

MCP Gateway for Users

Governed MCP Access for Your Whole Workforce

PRODUCT BRIEF FOR AKAMAI CONNECTED CLOUD

Your Team Is Already Using MCP

Employees are wiring Claude, Cursor, and ChatGPT into internal and third-party MCP servers today — usually with personal tokens, no security review, and no record of what was accessed. Blocking it drives it underground; ignoring it compounds the risk. The answer is a governed path that's easier than the workaround.

What Users — and IT — Need

> A Point of Discovery

One catalog of approved MCP servers, so finding the right tools doesn't mean hunting through Slack or wiring up something unvetted.

> Consistent Authentication

One sign-in through the corporate identity provider — not a personal token pasted into every tool for every server.

> Authorization

Access scoped to each team and user: Finance sees finance tools, Engineering sees engineering tools, nobody sees everything.

> Observability

A live view of MCP usage across the organization — which servers, which tools, how much, by whom.

> Audit

One correlated trail of every tool call, ready for compliance reviews and incident response.

> Guardrails

Protection that travels with every call — sensitive data caught before it leaves, malicious content caught before it lands.

Inside AAM: MCP Gateway for Users

Akamai AI and API Manager (AAM) is the governed front door between your workforce's AI tools and every MCP server they use — on Akamai Connected Cloud.

> Central Catalog

Security reviews a server once; it's then discoverable org-wide. Curated, default-deny tool catalogs make the official path the easy path.

> One Login Through Your IdP

Twelve identity-provider presets plus any OIDC provider. The gateway brokers and rotates every downstream credential — users never handle tokens.

> Tool-Level RBAC

Roles and groups from your IdP drive per-tool access. Non-permitted tools are hidden and refused — and revocation is instant when someone leaves.

> Unified Observability

Every call lands in one place: typed events with OpenTelemetry tracing, streaming to Splunk, Datadog, and 10+ platforms in real time.

> Audit-Grade Trail

Which user, via which AI tool, called which capability, with what result — correlated end to end, and privacy-first by default: metadata, not payloads.

> Guardrails on Every Call

DLP redaction, prompt-injection and tool-poisoning screening, and per-user rate limits — with Akamai Firewall for AI as native policies.