noname | Kong

Noname Security and Kong Gateway: Full Featured API Management

API management is the process of developing, designing, monitoring, testing, securing, and analyzing APIs for organizations.

A full featured API management platform typically includes the following tools:

Developer portals

A site where developers can find the information and credentials required to use APIs in their client apps. A developer portal can provide interactive documentation, developer-facing analytics, monetization information, app approval status, and other tools and services for developers.

Design and development

A developer experience and set of tools for designing and building API products, and for enabling APIs to be used by existing systems.

Testing

Allows for a wide range of testing, from mock testing to functional testing, performance and security testing of APIs.

API gateways

An API gateway performs mediation and enforcement of API calls at runtime.

Analytics and monitoring

Operational metrics, such as usage over time, allow developers to increase speed of API deployment and reliability. Monetization and business metrics, such as the revenue driven through a particular API, let organizations measure the business health of their API ecosystem.

Policy management

Policies define the operation of an API, including how often it caches data, how it translates protocols, and quotas for its use. Managing these policies is an important facet of maintaining an API.

Security and governance

APIs require consistent standards for authorization, authentication, abuse prevention, and connecting identity to client and developer credentials.

Analytics help with end-to-end reporting on all aspects of the API program such as developer engagement, geolocation of consumers, errors, latency, performance and more. In particular, analytics allows project managers to optimize API program adoption and performance by providing granular visibility and reporting. API monitoring ensures that the APIs are available and performing as expected to maintain a seamless experience for your consumers. A full-featured API management platform should include API monitoring tools to perform the following functions:

Traffic analysis

Analyze overall traffic across various geographies, looking for traffic and usage metrics like the success rate of API responses, common error codes, or transactions per second. Traffic analysis tools can identify the source of traffic and determine which application is generating traffic. For instance, is the traffic coming from a bot, a browser, or a library? What device is the traffic coming from?

API tracing and observability

Help with troubleshooting and monitoring API proxies running on an API management platform. API tracing lets you probe the details of each step through an API proxy flow, and observability helps developers understand the latency, performance and execution from each step as it is performed in real-time.

Performance analysis

Performance analysis tools can measure API response time, target response time, and error count across geographies while determining latencies of API proxies and targets. API performance monitoring analyzes error codes and error composition across proxies and targets.

Availability and performance monitoring

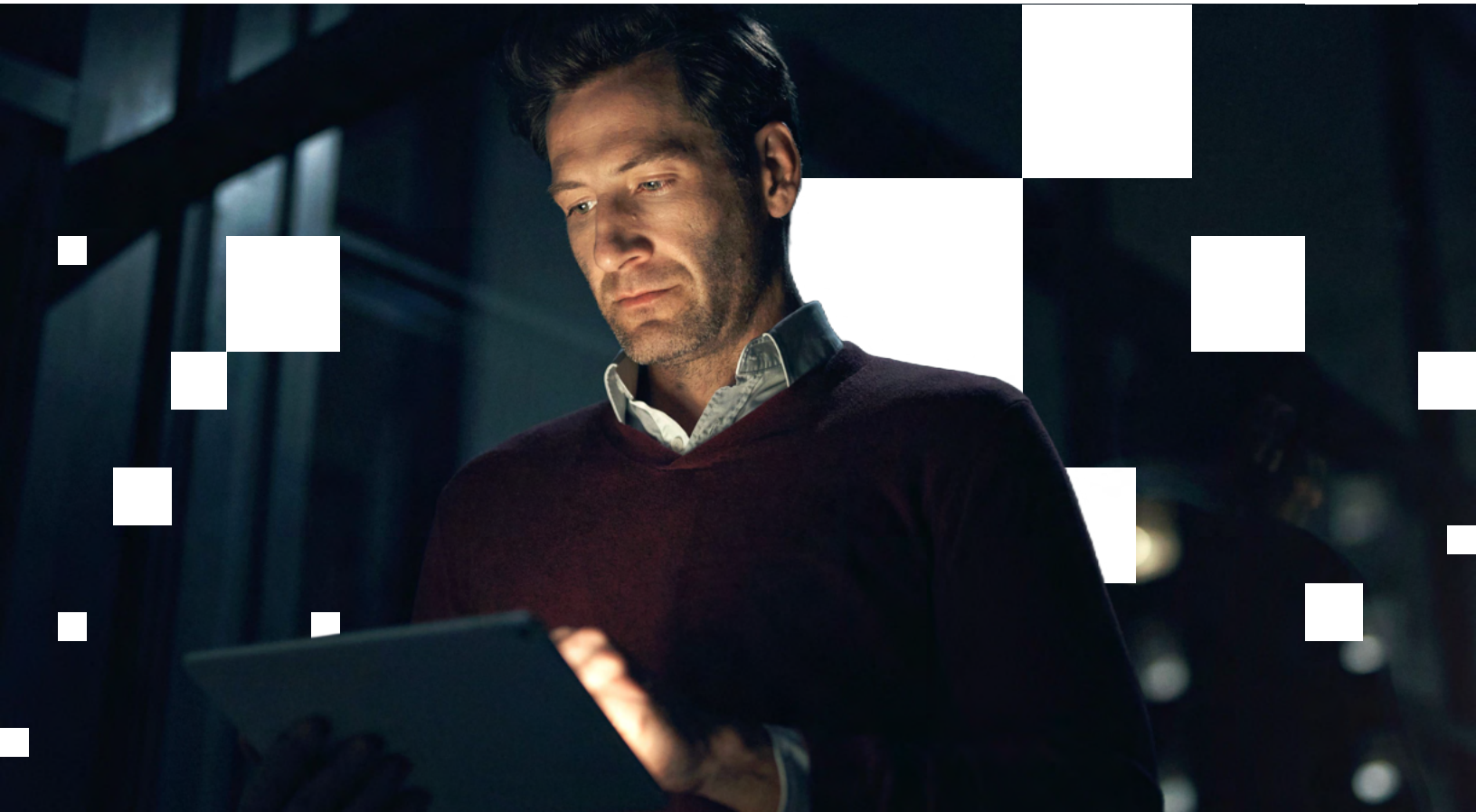
API monitoring tools track the availability and performance of APIs across the entire value chain with granular levels of detail. Monitoring tools can generate alerts when errors occur and reduce resolution times by identifying the source of errors, whether in the developer application, proxy layer, or backend target.

Developer engagement

API monitoring tools can also analyze how developers are interacting with APIs. For instance, which developers are generating the most API traffic? How are they consuming APIs? Did they read the documentation in the developer portal?

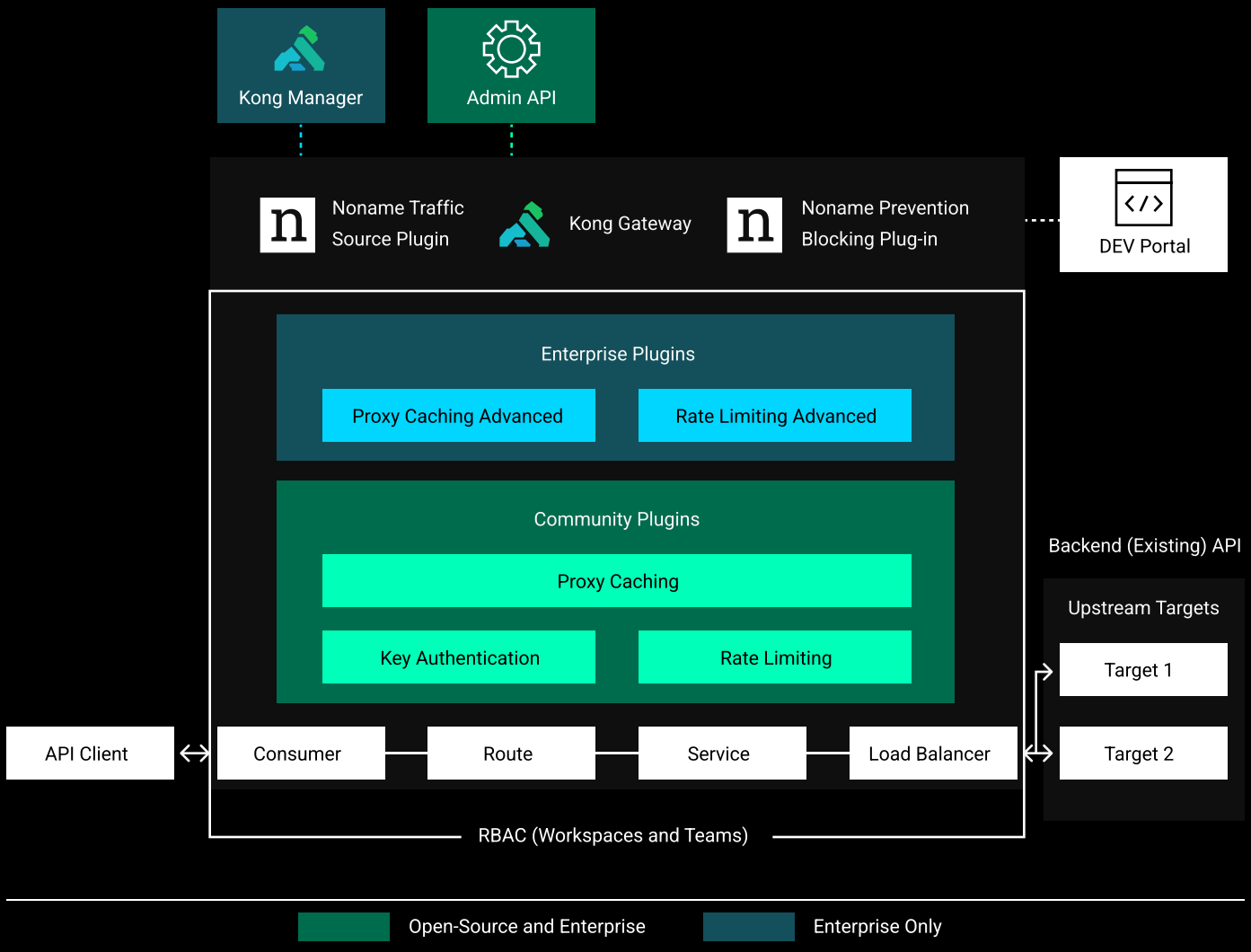
Resources

- The world's most adopted API gateway →
- Multi-cloud and cluster service mesh →
- Kubernetes-native API management →
- AI-focused API Management →



noname

Kong-Noname Architecture



 |

	Kong API Gateway	noname
API Management		
Fast, Lightweight, Cloud-Native	✓	✗
End-to-End Automation	✓	✗
Kubernetes Native	✓	✗
Gateway Mocking	✓	✗
Plugin Ordering	✓	✗
Federated API Management	✓	✗
Data plane Resilience	✓	✗
Consumer Groups	✓	✗
API Governance		
OpenTelemetry	✓	✗
Developer Portal	✓	✗
Service Hub	✓	✗
API Analytics	✓	✗
Data Retention Period for Observability	✓	✗
Admin GUI	✓	✗
Gateway Event Hooks	✓	✗
Audit Logging	✓	✗
Operational Efficiency		
Hosted control plane	✓	✗
Hosted Database	✓	✗
SLA on Gateway control plane and database	✓	✗
Effortless Upgrades	✓	✗
Traffic Management and Transfomation		
Basic Traffic Control Plugins	✓	✗
Simple Data Transformations	✓	✗
GraphQL	✓	✗
Kafka Integrations	✓	✗

		Kong API Gateway	noname
API Management	Multi-protocol Plugin Support	✓	✗
	Request Validation	✓	✗
	Advanced Data Transformation	✓	✗
	Advanced Rate Limiting	✓	✗
	Routing Engine	✓	✗
	Security and Compliance		
	Basic Authentication	✓	✗
	Advanced Authentication	✓	✗
	Role-Based Access Control (RBAC)	✓	✗
	Basic Authorization (Bot Detection, CORS controls, ACLs)	✓	✗
	Advanced Authorization (OPA)	✓	✗
	OOTB integration with 3rd party secret management tools	✓	✗
	FIPS 140-2 Compliant Data Planes	✓	✗
	Software Bill of Materials	✓	✗
	Enterprise Support and Services		
	Enterprise support	✓	✗
	Customer Success Packages - Add-on	✓	✗
Discovery	Discover internal APIs	✗	✓
	Discover external APIs	✗	✓
	Discover external APIs not routed through an API gateway, WAF, or WAAP	✗	✓
	Discover outbound APIs	✗	✓
	Discover new APIs	✗	✓
	Discover depricated APIs	✗	✓
Analyze	**Security Misconfigurations**		
	API not routed through API gateway	✗	✓
	API lacking authentication	Limited	✓

		Kong API Gateway	noname
Analyze	API with weak authentication	Limited	✓
	API gateway without OWASP policy	Limited	✓
	API without rate limiting	Limited	✓
	Internal API exposed to the internet	✗	✓
	Policy Violations		
	Unauthorized data type in API	Limited	✓
	Bad combination of data types in API	Limited	✓
	Data type exposed to the internet	✗	✓
	Changes		
	New data type in API	✗	✓
	New field in API	✗	✓
	Changes to header (e.g. auth, algorithm, userid, etc.)	✗	✓
	Changes in volume	Limited	✓
	Changes in records returned	✗	✓
	API begins handling sensitive data	✗	✓
Analyze	**Anomalies**		
	Detect brute force attempts	✗	✓
	Detect credential stuffing	✗	✓
	Detect account take-over	✗	✓
	Detect directory traversal	✗	✓
	Detect business logic errors	✗	✓
	Broke Object Level Authorization	✗	✓
	Excessive data exposure	✗	✓
Remediate	Integrate with workflows (e.g. Jira, Slack, Trello, ServiceNow, Webhooks, etc.)	✗	✓
	Integrate with existing infrastructure (e.g. API gateway, WAF, firewall, load balancer, etc.)	Noname informs Kong of attackers to block with the prevention plugin	✓

		Kong API Gateway	noname
Remediate	Provide detailed remediation instructions	⊗	✓
	Integration with Security Orchestration Automation and Response (SOAR).	⊗	✓
Test	Authentication Tests	⊗	✓
	Authorization Tests	⊗	✓
	Load Tests	⊗	✓
	Common Vulnerability Tests	⊗	✓
	Sensitive Data Type Tests	⊗	✓
	JWT Vulnerabilities Tests	⊗	✓
Plus	Time to deploy	Minutes	Hours
	Impact on latency	Minimal	none
	Required network configuration changes	✓	none

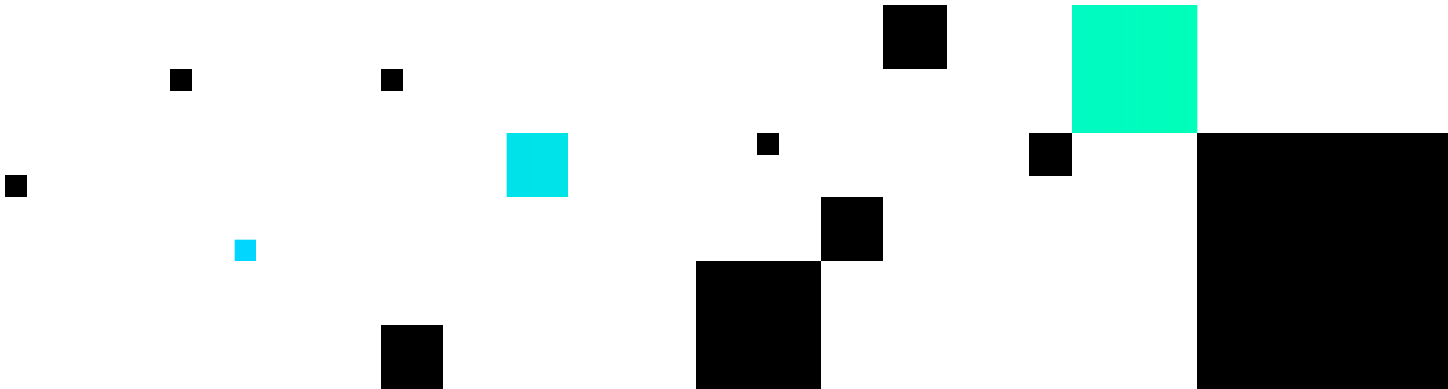
Differences between Kong and NGINX

API Management: Kong is designed specifically for API management, while NGINX is designed to serve web content.

Plugin architecture: Kong has a plugin architecture that allows users to easily add features like authentication, rate limiting, and logging. NGINX can also be extended with modules, but it requires more effort to customize than Kong.

Ease of use: Kong is designed to be easy to use out of the box, while NGINX requires more configuration and tuning to get optimal performance.

Scalability: Both Kong and NGINX are highly scalable, but Kong is specifically designed for managing large numbers of APIs and services.



How Noname Can Help Kong Customers

Discover Your API Estate

Automatically discover APIs, domains, and issues. Build a robust API inventory and easily find exploitable intelligence, such as leaked information, to understand the attack paths available to adversaries.

Documentation & Interoperability

Auto-generate Swagger documentation for all API's in the Inventory. Call Flows and N-Graph provide graphical representation of interoperability between APIs. Enhancing your ability to drive speed, agility, and reuse when building new capabilities for the business

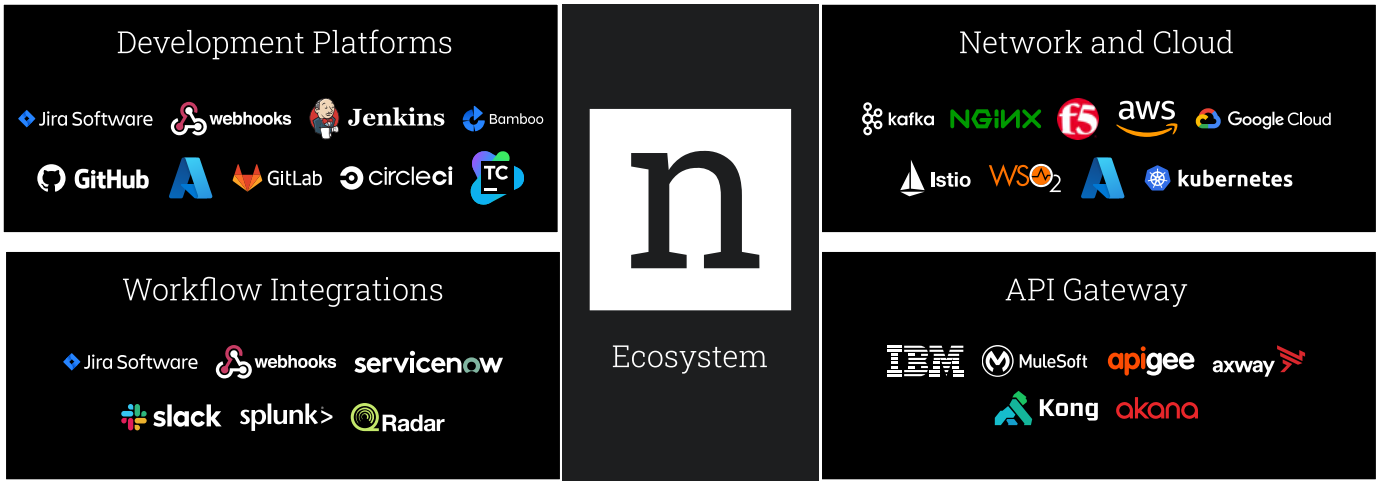
Strengthen Security & Governance Posture

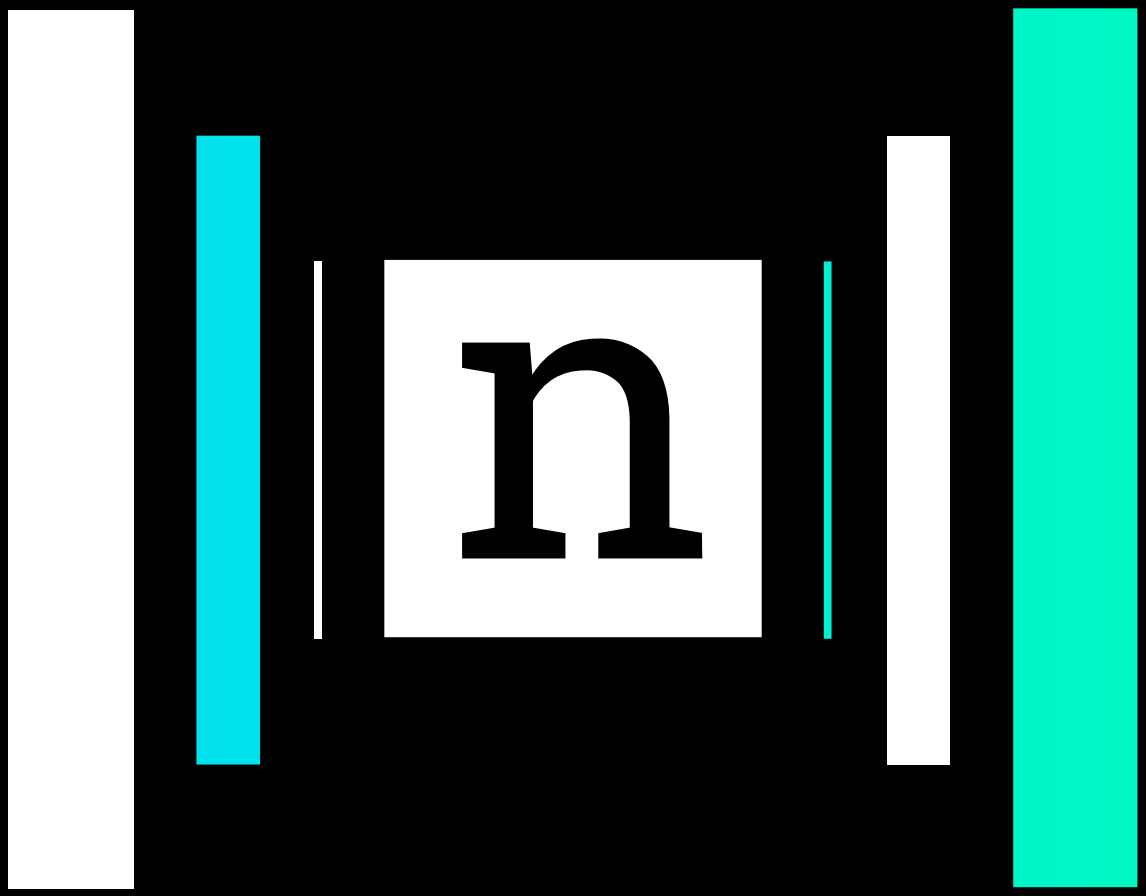
Understand every API in your organization's ecosystem with full business context and enforce corporate standards and policies. Uncover misconfigurations and out-of-policy APIs, find vulnerabilities, protect sensitive data, and proactively monitor changes to de-risk your APIs.

Active Testing

Add security to your CI/CD pipeline. Ensure adherence to standards, remediate vulnerabilities, and deploy more secure APIs faster with Noname's purpose-built API security testing solution.

Automating PCI 4.0 Compliance →





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