Akamai Customer Story

Fortune 100 Beverage Retailer Secures APIs and Data

Customer data protected by identifying key API vulnerabilities and repairing the damage from previous fraud, abuse, and theft

Application programming interfaces, or APIs, enable retailers to build end-to-end personalized experiences for customers while streamlining operations. Every variable that places a beverage in the hands of consumers — including inventory data, order submissions, location data, payments, and even rewards programs — is delivered by APIs. APIs have revolutionized the shopping experience by connecting the ecosystem of retailers, their partners, and their customers. But their constant proximity to sensitive data also makes them a risk.

Although consumers enjoy the new digital retail experience, they are often concerned about how well their personal information is protected, and rightly so. APIs are increasingly becoming a preferred attack vector by cybercriminals. For this reason, a Fortune 100 retail beverage company sought out Noname Security (now an Akamai company) to address vulnerabilities in its API security posture.

Challenges of a growing API footprint

In our initial conversations, the company expressed concerns about its inability to achieve meaningful API governance and security at a global scale. To gather evidence, it commissioned a publicly documented bug bounty that identified a huge vulnerability; the names, addresses, emails, and phone numbers of nearly 100 million users could have been exfiltrated. Luckily, this was a bounty program, and the issues were remediated without harm.

Retail Beverage Company

Location

United States

Industry

Retail, Travel & Hospitality

Solution

Akamai API Security

Key Impacts

- Billion+ API calls a day protected
- 5,000 requests per second secured
- 200+ issues identified and resolved

Akamai

The company also had inadequate production API visibility and monitoring, which resulted in an inability to adequately assess risk, and its Apigee data did not provide contextual details (e.g., data types, user behavior, baselines, vulnerability forensics). Because of these API vulnerabilities, fraud, abuse, and theft ensued. This consequently led to high operational costs for the retailer.

Strengthening its API security posture

The Noname API Security Platform (now part of Akamai API Security) was able to inventory the customer's APIs and provide behavioral analysis, real-time attack detection, and vulnerability management, including API-specific AppDev testing. As a result, the customer was able to detect and remediate API attacks that were missed by existing controls. The application security, or AppSec, team was able to increase efficiency and improve prioritization of high-risk issues.

Akamai also supports up to 50,000 APIs per engine with no operational latency. With our platform as the core, the customer has developed a global API security program. It now enjoys full visibility into its API inventory with contextually relevant API details. In addition, the company gained actionable intelligence that was not available with existing tools. This has enabled cost-effective capabilities for efficient API vulnerability management and real-time threat detection.