AVIATRIX®

SOLUTION BRIEF

Aviatrix Cloud Native Security Fabric

The Containment Platform for Cloud Workloads

A New Security Paradigm for the Cloud

In early 2026, five major software ecosystems were compromised in twelve days. The attack used trusted packages, trusted channels, and trusted update mechanisms. The detection stack generated no alerts because trusted code executing in a trusted pipeline is not an anomaly. The architecture that most enterprises rely on was not designed for this Cascade of attacks.

That architecture has a name: Chokepoint Security. A centralized firewall in a transit VPC governs traffic that crosses it. Kubernetes pod egress, serverless functions, east-west VPC traffic, and policy propagation gaps all bypass it entirely. The Architectural Divide between workload deployment velocity and security enforcement capability grows wider with every new cloud account, every new container, every new AI agent.

The Containment Era demands a different answer. Containment is the architectural enforcement of explicit communication policy at every workload - governing what it can reach and what can reach it, at the granularity of workload identity and protocol - on every path available to it, independent of whether a compromise has been detected. Blast Radius, not detection speed, is the metric that determines whether an incident becomes a catastrophe. Aviatrix Cloud Native Security Fabric is the Containment Platform that closes the Architectural Divide.

Chokepoint Security	Communication Governance
Chokepoint Security governs traffic that crosses it	Communication Governance governs every path at every workload
Implicit trust zones, permissive by default	Default-deny enforcement across every path
Fragmented visibility across 76 tools	Unified policy and telemetry plane
Manual IP-based rules that drift as workloads scale	Identity-aware policy that follows workloads automatically
Ungoverned egress; Blast Radius limited by SOC speed	Blast Radius bounded by architecture before any alert fires

Per-cloud tool sprawl across every environment	One fabric across every cloud and region

The Containment Platform for Cloud Workloads

Aviatrix Cloud Native Security Fabric delivers a dynamic, real-time, policy-driven enforcement layer embedded inside a distributed cloud network. Every workload, on every path, is subject to explicit Communication Governance.

Communication Governance by Default

Aviatrix Cloud Native Security Fabric embeds distributed enforcement directly inside cloud native constructs. Every workload communication path is governed, including the Kubernetes pod egress, serverless function calls, and east-west VPC traffic that Chokepoint Security never sees. Blast Radius is bounded by architecture, not by the speed of your SOC.

Blast Radius Bounded at Every Workload

Default-deny Communication Governance means a compromised workload cannot reach anything it was not explicitly permitted to reach, because the path does not exist. The Fortune Global 500 enterprise that stopped the Cascade did so with one policy update, propagated to every VPC and every region simultaneously, before any detection tool flagged the compromise.

Continuous Audit Evidence

Aviatrix CoPilot captures every policy decision, flow, and topology change across clouds. Every DENY entry is a forensic record: which workload, which destination, what time. Security, risk, and compliance teams share one source of truth for policy and one audit trail for proof, mapped to CISA Zero Trust Maturity Model, NIST CSF, HIPAA, DORA, GDPR, and NIS2.

Constant Readiness through Resiliency

The high-availability data plane, active-active architecture, backup and restore options, telemetry, and logging keep the fabric operational under traffic surges, regional failures, and cyberattacks. Policies stay enforced even when infrastructure is under pressure.

Streamlined Operations

Centralized management and Infrastructure as code integrations remove manual processes for DevOps and architecture teams. Policy is defined once and propagated universally in subseconds. No per-firewall commit cycles. No manual rule updates when workloads scale.

Cost Efficiency and Optimization

Cloud Native Security Fabric consolidates networking, security, and observability onto a single platform, eliminating the tool sprawl that compounds the Fragmentation Gap. FinOps teams gain governance over cloud spending with advanced routing controls, flat-rate pricing, and predictable billing.

The Architectural Divide and How Cloud Native Security Fabric Closes It

Cloud infrastructure operates on implicit trust by default. When you deploy a workload on AWS, Azure, or GCP, the initial security posture is open. Every new workload type adds a new egress path. Every new cloud account is a potential policy drift point. Security teams that inherited this infrastructure face three compounding gaps:

The Fragmentation Gap. The average enterprise manages 76 distinct security tools with no unified policy plane. Shadow workloads and shadow AI operate ungoverned. Lateral movement finds the seams between tools.

The Runtime Enforcement Gap. Posture management tools scan and advise. They do not sit in the data path and stop a threat in motion. Visibility without inline enforcement is a monitoring strategy, not a Containment Era architecture.

The Ownership Gap. Platform engineering, application teams, security teams, and cloud operations each own a piece of the stack with no shared enforcement plane.The first thirty minutes of an incident are spent determining which team owns the workload.

Chokepoint Security governs the traffic that crosses it.
Communication Governance governs every path.

Aviatrix Cloud Native Security Fabric addresses all three gaps at the architecture level, with runtime enforcement, simplified management, and centralized control embedded in the cloud fabric itself.

- Communication Governance for north-south and east-west traffic to bound Blast Radius and prevent lateral movement from spreading
- Unified visibility and control to detect anomalies and investigate potential threats in real time, with every flow attributable to a workload, policy, and timestamp
- Distributed and dynamic policy enforcement that propagates universally in subseconds from a single control plane
- High-performance Encryption based on a patented IPSec model that delivers security and performance at up to 100 Gbps
- Unity for security, networking, and DevOps teams through Infrastructure as Code automation and enforcement that is transparent to developer workflows

> **The Aviatrix Cloud Network Security platform intelligently programs the native cloud network constructs and goes well beyond that by adding network segmentation policies, rich visibility, and automation that we require to support our customers. Aviatrix makes cloud networking much easier for us and our customers."**
>
> - John Goodson
> SVP And General Manager
> Of Products, Verint

One Fabric. Any Location. Any Cloud.

Aviatrix Cloud Native Security Fabric delivers advanced networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers natively. Aviatrix software leverages public cloud provider APIs to interact with and directly program native cloud networking constructs, abstracting the unique complexities of each cloud to form one network data plane with Communication Governance enforcement at every workload.

Security Teams

Govern what every workload can reach, not just what enters the perimeter

- Apply Communication Governance to workload-to-workload and egress traffic to bound Blast Radius
- Enforce consistent policy across all clouds, accounts, and regions from one control plane
- Encrypt all data in motion at cloud scale and performance
- Gain visibility into hidden attack paths with deep traffic flow intelligence

Network Teams

Architect for containment, not just connectivity

- Build high-availability multicloud transit with enterprise-grade routing and resiliency
- Control traffic flows with intelligent policy enforcement and route intelligence
- Eliminate cloud native networking limitations like source network address translation and asymmetric routing
- Visualize, troubleshoot, and optimize global traffic from a single control plane

DevOps and Platform Engineering Teams

Ship fast without sacrificing containment posture

- Automate cloud network and security deployment with a unified Terraform provider
- Detect and resolve performance bottlenecks with full-stack observability
- Empower developers with secure, self-service infrastructure and security guardrails
- Standardize infrastructure as code across every cloud environment

Aviatrix CoPilot

Day-two operations across every cloud

- Cloud network flow analysis and geographical source-destination heat maps
- Time series traffic analysis to identify flow anomalies
- Communication path evaluation to verify policy enforcement and compliance posture
- Continuous compliance evidence mapped to CISA Zero Trust Maturity Model, NIST CSF, HIPAA, DORA, and NIS2

Simplified, Embedded, and Scalable by Design

Aviatrix Cloud Native Security Fabric embeds Communication Governance directly into the network layer. No agents. No bolt-ons. Unlike legacy models that rely on edge firewalls or third-party enforcement tools, it delivers real-time, inline policy enforcement that travels with the workload across every cloud and region.

Embedded in the fabric

Communication Governance policies live inside the infrastructure itself. Enforcement is not a sidecar or a bolt-on. Every workload communication path is governed where the workload runs.

Dynamic and distributed

Policy follows workloads automatically as they scale, move, or are replaced across clouds and availability zones. No stale access control lists.

Pervasive by default

Covers cloud, data center, and edge environments, including rapidly scaling AI workloads. The 144-to-1 machine identity ratio is governed by architecture, not by exceptions.

Agentless and inline

No software agents to deploy, no performance overhead, no reliance on legacy appliances. The fabric enforces policy in the data path.

Developer transparent

No application code changes required. Containment architecture is embedded in infrastructure without breaking developer workflows.

Real-time enforcement

Policies are evaluated and enforced as traffic flows. Every DENY is logged, attributable, and audit-ready.

Aviatrix AgentGuard: Shadow AI Discovery and AI Workload Governance

Aviatrix AgentGuard extends Aviatrix Cloud Native Security Fabric into AI agent infrastructure, discovering every AI workload in your environment from the network itself rather than waiting for developers to instrument it. This enables security teams to see and govern the 144 machine identities that exist for every human in the enterprise, including the AI agents, large language model API consumers, MCP servers, and retrieval-augmented generation pipelines that code-based tools miss entirely.

- Discovers every AI workload via network flow analysis, DNS inspection, and Cloud Asset Inventory integration, with no gateway, no agent, and no code changes required
- Surfaces a risk-scored inventory of every large language model consumer, MCP server, and cloud native AI service in minutes, with shadow AI flagged and ready for policy targeting
- Feeds discovered workloads directly into Communication Governance enforcement via Zero Trust for AI Workloads on the same Aviatrix fabric
- Complete your first AI workload inventory in fifteen minutes, no gateway required
- Quantify shadow AI exposure for the board with a risk-scored executive dashboard
- Move from discovery to default-deny enforcement on the same fabric, the same day

Aviatrix Zero Trust for AI Workloads: Default-Deny AI Egress, Across Every Cloud

Every AI agent interaction traverses the network, which makes the network the only universal control point for AI governance. Aviatrix Zero Trust for AI Workloads delivers default-deny, network-layer enforcement for every AI workload using Aviatrix-managed AI WebGroups and SmartGroups, governing which large language model providers, MCP servers, and vector databases each workload can reach across AWS, Azure, GCP, and OCI with no code changes, no SDK integration, and no TLS decryption required.

- Enforces default-deny AI egress via Aviatrix-managed AI WebGroups covering every major large language model provider, MCP platform, vector database, and agent framework, updated centrally so enterprises never maintain domain lists manually
- Uses SmartGroups to identify workloads by Kubernetes pod label, cloud tag, Lambda ARN, or Bedrock Agent identity, so policy follows the workload as it scales or moves rather than chasing IP addresses
- Stopped the Cascade in production at a Fortune Global 500 customer: four IP addresses, one engineer, zero credentials exfiltrated, with universal propagation across every VPC, every region, and every Kubernetes environment simultaneously

- Blocks shadow AI at the network layer, including workloads that bypass every application-layer gateway
- Contains compromised AI agents before they reach anything they were not explicitly permitted to reach
- Produces continuous audit evidence for EU AI Act, SOC 2, HIPAA, and PCI-DSS from every AI egress decision logged in CoPilot

Try Aviatrix Cloud Native Security Fabric Today

Schedule a demo or sign up for a free security assessment

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.