noname

Noname Security Platform for API Asset Management

The proliferation of APIs in an organization has made it more difficult, if not impossible, to track and inventory APIs manually. APIs also come in many different types and usage patterns, exacerbating the problem. To avoid gaps in inventory, Noname Security provides automated classification and inventory of your APIs for both internal and external users.

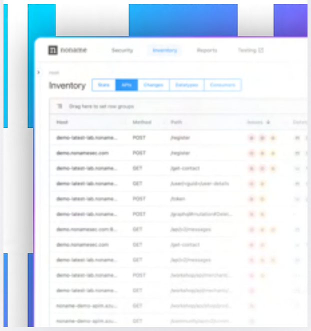
As input for building a comprehensive inventory, the Noname Security platform uses various sources like API Gateways, Web Application Firewalls, Public Cloud Services, Network Traffic, API documentation, etc. This ensures that any dynamic changes made during operational usage of your APIs are automatically reflected in the Noname Security system.

The Noname Security Platform.

The Noname Security Platform consists of 4 integrated pillars, providing end-to-end API asset management and security.

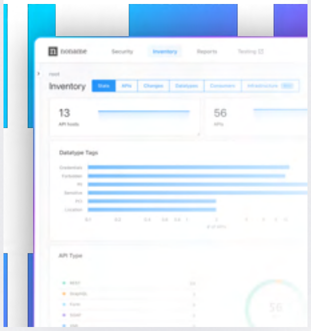
Discovery

Locate and inventory all of your APIs and related risk, from both the inside-out and outside-in



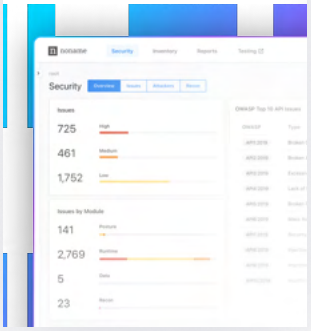
Posture

Uncover vulnerabilities and misconfigurations to speed remediation and ensure compliance



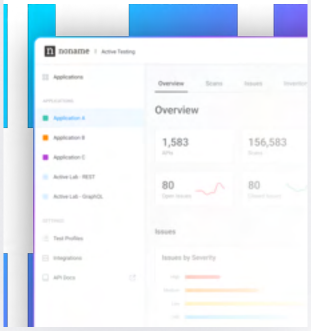
Runtime

Detect and block API attacks with real-time traffic analysis powered by machine learning



Testing

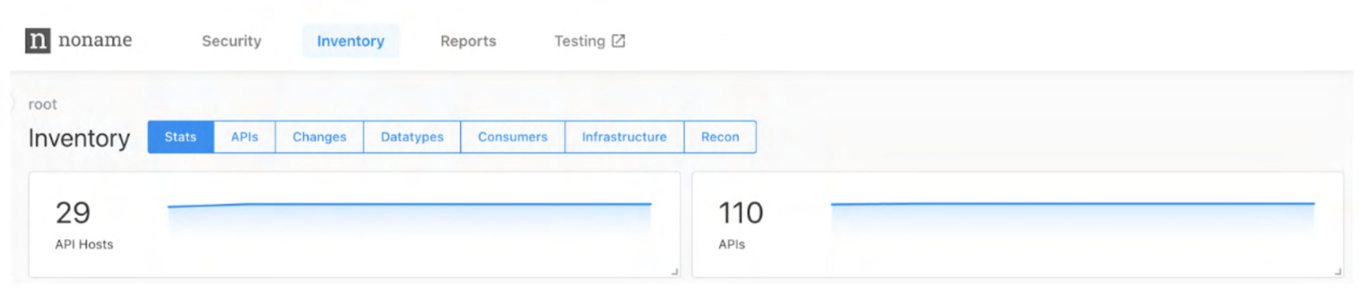
Find and remediate API vulnerabilities during the development lifecycle



For asset management, the starting point is the Discovery Pillar. Taking input from your specific environment through traffic sources, the platform determines how many APIs you have and automatically classifies them on the basis of various frameworks.

API Catalog

The Noname Security Platform will present you with a full catalog of your existing APIs, identifying the systems, exposing those APIs, and the full taxonomy of each individual API.



29 API Hosts

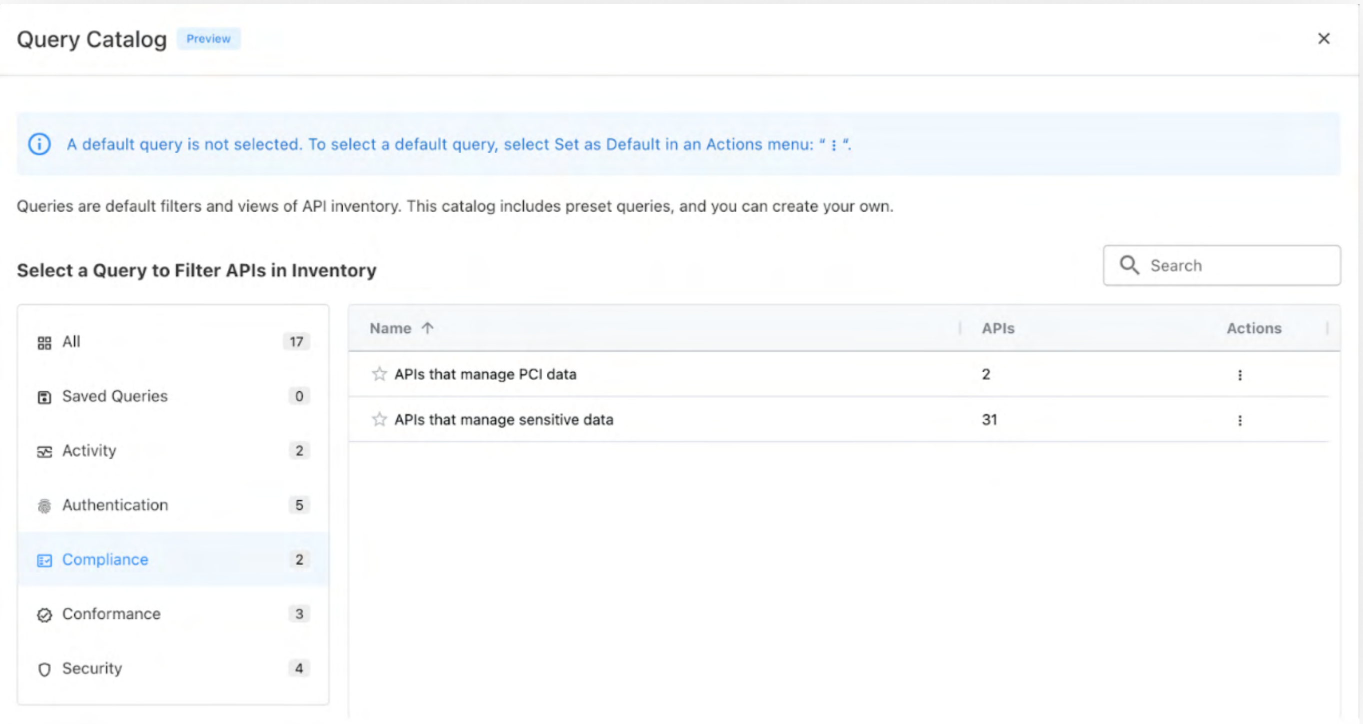
110 APIs

The Noname Security Platform also tracks any changes made to the APIs and provides the ability to export up-to-date documentation, as an OpenAPI Spec file, on the basis of said tracking. The system can also notify you if any new APIs are added to your environment.

Because of the comprehensive administrative API of the Noname Security platform itself you can use the discovered APIs and extract this information as a centralized API CMDB.

Query Catalog

The Noname Security Platform provides a built-in query catalog, which lets you easily explore and manage your inventory according to your specific use-cases or regulatory frameworks.



ⓘ A default query is not selected. To select a default query, select Set as Default in an Actions menu: " ⋮ ".

Queries are default filters and views of API inventory. This catalog includes preset queries, and you can create your own.

Select a Query to Filter APIs in Inventory

All	17
Saved Queries	0
Activity	2
Authentication	5
Compliance	2
Conformance	3
Security	4

Name ↑	APIs	Actions
☆ APIs that manage PCI data	2	⋮
☆ APIs that manage sensitive data	31	⋮

For each API, the system will provide the API Owner, the API type, the types of data processed, the supported authentication methods, the source and location of the API, a validation if the detected API matched the API specification/documentation, the infrastructure behind the API, the API call flows, a full network graph showing the API dependencies, and more.

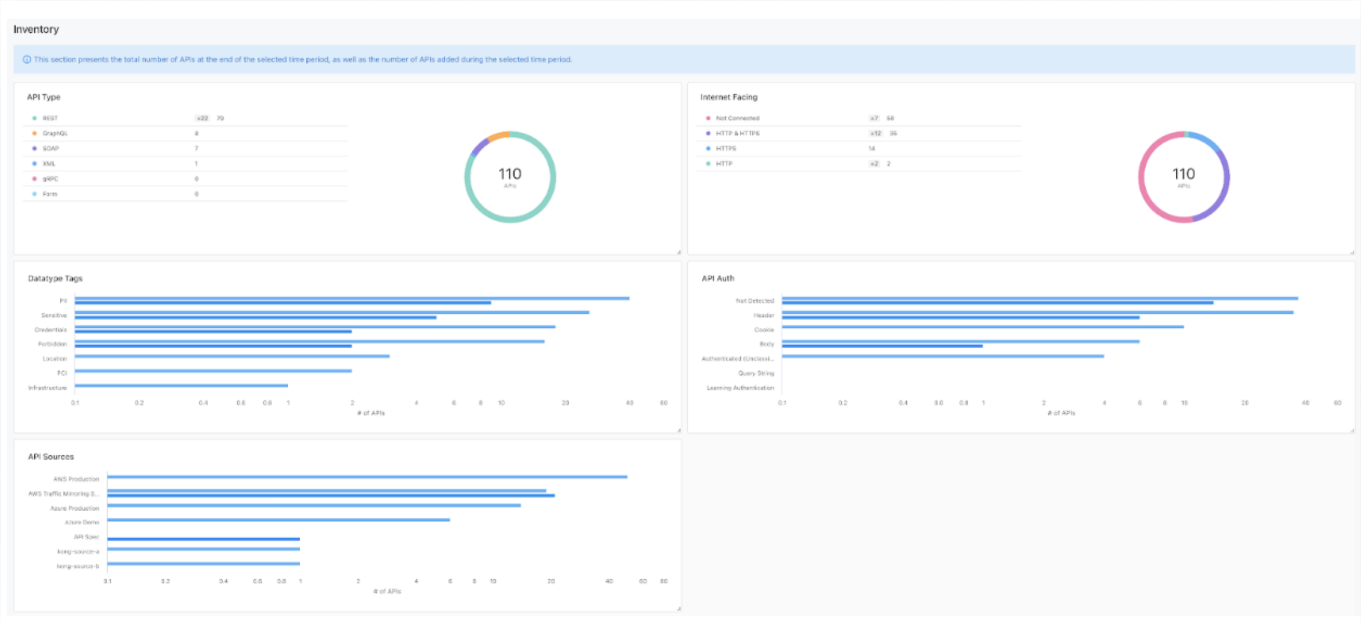
Leverage API Standards

The platform also allows you to upload, view, and analyze your own OpenAPI Spec files and/or linting rules files. Noname includes a default (spectral) linting rules set that you can use. In addition, you can upload RAML, WSDL, and WADL spec files. This allows you to leverage existing or define your own API standards and enforce them in your environment. These standards can be sector specific like for example standard open banking APIs for the Financial Services Industry on the basis of BIAN.

In addition, the system will also detect drift from the standard and allow you to define remediation policies to address these types of detections. The system will also detect and import APIs from your Spec files, and compare those with actual network traffic. Using the Noname Security Recon module, we can also detect and import external APIs on the basis of simple domain name information.

Drive API reusability

By leveraging our comprehensive API inventory and catalog, you can easily drive better reuse of your APIs, as you limit any blind spots in your environment for developers and security professionals alike.



Inventory

ⓘ This section presents the total number of APIs at the end of the selected time period, as well as the number of APIs added during the selected time period.

API Type

● REST	+22	79
● GraphQL		8
● SOAP		7
● XML		1
● gRPC		0
● Form		0

Internet Facing

● Not Connected	+7	58
● HTTP & HTTPS	+12	36
● HTTPS		14
● HTTP	+2	2

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

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