noname

Product Brief

The Noname API Security Platform

The Noname API Security Platform is the only solution to proactively secure your environment from API security vulnerabilities, misconfigurations, design flaws, and provides API attack protection with automated detection and response.

Accelerate Innovation and Protect Your APIs

APIs are a centerpiece of digital life. APIs are an efficient and developer-friendly means to unlock value, enabling interoperability of software and data assets with flexibility, speed, and portability. Many digital transformation initiatives are accelerating API adoption, including:

- Public cloud services
- Microservices application design
- Open banking
- Mobile healthcare
- New business and developer ecosystems
- Back office digitization

As enterprises build their business upon APIs, they have experienced a significant increase in API security incidents. According to Gartner, APIs will be the top attack vector for web applications in 2022, and according to IBM, two thirds of cloud breaches are tied to API misconfigurations.

Noname Security protects APIs in real-time and detects vulnerabilities and misconfigurations before they are exploited. The Noname API Security Platform is a modern, flexible solution that integrates with your API gateways, load balancers, WAFs, and much more to offer deeper visibility and comprehensive API security.

The Noname API Security Platform

API Posture Management

Inventory every API, including legacy and shadow APIs, with **data classification.**

Identify **misconfigurations** and **vulnerabilities** in source code, network configuration, and policy.

Runtime API Protection

Behavioral-based models for **runtime API threat detection.**

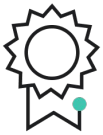
Automated and semi-automated **attack blocking** and **vulnerability remediation**.

"Shift Left" and API Security Testing

Continuously test APIs to identify API risks before they emerge.

Automated and dynamic test development and incorporation into CI/CD pipelines.

Key Capabilities & Features



One Complete, Unified Solution for API Security Management

The Noname API Security Platform is a complete, unified API security solution that provides API security posture management, runtime security, and secure API development.

Unlike other products that only cover a part of the API lifecycle and provide only partial coverage, Noname empowers customers to protect their all of their APIs and critical assets from cyber attacks, establish an effective API security program, and align their security and development teams to support the organization's growth goals. Because Noname brings together all of the critical capabilities in API security in one platform, Noname provides broader, deeper, and smarter security than siloed systems and point solutions.

Furthermore, the Noname API Security Platform easily integrates with existing infrastructure and programs, improving the return on those investments.

Discover & Understand All Your APIs

Through integrations with cloud platforms and other devices in the customer's environment, the Noname API Security Platform provides visibility into API traffic transmitted to and from the customer network as well as within it. The Noname engine analyzes the traffic and discovers and maps all the customer's APIs.

Real-time traffic analysis identifies new APIs and changes in existing APIs, and the data is recorded and updated in the customer's dashboard.

Because the Platform does not rely on agents or sidecars, and because it integrates with the cloud infrastructure, it sees every API regardless of whether the API is registered with an API gateway.

Internal and external APIs, legacy APIs (those that predate the API gateway), and shadow or rogue APIs (those not routed through a gateway) are all discovered, providing the customer with unprecedented visibility into the API attack surface.

Manage API Security Posture

The Noname API Security Platform provides a comprehensive view of traffic, code, and configurations to assess the organization's API security posture.

Noname intelligently identifies and prioritizes potential vulnerabilities, which can be remediated manually, semi-automatically, or fully automatically through integrations into WAFs, API gateways, SIEMs, ITSMs, workflow tools, or other services. Examples of vulnerability detection include: detecting sensitive data types and any data leaks to meet compliance requirements, detecting if API authentication is enabled and authentication types, detecting if an API is accessible to the internet, and more.

Enable Application Teams to Validate API Security Before Production

Noname is also an active testing platform, which means an application team can create and execute testing suites on any group of APIs. Security and development teams are able to validate the security of APIs and scan for vulnerabilities in a pre-production environment. Examples of testing suites that can be executed include: JWT vulnerabilities, authentication, authorization, common vulnerabilities, forbidden headers, etc. The Platform can be integrated with your existing CI/CD pipeline, including tools such as Jenkins.

Detect Changes and Create Actionable Reports

The Noname Platform can detect meaningful changes such as the way an API or user performs authentication and other actions that might signal an anomaly or vulnerability, as well as changes in the API itself (in both the header and the body).

Users can also create data loss prevention (DLP) policies associated with APIs and specific data types and then use those policies to protect sensitive data and to report on issues associated with the APIs.

The Platform also provides custom and configurable reports per user or per team, along with key performance indicators and the relevant information for that user or team.

Powerful Artificial Intelligence & Machine Learning (AI/ML)

The Noname Platform leverages Noname's proprietary artificial intelligence & machine learning (AI/ML) algorithms based on classic unsupervised machine learning, along with distance- and density-based anomaly detection to identify anomalous behavior and vulnerabilities.

A behavior model is created for every API and continuously updated with the API's most recent behavior.These baselines enable the behavior model to be specific and highly accurate. Users still have the ability to change the sensitivity of anomaly detection per API or per issue.

In the rare event that an anomaly is determined to be a false positive, confirmation by the user will be used to update the model (supervised learning) and reduce the chances of the same false positive recurring.

Identify Anomalous Behavior And Vulnerabilities

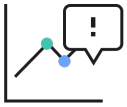
AI/ML-based behavior models enable the Noname API Security Platform to detect anomalous behavior with a high degree of accuracy, which results in less false positives and greater confidence in the anomalies reported. Noname pioneered the creation of new algorithms for detecting anomalies in API traffic, providing customers with the most comprehensive runtime protection possible.

The Noname API Security Platform also looks at the widest possible set of sources to detect vulnerabilities, including log files, replays of historical traffic, configuration files, and much more. The platform detects all vulnerabilities in the OWASP API Security Top 10, plus much more, and protects all APIs from data leakage, authorization issues, abuse, misuse, and data corruption.

Actionable Insights on Anomalies

When an anomaly is detected, the Noname Platform provides full details for all calls and responses triggering the alert.

For example, in a brute-force attack, the Platform will provide all invalid login attempts, all associated 403 errors, and the successful login request and response. Also, the event description provides all the network traffic information typically used for incident response or remediation. This includes all API packet header information, the IP addresses, the API body (where recorded), the EC2 instance involved, etc. Each packet includes the request and response including the body and headers and information about the adversary that triggered the vulnerability. This information is valuable for the ensuing investigation, incident response, and root-cause analysis.



Generate Alerts On Critical Findings

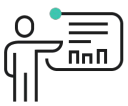
The Noname Platform generates detailed alerts for every issue discovered.

Security teams can easily access an alert's key findings to gain a deeper understanding of the alert and to understand context.

Teams are also provided with recommendations for remediating the issue. Additionally, teams of users can be created with groups of APIs assigned to them.

API groupings can be created automatically using filters such as domain or instance ID, or they can be created manually by filtering on any characteristic of an API including information found in its header, body, or environment (API gateway).

If groups of APIs are assigned to teams, issues, alerts, and findings can all be reported automatically to the responsible teams using the Platform's integrations with IT management workflows such as Jira, Trello, ServiceNow, Slack, Webhooks, etc.



Remediation Guidance For Critical Alerts

The Noname Platform provides a detailed description of each issue along with its security impact and comprehensive guidance on remediating and reproducing the problem.

Guidance is based on best practices and industry-standards, such as those recommended by OWASP, plus proprietary research from Noname Security's team of elite cybersecurity researchers.

API Security Program Enablement

Noname's team of accomplished CISOs and API security experts advise and support customers in their development of an effective API security program.

This includes providing strategy guidance, KPIs/KRIs, common policies and standards, training, and research for the broader cybersecurity community.

Customers receive:

- A blueprint (methodology and toolkit) to enable and establish an effective API security program through best practices
- API security reference architectures for clear guidance to developers and engineers
- Role-specific API development and security training
- Research into the current API threat landscape in conjunction with partners

Proven Partnerships

Noname Security's market leadership has attracted the best partners in cybersecurity, from channel partners to technology partners, making Noname easy to buy, implement, and integrate.

Official technology partnerships include:

- Amazon Web Services (AWS)
- Microsoft Azure
- MuleSoft
- Kong
- Apigee
- Akana
- Layer 7 Technologies
- *And more*

Smooth Implementations

Noname Security offers easy, efficient implementations driven by experts in API security:

- No agents or sidecars needed
- No network modifications
- Integrations with API Gateways
- Integrates with load balancers, WAFs, log aggregators
- SaaS, on-premise, and hybrid deployment options as needed

Extensive Integrations

Noname connects with mission-critical systems across the software development lifecycle, including:

- CI/CD
- WAFs
- API Gateways
- Load Balancers
- SIEM
- ITSM
- Container Orchestration
- Service Mesh
- Workflows
- *And more*

Flexible Deployments: Choose From On-Premises Or In The Cloud

The Noname Platform's components, data, and traffic can be confined to the customer's environment so the Platform can operate completely on-premises. Any external connectivity (e.g., updates, telemetry) is optional.

Integrate With SIEMs and ITSMs

The Noname Platform offers simple out-of-the-box integrations with different tools including Jira, ServiceNow, Slack, Snowflake, Splunk, Webhooks, PagerDuty, and more.

Out-of-band and Asynchronous

The Noname Platform processes (i.e., discovers, analyzes, and models) API requests and responses out-of-band and asynchronously.
As a result, no network configuration changes are required to implement the Platform and its implementation has no impact on an API's execution, performance, latency, etc. Out-of-band processing also eliminates an additional point of failure.

Integrate with API Gateways and Load Balancers

The Noname Platform offers out-of-the-box integration with multiple network components including gateways (e.g., Apigee, MuleSoft, Kong, IBM, Amazon API GW, Akana, WSO2, Azure Application GW) and load balancers (e.g., NGINX, Envoy, F5, Avi Vantage). In addition, the Platform supports direct integration with cloud infrastructure (e.g., AWS, Azure, GCP).

A Proven API Security Strategy: D.A.R.T.

Discover

Categorize API information:

- Inventory APIs, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC.
- Internet-facing or internal-only
- Authentication methods
- Data types
- Most Used/Least Used
- Automatically generate Swagger/OAS Specifications of APIs

Analyze

Automated AI-based detection:

- Data leakage
- Data tampering
- Misconfigurations
- Changes and Drift
- Data Policy Violations
- OWASP API Top 10
- Network graph for in-depth analysis

Remediate

Stop attacks and fix vulnerabilities in real-time:

- Break the TCP session of suspicious behavior
- Webhook into WAFs to create new policies against suspicious behavior
- Automatically update firewall rules to regulate suspicious behavior
- Policy on API gateway regulating information to target or client
- Optional inline prevention to block users or APIs when needed
- Integrate with existing workflows (ticketing, SIEMs, etc)
- Track mean time to assign, handle, and resolve (MTTR)

Test

Active API testing in pre-production and production environments:

- Automate testing and schedule tests at regular intervals
- 100+ static and dynamic tests
- Integrate into existing CI/CD pipelines
- Connect with Postman, Jenkins, etc.
- Deploy in any test environment, including development, staging, and production
- Enhance testing with real-world traffic and simulated attacks
- Initiate tests from new findings in posture management scans

noname

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

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 Secure API SDLC. Noname Security is privately held, remote first with headquarters in Silicon Valley, with an office in Tel Aviv and Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371