noname

Solution Brief

Integrated API Security for KONG API Management

Noname Security is the only company to deliver **API security posture management,** provide **API detection and response,** and secure your **API development life cycle.**

API-Led Digital Transformation

Digital transformation initiatives are top priorities as organizations look to improve the digital experience for customers while reducing operational costs. The effort to attract new and keep existing customers by delivering additional value has resulted in more application services and supporting APIs.

APIs are the core of digital strategies when creating and operating applications with public or private clouds that interact with other applications located across the Internet. Continuously developed and deployed microservices-based applications have driven an explosion of API-centric communication and interaction services to internal applications and data sources as well as third party providers. The proliferation of APIs has greatly expanded the attack surface and led to APIs becoming the most targeted attack vector by cyber criminals who target payments fraud, and data theft.

Noname Security enables organizations to better secure all of their APIs with integration with their KONG API Management platform. Noname Security provides automated discovery and analysis that drives remediation of API security issues. Together Noname Security and KONG enable organizations to quickly develop and evolve their applications with full confidence in their API interactions.

API Posture Management

Inventory every API, including legacy and shadow APIs, with **data classification.**

Identify **misconfigurations** and **vulnerabilities** in source code, network configuration, and policy.

Runtime API Protection

Behavioral-based models for **runtime API threat detection.**

Automated and semi-automated **attack blocking** and **vulnerability remediation**.

"Shift Left" and API Security Testing

Continuously test APIs to identify API risks before they emerge.

Automated and dynamic test development and incorporation into CI/CD pipelines.

Kong

Industry-Leading Approach to API Security

Discover All APIs, Data, and Metadata

Find and inventory every kind of API, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, and gRPC. Discover legacy and rogue APIs not managed by an API gateway, and catalogue API attributes and metadata.

Analyze API Behavior and Detect API Threats

Use automated AI-based detection to identify the broadest set of API vulnerabilities, including data leakage, data tampering, misconfigurations, data policy violations, suspicious behavior, and attacks.

Prevent Attacks, Remediate API Vulnerabilities

Prevent attacks in real-time, fix misconfigurations, automatically update firewall rules, webhook into your WAFs to create new policies against suspicious behavior, and integrate with existing workflows (including ticketing and SIEMs).

Actively Test APIs Before Production

Most applications are tested before they are deployed into production. Most APIs are not. Actively test APIs as part of the software development lifecycle to identify issues before production.

noname

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD API Security category North America

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD Fastest Growing Cybersecurity Company North America

TOP 10 BLACK

TOP 10 CYBERSECURITY EXPERTS

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 three pillars — Posture Management, Runtime Security, and Secure API SDLC. Noname Security is privately held, remote first with headquarters in Silicon Valley, with an office in Tel Aviv and Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371