AVIATRIX®

5 Data Center Edge Challenges Solved with Aviatrix

Navigating the Complexities of Securing Hybrid Cloud Environments

The hybrid cloud has become the backbone of enterprise IT. But securing the data center edge remains one of the most complex and high-stakes challenges for networking, security and GRC (governance, risk, and compliance) teams. The recent Salt Typhoon attack, one of the largest infrastructure breaches in U.S. history, exposed vulnerabilities in hybrid environments, where data flows across public and private networks. This breach underscores the critical need for end-to-end encryption, dynamic segmentation, high availability, and real-time traffic visibility.

Many organizations initially embraced cloud-only strategies, but quickly realized that sensitive workloads must remain on-premises for security, compliance, and performance reasons. As a result, hybrid environments–combining on-premises data centers with public cloud deployments–have become the norm. However, this shift introduces new security and operational complexities at the data center edge, the critical point of connection between the two environments.

Modern AI, machine learning, and data-intensive applications exacerbate this complexity by requiring vast amounts of data to move seamlessly between cloud and on-prem environments. Unprotected data that travels over the public internet or service provider networks can introduce the risk of man-in-the-middle (MitM) attacks, data exfiltration, and packet injection, further complicating the landscape.

Protecting data while ensuring seamless operations for real-time applications requires a new approach.

In this data-intensive, hybrid-cloud world, your requirements are clear: end-to-end encryption, automated failover, centralized management, and comprehensive visibility.

But achieving these requirements is anything but simple. There are several data center edge challenges that many organizations struggle with:

- Balancing security and performance requires unacceptable compromises
- Network disruptions require manual intervention
- The environment is complicated to manage
- Visibility into performance is limited
- Deployments are complex and slow

Chances are, at least one of these is making your ability to provide secure hybrid-cloud connectivity harder than it needs to be. With Aviatrix, you can address all of these issues so you can deliver the performance, security, reliability, and visibility your hybrid-cloud infrastructure needs.

Aviatrix Cloud Native Security Fabric: A Quick Overview

Aviatrix Cloud Native Security Fabric (CNSF) offers a comprehensive solution for managing hybrid cloud connections, providing deep visibility, advanced traffic engineering, and enhanced troubleshooting capabilities across hybrid-cloud environments. The solution enables high-performance encryption using Aviatrix patented IPSec encryption technology, providing secure and scalable networking. And it integrates seamlessly with native cloud services like AWS Transit Gateway and Azure Virtual WAN, overcoming their limitations.

This solution is ideal for enterprises managing complex, distributed networks–helping them reduce operational costs, increase uptime, and accelerate hybrid cloud deployment timelines.

The Top 5 Secure High-Performance Data Center Edge Challenges and How You Can Solve Them With Aviatrix

1 Balancing security and performance without compromises

Networking and security teams are often forced to choose between line-rate performance and robust encryption. Standard encryption methods can introduce latency, causing bottlenecks that negatively impact performance. Conversely, prioritizing performance can expose data to interception. The Salt Typhoon attack demonstrated how unencrypted traffic between environments becomes a prime target for attackers.

The Aviatrix solution:

- **Encrypted Dataplane by default:** Aviatrix encrypts the entire data path out of the box, ensuring data is protected across all environments.
- **High-Performance Encryption (HPE):** For high-throughput environments, Aviatrix's patented HPE delivers line-rate encryption without performance degradation.
- **Intelligent Traffic Engineering:** Aviatrix optimizes routing, reducing latency while ensuring segmentation between environments, limiting lateral movement of threats.

Why this matters:

Security teams can deploy full encryption at scale without compromising network speed or user experience, directly aligning with **CISA's call for end-to-end traffic encryption** in the wake of the Salt Typhoon cyberattack.

2 Manual failover leads to longer network downtime

Failover mechanisms are critical to ensuring high availability, but many legacy solutions require manual intervention during outages. This introduces delays, leaving applications vulnerable to downtime and potential data exposure during disruptions. In the context of Salt Typhoon, delays in addressing disruptions allowed attackers to maintain access and persist within networks.

The Aviatrix solution:

Automated Dynamic Failover: Aviatrix automates failover processes, instantly rerouting traffic to backup paths when disruptions are detected.

Self-Healing Networks: Aviatrix continuously monitors network health, proactively addressing failures to maintain uninterrupted connectivity.

Why this matters:

Automated failover eliminates operational delays, ensuring critical workloads remain online and secure, reinforcing CISA's guidance around uptime and resilience.

3 The environment is complicated to manage

Hybrid environments combine on-premises and multicloud deployments, introducing operational complexity. Security teams must manage multiple vendors, policies, and configurations across distributed environments, increasing the risk of misconfigurations, security gaps, and inconsistent enforcement.

The Aviatrix solution:

Centralized Policy and Control: Aviatrix centralizes network management, enabling unified control over policies, segmentation, and encryption across cloud and on-premises environments.

Multicloud Orchestration: Seamless integration with AWS, Azure, and GCP ensures consistent policy enforcement and uniform security across platforms.

Why this matters:

By consolidating management through a single interface, networking and security teams reduce complexity, eliminate errors, and minimize attack surfaces targeted by state-sponsored threats like Salt Typhoon.

4 Limited visibility into network traffic increases risk

Partial visibility across hybrid networks prevents security teams from detecting and mitigating breaches before damage occurs. Blind spots in east-west traffic and across public internet routes increase the risk of undetected infiltration.

The Aviatrix solution:

End-to-End Traffic Visibility: Aviatrix provides real-time monitoring across cloud and on-premises environments, offering insights into traffic flows and potential anomalies.

Integration with SIEMs: Aviatrix logs integrate directly with SIEM tools like Splunk and Datadog, ensuring threat intelligence feeds are enriched by network data.

Why this matters:

Security teams gain actionable insights into network activity, enhancing detection and response capabilities in alignment with CISA's centralized logging guidance.

5 Hybrid deployments are slow and complex

Deploying hybrid cloud environments requires significant integration between disparate on-premises and cloud systems. Traditional deployments are manual, error-prone, and slow, delaying critical security infrastructure and increasing exposure.

The Aviatrix solution:

Infrastructure as Code (IaC): Aviatrix automates deployment through IaC, enabling rapid, repeatable deployments with consistent configurations.

CI/CD Integration: Aviatrix integrates with CI/CD pipelines, allowing seamless deployment of security controls alongside application development.

Why this matters:

Faster deployments accelerate response times to evolving threats, ensuring hybrid environments remain hardened against advanced attacks like Salt Typhoon.

Ready to increase the security and performance of your data center edge?

Salt Typhoon reinforced the need for full-path encryption, automated failover, centralized management, and comprehensive visibility at the data center edge. With Aviatrix, networking, security, and compliance teams can enhance resilience and protect their hybrid environments against sophisticated threats.

Schedule a demo today to explore how Aviatrix can fortify your network security at the data center edge.

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.