



JetStream AI BlueprintsTM

Making enterprise agentic workflows visible,
attributable, and governable.

A product briefing from JetStream Security Inc.

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

v2-260318

© 2026 JetStream Security, Inc. All rights reserved

Table of Contents

Governance is a Key AI Pillar	03
What Are JetStream AI Blueprints™?	03
Why Blueprints Matter	04
The Prerequisite: JetStream AI Manifest™	05
How JetStream AI Blueprints™ Are Created	06
Continuous Monitoring and Drift Detection	07
Governance, Security, and Compliance Outcomes	07
Putting It Together: The JetStream Control Outcomes	08
Use Cases and Example Scenarios	08
Closing Summary	09
About JetStream Security	09

Governance is a Key AI Pillar

Executives everywhere are confronting the same emerging risk: AI is now acting autonomously across their business. **However, leadership often lacks a clear line of sight into what it's doing, why it's doing it, and who is accountable.**

As agents trigger actions across systems, tools, datasets, and identities, traditional oversight breaks down. AI is creating real exposure during audits, incidents, and board reviews. Furthermore, legal and compliance teams are often not fully considering the impact of AI on legal, compliance, and data privacy. Leaders aren't worried about AI's potential; they're worried about **losing control and being held responsible** for behavior they can't fully see, explain, or govern.

The lack of trust in AI is a major barrier to its successful production-level adoption. **JetStream AI Blueprints™** enables operational trust by revealing the inner workings of the who, what, when, and how of AI so teams can govern agentic workflows with confidence.

GPUs aren't the blockers to scaling AI. The blocker is AI-aware governance.

Unclear ROI, security compliance, data quality, and integration—each solvable with modern AI governance—are the top reasons only 17% of enterprises currently operate AI at scale.

UBS AI Research, Dec 2025

What Are JetStream AI Blueprints™?

JetStream AI Blueprints™ are dynamic, system-generated groupings of all resources that are working towards a common purpose or goal. Blueprints synthesize and track how AI operates in your environment at any given moment. Each Blueprint maps the dependencies among agents, the models they invoke, the datasets they touch, the tools and services they call, and the identities under which actions occur whether that be human, agentic, or non-human.

Unlike static, often stale architecture diagrams, Blueprints are grounded in observed runtime behavior. They dynamically update as your environment changes, so operations, security, and compliance teams can rely on them as an up-to-date source of truth. In short, a Blueprint is the **operational contract** for an AI workflow making behavior visible, attributable, and governable.

Why Blueprints Matter

Agentic AI changes quickly. Tools are chained on the fly. Models are swapped. New data sources appear. And people hate to document. Without a dynamic map, it's hard to answer basic questions: **What ran? Who initiated it? What data did it use? Did it follow the rules? How do I fix something that did not produce the right results? What did it cost?**

Blueprints solve this by giving precise, shared context. Security sees the boundaries to enforce. Engineering sees the reality of execution. Compliance gets lineage that stands up to scrutiny. Most importantly, **leadership can let teams move faster** because there is a clear baseline and an automatic way to spot when behavior strays beyond its approved authority. Blueprints also capture per-blueprint cost data, giving leadership direct visibility into what each AI workflow is actually spending.

Blueprints dynamically document AI workflows and answer critical question including:

- What did it do?
- What did it touch?
- Did it exceed its authority?
- Did it stay within budget?



The Prerequisite: JetStream AI Manifest™

You cannot map a workflow until you know what exists. The JetStream AI Manifest™ provides that foundation. It maintains a live catalog and registry of agents, AI-enabled apps, models, datasets, identities (human, agentic, NHI), MCP servers, and JetStream browser extensions. It also tracks ownership and relationships, so every asset is tied to an accountable identity via **JetStream Identity Broker™**.

With the Manifest in place, Blueprints have reliable building blocks. **The Manifest supplies the parts; Blueprints assemble those parts into the true picture of behavior.** This sequence is intentional: **inventory first, governance map second.**

Together, Manifest and Blueprints create a clear progression of AI activities:

See → Understand → Enforce → Prove

The JetStream SAIG™ Platform regularly introduces new integrations.



AWS



Azure



GCP



Microsoft Entra ID



Okta



GitHub



OpenAI



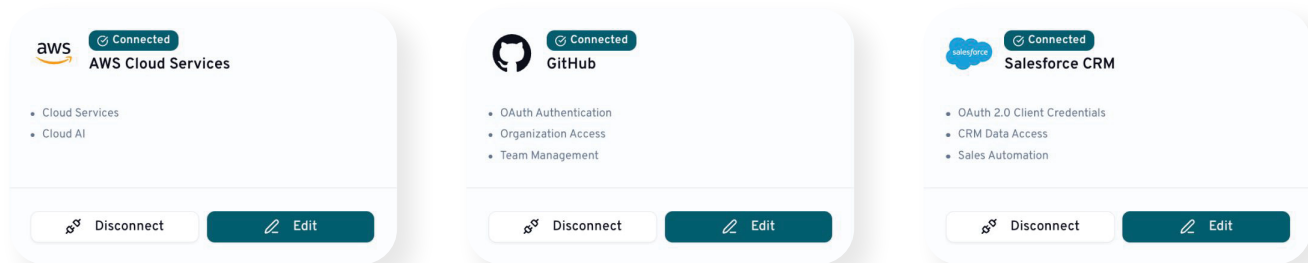
Hugging Face



Salesforce

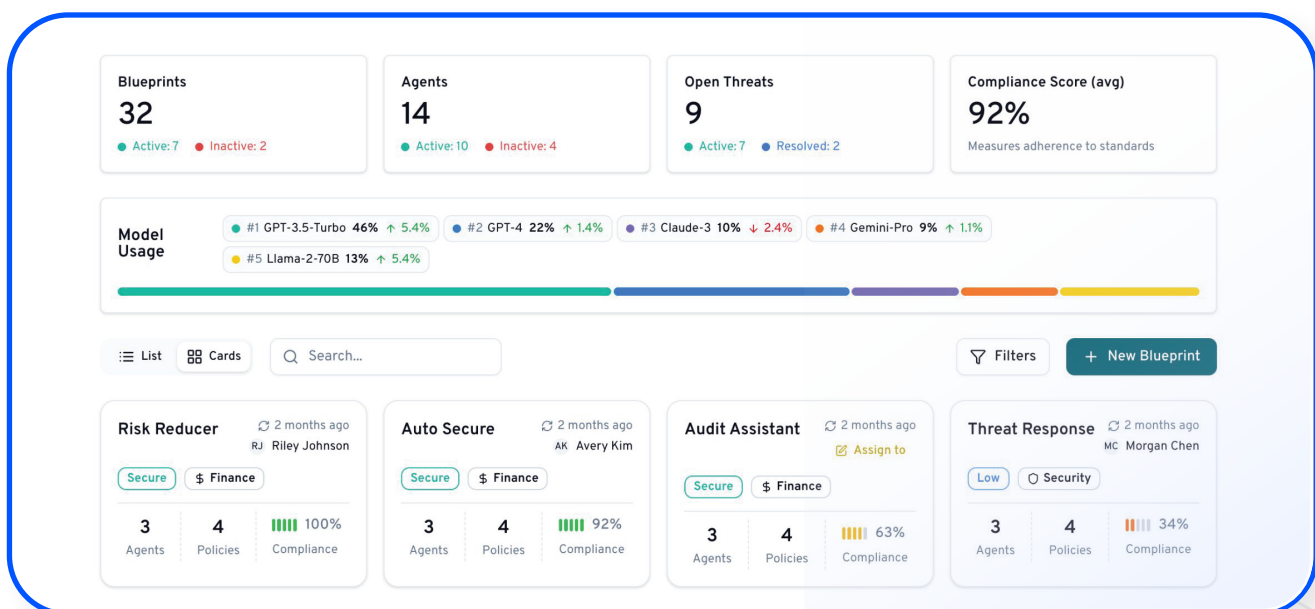
How JetStream AI Blueprints™ Are Created

JetStream integrates with **AI model providers, EDR products, SaaS and cloud providers, identity systems, MCP servers, and the JetStream enterprise browser extension.**



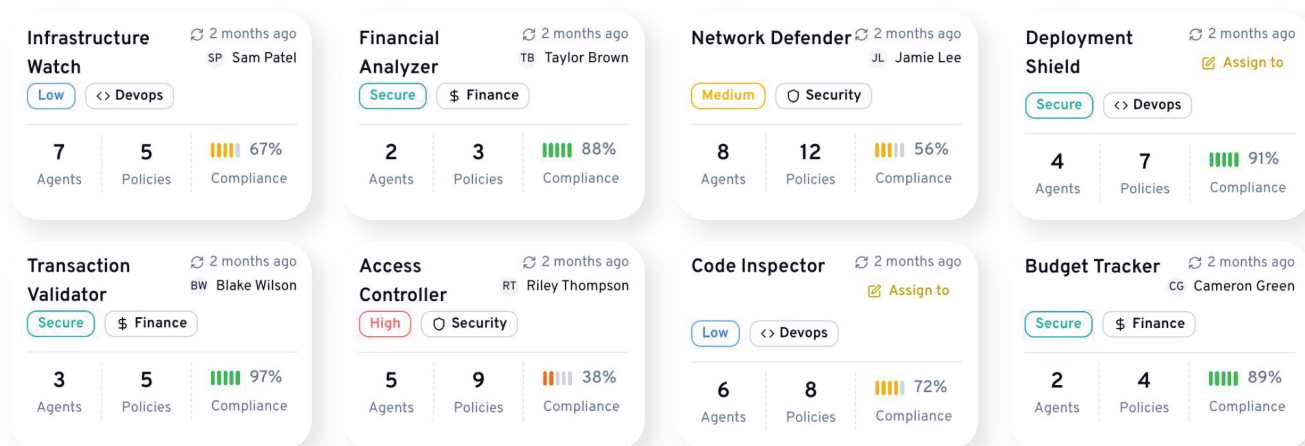
That telemetry first enriches the Manifest. The Blueprint engine then synthesizes events into coherent workflows to document each agent:

- 01 Correlate runs** to link related calls and actions into an end-to-end sequence.
- 02 Resolve relationships** to bind agents to models, datasets, tools, and identities.
- 03 Construct graphs** to render nodes (assets and identities) and edges (flows and decisions) backed by time-stamped evidence.
- 04 Establish a baseline** to capture the approved pattern of behavior for governance and future comparison.



Continuous Monitoring and Drift Detection

Once a baseline exists, **JetStream AI Drift Detection™ watches for divergence**. Drift is flagged when actual execution deviates from the Blueprint in meaningful ways. Examples include an agent touching an unapproved dataset, calling a tool that isn't in the plan, switching identities unexpectedly, using an unapproved model, chaining systems across organizational boundaries, or exceeding its per-blueprint cost threshold.



Drift alerts are specific and actionable. They show the step that changed, the identity under which it happened, and the assets involved. Teams can **review, approve a change into the baseline, or block it through policy without guesswork**.

Governance, Security, and Compliance Outcomes

Blueprints turn visibility into outcomes that matter day-to-day:

Audit-ready lineage

Every step is explainable and attributable.

Identity accountability

Actions map to human heartbeats, agents, or NHIs.

Regulatory alignment

Lineage, ownership, and change tracking support frameworks including the NIST AI RMF, EU AI Act, ISO 42001, and OWASP.

Runtime safety

The **JetStream AI Hub™** enforces what the Blueprint allows and prevents agentic overreach.

Operational clarity

Troubleshooting and change reviews start from a shared, accurate view of reality.

FinOps accountability

Cost tracking per Blueprint and owner.

Putting It Together: The JetStream Control Plane

JetStream provides a coherent control plane for enterprise AI:

AI Manifest™

gives complete, current visibility of assets and identities.

Identity Broker™

keeps every action tied to an accountable identity.

AI Hub™

enforces policies inline so workflows stay within bounds.

AI Blueprints™

translate that visibility into a live map of approved behavior.

Key Broker™

issues identity-bound, revocable virtual keys.

AI Drift Detection™

compares reality to the Blueprint and raises precise alert.

This stack lets organizations adopt AI quickly while maintaining control and confidence.

Use Cases and Example Scenarios

Unexpected data access

A support agent begins querying a financial dataset. This action was not previously approved. The Blueprint highlights this new situation in the workflow and raises a drift alert. Security reviews and blocks the change at the AI Hub while engineering investigates intent.

Model substitution

A team tests a different foundational model in production without updating approvals. This situation deviates from the baseline. The event is flagged. Leadership can decide whether to accept the change or revert. When accepted, JetStream tracks the change as a new version of the Blueprint, maintaining a history of the workflow's evolution.

Toolchain expansion

A developer introduces an unapproved MCP server into an agent flow. The new dependency appears in the Blueprint, which triggers a review. If approved, it's added to the baseline with clear ownership.

Budget Overrun

A workflow surpasses its approved token budget. JetStream flags the overrun, maps it to the responsible Blueprint, and alerts the owner.

These scenarios follow a repeatable pattern:

Manifest inventory



Blueprint mapping



Drift alert



Policy action

Closing Summary

JetStream AI Blueprints™ give enterprises the operational truth about how AI behaves.

JetStream AI Manifest™ ensures that truth rests on complete and current inventory.

Together with **AI Drift Detection™**, **AI Hub™**, **Identity Broker™** and **Key Broker™**, JetStream provides the visibility, control, and accountability required to **scale AI responsibly**.

About JetStream Security



JetStream makes AI governable at enterprise scale by providing unified visibility and control across all AI activities so that AI becomes a managed asset, not an unmanaged liability.

Our Mission

**Accelerate Enterprise
AI Adoption**

The Result

**Governance enables trust. Trust unlocks advantage.
Governance → Trust → Advantage**

Contact us at sales@jetstream.security



For more information about
JetStream Security

This document's version supersedes all previous versions. The information contained in this white paper 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.



© 2026 JetStream Security, Inc. All rights reserved

go.jetstream.security | sales@jetstream.security

v2-260318
5201 Great America Parkway
Suite 346
Santa Clara, CA 95054