AVIATRIX

CHECKLIST

Five Zero Trust Blind Spots That Put Your Cloud at Risk – and How to Eliminate Them

You've implemented zero trust for users–authentication, verification, segmentation–but that's just the beginning.

Your crown jewels - the applications and data driving your business - live in dynamic, multicloud environments that demand a different level of protection.

Extending zero trust to the cloud introduces critical blind spots–especially when it comes to zero trust for workloads. Here are five pitfalls to watch for before attackers find them first.

1. **Poor Segmentation:** Flat or loosely segmented cloud networks allow attackers to move freely. A small breach can escalate into a full-blown compromise before it's even detected.

2. **Inconsistent Controls:** With every cloud platform offering different native security models, it becomes nearly impossible to prove consistent enforcement. Compliance with frameworks like HIPAA, PCI DSS, or NIST 800-53 becomes a manual, high-risk effort.

3. **Tool Sprawl:** Juggling multiple security consoles, inconsistent policies, and vendor-specific tooling slows down your team and increases the likelihood of misconfiguration.

4. **Security Bottlenecks:** Application teams wait for approvals. VPNs can't scale. Firewalls aren't cloud-native. Security becomes a blocker–right when your business needs speed.

5. **Identity-Only Focus:** Most zero trust efforts stop at the identity layer. Without protection for east-west and egress traffic, your most sensitive workloads are left open to internal threats and exfiltration.

Enforce Zero Trust for Workloads—Across Any Cloud.

The **Aviatrix Cloud Network Security Platform™** enforces zero trust for workloads across multicloud environments–delivering the intelligent, secure network foundation that other tools simply don't reach.

We eliminate blind spots and deliver the visibility, protection, and agility you need to:

Contain Breaches Instantly: Stop lateral movement cold with identity-aware micro-segmentation. Dynamically isolate workloads based on cloud tags, attributes, and service identity–without relying on static IPs.

Simplify Compliance: Gain provable, audit-ready segmentation and encryption policies across clouds. Meet mandates from HIPAA, PCI DSS, and NIST 800-53–and align with the CISA Zero Trust Maturity Model 2.0.

Unify Multicloud Zero Trust: Eliminate policy drift with a centralized security control plane for AWS, Azure, GCP, OCI, and more. Apply consistent zero trust enforcement using Terraform, APIs, and CI/CD pipelines.

Secure at Cloud Speed: Automatically enforce policies in real time, based on workload identity and metadata. Integrate with DevOps pipelines to deliver security at the speed of cloud.

Protect Your Crown Jewels: Secure the internal traffic paths that identity solutions miss. Enforce encryption and segmentation for east-west and egress flows–protecting your apps and data from internal threats and data exfiltration.

Bottom Line: Most zero trust programs stop at the user. Aviatrix picks up where they leave off–embedding zero trust for workloads directly into your cloud network fabric. Architected for multicloud complexity, Aviatrix delivers the visibility, encryption, segmentation, and automation needed to build a complete zero trust strategy across all clouds.

Zero trust for workloads is here. Are you ready?

Learn More

Request a Demo

About Aviatrix

Aviatrix® is the cloud network security company trusted by more than 500 of the world's leading enterprises. As cloud infrastructures become more complex and costly, the Aviatrix Cloud Network Security platform gives companies back the power, control, security, and simplicity they need to modernize their cloud strategies. Aviatrix is the only secure networking solution built specifically for the cloud, that ensures companies are ready for AI and what's next. Combined with the Aviatrix Certified Engineer (ACE) Program, the industry's leading secure multicloud networking certification, Aviatrix unifies cloud, networking, and security teams and unlocks greater potential across any cloud.