AVIATRIX®

TECHNICAL SOLUTION BRIEF

Aviatrix Breach Lock

Rapid Response Program for Cloud Data Exfiltration

Overview

Cloud security incidents move quickly – often faster than DFIR teams can identify the origin, detect the tactics, and respond with corrective action. Once an attacker gains unauthorized access and establishes a foothold, data exfiltration is typically the next high value objective in their playbook. In modern cloud environments, data exfiltration can begin within seconds, long before situational awareness is established.

Aviatrix Breach Lock is a free rapid incident response program that gives organizations immediate visibility into and containment of cloud data exfiltration attempts during an active or suspected incident. The program analyzes cloud flow and DNS telemetry to identify high probability exfiltration attack vectors and, where supported, applies cloud-native, agentless egress enforcement policies to mitigate the risk of data loss – with no downtime and no architecture changes.

Every engagement includes a 48-hour Breach Containment Review and 30 days of Zero Trust for Workloads to maintain continuous monitoring and microsegmentation policy enforcement throughout the recovery phase.

The Problem Breach Lock Solves

Cloud service provider ecosystems make egress visibility extremely difficult to ascertain. NAT gateways obscure workload identities, logs are incomplete or non-existent, and cloud native consoles do not correlate telemetry. During an incident, teams often cannot answer the most critical questions:

- Who is the attack originator?
- What is the attack blast radius?
- Where, when, how, and why is data being exfiltrated?

Traditional tools detect compromise – but none provide cloud-native exfiltration containment. CNAPPs surface posture issues, EDR protects endpoints, and SASE secures the perimeter. Meanwhile, domestic and international compliance frameworks such as HIPAA ,PCI DSS , GDPR, and PrivacyMark expect rapid clarity that most DFIR teams cannot deliver under pressure.

Breach Lock fills this gap by restoring NAT-level attribution, surfacing anomalous and malicious egress traffic patterns, and enabling pervasive, granular containment where it is supported.

What Breach Lock Provides

Breach Lock delivers four essential outcomes during an exfiltration incident:

1. Immediate visibility into egress traffic
2. Attribution of each connection to the compromised workload
3. Identification of anomalous, malicious, or non-compliant destinations
4. Pervasive, granular cloud native containment (where supported)

The program is designed to help organizations contain behaviors aligned to MITRE ATT&CK Exfiltration (TA0010), including:

- T1020: Automated Exfiltration
- T1029: Scheduled Transfer
- T1030: Data Transfer Size Limits
- T1041: Exfiltration Over C2 Channel
- T1048: Exfiltration Over Alternative Protocol
- T1537: Transfer Data to Cloud Account
- T1567: Exfiltration Over Web Services

When to Use Breach Lock

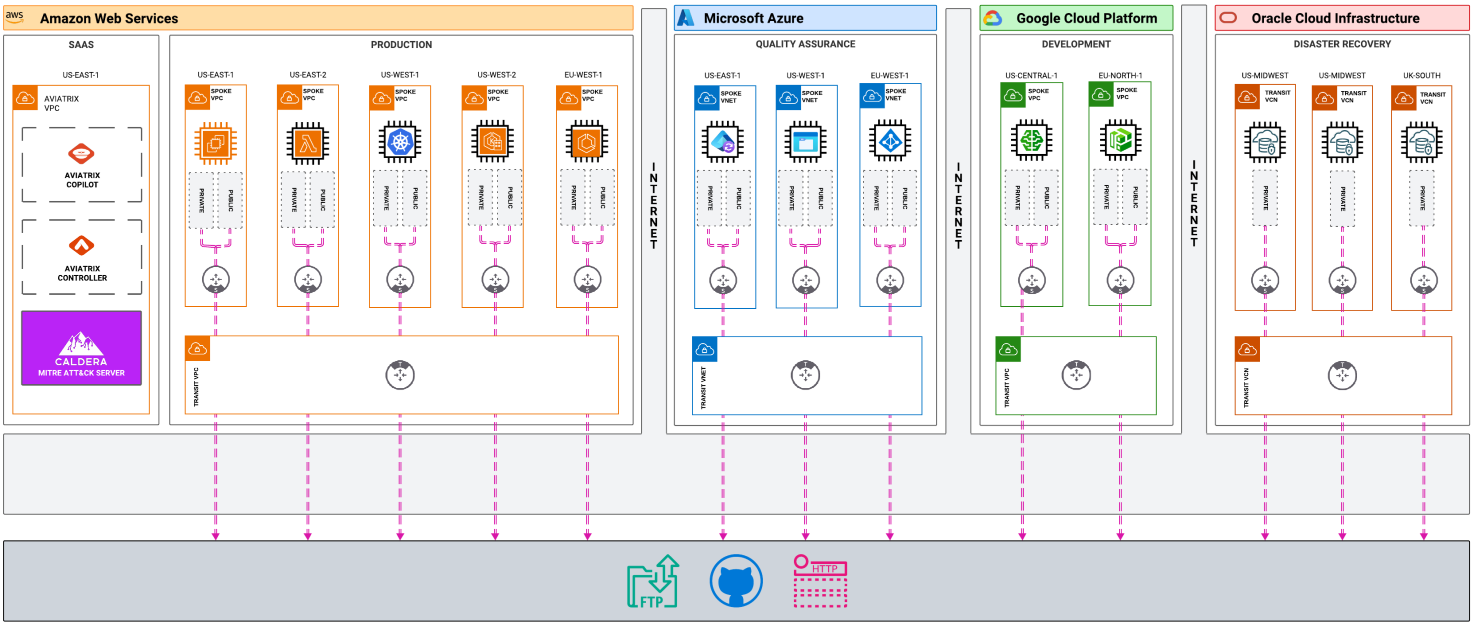
Organizations activate Aviatrix Breach Lock when they experience or suspect:

- Cloud data exfiltration
- Anomalous or malicious egress traffic
- C2 or botnet-like communication
- DNS beaconing or suspicious domains
- Unusual SaaS/ API connections
- Regulated data exposure (HIPAA, PCI, GDPR, PrivacyMark)

Breach Lock is designed for active incidents, high-risk signals, or suspicious egress behaviors.

Egress Security Architecture

How Aviatrix Enables Cloud-Native Exfiltration Containment



Breach Lock Telemetry Layer

- Flow log ingestion
- DNS log ingestion
- Metadata enrichment (tags, cluster ID, region, account)
- Threat intelligence, domain classification, geo/jurisdiction scoring

Attribution Engine

- Mapping NAT gateway → workload
- Source work-load reconstruction
- Workload identity tagging

Egress Behavioral Analysis

- Malicious IP detection
- Foreign jurisdiction detection
- SaaS/API risk categorization
- DNS beaconing
- MITRE ATT&CK Exfiltration techniques (T1020, T1029, T1030, T1041, T1048, T1537, T1567)

Enforcement Layer

- Aviatrix spoke and transit gateways
- DCF Policy engine
- Deny anomalous/ malicious traffic patterns
- Restrict egress Internet access
- Enforce egress encryption

Zero Trust Stabilization

- Runtime monitoring
- Policy enforcement
- Compliance-rea dy reporting
- 30-day stabilization window

1 Telemetry Collection (Agentless, Cloud-Native)

Breach Lock ingests existing cloud-native telemetry without deploying agents, sensors, packet capture, or requiring inline traffic inspection.

Sources may include:

- VPC,VNet,VCN flow logs
- DNS query logs
- Workload, region, and account metadata
- Threat intelligence, geo-location, and domain scoring

T Activating Breach Lock enables read-only ingestion and analysis of existing cloud flow and DNS telemetry, which is safe to turn on during a live incident and does not impact application traffic or routing.

2 Attribution Engine (Restores Visibility Behind NAT)

Aviatrix reconstructs the true source workload behind every egress connection.

The Attribution Engine maps:

- Source IP → NAT gateway → originating workload
- Workload identity → tags, cluster, function, or instance metadata
- Outbound request → destination FQDN/IP, SNI, and ports

This eliminates NAT blind spots and reveals which workloads are responsible for suspicious or malicious egress traffic.

3 Egress Behavioral Analysis

Breach Lock analyzes outbound flow and DNS telemetry using a dedicated analytics layer to identify high-risk egress behaviors associated with data exfiltration, command-and-control, and policy violations.

- Malicious IPs, TOR entry nodes, and C2 infrastructure
- Destinations outside approved jurisdictions
- Suspicious SaaS/API endpoints

- DNS beaconing or staged resolution
- Unencrypted or policy-violating egress traffic
- MITRE ATT&CK Exfiltration (TA0010) techniques:
  - T1020: Automated Exfiltration
  - T1029: Scheduled Transfer
  - T1030: Data Transfer Size Limits
  - T1041: Exfiltration Over C2 Channel
  - T1048: Exfiltration Over Alternative Protocol
  - T1537: Transfer Data to Cloud Account
  - T1567: Exfiltration Over Web Services

Each finding includes context, assurance, and recommended containment actions.

4 Cloud-Native Enforcement Layer (No Agents, No Downtime

Where the customer's cloud environment supports, Aviatrix applies cloud-native, agentless egress controls at distributed enforcement points already present in the environment.

Capabilities include:

- Blocking malicious or foreign destinations
- Restricting egress Internet access
- Enforcing egress limited to compliant destinatations
- Applying microsegmentation policies to high-risk workloads

Enforcement is:

- Reversible
- Granular
- Safe to apply during an incident
- Activated without IP reallocation, IP reassignment, or architectural redesign

5 Zero Trust Stabilization (30 Days Included)

All Breach Lock findings transition directly into Zero Trust for Workloads (PaaS), which provides:

- Continuous egress monitoring
- Runtime policy enforcement
- Microsegmentation and encryption validation
- Compliance-ready reporting

This 30-day stabilization window protects the cloud environment during incident investigation and recovery.

Breach Containment Review (Delivered Within 48 Hours)

The Breach Containment Review provides rapid, high-fidelity clarity into egress risk, including:

- Evidence of active or probable data exfiltration
- Egress attack surface analysis
- Compliance exposure (HIPAA, PCI DSS, NIS2, DORA, SEC, GDPR, JPM)
- Guidance when enforcement is limited
- Workload-to-destination attribution
- Encryption visibility and gaps
- Prioritized containment recommendations

This becomes the central artifact for DFIR teams, external investigators, regulators, legal, executive leadership, cyber insurance companies, and law enforcement agencies

Breach Lock Benefits

- Mitigate and remediate cloud data exfiltration
- Attribute anomalous or malicious activity to compromised workloads
- Reduce incident blast radius
- Regain control of egress traffic
- Produce regulator-ready evidence
- Maintain runtime zero trust enforcement during recovery

Why Breach Lock Is Different

Traditional tools merely detect compromise. Breach Lock contains it while permitting legitimate access and denying illegitimate access to business resources, improving RCA, minimizing MTTR, and facilitating adherence to RTO/RPO KPI's.

- CNAPPs highlight posture drift but cannot stop exfiltration.
- EDR protects hosts, but not cloud-native egress attack vectors.
- SASE and firewalls secure the perimeter, but not workload-driven egress traffic.
- DFIR firms investigate but cannot enforce microsegmentation containment.
- Cloud provider tools provide limited visibility without enforcement.

Aviatrix Breach Lock uniquely provides:

- Attribution
- Detection
- Cloud-native containment
- Zero trust microsegmentation

All delivered free, agentless, and safe during incident response

Summary

Aviatrix Breach Lock provides organizations the visibility and control they need during the most critical phase of a cloud incident: when attackers are exfiltrating data from the cloud environment. Through cloud-native telemetry analysis, NAT attribution, malicious destination identification, and high-assurance enforcement, Breach Lock helps organizations stop exfiltration quickly and confidently.

With a 48-hour Containment Review and 30 days of distributed zero trust enforcement included, Breach Lock gives organizations the ability to regain operational control, satisfy regulatory compliance requirements, and prevent further data loss – all without downtime, agents, or architectural changes.

Organizations facing or suspecting cloud data exfiltration can activate Breach Lock immediately at no cost.

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.