

Akamai AI Firewall & AAM AI Gateway

Complete AI Protection & Control Platform

INTEGRATION BRIEF FOR AKAMAI CONNECTED CLOUD

The Challenge of Securing Enterprise AI

Organizations deploying AI applications at scale face a dual challenge: maintaining operational control while ensuring comprehensive security. Traditional approaches force teams to choose between governance tools and threat protection, creating gaps that expose businesses to prompt injection attacks, data exfiltration, cost overruns, and compliance violations.

Introducing the Complete AI Solution

The integration of Akamai AI and API Manager (AAM) AI Gateway with Akamai's AI Firewall delivers comprehensive AI protection and control in a single platform.

> Unified AI governance and security

One platform manages LLM access, costs, and routing while simultaneously protecting against prompt injections, jailbreaks, and data exfiltration.

> Comprehensive threat protection

Advanced AI-powered security policies detect and block malicious inputs while filtering harmful outputs, all without disrupting legitimate AI interactions.

> Enterprise-scale deployment

Leverage Akamai's global edge infrastructure for low-latency AI security processing combined with AAM's self-serve productivity tools.

> Seamless integration

Deploy protection across any environment with flexible API-based architecture that works with existing AI applications and workflows.

Benefits of a Unified Platform

> Intelligent Threat Protection

Block prompt injections and malicious inputs in real-time through Akamai's AI Firewall before they reach your models. Eliminate security gaps that exist with standalone solutions.

> Unified Response Filtering

Screen AI-generated responses for harmful content, PII leakage, and compliance violations. Ensure every interaction meets safety and regulatory requirements.

> Automated Compliance

Policy-based controls enforce regulatory requirements automatically. Comprehensive audit trails support reporting while adaptive policies evolve with emerging threats.

> Dynamic Model Management

Intelligent LLM routing with automatic failover and hierarchical cost controls. Teams get self-serve access to secure AI endpoints within organizational governance.

> Real-time Observability

Track usage patterns, costs, and security events across all AI interactions. Complete visibility for governance and incident response through unified dashboards.

> Enterprise-scale deployment

Deploy anywhere via Akamai edge or REST API. Bank-grade security with OAuth, JWT, and mTLS across hybrid, cloud, and edge environments.

