wallarm | Kong

PARTNER SOLUTION BRIEF

Integrating Advanced API Security into Kong solutions

Kong and Wallarm together provide superior API management and security

APIs present a large and growing attack surface for modern organizations, but have outgrown the capabilities of traditional application security and management tools. To address your API management and security needs, you need a modern, cloud-native tech stack which delivers robust and high-performance protection.

The integration of Kong and Wallarm combines the most popular API gateway with an enterprise class API security platform that discovers all your APIs (not just those managed by Kong) and protects them from modern threats, business abuse and data theft.

Comprehensive Protection Against API Threats

Security teams choose Wallarm to discover all the APIs running in their environment, and to block attacks against them.

- **OWASP API Security Top-10.** Protect against well-known and advanced threats, such as Injections, BOLA, and authentication failures.
- **API Discovery.** Regain control over your API attack surface with runtime visibility across your entire API portfolio.
- **API Protection.** Defend your APIs in seconds without relying on tedious manual configurations and outdated or inaccurate API specs.
- **Virtual Patching.** Drastically reduce 0-day risks by applying virtual patches to critical issues on the fly.
- **Sensitive Data Exposure.** Meet compliance requirements by tracking and protecting sensitive data, including PII, financial & health data, credentials and more.
- **Credential Stuffing and Brute Force.** Prevent account takeover (ATO) and other behavior-based attacks which can lead to large-scale breaches.
- **JWT Attacks.** Automatically find and report JSON Web Token (JWT) weaknesses and attacks to deter unauthorized access.
- **Monitor Changes.** Minimize API drift and prioritize security efforts (like pen tests or bug bounties) with alerts on new, changed or deprecated endpoints.

Key Benefits

- **Active Blocking.** Wallarm is designed from the ground up to provide real-time blocking of API attacks. Don't just detect attacks, actually block them.
- **Integrated Deployment.** Wallarm integrates directly with your Kong gateways to provide an additional layer of security on top of Kong's industry leading API management.
- **Privacy-First Architecture.** API Security shouldn't add risk to your organization. Wallarm collects only the minimum data required to detect and block attacks. No risky third-party data lake here!

With Wallarm, we've been able to scale API protection to the scale we need and manage with our infrastructure as a code approach.

Gustavo Ogawa,
Head of Security at Rappi

Rappi

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107

wallarm

PARTNER SOLUTION BRIEF

Better Together

While Kong's API Gateway provides the foundational pieces to build and manage APIs in a secure manner, modern enterprises need to layer more advanced API protections to defend against growing API-specific threats. Kong and Wallarm work together to provide full spectrum API security:

API Security Fundamentals - Kong API Gateway

- Application and User Authentication (basic auth, API Key, OAuth/OIDC, LDAP, etc.)
- Access Control (ACLs, JWT scopes, etc.)
- Encryption Tunnels with digital certificate exchange (mTLS)
- Cross-Origin Resource Sharing (CORS)
- Rate Limiting & Caching

+

Advanced API Protection - Wallarm API Security

- OWASP API Security Top-10 risks (BOLA, Injections, etc)
- Automated API Discovery and Inventory (shadow APIs, new / changed endpoints, PII data, etc.)
- API Abuse Prevention
- API Risk Posture Assessment
- Block Malicious traffic sources (Tor actors, geos)

Integrating Kong & Wallarm

Wallarm API Security platform deploys directly into your Kong API Gateway, natively integrating the additional API security layer necessary to protect your API portfolio.

Unlike some offerings which only mirror traffic to their agents, Wallarm provides real-time detection and mitigation – no reliance on other tools or complicated workflows. And the unique Wallarm approach results in maximum performance and near-zero latency.

Wallarm integrates natively into your Kong API Gateway instances, including both Kong Enterprise and Kong Community (open source) editions. Deployment options include a Wallarm LUA plugin for the Kong Ingress Controller.

And Wallarm API Security integrates into your Kong API Gateway regardless of deployment scenario: cloud (including AWS, GCP, Azure, etc.), multi-cloud, private data centers, Kubernetes environments, and more.

The combination of Kong and Wallarm enables superior API management and security with a DevOps-friendly deployment and management delivery – not only does this approach allow you to manage your API Security layer with the same tools and manner that you use with your API Gateway, but it results in vastly improved API protection and reduced organizational risk.

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107