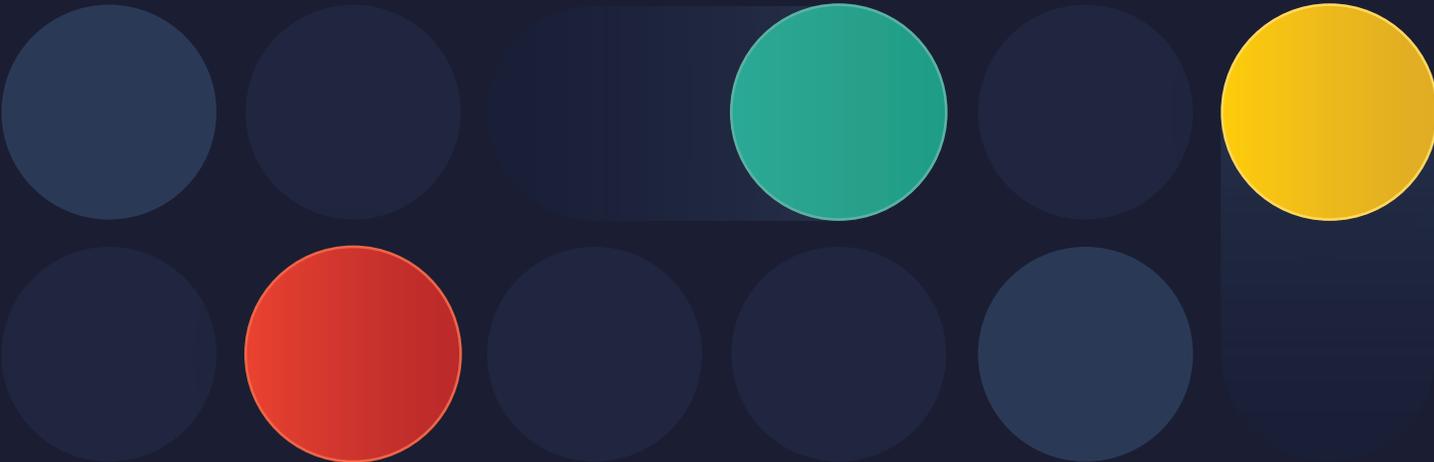# Active Testing

As part of the Noname API Security Platform, Active Testing allows organizations to Shift Left with API security testing to stop vulnerabilities before they reach production and innovate faster without compromising security.

Shift Left with API Security Testing

Prevent attacks and reduce vulnerabilities with every release.

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 Security Leads In API Security Testing

Proactively secure APIs by eliminating vulnerabilities before code reaches production and as your environment evolves with the industry's most comprehensive API security platform.

Powerful & Comprehensive

- **Total Coverage:** Automatically run 100+ dynamic tests that simulate malicious traffic, including against the OWASP API Top 10

- **Automatic Testing:** Scheduling tests to run automatically at desired intervals.

- **Intelligent Analysis:** Use real business logic to run tests and simulations, not fuzzing.

- **Spec Comparisons:** Compare Swagger files to assess conformance, based on real implementation results.

- **Flexible Deployment Options:** Test in development and staging environments.

- **Data Sources:** Import APIs from a wide range of sources with dynamic updates.

- **Purpose-Built:** Created to specifically address the challenges of API security.

- **Rapid Value:** Fast time-to-value (TTV) and faster implementation than runtime protection in production

Customizable

- **Test Suites:** Easily create test suites to align with business objectives, team structures, and more.

- **Customization:** Adjust test behavior and test severity to the needs of the organization,

- **Access Controls:** Streamline testing with role-based access controls, so only the right teams can access APIs for testing.

- **Grouping:** Group APIs automatically or manually based on application, business unit, functional capabilities, or any other characteristic.

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