Integrated API Security and Governance for Kong API Management
The Promise and Challenge of APIs

APIs have been the driving force for digital transformation, enabling organizations across every industry to create new services and new business models to accelerate growth.

Although business and engineering leaders have rapidly increased API usage and integration across their organizations, their ability to effectively scale and manage APIs remains a challenge. What’s more, APIs present a new and broad attack surface, making them the most targeted attack vector by cyber criminals.

In order to address this challenge, organizations must employ a full-lifecycle approach to both governance and security - including design, development, testing, deployment, operation, and remediation.

Together, Noname Security and Kong enable organizations to quickly develop and deploy APIs with confidence so they can predictably respond and scale with the business.

The Redundant Old Way

- Common functionality is duplicated across multiple services
- Systems tend to be monolithic and hard to maintain
- Difficult to expand without impacting other services
- Productivity is inefficient because of systems constraints

The Kong Way

- Kong orchestrates common functionality
- Build efficient distributed architectures ready to scale
- Expand functionality from one place with a simple command
- Focus on your product and let Kong do the REST
## Challenges

- Maintaining an API Inventory across the estate and finding unknown APIs
- Identifying non-compliant, misconfigured or vulnerable APIs
- Detecting and stopping API abuse or misuse, including attacks
- Building secure and consistent APIs without sacrificing speed or resources
- Establishing alignment and oversight of API security and governance programs
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.

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

Stop API Abuse and Attacks with Runtime Protection
Detect and block API attacks – including data leakage, data tampering, data policy violations, suspicious behavior, and more – with real-time traffic analysis, out-of-band monitoring, inline remediation options, and workflow integrations to increase SOC effectiveness.

Deliver Secure and consistent APIs Faster with 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.
Specific Noname Capabilities for Kong Users:

Integrations with the Kong Ecosystem

Noname supports integrated support for Kong Konnect SaaS, Kong Enterprise and Kong Open Source API gateways across multiple cloud platforms and deployment options.

Inspecting Kong API Traffic

Via the Noname Security traffic source plug-in, the Noname API Security Platform can inspect traffic directly from the Kong Gateway with no impact to network performance – allowing the full power of Noname’s machine learning capabilities to be applied to Kong environments. This plugin batches kong traffic and then sends it to a Noname remote machine learning engine adjacent to the Kong API gateway on the same local regional and/or private network subnet. The Noname machine learning engine then juxtaposes the runtime events on the wire to an expected baseline of normal kong API transactions and known message schemas and open API specification definitions.

Enforcing Security Policies

The Noname API Security Platform can be used to enforce security and other policies on API traffic with the noname prevention plug-in, preventing malicious activity and other unwanted API activity. Note that this prevention and blocking integration feature is generally available for Kong Open Source and Kong Enterprise and is in BETA QA for Kong Konnect managed instances of the Kong API Gateway. In the next major LTS release of the Noname product the Kong Konnect supported integration of this plug-in features support for

- Kong OSS, Kong Enterprise & Kong Konnect

For Kong Konnect the following parameters are included in the Noname integration configuration:

- V2 API Region, either US or Europe
- Bearer token, aka \texttt{PAT} (Personal Access Token)
- Control plane ID

nonamesecurity.com | © 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