AVIATRIX®

FAST FACTS

Aviatrix Zero Trust for Workloads

The Problem

Traditional security relied on a trusted perimeter, but the cloud erased that boundary, making zero trust—"never trust, always verify"—essential. While this approach has gained traction in concept, there are still obstacles standing in the way of practical execution:

- Most implementations secure network access (north-south) but ignore workload communication (east-west), leaving intra-cloud traffic unchecked.
- Cloud providers offer siloed controls, not cross-cloud visibility.
- East-west traffic often goes unseen, enabling lateral movement and data exfiltration.
- Encryption is inconsistent, creating exploitable blind spots.
- Dynamic Kubernetes and serverless workloads bypass static controls.

These gaps not only expose vulnerabilities but also hinder compliance with regulations like HIPAA, PCI DSS 4.0, DORA, NIS2, and ZTMM 2.0, which demand proof of zero trust enforcement.

How Aviatrix Enables Zero Trust for Cloud-Native Workloads

Aviatrix Zero Trust for Workloads delivers runtime zero trust enforcement for every workload—virtual machine, container, and cloud native or serverless service—across every major cloud. It extends protection beyond traditional compute to cover dynamic environments, such as AWS Lambda, ECS, Azure Functions, and GCP Cloud Run, where workloads are short-lived, highly distributed, and often invisible to perimeter- or agent-based tools.

With Aviatrix, you can

- Unify visibility, inline control, and audit-ready proof at runtime.
- Secure the parts of the cloud where traditional firewalls and posture tools can't reach.
- Enforce security consistently across clouds and cloud-native environments.

All of this is accomplished without agents, re-architecture, or developer disruption.

Key Capabilities

Aviatrix Cloud Firewalling	Inline enforcement for east-west and egress traffic through gateways positioned in existing cloud paths.
Inline Threat Prevention	Built-in intrusion prevention capabilities detect and block exploit traffic, malware, and command-and-control (C2) activity in real time.
SmartGroups and Identity-Based Policies	Dynamically group workloads by metadata, tags, namespace, or cloud service identity for adaptive policy accuracy.
CoPilot Visibility and Compliance	Real-time telemetry and policy monitoring mapped to ZTMM 2.0 and major frameworks.
High-Performance Encryption (HPE)	Line-rate, scalable encryption for cloud workload traffic (east-west, north-south, and cloud-to-cloud) with audit-ready telemetry and sub-second failover.

Why It Matters

Contain lateral movement: Block unauthorized east-west traffic.

Prevent data exfiltration: Stop malicious outbound flows before data leaves the cloud.

Accelerate zero trust maturity: Advance CISA ZTMM Network and Data pillars.

Secure cloud-native architectures: Protect Kubernetes and serverless without developer friction.

Eliminate workload egress blind spots: Detect and block runtime exploit traffic.

Demonstrate continuous compliance: Produce audit-ready evidence aligned with standards and regulations.

Get started now: **Schedule a Demo**

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® 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.ai.