

Aviatrix Clearance

Aviatrix Clearance gives every cloud workload clearance for the paths it needs and nothing else. It is the security offer on the Aviatrix Containment Platform, built on the Cloud Native Security Fabric.



The Exposure: Egress without Firewalls

Cloud workloads reach the internet on paths no firewall governs. In a Cybersecurity and Infrastructure Security Agency red team assessment of a large critical infrastructure organization, most servers, including domain controllers, allowed unrestricted outbound internet access, and the organization never detected the red team. Ransomware command and control, data theft and lateral movement all use these outbound paths.

JPMorganChase's technology leadership said aggressive filtering of outbound traffic from production systems "would have substantially mitigated the impact of incidents like Log4Shell, SolarWinds, and numerous supply chain compromises."

“

When prevention fails and detection is too slow, containment decides whether the incident becomes a catastrophic breach.

”

Why This Gap Remains Open

Every CISO knows the asymmetry: a breach that followed the playbook is survivable, but a firewall rule that breaks a revenue application often is not. So firewall rule changes can wait weeks for a change window. Chokepoint Security governs only the traffic routed through it. Meanwhile, a Toxic Combination of three forces are converging: industrialized attackers, AI that puts frontier offensive capability in millions of hands, and a cloud that is insecure by default.

29 min

Average eCrime breakout time in 2025 (CrowdStrike).

6.5x

More patch tickets closed, yet critical flaws open at day seven rose from 56% to 63% (Qualys).

144 : 1

Machine identities per human identity (Entro Labs).

The math has already decided. Attackers now begin exploiting a vulnerability an estimated seven days before its patch exists (Google Cloud, Mandiant, M-Trends 2026). You cannot patch or detect your way out. The only lever left is governing what every workload can reach, before anything is detected.

Aviatrix Clearance: Containment That Doesn't Break Production

Aviatrix Clearance restores control without breaking production or threatening developer velocity in four steps: **See, Insert, Enforce, Operate**.

Most teams start in monitor mode. The Shadow Rule Set produces the would-block report, showing what a policy would block on live traffic before anything is enforced.

1

See

The free Containment Assessment shows every workload, every path and what a compromise could reach.



2

Insert

One setting per virtual private cloud (VPC), with no agents, no network redesign, and one-action Backout. Most teams start in monitor mode, where the Shadow Rule Set produces the would-block report on live traffic before anything is enforced.



3

Enforce

Rules move to enforcement one at a time, one VPC at a time. Policy follows workload identity instead of IP addresses.



4

Operate

Active Defense keeps clearance current as the estate changes, inside guardrails your team sets.

Clearance is two controls and an autonomous defense layer, bought together or in any order. Outbound Containment for paths out of the estate, Lateral Containment for paths to anything else inside it, and Aviatrix Active Defense, the layer that keeps the clearance current as the estate changes.

AI agents are the hardest workloads to contain and the most valuable to reach. They are ephemeral, highly privileged, and shipped faster than security can review them. AI agent discovery and containment runs inside both controls at the agent grain, so each agent is cleared for its own job rather than its neighbor's. IBM found that 92% of organizations reporting an AI-related breach lacked proper AI access controls.

A Metric You Can Bring to the Board: Reachable Value at Risk

If a workload is compromised, you can state what it can reach, show the limit is enforced and logged, and size the exposure in dollars as Reachable Value at Risk, with outbound and lateral exposure reported separately. So ask the question your board will: if a valid credential is used against one of your workloads when no one is watching, what, architecturally, stops it from reaching your most valuable data?

Start Free, With No Time Limit

The Containment Assessment Phase 1 Self-Score takes about five minutes and returns a provisional Blast Radius. Phase 2, the Architecture Read, is read-only and agentless, measured from your production flows. Aviatrix Clearance has a Free Tier. It includes a free Containment Assessment and 15 workloads you can run in monitor or enforce mode, with no purchase and no time limit. Contact Aviatrix for pricing.

**See your provisional Blast Radius with a
free Containment Assessment.**

About Aviatrix

Aviatrix® is the network containment company. The Aviatrix Containment Platform sets what every cloud workload may reach before any attack, so a compromised workload does not become a company-wide breach. Built on the Cloud Native Security Fabric, it enforces that policy in the network, at every workload and in every cloud, with nothing to install and nothing to detect first, and encrypts the traffic it allows. It is simpler, safer, faster and less costly than the firewalls and agents it replaces. The Cloud Native Security Fabric is quantum safe. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.