

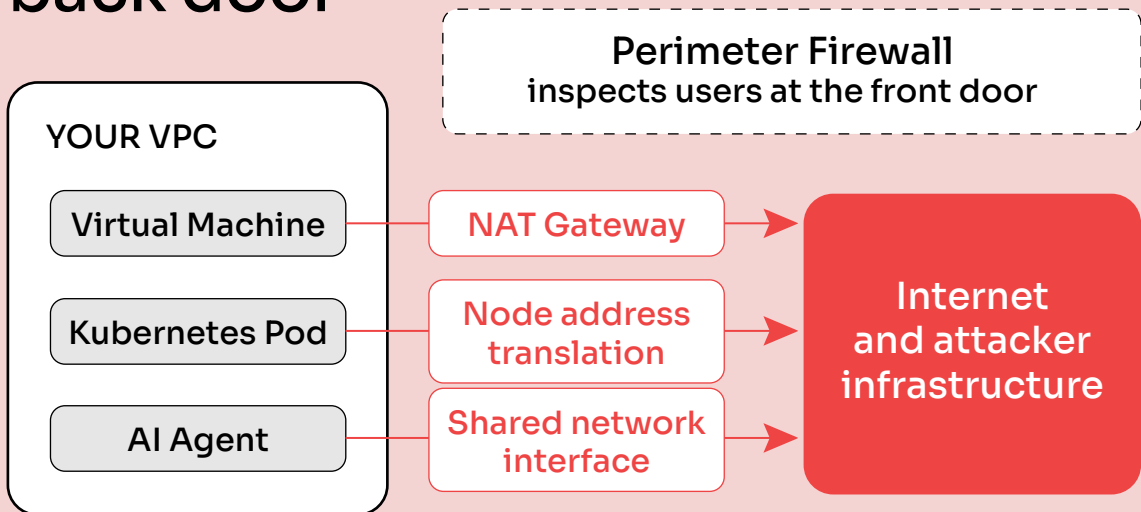
Nothing Leaves Without Clearance

Every cloud workload gets clearance for the paths it needs and nothing else, with no network redesign and no impact on production.

WKLD-API → payments.api	CLEARED
POD-7F → 203.0.113.9	DENIED
AGENT-12 → model.provider	CLEARED

THE PROBLEM

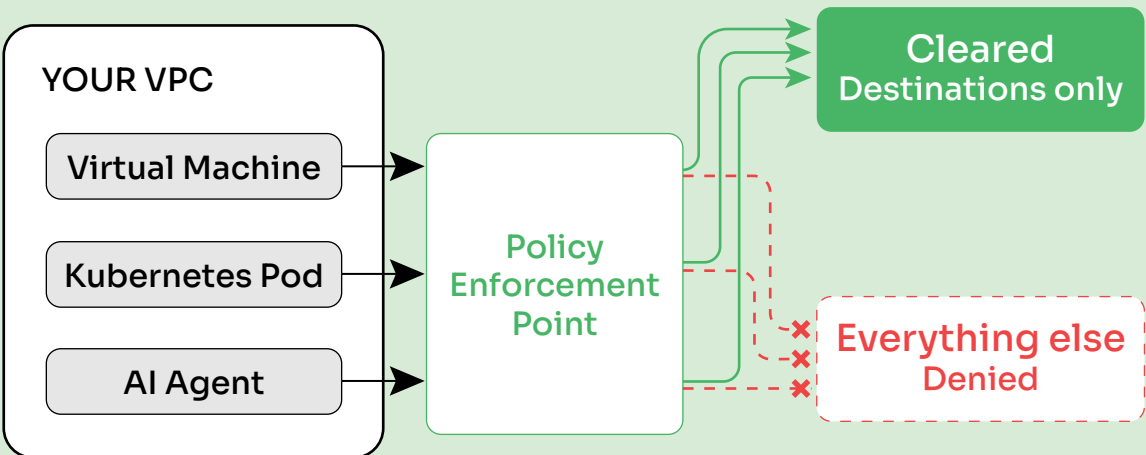
Workloads leave by the back door



Ransomware command and control, data theft, and lateral movement use these outbound paths. A chokepoint governs only the traffic routed through it.

THE SOLUTION

Every exit is cleared or denied



Policy follows workload identity instead of IP addresses. One toggle per virtual private cloud (VPC), no agents, and one-action backout.

WHY THE GAP STAYS OPEN

3 months

A federal red team spent 3 months inside a critical infrastructure network where most servers, including domain controllers, had unrestricted outbound access. No one ever detected it.

CISA Advisory AA23-059A

22 seconds

The median time from an attacker's first access to handing off to a second threat group in 2025. In 2022, it was more than 8 hours.

Mandiant M-Trends 2026

26%

Only 26% of known exploited vulnerabilities were fully remediated in 2025, down from 38% the year before. The median time to patch rose to 43 days.

Verizon 2026 Data Breach Investigations Report

Behind these numbers is the Toxic Combination: industrialized attackers, cheap AI offense, and clouds insecure by default.

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

HOW AVIATRIX CLEARANCE GETS YOU THERE

1 See

Free Containment Assessment returns a provisional Blast Radius in about five minutes.

2 Insert

One toggle per VPC. Monitor mode shows what policy would block before anything is blocked.

3 Enforce

Start with the control you need. Promote one rule, one VPC at a time.

4 Operate

Active Defense keeps clearance current as the estate changes.

The Free Tier includes a free Containment Assessment and 15 workloads you can run in monitor or enforce mode, with no purchase and no time limit. Fifteen workloads cover a typical VPC or VNet.

Get your provisional Blast Radius with a free [Containment Assessment](#).

About Aviatrx

Aviatrx® is the network containment company. The Aviatrx 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](#).

Sources: CISA AA23-059A (PDF), Mandiant M-Trends 2026 Executive Edition, Help Net Security: Verizon 2026 DBIR findings, Secureframe: 2026 Verizon DBIR insights, Qualys TRU: The Broken Physics of Remediation, eSecurity Planet: IBM 2026 Cost of a Data Breach key findings, Recorded Future: H1 2026 Malware and Vulnerability Trends, The Hacker News: CISA AA26-237A coverage