noname

SOLUTION BRIEF

Shift Left with API Security Testing

Leading organizations implement a “shift left” approach to API security testing to prevent attacks and reduce vulnerabilities with every release.

Test and secure your APIs from the start.

Shift left testing saves time by identifying issues earlier in the API lifecycle. More rigorous detection of errors and bottlenecks in advance enable testers to improve initial designs and develop alternatives. Ultimately, apps, microservices, and APIs are better protected because the organization can proactively shrink the attack surface. Shifting left for API security helps organizations to:

Deliver Secure Apps & APIs Faster

Automated API security testing enables teams to create and ship secure code without having to become security experts. By eliminating vulnerabilities early, organizations can focus on delivering the best products and services to their customers.

Reduce Risk

By proactively identifying and fixing vulnerabilities, organizations also reduce the potential number of threats and inadvertently exposed assets, reducing overall risk.

Lower Costs

Regular and frequent testing for API security early significantly reduces remediation costs, often by 10-100x. Automated testing also reduces the need for costly third-party pentesting efforts.

Increase Revenue

Automated testing allows developers to move quickly to meet customers' needs by ensuring that new releases are secure and unlikely to require refactoring or costly remediation in the future.

Stop Vulnerabilities Before Production

Prevent future attacks by shrinking the API attack surface.

- **Reduce the risk of successful attacks** in production, such as data leaks, manipulations, and more without any modifications to production infrastructure.
- **Remediate faster** and lower remediation costs by 10x to 100x by finding and fixing issues earlier.
- **Improve compliance** and avoid regulatory fines and reputational damage from incidents.

Innovate Faster

Improve security without sacrificing velocity.

- **Eliminate bottlenecks** while improving security without any extra manual steps.
- **Increase confidence** in the organization's APIs with continuous testing.
- **Reduce redundant pentesting** and other third-party security testing costs.
- **Deliver secure code** without having to become a security expert.

The Noname API Security Platform

Shift Left with API Security Testing

API Posture Management

Runtime API Protection

noname

SOLUTION BRIEF

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 three pillars — Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, and offices in Tel Aviv and Amsterdam.

🌐 nonamesecurity.com
✉ info@nonamesecurity.com
☎ +1 (415) 993-7371

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2022
GOLD
API Security
category
North America

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2022
GOLD
Fastest Growing Cybersecurity Company
North America

TOP 10
BLACK UNICORNS
2021
CYBER DEFENSE MAGAZINE

TOP 10
CYBERSECURITY EXPERTS
2021
CYBER DEFENSE MAGAZINE