AVIATRIX

PROGRAM BRIEF

Aviatrix Breach Lock Program

When you’re hit by a breach, every minute matters

Cloud computing has changed data breaches. Not only has it expanded the attack surface, but breaches tend to be larger in scale, and they are fast–often outpacing the time it takes for security teams to investigate, correlate telemetry, and take action.

But data exfiltration can begin within seconds, long before alerts trigger or investigations start. Moreover, cloud architectures aren’t set up to answer one of the most critical questions you have in this moment: Which workload is sending data out right now, and where is it going?

The missing component: Egress containment

Imagine a thief has broken into your home and stolen your most valuable possession. You want to be alerted to the break-in, but you probably care even more about preventing your prized item from being spirited away. Similarly, when it comes to cybertheft, the highest-impact starting point is egress containment. But while there is an entire ecosystem of traditional security tools that can help you detect a compromise, none of these can contain cloud-native exfiltration as it happens. You need an operational program to stop data from leaving the cloud during an attack, and that’s where Aviatrix comes in.

Aviatrix Breach Lock is a free rapid-response program designed to deliver immediate visibility into and containment of cloud data exfiltration during an active or suspected breach.

How Aviatrix Breach Lock works

Aviatrix Breach Lock leverages Aviatrix technology to analyze cloud flow and DNS telemetry to identify ongoing or likely exfiltration paths and, where supported, apply cloud native, agentless outbound controls to contain unsanctioned outbound data flows during a breach. This is all done with no downtime and no architectural changes required.

The service includes a **48-hour Breach Containment Review,** and **30 days of Aviatrix Zero Trust for Workloads**, PaaS edition, for continuous monitoring, enforcement, and audit-ready reporting throughout your recovery.

Program Benefits

Immediate exfiltration containment: Where enforcement is possible, targeted controls help stop malicious, foreign, and non-compliant outbound traffic.

Visibility behind NAT: Reveals the exact workload behind every outbound connection.

Cloud-native, agentless enforcement: Safe activation during an incident with zero downtime or architecture changes.

Compliance-ready evidence: Meets requirements for HIPAA 2025, PCI DSS 4.0, NIS2, DORA, and SEC.

Multi-cloud enforcement: Unified outbound control across all major clouds.

How to Activate Aviatrix Breach Lock

As soon as you realize you're under attack, visit **Aviatrix Breach Lock**. Our cloud security specialists are standing by.

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.