noname

Fortune 100 Designer Merchandise Retailer

Retail is undergoing a significant transformation through the adoption of digital processes, driven by the power of application programming interfaces. APIs are truly revolutionizing the way 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 e-commerce 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 of paramount importance 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 to secure their API attack surface.

Discovering their 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, it becomes essential to have a systematic approach to discover and manage these APIs effectively. And in this rapidly growing digital retail ecosystem, it is a vital first step in order to ensure your APIs are protected.

This retail leader was facing a lack of visibility for API inventory and traffic. Without governance over disparate platforms (on-prem & cloud) they were not able to develop scalable API SDLC protection. They engaged with Noname to provide auto API asset discovery to reduce risk and cost by identifying misconfigurations, vulnerabilities and non-compliance. As well as to integrate with their existing SecOps workflow (e.g., Splunk).

Preventing sensitive data exposure

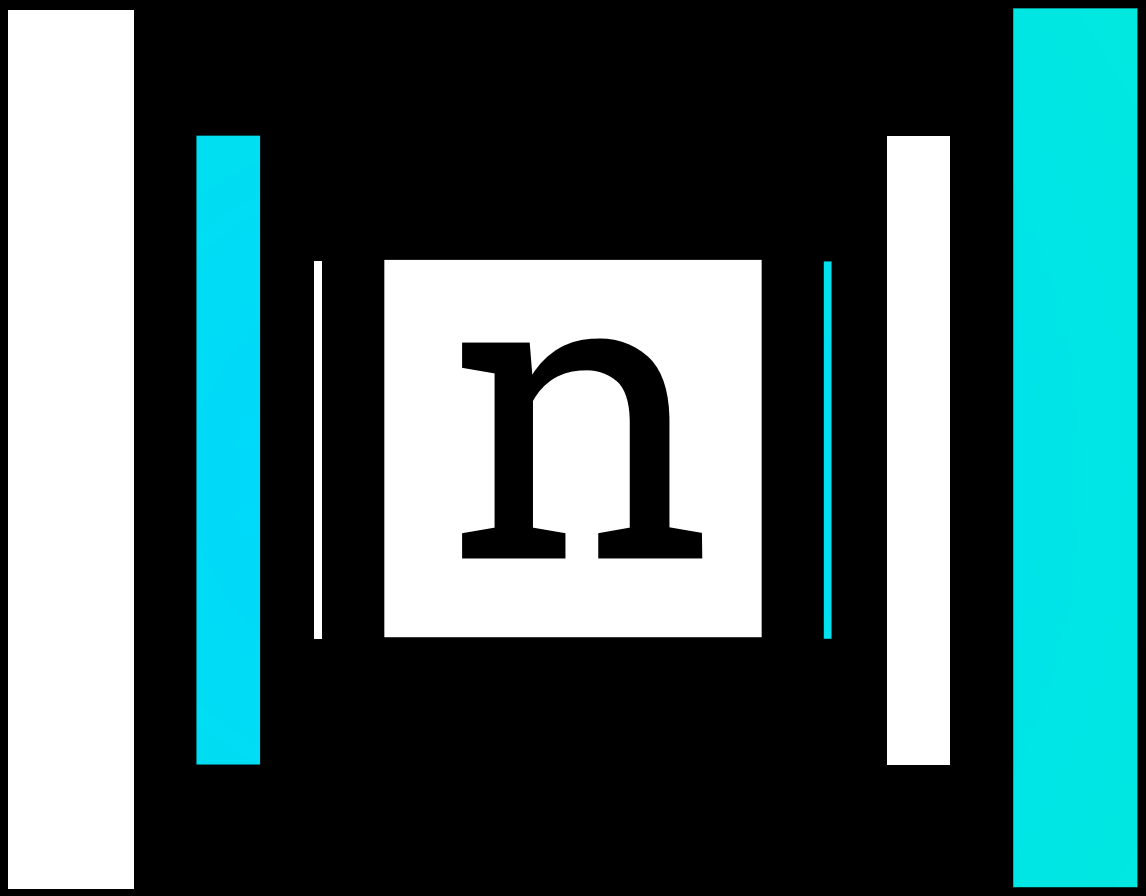
In the retail industry, there are several compliance regulations that organizations must adhere to. These regulations aim to protect consumer rights, ensure fair business practices, and maintain data privacy and security. APIs handling sensitive data must comply with these regulations to avoid legal consequences and reputational damage. Implementing proper API security measures ensures compliance with relevant industry standards and regulations.

Noname helped the Fortune 100 retailer to prevent sensitive data from being exposed publicly. They were using an old version of JIRA where a bug publicly exposed employee names, Jira usernames, as well as email addresses. Public facing APIs also presented posture risk for them.

The Noname API Security Platform was able to address gaps in their API security posture and remediate misconfigurations in their environment. For example, the poor architecture configuration opened the door for expanded risk via DDOS attacks and data leakage.

Going forward

The customer is actively engaged with the Noname team weekly to drive organizational adoption. They are also looking forward to exploring further integrations with their existing workflows. Noname intelligently identifies and prioritizes potential vulnerabilities, which can be remediated manually, semi-automatically, or fully automatically through integrations into WAFs, API gateways, SIEMs, ITSMs, workflow tools, or other services. And given the customers' rapidly expanding technology stack, there are a number of integrations they are reviewing.



About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371