noname

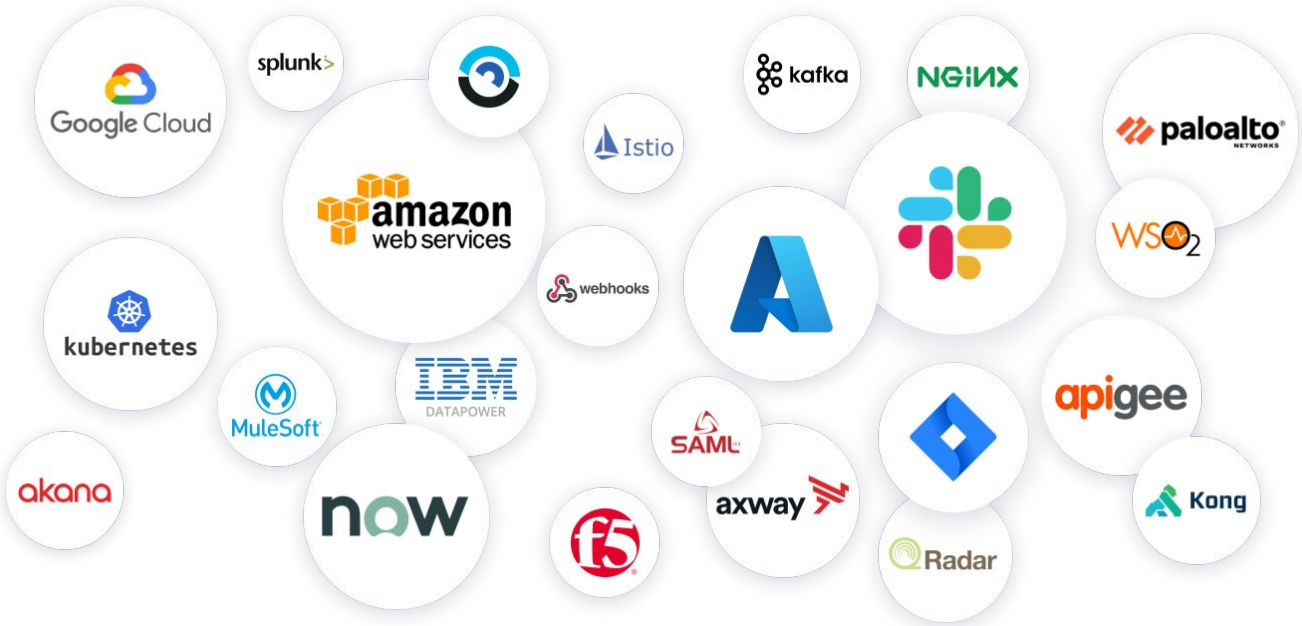
Product Brief

Seamless Integrations

The Noname API Security Platform easily integrates with mission-critical systems across the software development lifecycle, from proactive testing in pre-production and the CI/CD pipeline to real-time threat detection and remediation.

Easily Connect With Your Existing Infrastructure

The Noname API Security Platform is a non-disruptive solution that easily integrates with your existing systems and processes, allowing you to get more ROI out of your current IT investments, reduce remediation costs by catching vulnerabilities earlier, shrink your overall attack surface, and accelerate innovation with an extensive library of integrations, many of which were co-developed with our technology partners directly.



Noname's growing library of integrations includes:

- CI/CD Tools
- WAFs
- API Gateways
- App Delivery Controllers
- SIEM
- ITSM
- Container Orchestration
- Service Mesh
- Workflow Tools
- On-Premises Servers
- Multi-Cloud Environments
- *And more*

Integrate with API Gateways and Load Balancers

- The Noname API Security 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).

Discover API/Web Services Endpoints

- 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 Vulnerabilities & API Security Posture

- Through integrations, 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.
- Likewise, Noname analyzes the network structures of APIs, including which network components are connected to a particular API.

Generate Alerts On Critical Findings

- 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, etc.

Integrate With SIEMs and ITSMs

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

Detect Vulnerabilities Before Production

- Integrate the Noname API Security Platform with common continuous integration/continuous delivery (CI/CD) tools, such as Postman and Jenkins, to actively and continuously test APIs for vulnerabilities in development.

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

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 Palo Alto, California, and an office in Tel Aviv and Amsterdam.

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