

Fortune 100 Retailer Protects Digital Business with API Security

Complying with key regulations and closing the door on potential DDoS attacks and data leakage



Retail is undergoing a significant transformation with the adoption of digital processes driven by the power of application programming interfaces (APIs). APIs are revolutionizing how retailers operate, interact with customers, and manage their businesses.

Retailers are integrating their systems with various third-party applications and services through APIs, enabling seamless interactions across different platforms. For example, APIs allow retailers to integrate their ecommerce platforms with payment gateways, shipping providers, and inventory management systems. However, as this ecosystem scales, it creates an abundance of potential security vulnerabilities.

API security is paramount in today's digital landscape. As organizations increasingly rely on APIs to connect systems, share data, and enable integrations, ensuring the security of these interfaces becomes critical. For that reason, this Fortune 100 retailer turned to Noname Security (now an Akamai company) to secure its API attack surface.

Discovering the API attack surface

[API discovery](#) plays a crucial role in controlling API sprawl, which refers to the uncontrolled proliferation of APIs within an organization. As businesses increasingly adopt APIs to enable digital transformation and drive innovation, having a systematic approach to effectively discovering and managing these APIs becomes essential. In addition, in the rapidly growing digital retail ecosystem, it is a vital first step to ensuring your APIs are protected.



**Designer
Merchandise
Retailer**

Location

United States

Industry

Retail

Solution

[Akamai API Security](#)

Key Impacts

- Prevented data exposure
- Discovered API attack surface
- Reduced risk and cost



This retail leader was facing a lack of visibility for API inventory and traffic. Without governance over disparate platforms (on-prem and cloud), it was not able to develop scalable API SDLC protection. The company engaged with our team to provide continuous API asset discovery to reduce risk and cost by identifying misconfigurations, vulnerabilities, and noncompliance, and to integrate with its existing SecOps workflow (e.g., Splunk).

Preventing sensitive data exposure

In the retail industry, there are several compliance regulations that organizations must adhere to. These regulations aim to protect consumer rights, ensure fair business practices, and maintain data privacy and security. Enterprises must be able to see and secure APIs handling sensitive data to comply with key regulations and industry standards — and avoid legal consequences and reputational damage.

The Akamai team helped the Fortune 100 retailer prevent sensitive data from being exposed publicly. The retailer had been using an old version of Jira, which resulted in a bug publicly exposing employee names, Jira usernames, and email addresses. Public-facing APIs also presented posture risk for them.

The Akamai API Security solution was able to address gaps in the company's API security posture and remediate misconfigurations in its environment. For example, the poor architecture configuration opened the door for expanded risk via [DDoS attacks](#) and [data leakage](#).

Going forward

The customer actively engages with the Akamai team weekly to drive organizational adoption. It is also looking forward to exploring further integrations with its existing workflows. Akamai API Security intelligently identifies and prioritizes potential vulnerabilities, which can be remediated manually, semiautomatically, or fully automatically through integrations into [WAFs](#), API gateways, SIEMs, ITSMs, workflow tools, or other services. In addition, given the customer's rapidly expanding technology stack, there are a number of integrations it is reviewing.

