

Fortune 500 Fashion Leader Secured APIs and Retail Operations

APIs fueling convenient, personalized retail experiences were secured, while customers' data was safeguarded from breaches



Discovered all APIs



Identified vulnerabilities



Bolstered security posture

APIs have played an integral role in the retail industry's shift from traditional brick-and-mortar stores to ecommerce platforms. Behind every digital interaction, there's an API behind the scenes, enabling retailers to:

- Connect various systems, applications, and services seamlessly
- Integrate their online storefronts with back-end inventory management systems, payment gateways, shipping providers, and customer relationship management tools
- Facilitate a rapid exchange of data that makes online retail personalized and convenient

With protection of that data as a top priority, API security plays a critical role in ensuring the trust, integrity, and confidentiality of online business operations.

APIs' constant proximity to sensitive data makes them attractive targets for [cybercriminals](#) seeking to exploit vulnerabilities. A successful API breach can lead to the exposure of customer information, such as personal details, payment card data, and purchase history. For these reasons, this Fortune 500 fashion retailer turned to Noname Security (now an Akamai company) for help, as the company had been previously unsatisfied with its relationship with Salt Security.



Location

United States

Industry

Retail

Solution

[Akamai API Security](#)



Creating a programmatic approach to API Security

The Fortune 500 retailer was looking to create a complete end-to-end workflow in mitigating API security risks beyond [web application firewalls](#) and [API gateways](#). This would require a solid API security strategy with robust controls for API governance. The company also had a focus on bot mitigation – ultimately distinguishing between legitimate users and malicious bots, allowing it to protect its systems, data, and user experience.

Given the size of the project, the retailer and Akamai agreed on a phased approach. Phase one would entail locating all of its APIs, classifying sensitive data, implementing detection and response, as well as integrating with Splunk. Phase two would entail pivoting to a shift-left API security testing approach to expedite the creation of secure code.

Accelerated deployment decreased time to value

Despite phase one being a tall order, the Akamai team was able to deploy Noname's API discovery and runtime protection modules, while executing the Splunk integration, in just 120 days. API discovery plays a crucial role in managing API sprawl. It involves the systematic identification and cataloging of all APIs within an organization. By maintaining a centralized repository of APIs, developers can easily search and discover existing APIs before embarking on new development efforts. This helps eliminate duplication and promotes reuse, saving time and effort.

Akamai uses automated machine learning-based detection to identify API vulnerabilities, including data leakage, data tampering, data policy violations, suspicious behavior, and API security attacks. The Fortune 500 retailer can significantly improve the security and integrity of its APIs, protect sensitive data, and maintain the trust of users and partners.

