noname | Kong

Solution Brief

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.

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

Inspection of Kong API Traffic

The Noname API Security Platform can inspect traffic directly from the Kong Gateway with no impact on network performance using – allowing the full power of Noname's machine learning capabilities to be applied to Kong environments.

Security Policies Enforcement

The Noname API Security Platform can be used to enforce security and other policies on API traffic via a second 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.