AVIATRIX

One-Pager

Welcome to the Containment Era

THE INDUSTRY PROBLEM

We've reached a new era in cloud security. The cloud was designed to prioritize developer speed over security, and attackers are industrializing with AI tools. This Toxic Combination of factors makes AI workloads high-value targets that are nearly impossible to protect. These workloads are ephemeral enough to defeat agent-based defense, privileged enough to concentrate non-human identity risk, and shipped fast enough to outrun review.

How We Got Here: The Three Eras

The Perimeter Era (1990-2010)

Security teams build walls using firewalls, DMZs, and VPNs. Everything inside is implicitly trusted. The network had one perimeter.

The Detection Era (2010-2022)

When enterprises moved to the cloud, physical network perimeters dissolved. Security teams respond by specializing in threat detection and response through SIEM, EDR, XDR, and SOAR.

The Containment Era (2026-)

Detection tools alone cannot keep up with AI-accelerated attacks. Exploitable vulnerabilities are increasing, and attackers use legitimate credentials to perpetrate cascading supply chain attacks. Security teams can no longer protect data through detection alone: they must assume breach, contain, detect, and eliminate, in that order.

The Numbers: Why Detection is No Longer Enough

- Machine identities now outnumber human identities by 144 to 1. Many of them have excessive and unmonitored privileges, making them a hidden attack vector.
- AI has collapsed time-to-exploit from 771 days in 2018 to under a day in 2026.
- CISA KEV median time-to-exploit is now negative seven days, with known vulnerabilities weaponized before vendors disclose them.

When prevention fails and detection is too slow, containment decides whether the incident becomes a catastrophic breach. The ungoverned attack surface is not the endpoint, the perimeter, or the identity layer. Instead, it is the communication path between every workload, on every cloud where attackers can move laterally and exfiltrate data.

Aviatrix was built to protect that surface.

<1 Day	82%	27 sec
Mean Time to Exploit 2026	Breaches Use Valid Credentials	Fastest Breakout Observed

WHY AVIATRIX

Communication Governance at Every Workload

Aviatrix pioneered the Cloud Native Security Fabric (CNSF), the first platform purpose-built to govern every communication path in the cloud runtime. While posture tools find risk and SASE secures users, CNSF enforces policy inline at the workload.

Zero Trust for Workloads

Runtime microsegmentation and inline enforcement that stops lateral movement and data exfiltration at the workload level.

Zero Trust for Networking

Fabric-wide encryption and policy visibility across every VPC, VNet, region, and hybrid edge at up to 85 Gbps per gateway.

One policy plane. Universal propagation in seconds. No agents. No rip-and-replace.

WHAT SETS AVIATRIX APART

Five Properties Competitors Cannot Match

01 **Path-Complete:** Governs every communication path, including Kubernetes pod egress, serverless, VPC peering, and managed-service paths that bypass centralized inspection points.

02 **Identity-Aware at L7:** SmartGroups express policy in workload identity and application protocol, not IP and port, so enforcement survives cloud elasticity and workload re-creation.

03 **Detection-Independent:** Enforcement holds before, during, and after a breach without requiring the breach to first be detected. Blast radius is bounded by architecture, not alerting speed.

04 **Compute-Model Agnostic:** Agentless coverage across VMs, containers, serverless functions, managed databases, and AI agents. These are the workload categories growing fastest in 2026.

05 **Universally Propagated:** A single policy change enforces across AWS, Azure, Google Cloud, and on-prem Kubernetes within subseconds, not hours.

Built for the Cloud Runtime: Not Retrofitted for It

› Distributed Cloud Firewall
Inline east-west and egress enforcement through gateways in existing cloud paths. No traffic rerouting, no latency impact, no architecture change.

› SmartGroups & L7 Policy
Workloads grouped by metadata, tags, namespace, or cloud identity. Policy follows workload identity, surviving re-creation, scaling, and migration.

› High-Performance Encryption
Up to 85 Gbps per gateway, terabit-scale aggregation. Software-defined encryption for every path: east-west, north-south, cross-cloud, hybrid edge.

› AI Agents & AgentGuard
First network-layer enforcement substrate for Microsoft Agent Shield. Bounds blast radius of every AI agent in production across all clouds and on-prem Kubernetes.

› CoPilot Visibility
Real-time telemetry mapped to ZTMM 2.0 and compliance frameworks. AI-driven policy recommendations. Audit-ready enforcement evidence across every cloud.

How Aviatrix Compares

Capability	Others	Aviatrix
Governs all paths (incl. serverless)	Gaps	Path-complete
Agentless across compute models	Agent req.	No agents
Identity-based L7 policy	IP-based	SmartGroups
Detection-independent enforcement	Alert-dep.	Always-on
Sub-second universal propagation	Hours	Seconds
No rip-and-replace required	Often req.	Non-disruptive
AI agent governance (AgentGuard)	N/A	First to market

> "One Fortune Global 500 enterprise stopped the LiteLLM credential exfiltration in minutes with a single policy update, propagated across their entire cloud footprint. Same payload as 40,000 other environments. Different outcome, determined entirely by architecture."
>
> – Aviatrix Customer Reference, 2026

Schedule a demo

Discover how Aviatrix Cloud Native Security Fabric delivers the Containment Platform the era requires.

About Aviatrix

Aviatrix® is pioneering the Cloud Native Security Fabric – the architecture the Containment Era requires. The Cloud Native Security Fabric governs every workload communication path across every cloud, every VPC, every Kubernetes cluster, and every serverless function, from a single policy plane. One rule. Universal propagation. Enforced at the workload, not at a chokepoint. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.

BACKED BY

Leading enterprise technology investors
Strategic partnerships with AWS, Microsoft Azure, Google Cloud, and Oracle Cloud