JETSTREAM

Beyond The AI Gateway: Clearance to the Control Plane

What Zero Trust for AI Actually Requires

Almost every week brings another AI gateway. Gateways move requests. They route traffic, cache responses, translate protocols, and enforce rate limits. All necessary work but only the lower half of something larger.

The intelligent part above decides whether a request should move at all. It evaluates who is making the request, which approved design authorized it, what tool is being called, and what the specific action is about to do.

Together, these layers form the AI Control Plane.

Most enterprises are considering or have implemented an AI gateway. But most AI gateways lack enterprise-grade control. They discover the gap when an approved agent takes an action that would never have been approved in context. By the time the gateway logs the event, the action is already complete.

⚠ Firewalls had this problem first

For years, a firewall was a routing decision: receive a packet, check a port, pass it along. NextGen firewalls changed the question from "where is this going?" to "what is actually inside it?"

Now the thing you approved is an agent. A port waits to be used. An agent acts without being asked.

JetStream AI Gateway
Routes, caches, translates protocols, enforces rate limits.

JetStream Clearance
Evaluates every action in context, before it executes.

JetStream AI Control Plane
The whole, working from one live picture of the estate.

AI Control Plane Capabilities

Agent Workflow Visualizer and execution plan anchoring	Task-level Observability & evidence	MCP supply chain assurance	Continuous Identity Validation and Authorization	Risk posture and compliance alignment	AI economics management	Policy-based blast radius and overspend containment
JetStream AI Blueprints™	**JetStream Workstreams™**	**JetStream Verfied MCP™**	**JetStream Zero Trust**	**JetStream Risk Assurance**	**JetStream FinOps**	**JetStream AI Kill Switch™**

JetStream Clearance Reasoning Engine

req/resp guardrails	credential mgmt	MCP proxy	model routing	model failover	rate limits	semantic caching	token counter

AI Gateway Basic Functions

The gateway **moves the request.** Clearance **decides whether it should move at all.**
The control plane is **both halves, working from one picture.**

© 2026 JetStream Security, Inc. All rights reserved

How the loop works

Basic AI gateways fly blind. A Control Plane closes the loop.

Four stages, running continuously, evaluating everything your agents do.

Control

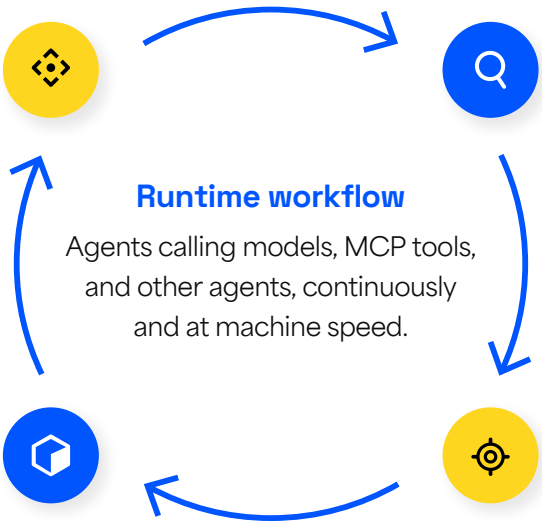
Real-time enforcement

Applied inline as live policy. Revoke, downshift, or stop.

Discover

Know what exists

Endpoint workload discovery. Every agent, model, tool, and dataset.



Reason

Decide in context

Every action evaluated against the approved design, before it executes.

Define

Approve how it should behave

The approved design of record for every agentic system, versioned.

What the runtime does is observed in the Blueprint. What the Blueprint knows informs every Clearance decision. What Clearance decides, the gateway enforces. The loop runs continuously, so policy is never older than the system it governs.

STATE 1 Access	STATE 2 Stage	STATE 3 Drift	STATE 4 Exfiltration
`[query_crm]` Customer renewal data accessed	`[create_email]` + `[attach_file]` Confidential data prepared for approved recipients	`[send_email]` New external BCC introduced	`[send_email]` Confidential attachment + unauthorized external BCC
✓ ALLOW + track sensitive context	✓ ALLOW + tighten outbound policy	⚠ HIGH RISK	⊘ BLOCK

The Governance Gap, Measured.

Benchmark you AI program with 40 questions. One clear picture of where your AI estate is governed and where it's running on trust alone.

For more information about JetStream Security

FedRAMP™

© 2026 JetStream Security, Inc. All rights reserved

This version supersedes all previous versions. The information contained in this document is provided for informational purposes only and does not constitute legal, compliance, financial, investment, or professional advice. The views and opinions expressed herein are those of JetStream Security, Inc. and do not necessarily reflect the positions of any affiliated entities, partners, or clients.

v1-08.31.2026

5201 Great America Parkway
Suite 346
Santa Clara, CA 95054
go.jetstream.security | sales@jetstream.security