noname

Fortune 100 Retail Beverage Company

Billion+	5K	200+
API calls a day	Requests per second	Issues identified & resolved

Application Programming Interfaces, or APIs, have enabled the retail industry to build end-to-end personalized experiences for their customers while streamlining business operations. Everything from inventory data, to order submissions, to location data, to payments, are all delivered via APIs. Even the rewards programs that drive customer engagement. The technology has truly revolutionized the shopping experience by connecting the ecosystem of retailers, their partners, and their customers.

Though consumers enjoy this new digital retail experience, they are very much concerned with how well their personal information is protected. And rightly so. APIs are increasingly becoming a preferred attack vector by cybercriminals. For this very reason, a Fortune 100 retail coffee company sought out Noname Security to address vulnerabilities in its API security posture.

Challenges of a Growing API footprint

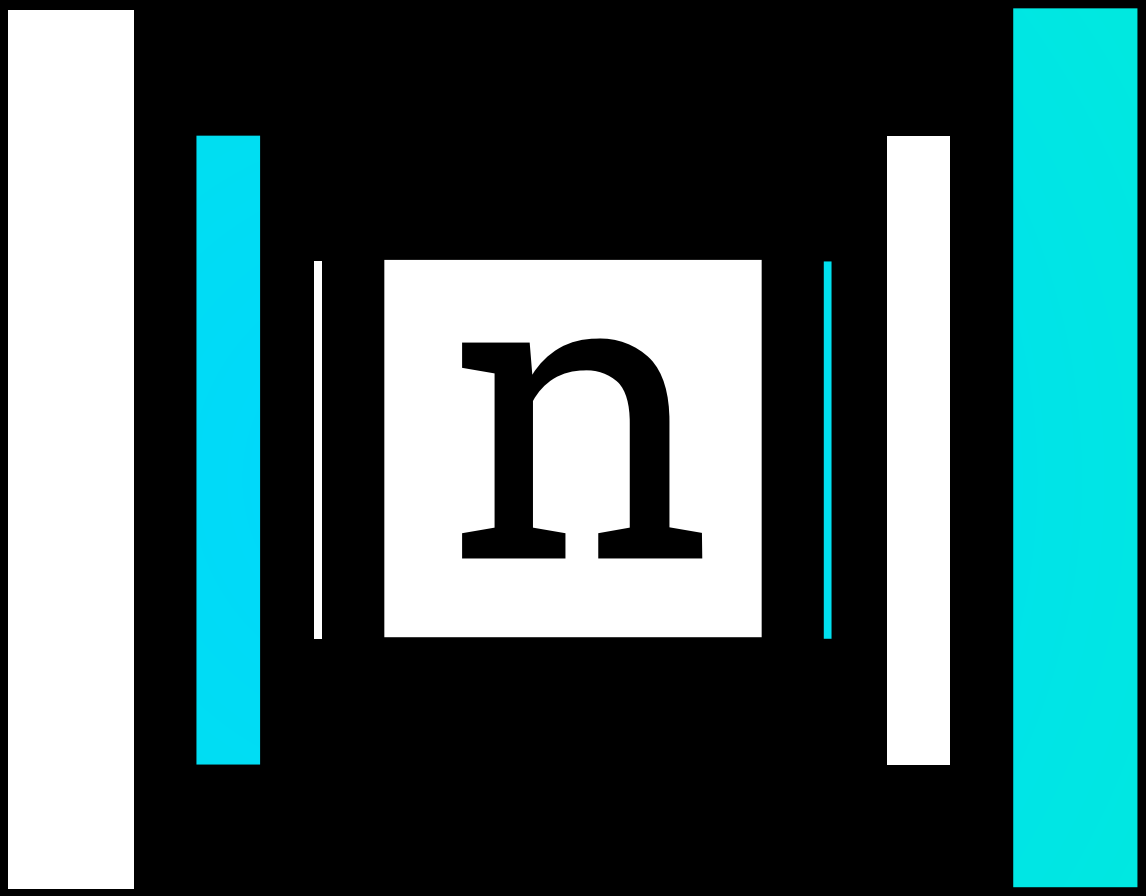
In our initial conversations, the company expressed concerns with their inability to achieve meaningful API governance and security at a global scale. As evidence, they commissioned a publicly documented bug bounty that identified a huge vulnerability. The names, addresses, emails, and phone numbers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

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

Strengthening Their API Security Posture

The Noname API Security Platform was able to inventory the customers 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.

Noname also supports up to 50k APIs per engine with no operational latency. With our platform as the core, the customer has developed a global API Security program. They now enjoy full visibility into their API inventory with contextually relevant API details. Not to mention actionable intelligence that was not available with existing tools. This enabled cost-effective capabilities for efficient API vulnerability management and real-time threat detection.



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