Noname Advanced Security for IBM

Increase API security across your enterprise with advanced AI-powered capabilities.
IBM is partnering with Noname Security to deliver advanced API protection

APIs play a critical role in driving digital business and transformation by facilitating the integration of software applications and systems, allowing for seamless exchange of data. This has led to an explosion in the usage of APIs, with a recent survey showing the average organization has 15,564 APIs in use, and a growth rate of 201% over the past 12 months1.

However, with the growing prevalence of APIs comes increased opportunities for security-related issues, especially when APIs are not properly managed or secured. This includes attacks by malicious actors to exploit API vulnerabilities. In fact, APIs are the number one attack vector for web applications2. While API gateways and web app firewalls provide a level of security, many industries and companies are starting to require additional security capabilities tailored to their APIs to outsmart the threat actors of tomorrow.

IBM, a leader in API management and application gateways, is partnering with Noname Security, a leader in API security, to deliver advanced API security capabilities. This joint solution will help you reach new levels of security confidence.

- **Find API security issues faster**
  - Intelligently identify and prioritize potential vulnerabilities. Remediate manually, semi-automatically, or fully automatically.

- **Discover the unmanaged**
  - Catch vulnerabilities and issues earlier, and prioritize based on impact, to reduce remediation costs.
Ensure compliance
Continuously monitor for compliance with regulatory requirements, industry standards, and internal policies.

Outsmart attackers
Conduct real-time traffic analysis with automated AI and machine learning detection, and use automated remediation to stop attacks in real-time.
Advanced API security for your entire API landscape with Noname Security and IBM

- **Discover all APIs in your estate**
  Use data classification and context-aware analysis to create an accurate and complete inventory of APIs to ensure all APIs are managed and secured.

- **Analyze and assess APIs**
  Identify misconfigurations and vulnerabilities and align to API security best practices using suggested remediation steps.

- **Detect abnormal API traffic in real-time**
  Monitor for data tampering and leakage, policy violations, suspicious behavior, and API attacks. Prevent attacks and misuse in real-time with partial or fully automated remediation.

- **Available as on-prem software or SaaS**
  Deploy on-premises or any cloud for maximum flexibility and choice.
Get started with Noname Advanced API Security for IBM

Talk to one of our API security experts to learn more about advanced API security and the value it could provide to your business.

Learn more

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 — Discovery, Posture Management, Runtime Protection, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in Tel Aviv and London.