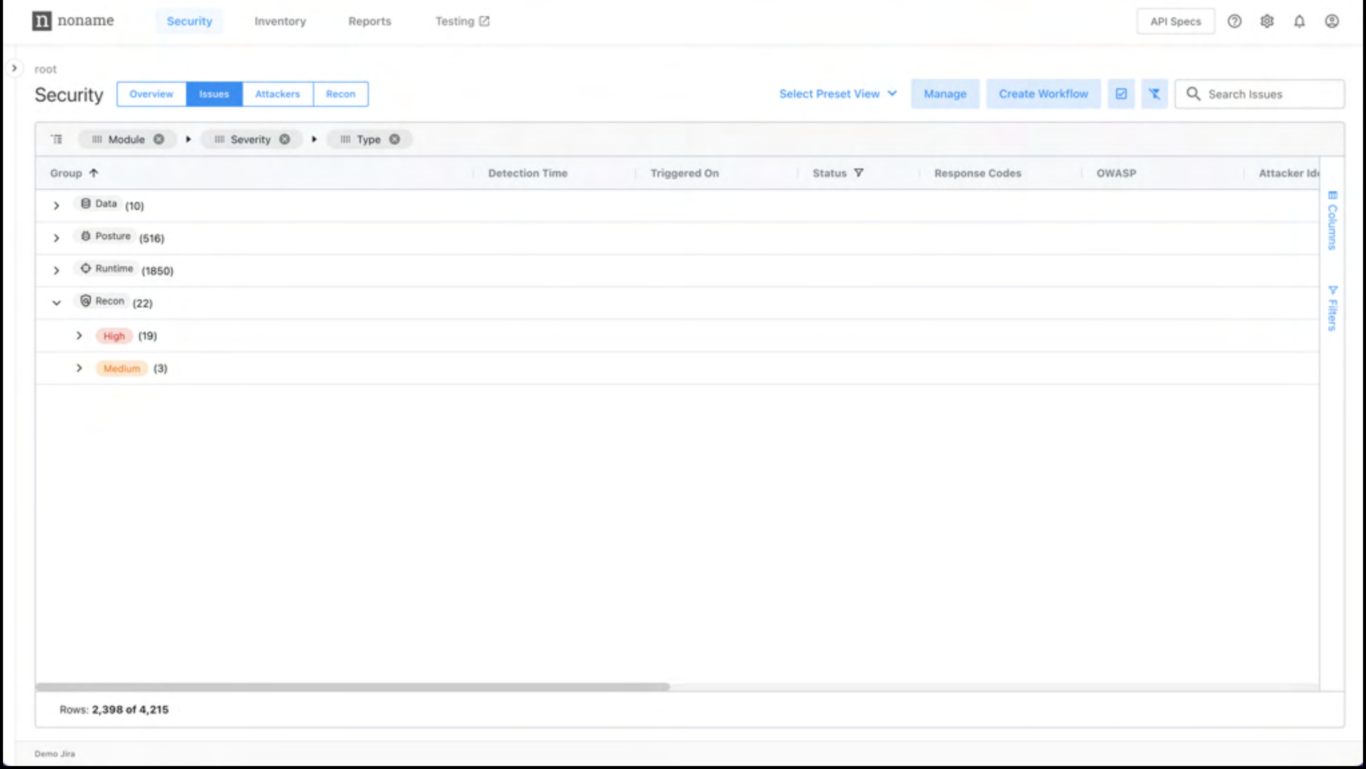
noname

Stay Ahead Of Attackers

Noname Recon is the easiest way to secure your APIs. Simulate attacker reconnaissance to rapidly find and fix issues without any integrations, installations, or implementations.



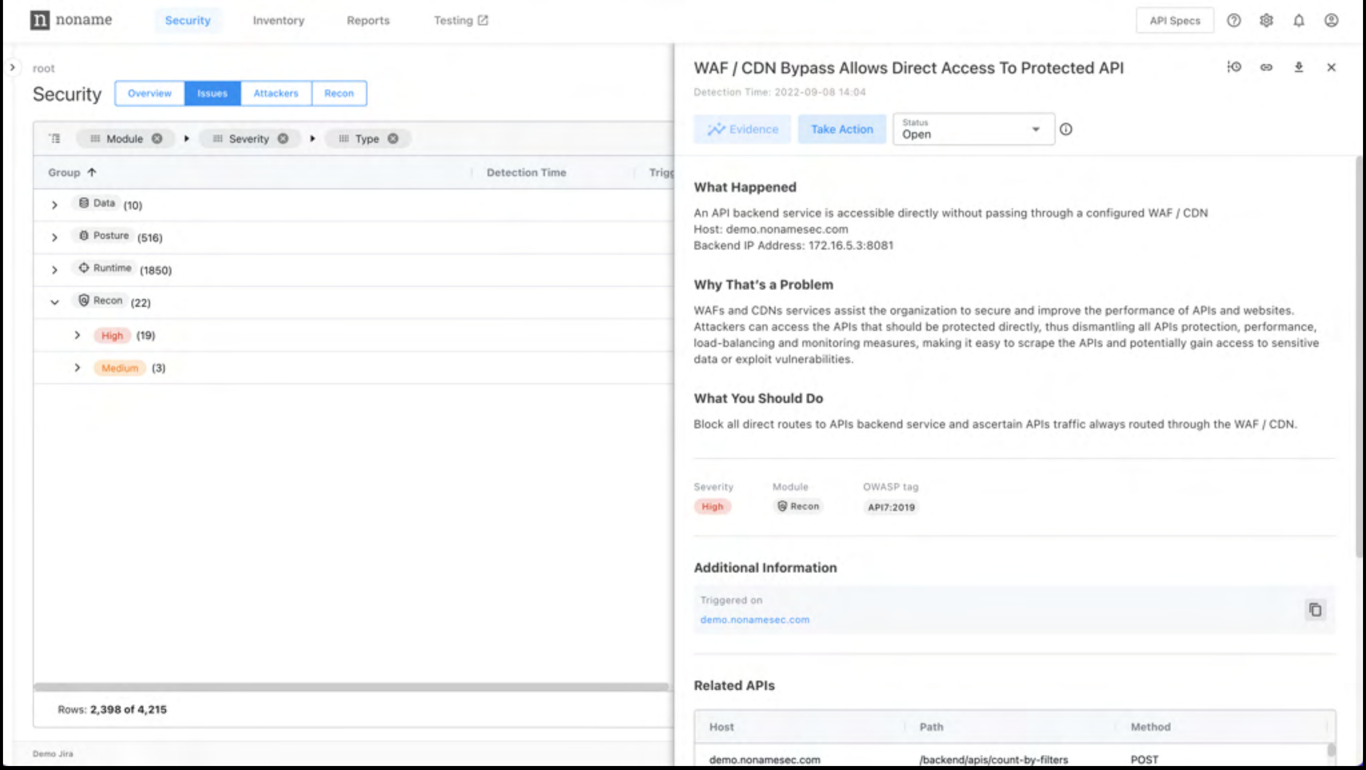
Group	Detection Time	Triggered On	Status	Response Codes	OWASP	Attacker Id
Data (10)						
Posture (516)						
Runtime (1850)						
Recon (22)						
High (19)						
Medium (3)						

Rows: **2,398 of 4,215**

Find Public Issues

Automatically discover public APIs, domains, and vulnerabilities. Easily find exploitable intelligence, such as leaked information, to understand the attack paths available to adversaries.

- Eliminate blindspots and find critical issues including API keys and credentials leakages, API code & schema exposure, API infrastructure misconfigurations, and other vulnerabilities in documentation, public resources, and more.
- Locate "shadow domains" and sub-domains that were previously unknown, unmanaged, or forgotten.
- Monitor for changes in APIs, domains, and developer activity to build a complete and current inventory of publicly accessible assets.



Group	Detection Time	Trigg
Data (10)		
Posture (516)		
Runtime (1850)		
Recon (22)		
High (19)		
Medium (3)		

Rows: 2,398 of 4,215

WAF / CDN Bypass Allows Direct Access To Protected API

Detection Time: 2022-09-08 14:04

Status
Open

What Happened

An API backend service is accessible directly without passing through a configured WAF / CDN
Host: demo.nonamesec.com
Backend IP Address: 172.16.5.3:8081

Why That's a Problem

WAFs and CDNs services assist the organization to secure and improve the performance of APIs and websites. Attackers can access the APIs that should be protected directly, thus dismantling all APIs protection, performance, load-balancing and monitoring measures, making it easy to scrape the APIs and potentially gain access to sensitive data or exploit vulnerabilities.

What You Should Do

Block all direct routes to APIs backend service and ascertain APIs traffic always routed through the WAF / CDN.

Severity	Module	OWASP tag
High	Recon	API7:2019

Additional Information

Triggered on
demo.nonamesec.com

Related APIs

Host	Path	Method
demo.nonamesec.com	/backend/apis/count-by-filters	POST

Fix Issues Quickly

Rapidly reduce risks and eliminate weaknesses before they can be exploited. Make smart, informed decisions about which issues to remediate first and shrink your attack surface in record time.

- Resolve high-severity issues in hours, instead of weeks or months, by finding them before exploitation. Take action immediately with integrations, and custom workflows through Noname Runtime Protection.
- Categorize vulnerabilities by severity automatically to align with your organization's risk tolerance and desired security posture.
- Share findings and feedback to inform development planning to deliver secure apps and API faster.

Prevent Breaches

Continuously secure your customer data, PII, internal documentation, intellectual property, regulatory standing, shareholder value, and more with automatic scanning and protection against evolving threats.

- Automate policy enforcement with custom policies, configurable severity, data classification, and more with the complete Noname API Security Platform.
- Avoid expensive regulatory fines and reputational damage from security incidents and confidently complete your next audit with no surprises, and no late-night projects.
- Extend protection to customers by easily finding vulnerabilities that they may accidentally create.

Protect your APIs and enable your business.

With Noname Recon, you can be sure that the vital connections between your applications – and with your customers – are secure and operational. Even better, continuous protection is only a few clicks away: simply provide a root-level domain to get started and Recon will find the other domains, sub-domains, APIs, vulnerabilities, and public issues that put your organization at risk.

Automatic Scans

Automatically scan your external attack surface at regular intervals to find vulnerabilities before attackers.

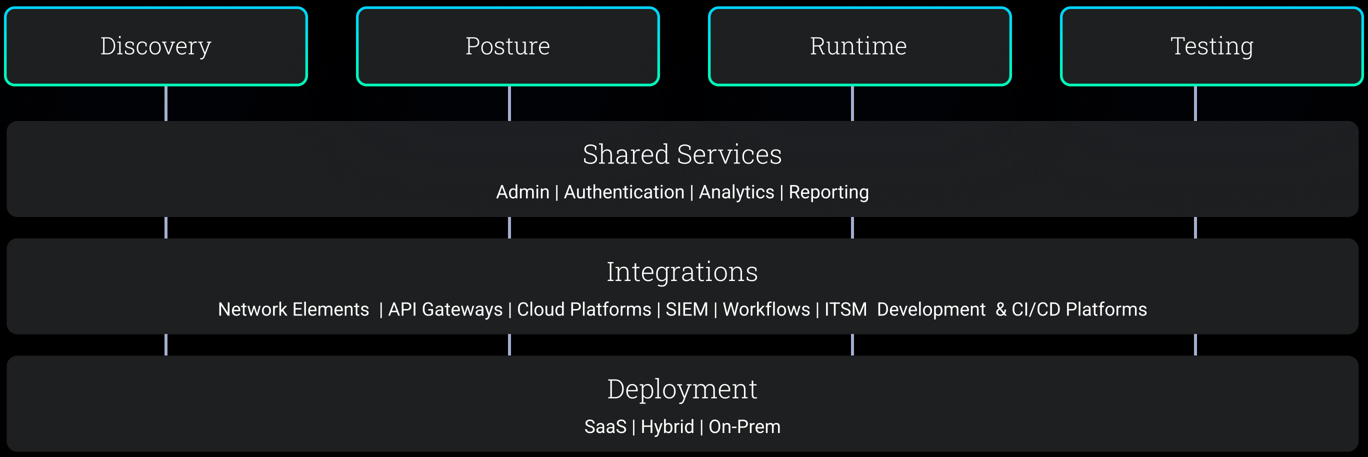
Shadow Domain Discovery

Go beyond known domains to discover forgotten, neglected, or otherwise unknown "shadow domains" that pose a security risk.

Broadest Coverage of Public API Issues

Automatically search for issues and vulnerabilities, including:

- API Credentials Leakages
- Internal API Documentation Leakages
- WAF / CDN Bypass
- Configuration Exposure
- API Returns Sensitive Data
- And more.



Discovery | Posture | Runtime | Testing

Shared Services
Admin | Authentication | Analytics | Reporting

Integrations
Network Elements | API Gateways | Cloud Platforms | SIEM | Workflows | ITSM Development & CI/CD Platforms

Deployment
SaaS | Hybrid | On-Prem

As part of the Noname API Security Platform, Recon works natively with Noname's Posture Management, Runtime Protection, and API Security Testing products. With Noname, you'll have a complete API security solution that protects the full lifecycle of your APIs, enabling your business to move faster and more confidently to drive revenue, lower costs, and reduce risk.

Actionable Intelligence

Take action immediately and directly with relevant, contextual data.

Contextual Information

View issues in context with other Posture Management and Runtime issues, plus guidance on the potential impact and recommended remediation actions for known issues.

Custom Policies

Create custom policies to identify high severity issues.

Customizable Severity

Create custom policies to identify high severity issues.

Custom Policies

Customize issue severity to align with your organization's risk tolerance, regulatory requirements, and internal policies.

Custom Workflows

Create custom workflows to take action immediately, from creating tickets or notifying key stakeholders to updating network configurations.

Integrations

Connect with your existing infrastructure to quickly remediate issues automatically when Recon is deployed with the entire Noname API Security Platform.

Learn more about **Recon** →

Book Live a Consultation →

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