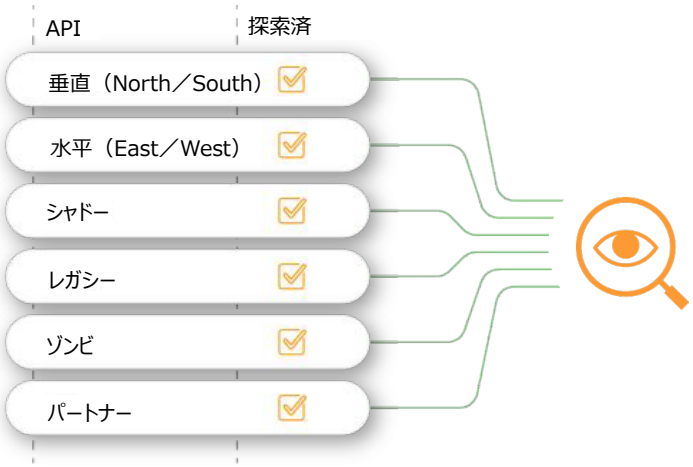
重要機能 1
継続的な API の探索とポスチャ管理

組織全体で使用されている 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 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（これは、セキュリティ侵害が発生した場合にセキュリティチームと開発チームの両方がノイズに惑わされず、最も大きな影響をもたらす可能性のある API を優先するのに役立ちます）
- OWASP Top 10 API セキュリティリスク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



重要機能 2
API のふるまいの可視化

実際の API のふるまい（API コール）を可視化する機能は、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。
- **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、どのレコードに対して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。トラフィックを分析し、ダッシュボードを更新するために関連するメタデータのみを送信するソリューションが必要です。

重要機能 3
ユーザーエンティティのコンテキストを介した API の悪用の発見

セキュリティチームは、IP アドレスやビジネス・プロセス・エンティティ（支払い ID など）といったエンティティに対する悪性アクティビティを追跡する機能を必要としています。これは、他の関連する識別子が API の悪用にコンテキストを付加できる場合に、さまざまな IP からの攻撃を相互に関連付ける機能と組み合わせると非常に役立ちます。

たとえば、不明なユーザーが、/api/getpaymentID/50 を ID として使用して、小売企業の API をコールしているとします。このシナリオでは、小売企業のセキュリティチームは、自社のプラットフォーム内の他のすべてのユーザーが 1 つのタイプの支払い ID に関連付けられていることを知っています。セキュリティアナリストが不意にそれに気付いたとき、不明なユーザーが繰り返しコールしていて、そのたびに ID 番号を少しずつ調整していたとしたら（/api/getPaymentID/51 … 52 … 53 … 54）、それは API 悪用の試みであることを示す重要な指標です。

非典型的なユーザーのふるまいに関するリアルタイムの知見を得ることは、侵害の試みを阻止するか API 攻撃が成功するかどうかの、分かれ目になります。

$943,162

過去 12 か月間に API セキュリティインシデントを経験したと報告した、米国に拠点を置く企業の CISO、CIO、CTO によると、インシデントの影響を修復するための平均コストは $943,162 です。

他社の見解や経験について、詳しくは 2024 年の API セキュリティの影響に関する調査をご覧ください。

重要機能 4
ふるまい分析と検知

ユーザーエンティティからの個々の API コール（または個々のセッション）を分析することはセキュリティチームにとって有益ですが、全体像に重点を置いた包括的な API 脅威検知を行うことが重要です。API 資産全体のふるまいパターンと異常を深く理解する機能を追求する必要があります。API のふるまいが異常であるかどうかを判断するためには、長期にわたって徹底的にふるまいを追跡することによって構築されたコンテキストの基盤を使用して、API の使用を長期にわたって分析する必要があります。これにより、セキュリティチームが継続的にふるまいを監視して異常を検知する際に、信頼性の高いベースラインが提供されます。

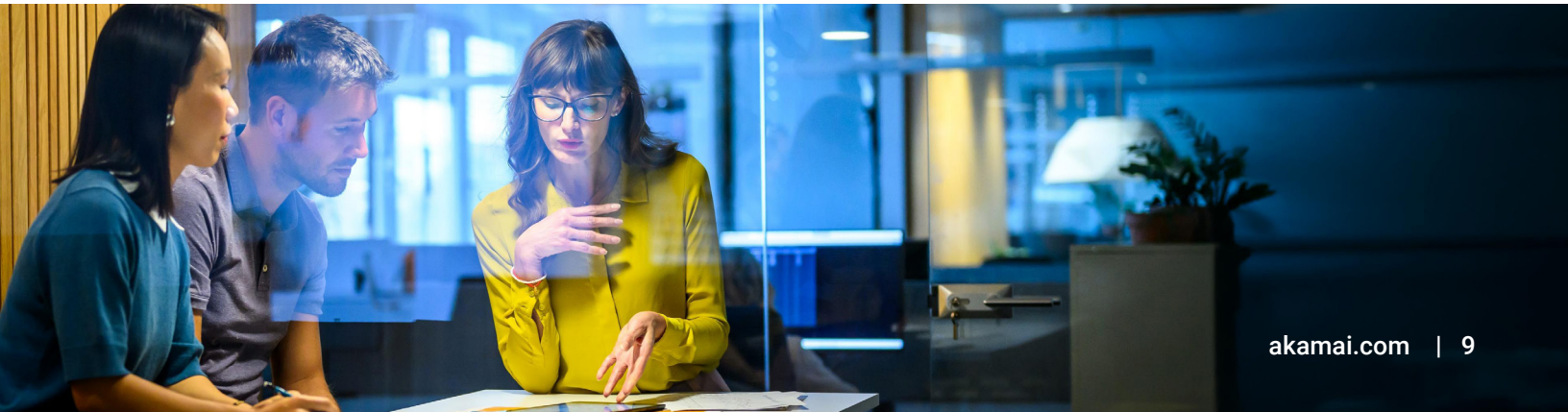
重要機能 5
API 仕様のドリフトの検知

API は、市場の需要とビジネス要件の変化に伴い、常に変化しています。そのため、組織は急速に進化する企業のニーズに対応し、バグを修正し、技術的な改善を導入するために、新しいエンドポイント実装を継続的にリリースしています。API 仕様に基づき、これらの変更と足並みをそろえて API ドキュメントを更新することは極めて重要であり、API トラフィックが常にその仕様に適合するように特別な注意を払う必要があります。

API の悪用や攻撃に対する回復力を持たせるために、組織は API 仕様のドリフトを検知する機能を追求する必要があります。この機能は、企業がリアルタイムの API トラフィックと定められた仕様とを継続的に比較し、API ドキュメントの不整合やギャップを特定するのに役立ちます。

API 仕様ドリフト検知機能は、不一致があることや、本番環境において文書化されていないエンドポイントへのアクセスが行われていることを発見した場合に、開発者やセキュリティチームに警告を発して以下のことを行えるようにします。

- 問題が深刻化する前に先んじて対処する
- API が意図したとおりに動作するようにする
- その API がサポートするアプリケーションのセキュリティを強化する
- 企業の API エコシステムの完全性を維持する



重要機能 6
B2B および East ／ West の 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（North ／ South、外向き）と水平方向（East ／ West、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（East ／ West）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 セキュリティポスチャ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。

重要機能 7
コンテキストに沿った有意義なアラート

組織が API アクティビティと大規模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。しかし、真の API 脅威に注意を向け、リソースを集中するためには、どうすればよいのでしょうか。攻撃確実度エンジンは、API のふるまい、ネットワークのトラフィックパターン、ジオロケーションデータ、脅威インテリジェンスフィード、その他のコンテキスト要素など、外部および内部のシグナルを評価するようトレーニングされた高度な機械学習アルゴリズムを使用し、検知されたランタイムインシデントが悪性アクティビティの結果であることの確実度を判定できます。この機能は、セキュリティチームが重大な脅威を迅速に特定するのに役立ちます。また、この機能は、可能性が高い攻撃に対する自動修正と通知のフローを作成する機能によって補完する必要があります。

重要機能 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コンテンツ・デリバリー・ネットワーク（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

API 脅威が増大するなか、すでに多忙なセキュリティチームとそのエネルギーを最大限に活用するために、組織はどのような支援ができるでしょうか。マルチアクションワークフローの作成と管理をシンプル化することによって効率と生産性を向上させる、自動化機能を探すことが重要です。適切な自動化機能とは、複雑なイベント応答プロセスを作成し、コア API セキュリティソリューションと無数のサードパーティサービス（ServiceNow、Jira、Azure DevOps など）との間でインシデント関連のデータを同期できる、コード不要のビジュアル・デザイナー・インターフェースを提供するものを指します。

重要機能 9
API トラフィック分析

組織は、データレイクを展開することなく、環境内の API トラフィックを記録、可視化、分析するための Always-on の機能を必要としています。通常の API アクティビティや異常な API アクティビティなど、アプリケーション環境全体で特定の条件に合致する API データフローを記録することで、組織は疑わしいユーザーや異常な API のふるまいのリスクを管理しながら、より効果的に脅威を探索できます。特定のユースケースに合わせてカスタマイズ可能な API トラフィック監査機能を備えていることが重要です。これにより、組織は事前に定められたフィルターやルールに従ってトラフィックをキャプチャし、保持することができます。

重要機能 10
厳格なリアルタイム API テスト

組織はイノベーションを急ぐあまり、脆弱性や設計上の欠陥がある API を本番環境にリリースしており、それらは検知されないことがよくあります。組織は、開発段階の API テストにシフトレフトアプローチを採用することで、これらの問題を防止できます。コア機能には次のものがあります。

- OWASP Top 10 API セキュリティリスクで取り上げられているタイプなどの悪性トラフィックをシミュレートする自動テストを実行する
- 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
- オンデマンドで、または CI ／ CD パイプラインの一環として API をテストする

重要機能 11
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、そのグループは多くの場合、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。多くの場合、組織はリバースプロキシ、API ゲートウェイ、WAF、CDN などの中間的なテクノロジーを使用します。それらはビジネス価値をもたらしますが、API の可視化を複雑にします。

これらの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 アクティビティを包括的に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 の両方（API ゲートウェイ利用の有無を問わない）

プラットフォームを選ばないアプローチでは、垂直方向の（North ／ South）API だけでなく、パブリック API、パートナー API、内部の水平方向の（East ／ West）API も可視化されます。

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、外部の脅威アクターからのリスクだけでなく、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。

結論

現代のクラウド中心のデジタル経済では、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、機微な情報の処理、セキュリティ制御の欠如により、API は重大なリスク要因となっています。

Akamai API Security は、このホワイトペーパーで取り上げた 11 の重要な機能のすべてを提供し、組織が次のような不可欠な機能によって既存のアプローチを強化できるよう支援します。

- API 探索
- リスクの評価（機微な情報への暴露を含む）
- API の悪用と API 攻撃の検知
- セキュリティリスクと脆弱性の有無に関する API のテスト

OWASP Top 10 API セキュリティリスクに対する防御方法について、詳しくご確認ください。

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。

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。 当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。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 ： 2025 年 1 月。