AVIATRIX®

FAST FACTS

Aviatrix Workload Attack Path Assessment

See your cloud the way an attacker does–transform runtime telemetry into actionable zero trust insights

The Problem: Zero Trust Stops at the Perimeter

Your cloud defenses have critical blind spots:

- Zero trust focuses on user access, but attackers move laterally across workloads without detection.
- Native cloud tools provide disconnected logs that don't show how real attacks unfold.
- Posture management detects drift but can't reveal actual attack progression.
- Dynamic cloud architectures outpace static security controls.
- Teams lack runtime evidence to prove zero trust effectiveness.

The Solution: Aviatrix Workload Attack Path Assessment

– a free, agentless assessment that reveals how real attacks could move through your cloud.

The Aviatrix Workload Attack Path Assessment uses AI-assisted correlation to transform flow and DNS telemetry into actionable runtime insight. It connects behaviors such as DNS beaconing, lateral movement, and suspicious egress into Workload Breach Chains that mirror real attacks–helping teams identify exposure, validate controls, and advance Zero Trust maturity.

How It Works

1. **Telemetry Ingestion** – Ingests existing AWS or Azure flow logs and DNS data
2. **Behavior Detection** – Identifies patterns like beaconing, lateral movement, suspicious egress
3. **Breach Chain Correlation** – Connects behaviors into attack sequences showing progression
4. **Visualization and Prioritization** – Prioritizes recommendations in an interactive dashboard
5. **Path to Enforcement** – Findings feed directly into Aviatrix Zero Trust for Workloads for ongoing protection

What Makes It Different

Traditional Approach	Aviatrix Assessment
✗ Isolated alerts and logs	✓ Connected attack patterns
✗ Static posture snapshots	✓ Runtime behavioral insight
✗ Generic threat intelligence	✓ Your environment-specific analysis
✗ Overwhelming noise	✓ Prioritized, actionable guidance

Key Benefits:

Expose Runtime Blind Spots – Identify unseen lateral communication and egress routes that enable attacker movement

Validate Zero Trust Controls – Confirm whether segmentation policies would contain real breaches

Prioritize Remediation – Focus on high-impact areas that break multiple attack paths

Align Security Teams – Unite around shared runtime evidence, not just static posture data

AI-Driven Insight & Detection:

AI-Driven Context Discovery – Automatically discovers applications, environments, and workload roles using AI-based analysis of names, tags, and patterns–creating instant context with zero manual input.

Unencrypted Traffic Visibility – Detects clear-text HTTP and other unencrypted flows to expose gaps in data protection and validate the need for network-level encryption.

AI & External Dependency Risk Detection – Identifies outbound calls to AI/ML APIs and public package sources that may expose data-sovereignty or software-dependency risks.

Key Features:

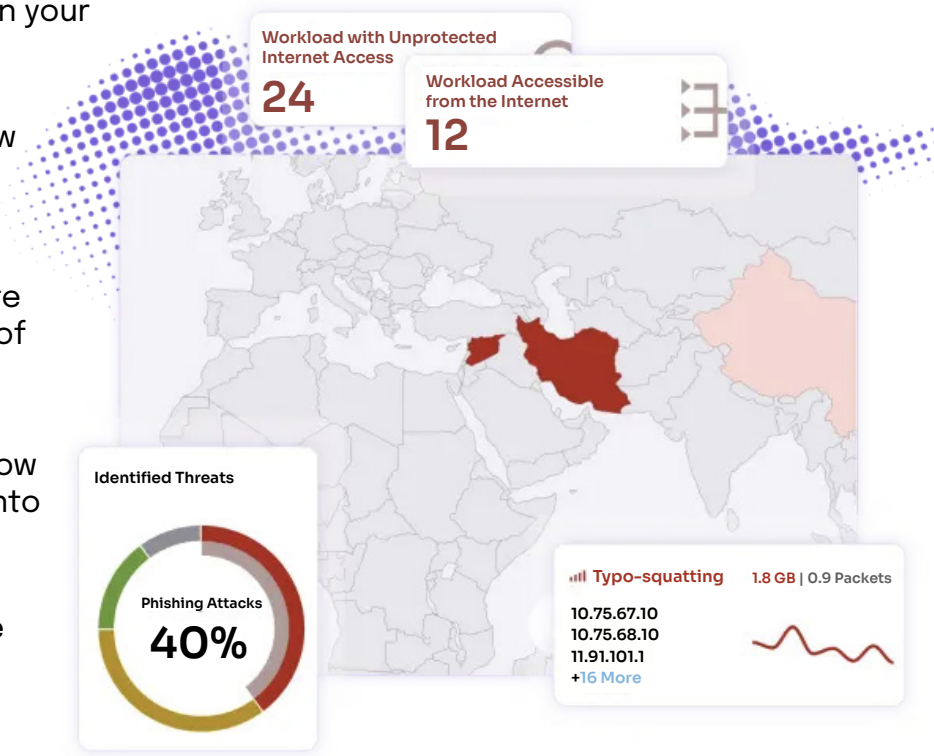
Attacker-Realistic Visibility – Understand how breaches would progress in your environment

Actionable Prioritization – Know where to focus controls for maximum impact

Zero Trust Validation – Translate runtime findings into evidence of control effectiveness

Connected Context – Reveal how individual detections connect into full attack paths

Agentless Simplicity – Leverage existing telemetry with zero deployment overhead



Assess Risks with Confidence

Available now — completely free, no deployment required.

Ready for your free assessment? → **Get Started Today**

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit www.aviatrix.ai.