Signal Sciences

Signal Sciences + Kong Integration

Joint Solution Brief

Kong is the most popular open source microservice API management gateway. Key benefits to deploying Kong include sub-millisecond latency, a RESTful interface, and a platform agnostic support model. With superb extensibility via their plugin marketplace, Kong supports management and authentication for serverless functions, including Lambda, Azure, and OpenWhisk.

API developers can get insight via Signal Sciences into attacks on their APIs and serverless functions. Legacy web application firewall (WAF) and RASP solutions can't get visibility into these attacks because of where they install. WAFs require additional infrastructure and hops in your network topology since they have to be deployed in front of the API and serverless architecture, negating the benefits of serverless. RASPs have to be deployed at the runtime framework layer, which doesn't exist in serverless architectures. Only Signal Sciences with Kong Microservice API Gateway can provide production application coverage and protection across all platforms.

Answer important questions with Signal Sciences & Kong:

Visualize Attack Protection and Monitoring

How are your APIs, microservices, and serverless functions getting attacked at the source?

Alert and Report on Attacks, Anomalies, and Feature Abuse

Where are the most attacks coming from? Are there anomalies and feature abuse coming from authenticated users?

Get Developers and Operations Involved

Why did a sensitive transaction spike? What endpoints are being attacked the most? Is the attack a security issue or an operations one?

SUMMARY

Signal Sciences integrates natively with Kong Microservice API Gateway via a NGINX lua module, allowing business of all sizes to secure their apps, APIs, and serverless functions natively.

LUA PLUGIN BENEFITS

- Simple 6-step install to add Signal Sciences to Kong Microservice API Gateway
- Enforce requirements for developers to use application layer security

SIGNAL SCIENCES BENEFITS

- **See:** Empower all teams with intuitive dashboards and integrations that show insights and attack details.
- **Secure:** Provide reliable blocking decisions across OWASP Top 10, ATO, feature abuse, API misuse, and more.
- **Scale:** Run anywhere with the lowest TCO, no signatures to manage, and no impact on performance.