AVIATRIX

QUICK BRIEF

Data Exfiltration: What You Need to Know

What is it?

Data exfiltration is the unauthorized transfer of data from an enterprise resource or network to an external location. Simply put, it's data theft.

Why does it matter?

Many cybersecurity controls–identity and perimeter security tools in particular–focus on keeping bad actors out of the network. This is important, but it's not enough. There is no such thing as a 100% impenetrable defense, so what happens when a cybercriminal is able to slip inside? Too often, they are now free to move laterally, accessing other systems, and then transferring sensitive and valuable data to servers that are under their control and out of your reach. This is exactly what happened in the MGM International and **MOVEit** breaches, among others. Without data exfiltration controls as part of your overall defense-in-depth security posture, your company and customer data is vulnerable and you're at risk for regulatory fines and penalties.

How does it happen?

Enterprises often assume that egress is covered in their cloud security, but there are gaps–particularly in multicloud and hybrid environments with shared infrastructure–that cybercriminals actively target. Unmanaged egress (outbound) paths are the most exploited blind spot in cloud architectures. Other gaps include lack of consistent policy enforcement across clouds and blind spots in cloud traffic.

What can you do about it?

Implementing a zero trust architecture–which operates on the principle of never trust, always verify–ensures that every connection, device, and user is treated as a potential threat that must be verified and authorized. It's no longer enough to just have credentials; the activity must adhere to policy or it will not be allowed. Effective zero trust is embedded directly into the runtime path of cloud traffic to enforce identity-based policies consistently across regions and platforms.

Data exfiltration security is woven throughout **Aviatrix Cloud Native Security Fabric™ (CNSF)**. Aviatrix provides cloud-native visibility into outbound data flows, policy enforcement at cloud scale, and risk metrics that translate to board-level reporting–capabilities traditional tools can't deliver. The solution embeds inline enforcement and SmartGroup-based segmentation directly into the cloud fabric, enabling real-time control without detouring traffic through legacy firewalls.

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.