noname | WIZ

Wiz Cloud Security Integration

Gain complete visibility, context, and control of all your highly sensitive, mission-critical APIs across your entire cloud estate

Securing Cloud APIs and Their Underlying Infrastructure

APIs drive business value. Their usage has skyrocketed over the years as organizations have adopted microservices architectures, cloud services, and CI/CD practices. Today, many businesses are awash in APIs over which central IT and security teams have little visibility and control. Many of these APIs provide direct access to mission-critical systems and confidential data.

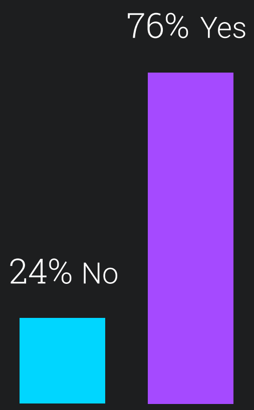
APIs are a favorite target for threat actors, as hackers routinely exploit poorly secured APIs to orchestrate attacks and exfiltrate data. According to Gartner, APIs are the number one attack vector for web applications. And in a recent Noname survey, 76% of respondents said they experienced an API security incident in the past 12 months. To make matters worse, 74% said they did not have a complete API inventory or know which APIs return sensitive data.

Have you experienced an API security incident within the past 12 months?

The API Security Disconnect

Research from Noname Security on API Security Trends in 2022

Read full report →



How Noname Security Addresses API Threats

Noname and Wiz have partnered to help businesses eliminate API security vulnerabilities and blind spots, and mitigate risk. Wiz is a cloud-agnostic, agentless security platform that scans your entire cloud infrastructure, providing full visibility into anything that runs in it. Noname uses Wiz's in-depth inventory data to provide contextual insights into your APIs. The tightly integrated solution helps you boost your security posture, accelerate discoveries and remediations, and improve compliance with data privacy mandates and cybersecurity regulations.

Together, Noname and Wiz provide unprecedented visibility and control over all your cloud APIs and the infrastructure supporting them. Our joint solution helps you identify potential exposure, prioritize risk, and focus on the issues that matter most. Specifically, Noname displays counts of posture issues and their severities identified by Wiz next to the appropriate infrastructure resources. From there, security teams can view issues directly in Wiz, and immediately prioritize and resolve issues.

Wiz's Cloud Native Application Protection Platform connects in minutes, examining all your cloud infrastructure (PaaS resources, virtual machines, containers, serverless functions, etc.) to generate a complete inventory of your entire cloud estate. Ideal for hybrid cloud and multi-cloud environments, the Wiz platform supports all popular public and private cloud platforms including AWS, Azure, GCP, Oracle Cloud Infrastructure, Alibaba Cloud, VMware vSphere, Kubernetes, and Red Hat OpenShift.

Our Noname-Wiz integration makes it easy to understand your APIs' security posture in context. Noname provides a comprehensive view of all your APIs across all your on-premises and cloud-based resources, enriched with Wiz insights that help you efficiently identify critical issues with the supporting infrastructure. Contextual visualizations let you easily identify API dependencies and examine API call flows, so you can quickly find toxic combinations, uncover potential security weaknesses, and take corrective actions.

WIZ

Certified Wiz Integration

Increase Insights and Accelerate Risk Reduction with Noname and Wiz

Proactively improve your security posture

Gain full visibility into all APIs across all infrastructure

Identify vulnerabilities and increase situational awareness

Make data-driven decisions

Find and fix breaches faster

Gather contextual insights to assess risks and prioritize mitigations

Analyze adversarial behavior, identify attack paths, and automate remediations

Address security issues before threat actors exploit them

Ensure compliance

Identify, monitor, and control sensitive APIs

Comply with data privacy mandates and cybersecurity regulations

Enforce mandatory security controls and streamline audits

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