Akamai お客様事例

Fortune 500 に名を連ねるファッション業界のリーダーが API と小売事業の両方のセキュリティを確保

小売体験のパーソナライズと利便性を促進する API のセキュリティを確保すると同時に、顧客のデータを侵害から保護

すべての API を探索 | 脆弱性を特定 | セキュリティ体制を強化

API は、小売業界が従来の実店舗から E コマースプラットフォームに移行する上で重要な役割を果たしてきました。すべてのデジタルインタラクションの背後には API があり、小売企業が次のことを行えるようにしています。

- さまざまなシステム、アプリケーション、サービスのシームレスな接続
- オンラインストアと、バックエンド在庫管理システム、決済ゲートウェイ、配送業者、顧客関係管理ツールの統合
- オンライン小売をパーソナライズして便利にする高速データ交換の促進

このようなデータの保護は最優先事項とされているため、API セキュリティはオンライン事業の信頼性、完全性、機密性を確保する上で重要な役割を果たします。

API は、機微な情報に常に近接しているため、脆弱性を悪用しようとするサイバー犯罪者にとって魅力的なターゲットです。API の侵害が成功すると、個人情報、決済カードデータ、購入履歴などの顧客情報が漏えいする可能性があります。そのため、それまでの Salt Security との関係に満足していなかったこの Fortune 500 のファッション小売企業は、Noname Security（現在は Akamai 傘下）に助けを求めました。

Fashion Retailer

所在地

米国

業種

小売

ソリューション

Akamai API Security

Akamai

API セキュリティに対する計画的アプローチの考案

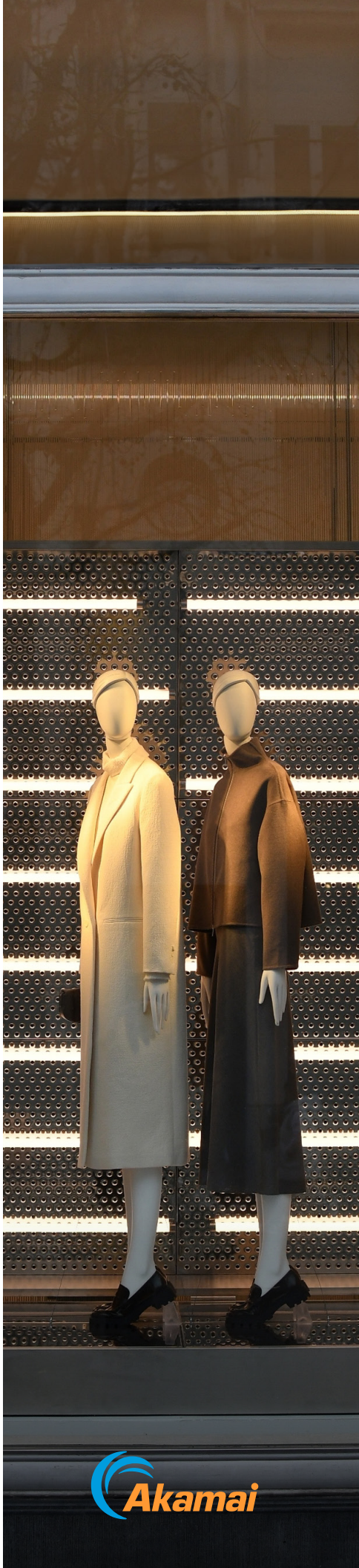
この Fortune 500 の小売企業は、Web アプリケーションファイアウォールや API ゲートウェイを超えた、API セキュリティリスクを緩和するための完全なエンドツーエンドワークフローを構築しようとしていました。これには、API ガバナンスのための強固な制御機能を備えた、確固とした API セキュリティ戦略が必要です。また、同社はボットの緩和にも重点を置き、最終的には正当なユーザーと悪性ボットを区別して、システム、データ、ユーザー体験を保護できるようにしたいと考えていました。

プロジェクトの規模を考慮し、この小売企業と Akamai は段階的アプローチを採用することにしました。フェーズ 1 では、すべての API の特定、機微な情報の分類、検知と応答の導入、Splunk との統合を行います。フェーズ 2 では、シフトレフト API セキュリティ・テスト・アプローチへ転換し、安全なコードの作成を迅速化します。

迅速な展開により、価値実現までの時間を短縮

フェーズ 1 は難しい注文でしたが、Akamai チームは Noname の API 探索モジュールとランタイム保護モジュールを展開し、Splunk との統合をわずか 120 日で実行することができました。API 探索は、API スプロールを管理する上で重要な役割を果たします。それには、組織内のすべての API を体系的に識別してカタログ化しなければなりません。API の一元的なリポジトリーを維持することで、開発者は新しい開発作業に着手する前に既存の API を簡単に検索、探索することができます。これにより、重複を排除し、再利用を促進し、時間と労力を節減できます。

Akamai は自動化された機械学習ベースの検知を利用して、API の脆弱性（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 セキュリティ攻撃など）を特定します。この Fortune 500 の小売企業は、API のセキュリティと完全性を大幅に向上させ、機微な情報を保護し、ユーザーやパートナーの信頼を維持することができます。



 | 公開日：2024 年 8 月