Noname Security case study

Securing APIs to enable the burgeoning digital economy with Noname API Security and Microsoft Azure

API proliferation means a steep increase in security incidents

Typical organizations deploy thousands of APIs, challenging risk management. The recent Log4Shell vulnerability in the Apache Log4j API is just one example of a far-reaching API security issue.

Discovering and securing APIs in the Microsoft Azure cloud

Noname Security lets organizations effectively manage the API lifecycle, improving development velocity and reducing operational risk.

Protecting APIs and critical assets while delivering secure apps

The Noname API Security platform enables organizations to rapidly deliver secure apps and APIs without having to become security experts.

Microsoft

A real-time view of API traffic with Noname Security and Microsoft Azure services

Founded in 2020 and based in Palo Alto, California, Noname Security helps organizations protect their APIs and critical assets from attack while more quickly delivering secure apps and application programming interfaces (APIs). The company's platform, available in the Microsoft Azure Marketplace, secures APIs in production as well as in development. Its integrations with Azure Load Balancer, Azure API Management, Azure App Service, Azure Storage, and Azure Virtual Machines enable a real-time view of all API traffic.

Noname Security has been working with Microsoft for Startups since November 2021, and Microsoft has provided significant expertise and support for integrations with Azure services. Noname Security's reputation has flourished with support in the Azure Marketplace as well as within the Microsoft Partner Center. Noname Security has built a strong reputation in the security space, currently working with 20 percent of Fortune 500 companies.

'A seamless experience for customers'

The emerging digital economy has fueled explosive growth and dependence on APIs. But as companies grow and innovate, API security can be an afterthought. In 2021, multiple API-based security breaches exposed the private data of millions of users worldwide. High-profile vulnerabilities like Log4Shell pushed security to the forefront, and many organizations with aggressive digital programs had to switch gears while they retrofitted their application infrastructure. Remediation of APIs in production is time-consuming and can potentially create new risks and impact the customer experience.

"As we've seen in recent security breaches, there is a major need to focus on API security across industries," said Oz Golan, CEO of Noname Security. "Working with Microsoft Azure creates a seamless experience for customers as they look to test and secure their APIs."

Noname Security's artificial intelligence and machine learning-based analysis builds a complete picture of API security and configuration issues and provides instructions to remediate each issue. Noname Security allows developers to test APIs before deployment to ensure those released into production are completely tested and pose no risk. For applications in production, Noname Security continually monitors all Azure traffic to discover APIs and analyze them. Misconfigurations and security issues are surfaced and prioritized for remediation, while the management console enables faster compliance adherence and reporting with a catalog view of all APIs.

"Noname's integration with Microsoft Azure Cloud—the premier cloud platform—is an important step as we work to provide API security to our customers, many already using Azure. Our integrations enable us to build a complete view of all APIs in development or in production to deliver true end-to-end visibility and control for APIs."

- Oz Golan, CEO, Noname Security