

Fortune 100 の小売企業、 API Security でデジタル ビジネスを保護

主要な規制に準拠し、潜在的な DDoS 攻撃やデータ漏えいを阻止



アプリケーション・プログラミング・インターフェース（API）の力により、小売企業ではデジタル・プロセスが採用され、大きな変革が起きています。API は、小売企業の運営、顧客とのやり取り、ビジネスの管理方法に革命をもたらしています。

小売企業は、API で自社のシステムをさまざまなサードパーティ製アプリケーションやサービスと統合し、さまざまなプラットフォーム間でシームレスなやり取りを実現しています。たとえば、API を使用することで、小売企業は e コマースプラットフォームを支払ゲートウェイ、配送業者、在庫管理システムと統合できます。しかし、このエコシステムが拡張されると、セキュリティ上の脆弱性が大幅に生じる可能性があります。

API セキュリティは、今日のデジタル環境における最重要事項と言えます。システムの接続、データの共有、統合の有効化に API を使用する企業がますます増えていくにつれ、こうしたインターフェースのセキュリティが重要になっていきます。そのため、この Fortune 100 の小売企業は API アタックサーフェスのセキュリティを確保するために Noname Security（現在は Akamai 傘下）に着目しました。

API アタックサーフェスの探索

API 探索は、API スプロール（組織内で API が無秩序に拡散すること）を制御する上で重要な役割を果たします。企業が API を採用してデジタルトランスフォーメーションを実現し、イノベーションを推進するにつれ、これらの API を効果的に探索して管理できる体系的なアプローチが不可欠になります。さらに、急速に拡大するデジタル小売エコシステムにおいて、API を確実に保護するための重要な第一歩となります。



**Designer
Merchandise
Retailer**

所在地

米国

業種

小売

ソリューション

Akamai API Security

主な効果

- データの露出を防止
- API アタックサーフェスを探索
- リスクやコストの削減



この小売業界のリーダーは、API インベントリとトラフィックの可視性が欠如している問題を抱えていました。異なるプラットフォーム（オンプレミスとクラウド）のガバナンスがなく、スケーラブルな API SDLC 保護を開発できなかったのです。同社は当社のチームと連携しながら、継続的な API アセット探索を用いて不適切な構成、脆弱性、ノンコンプライアンスを特定し、既存の SecOps ワークフロー（Splunk など）と統合してリスクやコストを削減しました。

機微な情報の露出の阻止

小売業界には、組織が遵守しなければならないコンプライアンス規制がいくつかあります。これらの規制は、消費者の権利を保護し、公正なビジネス慣行を確保し、データプライバシーやセキュリティを維持することを目的としています。エンタープライズは、機微な情報を処理する API の確認およびセキュリティ確保を行って重要な規制や業界標準に準拠して、法的な影響や評判の低下を回避できなくてはなりません。

Akamai のチームは、機微な情報が露出しないよう Fortune 100 の小売企業をサポートしました。この小売企業では Jira の旧バージョンを使用していたことにより、バグによって従業員名、Jira ユーザー名、メールアドレスが露出したことがありました。また、公開されている API がセキュリティ体制上のリスクとなっていました。

Akamai API Security ソリューションで、企業の API セキュリティ体制のギャップに対処し、環境内の不適切な設定を修正することができました。たとえば、アーキテクチャが適切に構成されていないことで、**DDoS 攻撃**や**データ漏えい**によるリスクが増大する可能性があります。

今後について

お客様は、毎週 Akamai チームと積極的に連携して組織的な採用を促進していきます。また、既存のワークフローとの統合をさらに検討することも期待されています。Akamai API Security は、潜在的な脆弱性をインテリジェントに特定して優先順位付けします。このソリューションを **WAF**、API ゲートウェイ、SIEM、ITSM、ワークフローツール、またはその他のサービスに統合することで、手作業、半自動、全自動で脆弱性を修正できます。さらに、お客様の技術スタックが急速に拡大しているため、数多くの統合が検討されています。

