



Akamai AI and API Manager

vs. Cloudflare AI Gateway

AI GATEWAY GOVERNANCE ON AKAMAI CONNECTED CLOUD

Both Akamai AI and API Manager (AAM) and Cloudflare provide powerful AI gateways, but AAM is purpose-built for developer-first enterprises with hierarchical governance, cost transparency, semantic caching, and proactive alerts, enhancing control and safety across AI workloads.

AI Gateway Comparison

Feature		Cloudflare
Governance	Self-serve access with hierarchical governance. Developers spin up virtual apps safely within guardrails.	Centralized policy management. No team hierarchies for delegated or inherited governance.
Observability	Real-time dashboards + alerts. Set token, budget, and request thresholds with proactive warnings before limits are hit.	Logs and metrics on usage and costs. No built-in alerts for tokens, budgets, or requests.
Programmability	Fully programmable: build custom guardrails, filters, and org-specific policies.	Fixed controls managed through Cloudflare dashboard. Limited customization.
Cost Management	Semantic Caching reduces spend by caching by meaning, not just exact requests. Multi-level cost limits.	Standard caching with TTLs. No semantic caching. No hierarchical quotas.
Security Controls	Enterprise-grade protection via Akamai AI Firewall (PII detection, prompt injection blocking, toxic content filtering). SOC 2 Type 2 certified with OAuth, JWT, and mTLS.	Rate limiting, caching, authentication, and WAF protections. Real-time content moderation available.
Dynamic Routing	Route intelligently across models based on cost, performance, availability; seamless model migration.	Dynamic routing (visual, content-based, geography, A/B testing) and fallback support available.
LLM Provider Support	OpenAI, Anthropic, Google, Mistral, plus pluggable support for additional services.	Fixed list including OpenAI, Anthropic, Hugging Face and Workers AI.



AI and API Manager
Built into Akamai Connected Cloud

AI Firewall

Semantic caching

Hierarchical governance

SOC 2 Type 2