noname

Rapyd

Rapyd is the fastest way to power local payments anywhere in the world, enabling companies across the globe to access markets quicker than ever before. By utilizing Rapyd's unparalleled payments network and fintech as a service platform, businesses and consumers can engage in local and cross-border transactions in any market.

The Rapyd platform is unifying fragmented payment systems worldwide by bringing together 900-plus payment methods in over 100 countries. Rapyd's investors include Stripe, General Catalyst, Oak HC/FT, Coatue, Tiger Global, Durable Capital, Target Global, Fidelity Management and Research Company, Altimeter Capital, BlackRock Funds and Tal Capital. To learn more about the company that is accelerating the fintech as a service revolution, visit www.rapyd.net, read our blog, or follow us on LinkedIn and Twitter.

Problems

1

Rapyd's main product is its public payments API, which handles billions of dollars of transactions 24/7. Even minor instances of disruptions, fraud, or abuse could mean millions of dollars in lost revenue, significant remediation costs, and a loss of customer trust for both Rapyd and its customers.

2

Although Rapyd runs an active bug bounty program, significantly customized its web application firewall (WAF), and considered API security mission-critical, its APIs were a "black box" to its security team. They lacked granular visibility into API usage and behavior, business logic was unknown, and it was difficult to identify (let alone stop) attacks in real-time.

3

Consequently, Rapyd's security team needed a better way to secure both its public API and its hundreds of internal APIs in a highly complex system operating in Amazon Web Services (AWS) at a global scale. This meant a purpose-built API security solution that didn't have the blind spots of their existing infrastructure, including WAFs and API gateways. They specifically needed a granular inventory of all their APIs, visibility into mistakes or misconfigurations creating vulnerabilities in their security posture, intelligently prioritized alerts so security analysts could focus on the most important risks, and the automation and integrations necessary to stop attacks.

Solutions

1

Rapyd's CISO evaluated a number of established purpose-built API security solutions, including from vendors with numerous patents and long track records. However, most fell short of providing complete API security because they lacked important capabilities, such as full packet capture for deep analysis of attacker behavior, visibility beyond traffic and anomalies into their global API security posture, and the backing of world-class security researchers.

2

Unlike other vendors and the "API security" features of their current infrastructure, only Noname Security provided the combination of comprehensive visibility from code to production, discoverability, automation, integrations, and intelligent behavior-based anomaly detection that Rapyd needed.

3

From their first meeting, Noname Security demonstrated an intense customer focus, level of expertise, and industry leadership that surpassed other vendors.

4

After evaluating each vendor's holistic combination of product and team capabilities, Noname Security emerged as the clear leader. The CISO's team quickly deployed the Noname API Security Platform – with posture management, runtime protection, and active testing in one unified solution – across all of their AWS regions globally.

Results

With the Noname API Security Platform, Rapyd can protect its APIs and critical assets from cyber attacks with:

- ✓ Easy, effective, and accurate API behavioral prevention, detection, and response
- ✓ Effective resource utilization to proactively de-risk the environment
- ✓ Evidence of security control and demonstration of compliance
- ✓ Secure handling of sensitive data and third-party risk exposure

Rapyd can now confidently grow its global business both quickly and securely, as real data from blocked attacks and production vulnerabilities inform their development efforts and new code can be easily tested before going live. Rapyd will also have full architectural freedom to deploy Noname as fully cloud-based, fully on-premises, or any hybrid combination as needed as they continue to expand into new markets and regulatory environments.

> “Noname Security is the lighthouse for my AppSec team: now we know what to focus on. It’s a major data security tool for us. The deployment was very easy and they were true partners in the process. Now we can assess our risk in the most scientifically true way possible and control our destiny.”

Nir Rothenberg
CISO, Rapyd

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