AVIATRIX®

CASE STUDY

How Republic Airways Turned Their Hybrid Cloud Network into a Zero Trust Security Fabric

Republic Airways

Founded in 1974 and headquartered in Indianapolis, Indiana, Republic Airways is one of the largest regional airlines in North America. Republic operates a fleet of 240+ aircrafts and offers scheduled passenger service with 1,000 daily flights to 100 destinations in the U.S., Canada, the Caribbean, and Central America.

The company leverages public cloud infrastructure primarily to support corporate services, development environments, and specific operational platforms that benefit from the cloud's scalability and elasticity. The entire network infrastructure is managed by a team of two, who are actively transitioning critical workloads to the cloud in a complex hybrid infrastructure.

"We're mid-journey; core applications are still in our private data centers, but many of our new deployments are cloud-native," said Brent Fowler, Senior Network Engineer at Republic Airways. "Cloud connectivity has become mission critical." As the line between networking and security blurs, **Republic Airways needed more than just fast transit; they needed an enforcement fabric**. Aviatrix Secure High-Performance Datacenter Edge (DCE) gives the team a unified control point for encrypted connectivity, segmentation, and policy enforcement between cloud and on-premises environments.

Legacy connectivity tools created security and visibility gaps

Republic initially faced significant hurdles with cloud connectivity. Their architecture relied on a complex "load balancer sandwich" approach, which was heavily dependent on native cloud service provider (CSP) constructs and traditional networking appliances. *(Continued)*

COMPANY

- Republic Airways is one of the largest regional airlines in North America
- A small team manages a complex, evolving hybrid environment with multiple CSPs and an on-premises environment

CHALLENGES

- Native CSP tools lacked visibility, policy control, and segmentation
- Tunnel-based connectivity (VPNs/IPSec) introduced instability and overhead
- No unified control plane to enforce encryption and access policy between environments
- Operational and security silos between networking and security teams
- Difficulty meeting compliance and audit requirements with fragmented logging

RESULTS

- Secure connectivity fabric for hybrid cloud enforcement
- Runtime encryption from on-premises to cloud with a 150 Mbps performance boost
- Zero trust microsegmentation reduced lateral movement risk
- Real-time telemetry and routing visibility improved MTTR from 1 day to <1 hour
- Audit-ready encrypted data paths and centralized logging support FAA compliance
- Enabled networking and security teams to coordinate policy enforcement
- Unified, cloud-agnostic architecture accelerated deployment across AWS and Azure

The native CSP tools lacked the operational depth required for enterprise-grade networking, and manual configurations made the environment fragile and difficult to scale. Without centralized telemetry or policy enforcement, diagnosing outages and performance issues became a time-consuming and reactive process. Further, Republic's reliance on VPC and VNet peering–combined with IPSec VPNs to firewalls–led to frequent tunnel disconnects and instability. Even attempts to establish private, secure connections between their carrier and CSPs yielded only marginal improvements and came at a high cost.

Lastly, encrypting traffic between the data center and the cloud introduced performance bottlenecks due to appliance limitations. Once traffic entered the cloud, visibility dropped sharply. From a compliance perspective, the lack of consistent logging and policy enforcement left the team without the assurance they needed to meet regulatory standards. Security responsibilities at Republic Airways are shared across teams. While a dedicated security team manages firewalls, Zscaler, and vulnerability scans, the network team increasingly plays a role in cloud security and visibility. "We have a security team… but that line is starting to blur," explained Fowler. Both teams knew there had to be a more efficient and resilient way forward.

Aviatrix DCE turns hybrid networking into a security control plane

Aviatrix Secure High-Performance Datacenter Edge goes beyond hybrid networking–it delivers true zero trust at the network layer with built-in encryption, micro-segmentation, and real-time traffic inspection. It transforms cloud connectivity into a secure, policy-driven perimeter. For Republic Airways, this means secure, observable, and scalable connectivity across on-premises and multicloud environments. "We can spin up connectivity in a new region in under one day and have a full environment ready to go," said Fowler. "That agility is very important to us as we have a small team and need to react to business needs quickly."

Simple to provision, deploy, and manage, Aviatrix allows Republic Airways to simply and flexibly connect resources running anywhere over a common data plane. Aviatrix's automated infrastructure as code (IaC) deployments provide consistent configurations, cut setup time, and reduce disruptions, ensuring reliable performance across hybrid environments. This automation empowered the team to spin up new VPCs or VNets in just minutes–regardless of the environment. **"We don't have to worry about whether it's AWS or Azure, it's just Aviatrix,"** said Fowler. "Having one unified architecture and the automation and orchestration that Aviatrix provides makes us faster and more agile." *(Continued)*

> **"We can spin up connectivity in a new region in under one day and have a full environment ready to go."**
>
> *Brent Fowler,*
> *Senior Network Engineer*
> *at Republic Airways*

Aviatrix transforms raw connectivity for new cloud regions into a secure, observable, and policy-driven environment. “If we need to spin up new connectivity in a new region, it’s literally as quick as click, click… maybe a couple more clicks and some typing,” said Fowler. “We can get into a new region in Azure in 5-10 minutes.” Aviatrix DCE runs as a secure overlay, **enforcing encryption from day one, applying segmentation policies at runtime, and delivering traffic visibility essential for threat detection and audit assurance.**

From transit to security fabric

With Aviatrix DCE, what started as a transit solution quickly became Republic’s security control plane. The team now enforces encryption policies, audits routing paths, and validates segmentation boundaries from a single interface without additional appliances or operational complexity.

Aviatrix offers High-Performance Encryption (HPE) over private or public connectivity that boosts both security and performance. Republic Airways now has full encryption from on-premises to the cloud, running at line rate. Their traditional router created a performance ceiling that they couldn’t exceed. With Aviatrix, the performance boost was immediate with traffic moving 150 Mbps above the previous plateau. Aviatrix HPE also puts Republic in a good position to pass audits that the Federal Aviation Administration (FAA) performs to ensure that enterprises in the airline space have good encryption practices for data in transit and at rest.

The solution’s unified management console provides power to oversee and orchestrate complex hybrid networks for streamlined operations and improved efficiency. “Within the first few weeks, Aviatrix gave us immediate visibility into routing paths, traffic flows, and encryption status,” said Fowler. With real-time telemetry, traffic flow visualization, and topology mapping, the team can proactively detect anomalies and troubleshoot issues in minutes instead of hours. Aviatrix DCE gives Republic Airways the ability to observe and enforce security policies in real time–whether isolating abnormal flows, validating segmentation boundaries, or detecting configuration drift. These controls help the team respond to not just performance issues but also potential security incidents in minutes, not hours. **“Our MTTR has drastically improved with Aviatrix’s telemetry and diagnostics–issues that used to take a full day to isolate are now resolved in under an hour,”** said Fowler. Aviatrix FireNet and ThreatIQ extend the security foundation that Aviatrix DCE provides. With FireNet integrating next-generation firewalls (NGFWs) into the fabric and ThreatIQ automating IP reputation enforcement, Republic reduces lateral movement risk and strengthens zero trust posture across all entry points. By enforcing zero trust and enabling micro-segmentation, Republic Airways has reduced lateral risk and improved compliance and confidence in their overall security posture.

As the company continues to evolve its networking infrastructure, Aviatrix will remain a key enabler. For example, the team is considering eliminating on-premises compute and moving it to a cloud or cloud-adjacent environment. “No matter what we decide, Aviatrix makes the transition seamless,” said Fowler. **“We have a reliable, unified architecture so we can hit the ground running with less new stuff to learn.”**