Akamai お客様事例

Akamai API Security によって顧客を保護

セキュリティのリーダー企業が、何千もの顧客のコンプライアンスの維持と何万ものAPIのセキュリティの確保を支援

Netskopeは、クラウド、データ、ネットワークのセキュリティを再定義しているサイバーセキュリティの世界的リーダー企業です。Fortune 100の25社以上を含む何千もの顧客がNetskopeを利用して、進化する脅威に対処し、テクノロジーの移行を促進し、規制要件への準拠に取り組んでいます。

Netskopeは、同社が保護する多くのミッションクリティカルなテクノロジー分野の中で、世界中で数万ものAPIを保護する責任を担っています。そのためには、従来のアプリケーションセキュリティを超える新しいアプローチが必要だと認識するようになりました。顧客のAPIセキュリティ体制のギャップを発見した後、Netskopeは、悪性のAPI攻撃から顧客を保護するために必要な次世代ツールを求めて、Noname Security（現在はAkamai傘下）に着目しました。

ファイアウォール以外のセキュリティを求めて

小規模なアプリケーションを展開している顧客も、無数のマイクロサービスを使用して大規模なアプリケーションを展開している顧客も、実際には全ての顧客がAPIを使用しています。つまり、公開されているすべてのAPIがアタックサーフェスの一部となるのです。たとえば、Netskopeは、顧客のAPI資産内に検知されなかった脆弱性やNetskopeが認識できなかった脆弱性があることを発見しました。そのため、NetskopeのAppSecチームは、自社と顧客の両方のAPIとその他の公開デジタル資産のセキュリティを確保するソリューションを探し始めました。

Netskopeは、この問題が従来の問題ではないことを認識していました。つまり、Webアプリケーションファイアウォールなどのレガシーソリューションを使用したり、従来のアプリケーション・セキュリティ・テストを実行したりすることはできませんでした。ログの量、発生していた攻撃の種類、APIの悪用の種類が原因で、異なるアプローチが求められました。

netskope

所在地

カリフォルニア州サンタクララ
netskope.com

業種

ハイテク

ソリューション

Akamai API Security

主な効果

- API ライフサイクル全体のセキュリティを確保
- API 攻撃をリアルタイムでブロック
- API の仕様書を自動で作成

Akamai

また、Netskope の Deputy CISO である James Robinson 氏は、エンタープライズレベルでスケーリングを試みる際に、チームが機械学習や高度なツールを活用して自社の API 資産を完全に可視化する必要があることを理解していました。しかし、新しいツールを取り入れるためには開発者と協力する必要があることを、セキュリティチームは十分に認識していました。

セキュリティチームにとって大成功

Netskope は、Noname API Security Platform（現在は Akamai API Security の一部）を使用して、稼働前と稼働中の両方の API を保護することを決定しました。本番環境の API を保護するために、Akamai API Security の探索モジュールを使用して、社内、社外、およびサードパーティの API の正確なインベントリーを取得し、これらの API を通過した機微な情報を分類しました。正確なインベントリーが得られたら、ランタイム保護モジュールを使用して異常を検知し、API 攻撃をリアルタイムでブロックしました。

稼働前については、Netskope は Akamai の API セキュリティ・テスト・ソリューションを使用しました。このソリューションは、組織が API を展開する前に脆弱性や誤設定がないかテストするために役立ちます。このソリューションは、悪性トラフィックをシミュレートする 100 以上の動的テストを自動的に実行できます。これにより、組織の開発者がコードを保護できるだけでなく、顧客向けにリリースしようとしている API 製品の安全性が確保されます。

評価段階で、開発者はすぐに仕事が楽になる機能を見出しました。API が古すぎるため開発者が仕様書を持っていない場合でも、Akamai のソリューションを利用すれば仕様書が自動的に作成されるため、API を理解するためにコードを調べる必要はありません。ログとトランザクションについても同じです。開発者は、さまざまなシステムでクエリーを実行し、ログラインを確認できます。

当然のことながら、このプラットフォームはセキュリティチームにとっても大成功でした。チームは従来の攻撃だけでなく、より高度な脅威も検知できるようになりました。

> 社内的には、ソリューションを検討し始めたときに、開発者をセキュリティチームと連携させる必要がありました。重要なシステムは基本的にアプリケーションの中核であるため、開発者のサポートなしに足を踏み入れることはできません。
>
> – James Robinson 氏
> Netskope、Deputy CISO

今後の展望：顧客のコンプライアンスを維持

今後、Netskope は Akamai を使用して API ガバナンスに対処し、自社や顧客が世界中で拡大しているデータプライバシーに関する法律や義務に準拠した状態を維持できるようにする予定です。また、クラウドとオンプレミスの両方に Akamai API Security を展開したため、さまざまなユースケースを引き続き検討する予定です。オンプレミスの展開は、同社にとっても、公共部門やその他の規制の厳しい業界の顧客にとっても大きな変革となりました。

> 当社にとって、Noname は最適な選択肢であっただけではありません。Noname のサポートを受け、より適切かつ迅速に展開し、市場投入までの時間を短縮することができました。
>
> – James Robinson 氏
> Netskope、Deputy CISO

組織はセキュア・アクセス・サービス・エッジ（SASE）アーキテクチャを迅速に導入して、データがどこに移動しても保護し、デジタルトランスフォーメーションの取り組みをサポートし、テクノロジーから得られる効率性と投資収益率（ROI）を向上させています。Netskope はすでに CASB、SWG、ZTNA、サービスとしてのファイアウォール（FWaaS）、およびセキュリティ・サービス・エッジ（SSE）のその他のコンポーネントのエキスパートおよびイノベーターとして広く認知されています。これらはいずれも SASE アーキテクチャの成功に不可欠なセキュリティサービスです。

しかし、SASE が注目されている一方で、ベンダーが紛らわしいメッセージを製品セットに添えて、「SASE」として疑わしいマーケティングをすることがよくあります。このような製品のほとんどは、ネイティブに統合されておらず、テクノロジー環境をシンプル化することもできません。また、重要なネットワークおよびインフラ変革機能が欠如しているため、高度なセキュリティインシデント、ネットワークダウンタイム、低水準の ROI といったリスクがもたらされます。

Netskope Borderless SD-WAN と Netskope Intelligent SSE を組み合わせた完全統合型の SASE プラットフォームは、独自の方法でこれらの課題に対処します。

| 公開日：2024 年 9 月