API Discovery

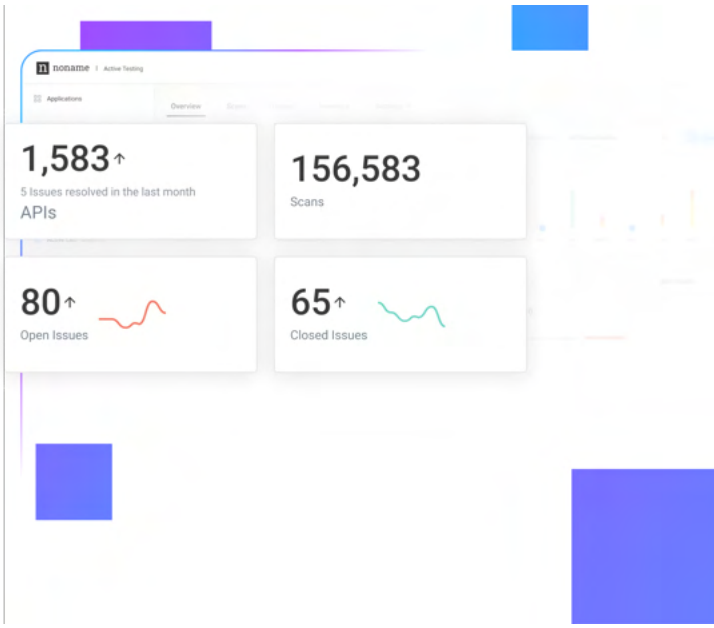
API Posture Management

API Runtime Protection

API Security Testing

Discovery

API Discovery is the first step to understanding and ultimately securing your entire API estate. It goes without saying, you can't secure what you can't see. Without an accurate inventory your organization is exposed to a range of security risks, using our API discovery we will locate and inventory all of your APIs regardless of configuration or type.



Why you need API Discovery

API discovery is important because it helps organizations to quickly find all their APIs, which helps them to mitigate risks by uncovering hidden vulnerabilities, like shadow APIs that are utilizing sensitive data like credit card info, social security numbers, and other personally identifiable information (PII). APIs by their very nature exist in many distributed environments: some are routed through API Gateways, some are not and connect east-west bound services and applications, some are managed, some are not and tend to become zombie or shadow APIs over time.

The importance of API discovery is rapidly increasing as more companies are using APIs to build their products and services.

 © Noname Security

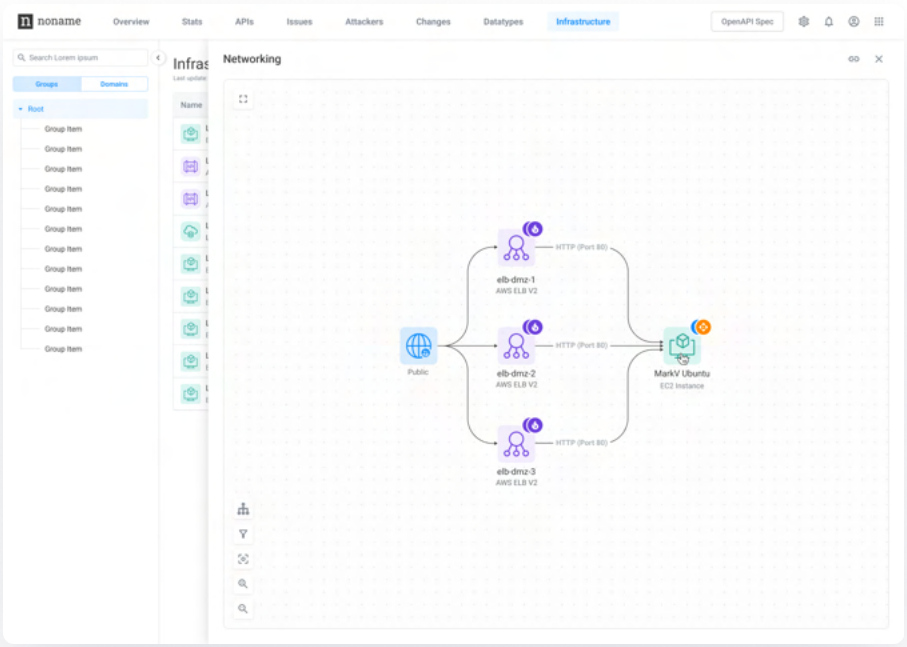
Noname Security API Discovery

Noname provides wider visibility and deeper insights: Noname finds APIs, domains, and related issues from both inside and outside the customer's network perimeter, and uses intelligent data classification and context-aware analysis to create the most accurate and complete inventories.

Your business is exposed to a range of security risks without an accurate inventory. Stop the guesswork and let us help you:

- Locate and inventory all of your APIs regardless of configuration or type—including RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC
- Detect dormant, legacy, and zombie APIs
- Identify forgotten, neglected, or otherwise unknown shadow domains
- Eliminate blindspots and uncover potential attack paths, including through existing systems like API Gateways, WAFs, etc.

As APIs don't exist in a vacuum, Noname also provides visibility in the context of the physical and virtual infrastructure powering the APIs, and the related API call flows. This will allow you to understand the dependencies of your API infrastructure and identify potential security weaknesses.



 © Noname Security

Using Noname Discovery you will be able to:

- Understand your API attack surface
- Reduce costs of API inventories and updating documentation
- Encourage re-use of APIs with better inventories
- Improve compliance with regulatory requirements and internal policies

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