

# Mission Possible: Enforcing Zero Trust for AI Workloads



AI is revolutionizing business...but also making it difficult to enforce zero trust principles. Protecting these powerful new AI workloads means rethinking zero trust from the ground up.

## Why It Matters

AI workloads don't run in silos—they depend on distributed, dynamic cloud infrastructure in order to function. This dynamic infrastructure includes new data pipelines, model training flows, inter-cloud API calls, and compute clusters spanning regions and providers. These aren't just new workloads but entirely new traffic patterns, often hidden from or neglected by traditional security tools.

For CISOs, this creates an urgent blind spot: AI projects can rapidly access, process, and move sensitive data ... all without the visibility, segmentation, or enforcement needed to stay compliant and secure. When zero trust policies stop at the login screen, AI becomes an oversight that can quickly accelerate across the cloud.

Only **14%**

**of organizations  
are confident  
they have the  
right people and  
skills needed in  
the face of rapid  
AI adoption**

WEF

## New Research Shows

- **90% of companies** have either implemented AI or plan to do so this year ([Aviatrix](#))
- **Only 54%** of respondents believe their organizations **have responsible AI policies in place**, and 25% think **no such policies exist** ([KPMG](#))
- **Only 14% of organizations are confident** they have the right people and skills needed in the face of rapid AI adoption ([WEF](#))
- And **47% of organizations leverage public cloud for AI data storage**—where east-west traffic often goes unmonitored and uncontrolled ([Flexential](#))

These gaps leave room for unregulated lateral movement, unauthorized data access, and policy violations, with limited logging or observability to investigate if something goes wrong.

Whether training sensitive AI agents, handling regulated data, or running inference at scale, AI initiatives must align with enterprise zero trust standards in order to prevent potential blind spots.

## What's At Risk:

- Unmonitored east-west traffic can expose sensitive training data or model IP
- Cloud-native AI services (like LLMs and GPU clusters) often bypass existing controls
- Lack of runtime enforcement and visibility leaves CISOs liable for blind-spot breaches
- Lack of microsegmentation of resources allows AI agents to access resources without regulation
- Regulatory scrutiny is intensifying to set AI monitoring and control paths in orgs—from the EU AI Act to internal board oversight

### A CISO's Perspective: Before and After Zero Trust for AI

#### Before

The CISO sees AI exploding across their org—but without the controls to govern it. Projects spin up in the cloud with minimal oversight. There's little clarity on what data's being used, where it flows, or who can access it. They worry about shadow AI use, sensitive data exposure, and the inevitable board question: "Are our AI systems secure?"

#### After

With Aviatrix, the CISO gains real-time visibility and policy enforcement across all AI infrastructure. Every project—whether it's training a model or making live predictions—automatically inherits zero trust guardrails. The CISO can track data flows, block policy violations, and prove compliance. Now, they greenlight innovation with confidence—and show up at board meetings as a forward-thinking, risk-aware leader.

## Aviatrix Makes AI Workloads Zero Trust by Design

Aviatrix embeds security directly into the network fabric instead of bolting on individual point solutions, so AI infrastructure gets zero trust protection automatically.

That includes:

- ✓ Real-time visibility into east-west flows between AI clusters and data stores
- ✓ Segmentation and access enforcement across clouds, regions, and APIs
- ✓ Runtime control for cloud-native services, including GPU farms and ML pipelines
- ✓ No reliance on CSP-native tools that can't see or stop lateral movement

**Ready to See  
AI Security  
in Action?**

Request a demo to see how we help secure AI infrastructure across every cloud.

**Request Demo**

### About Aviatrix

For enterprises struggling to secure cloud workloads, [Aviatrix](https://www.aviatrix.com)® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit [www.aviatrix.com](https://www.aviatrix.com).