

Kong Built Secure AI Infrastructure with Akamai

AI connectivity company Kong helped organizations securely govern and scale production AI with Akamai



Governed
APIs and AI



Secured AI
interactions



Scaled AI
infrastructure

Building secure AI infrastructure for production environments

Kong helps organizations manage APIs and AI traffic across hybrid, multicloud, and distributed environments. As customers shift from traditional APIs to AI applications, they encounter three new challenges: securing APIs, governing AI interactions, and running AI workloads at scale.

To meet these evolving customer needs, Kong and Akamai expanded their partnership through three complementary integrations. The partnership combined API governance, AI security, and cloud infrastructure into a unified platform. The result is a trusted foundation for deploying, securing, and scaling production AI.

Helping organizations govern APIs across distributed environments

Organizations are modernizing applications with microservices, APIs, and AI services. This makes governance at scale increasingly difficult.

“Our platform helps organizations meet consistent requirements and control traffic across complex environments,” explained Harish Madhavan, Head of Partner Solutions for Kong.

Kong helps customers manage API traffic, enforce policies, and maintain compliance across distributed environments. Its APIOps capabilities also support shift-left security by applying governance throughout the API lifecycle.

But as API environments grow and AI services proliferate, many organizations lose visibility into every API and AI endpoint. “Our customers struggle to know how many APIs and LLM endpoints are deployed in their environments,” Madhavan said.

That visibility gap became the starting point for the Kong–Akamai partnership.



Location

San Francisco, California
konghq.com

Industry

Software and SaaS

Solutions

Cloud Computing

Security

Products

API Security

Firewall for AI

LKE: Managed Kubernetes Engine



Securing APIs from discovery through enforcement

To help organizations secure growing API environments, Kong integrated [Kong AI Gateway](#) with Akamai's [API Security](#) solution. Each solution plays a distinct role:

Kong AI Gateway

- Routes and manages API traffic
- Applies authentication, rate limiting, and governance policies
- Controls API and AI traffic across distributed environments

API Security

- Discovers known and unknown APIs
- Detects threats and business logic abuse
- Identifies vulnerabilities through continuous traffic analysis

The solutions provide both visibility and enforcement. Akamai continuously discovers APIs and analyzes behavior, while Kong automatically applies policies to protect those APIs.

"With this integration, joint customers can easily discover, audit, and secure their APIs, including LLM endpoints across hybrid and multicloud environments," said Madhavan.

Extending governance from APIs to AI

As organizations move from API management to production AI, they encounter a new set of security challenges. Modern AI applications often combine multiple large language models (LLMs), AI agents, vector databases, Model Context Protocol (MCP) servers, and APIs. Managing these components at scale quickly becomes difficult.

"It's challenging to manage multiple providers, external tools, and emerging ecosystems consistently across environments," Madhavan explained.

To solve this problem, Kong expanded the partnership by integrating Kong AI Gateway with Akamai [Firewall for AI](#). Again, each solution serves a different purpose.

Kong AI Gateway

- Routes and governs traffic across multiple AI models
- Governs and controls AI traffic with centralized policies and guardrails
- Connects AI agents, MCP servers, models, and enterprise services
- Manages AI usage, performance, and cost with capabilities including caching and token controls

Firewall for AI

- Inspects prompts and responses for AI-specific threats
- Detects prompt injection, AI threats, and other malicious interactions
- Enforces security policies to block or mitigate threats before they reach models or applications
- Provides a dedicated AI security layer that complements Kong's traffic governance and control

The combination enables organizations to consistently govern AI traffic while automatically enforcing AI security policies across rapidly evolving AI environments.



**Kong and Akamai
help customers
move from AI
experimentation to
secure production.**

Harish Madhavan
Head of Partner Solutions, Kong

“Together, Kong and Akamai provide complementary layers of AI security: Kong governs and controls how AI traffic flows across models, agents, MCP servers, and enterprise services, while Akamai adds specialized inspection and threat protection for prompts and model responses,” Madhavan said.

Running AI workloads on scalable cloud infrastructure

Securing AI is only part of the equation. Organizations also need cloud infrastructure that can reliably run production AI workloads.

Kong expanded the partnership again by hosting the Kong AI Gateway runtime on Akamai Cloud using [LKE: Managed Kubernetes Engine](#). The solutions work together to separate management from execution.

The Kong Konnect platform manages service configurations through its control plane and distributes them to Kong AI Gateway data planes running on Akamai Cloud. Meanwhile, Akamai provides the Kubernetes-based infrastructure those runtime environments depend on. That includes compute, networking, storage, load balancing, and built-in security.

The architecture enables organizations to:

- Standardize governance across AI, LLM, and MCP traffic
- Reduce dependence on a single AI provider
- Centralize observability and policy enforcement
- Scale AI workloads securely across distributed environments
- Accelerate deployment of production AI applications

Building a trusted foundation for production AI

As AI architectures become more distributed, individual security tools aren't sufficient. Organizations need an integrated platform that connects governance, security, and infrastructure.

Kong and Akamai built that platform step by step. They first helped customers discover and secure APIs. Next, they extended governance into AI applications and MCP environments. Then they provided the cloud infrastructure to run those applications at scale.

“Our partnership helps customers move from AI experimentation to secure production,” Madhavan concluded.



Kong is the AI connectivity company. Its mission is to build the connectivity layer AI needs to reach its full potential with AI governance from day one. Trusted by the Fortune 500 and AI-native startups alike, Kong's unified platform enables organizations to secure, govern, accelerate, and monetize the flow of intelligence across AI and API traffic — on any model, any cloud. For more information, visit konghq.com.