Akamai お客様事例

米国大手銀行、API トラフィックのセキュリティを確保して可視性を強化

API のアタックサーフェスをかつてないほど可視化して、厳格な規制コンプライアンスを維持

銀行業界は近年、アプリケーション・プログラミング・インターフェース（API）の採用により大きな変革を遂げています。こうした API の普及により、銀行は新たな機会を活用し、顧客体験を強化し、ビジネスの成長を促進することができるようになりました。

API は、銀行エコシステム内のさまざまなシステムとアプリケーション間でシームレスな統合を実現する上で重要な役割を果たしています。銀行は、API を介してサービスやデータを公開することで、サードパーティの開発者、FinTech（フィンテック）の新興企業、その他の金融機関とコラボレーションして、革新的なソリューションを生み出し、サービスを拡大できるようになりました。しかし、このような明確な利点がある一方で、API の公開には必ずリスクが伴います。

API のセキュリティリスクは、API の機密性、完全性、可用性に重大な脅威をもたらす可能性があります。これらのリスクには、不正アクセス、インジェクション攻撃、サービス妨害攻撃、不適切な認証および権限昇格、入力検証の欠如、安全でない認証情報保管、不適切なロギングおよび監視などが挙げられます。このようなリスクに対処するために、銀行業界のリーダーである同社は Noname Security（現在は Akamai 傘下）と提携を結ぶことになりました。

コンプライアンスの維持

金融サービス業界では、公正かつ透明性のある慣行の確保、消費者の保護、金融システムの健全性の維持において、規制の遵守が最も重要となります。顧客確認（KYC）およびアンチ・マネーロンダリング（AML）規制において、金融機関は顧客の身元を確認し、マネーロンダリングやテロ資金供与に関連する潜在的なリスクを評価し、疑わしい活動を報告することが求められます。

Banking Leader

所在地

米国

業種

金融サービス

ソリューション

Akamai API Security

主な効果

- 規制コンプライアンスを強化
- F5 本番環境と統合
- 継続的な API 識別を提供

Akamai

その他には、クレジットカード業界データセキュリティ基準（PCI DSS）の規制が挙げられます。これは、カード所有者のデータを保護するために大手クレジットカード会社によって確立された一連のセキュリティ基準です。金融規制に関して言えば、これらの規制はごく一部にすぎません。そのため、金融サービスのリーダーにとって、API を通過するデータを把握することが極めて重要でした。

同社では、API の探索、データ分類、脆弱性、異常検知に重点を置き、API エコシステムの全体的な可視性を向上させてリスクを把握、管理、緩和する必要がありました。また、F5 の本番環境との統合にも重点が置かれました。

API フットプリントの明確化

Noname API Security プラットフォーム（現 Akamai API Security の一部）により、お客様のネットワークとの間で送受信される API トラフィックが、プラットフォーム内と同様に可視化されました。Akamai API Security エンジンでは、トラフィックの分析が行われ、金融サービスリーダーの API がすべて探索されました。リアルタイムのトラフィック分析で新規 API や既存 API の変更が識別され、お客様のダッシュボードでデータの記録および更新が行われました。

このプラットフォームはエージェントやサイドカーに依存せず、クラウドインフラと統合されているため、API が API ゲートウェイに登録されているかどうかに関わらず、すべての API を認識します。内部および外部 API、レガシー API（API ゲートウェイより前から存在する API）、シャドウ API、不正 API（ゲートウェイを経由してルーティングされていない API）がすべて探索され、API アタックサーフェスがかつてないほど可視化されます。

今後の展望

銀行業界のリーダーは、一連の基準を用いて正常な API セキュリティを評価します。その中で Akamai がサポートしているものの 1 つが、迅速なトリアージ（対処の優先順位付け）です。主な目的は、発見された問題の重大度を分析する方法を決定することであり、SOC はこれによって迅速に評価、トリアージ、アラートへの対応を行えるようになります。

 | サポート | | 公開日：2024 年 8 月