Tip Sheet

AVIATRIX®

4 Cloud Egress Traffic Risks You Need to Know About

Your cloud environment is a two-way street–data flows in and data flows out. But unlike a two-lane highway where the only difference is the direction of the traffic, ingress (inbound) and egress (outbound) traffic are often treated differently. Many security models–whether implemented with cloud-native security tools or third-party solutions such as next-generation firewalls (NGFWs)–are ingress-centric. Of course, securing inbound traffic is vital. But if you don't put a corresponding level of care and attention into your outbound traffic, you could put your organization's security posture, compliance, cloud budget, and team productivity at risk.

Here are four types of risk you need to know about cloud egress traffic–and how you can address them with Aviatrix Cloud Firewall™.

1 Deprioritized focus on egress creates security risk

Cloud service providers (CSPs) often handle ingress and egress security protocols separately with a focus on ingress. This protects your environment from malicious data coming in from external sources, which is critically important, but you also need to protect against data exfiltration, i.e., data theft. Inbound protections will stop a lot of malware and other threats whose ultimate intent is data exfiltration, but there are other ways for bad actors to initiate unauthorized data transfers, leaving you with security gaps. You need better protections on egress traffic than the basic features you get from the cloud-native security tools.

2 Data transfer costs create budget risk

Cloud-native NAT gateway pricing typically includes a couple of different fee types. There is a metered volume component that charges based on throughput. And while data ingress is free, there are data egress fees. On top of all that, there are no mechanisms for selectively blocking outbound traffic, which means you have no way of controlling data transfer costs, which can quickly spiral out of control.

3 Lack of visibility and control create issue response risk

One of the main value propositions of working with a CSP is that they take on the heavy lifting of infrastructure maintenance and management. This also means that you give up the granular access to data and detailed traffic flows that you have in on-premises environments, making it difficult to analyze traffic patterns, assess threats, and troubleshoot issues. This will increase your mean time to response (MTTR) in the event of an incident.

4 Inconsistent policy enforcement and manual tracking creates compliance risk

There are numerous regulations and industry standards governing data security–HIPAA, GDPR, PCI-DSS, DORA, and others–that require robust security controls. Even with the compliance tools included with your cloud-native solutions, there's no way to ensure that regulatory and governance standards are applied consistently across all of your cloud environments. You also need to maintain stringent audit trails and produce compliance reports. It's on your team to gather all the logging data from the CSPs, which is a time-consuming, manual process that is inefficient and error-prone.

De-risk Cloud Egress With Aviatrix Cloud Firewall

The Aviatrix Cloud Firewall is a cutting-edge solution designed to enhance cloud network security by integrating advanced features such as enterprise-grade NAT capabilities, centralized management, and AI-powered discovery and enrichment of egress traffic flows. This firewall offers comprehensive visibility and control over network traffic, enabling faster root cause analysis and improved security posture. With its unique flat-rate billing model, the Aviatrix Cloud Firewall ensures cost efficiency while providing robust protection against both external and internal threats. Its seamless integration and automated deployment make it an ideal choice for modern cloud environments, ensuring scalability and resilience.

The Aviatrix Cloud Firewall addresses the four big cloud egress traffic risks with:

- **Advanced security capabilities**–including support for transport layer security (TSL)/secure sockets layer (SSL) decryption, fully qualified domain name (FQDN) filtering, and intrusion detection–aligns with a Zero Trust security posture and ensures that all egress traffic is both trusted and secure.
- **Advanced network segmentation and micro-segmentation** enables you to divide the network into smaller segments to help isolate workloads and limit lateral movement of potential threats.
- **Centralized management** provides a single interface from which you can view, monitor, and manage multiple cloud networks.

Comprehensive visibility with detailed, holistic monitoring, analytics, and visualization tools across all cloud environments, all from a single pane of glass. Aviatrix Cloud Firewall, together with Aviatrix CoPilot, gives you deep insight into both the traffic and the health of each individual gateway, and CoPilot offers a wide array of sophisticated troubleshooting tools that can drastically improve MTTR, reducing or even eliminating downtime.

Unified security policy allows you to define policies centrally but enforce them in a distributed manner closer to the workloads across accounts, platforms, and locations.

Automated policy enforcement and auditing capabilities ensures that compliance policies and governance standards are continuously enforced across all environments, increasing accuracy while eliminating manual checks and updates.

"All you can eat" traffic processing pricing model caps costs with flat hourly billing and no additional costs for throughput. And, you can selectively block egress traffic, enabling you to control data egress charges. In fact, Aviatrix customers routinely save 25% annually on their cloud bills.

What are your organization's biggest cloud egress traffic risks?

Request a demo and one of our cloud egress specialists will work with you to address all of your cloud egress challenges.

Request a Demo

About Aviatrix

Aviatrix® is the cloud network security company trusted by more than 500 of the world's leading enterprises. As cloud infrastructures become more complex and costly, the Aviatrix Cloud Network Security platform gives companies back the power, control, security, and simplicity they need to modernize their cloud strategies. Aviatrix is the only secure networking solution built specifically for the cloud, that ensures companies are ready for AI and what's next. Combined with the Aviatrix Certified Engineer (ACE) Program, the industry's leading secure multicloud networking certification, Aviatrix unifies cloud, networking, and security teams and unlocks greater potential across any cloud.