AVIATRIX

CASE STUDY

Global Animal Health Leader Closes Cloud Security Gaps and Unifies Multicloud Networking with Aviatrix Cloud Native Security Fabric

A Global Animal Health Technology Leader serves more than 100,000 veterinary practices across North America, Europe, and Asia-Pacific, supplying integrated supply chain services, prescription management, and cloud-based practice management software. With over $4.7 billion in annual revenue and operations spanning multiple continents, the company depends on highly reliable, secure, and scalable cloud infrastructure to support the veterinary professionals and pet owners who rely on its platforms every day.

The company had made a strategic commitment to a multicloud architecture across both AWS and Azure, hosting business-critical applications including practice management platforms, supply chain systems, analytics workloads, and a mission-critical SAP environment that serves as the backbone of its global supply chain and financial operations. As cloud adoption accelerated, the limitations of native cloud networking became impossible to ignore. Fragmented connectivity, inconsistent security enforcement, and a lack of centralized visibility were creating operational risk and inhibiting the company's ability to scale securely.

To address these challenges, the company turned to Aviatrix Cloud Native Security Fabric (CNSF), deploying a unified, high-availability transit architecture across AWS and Azure, and activating the Aviatrix Distributed Cloud Firewall (DCF) to enforce Zero Trust east-west policies across workloads.

Fragmented Networking and Gaps in Cloud Security Coverage Stalled Growth

The company's reliance on native cloud networking in AWS and Azure, combined with chokepoint or Next-Generation Firewalls (NGFWs) based security enforcement built historically for traditional on-premise infrastructure, left the architecture increasingly exposed as modern cloud workloads scaled. As the cloud footprint expanded to support tens of thousands of veterinary practices globally, the limitations of each layer compounded: connectivity was fragile and difficult to operate across two clouds, and the NGFWs that were meant to protect the environment had meaningful blind spots that grew with every new workload type introduced.

01 Multicloud Connectivity Complexity

Managing separate, cloud native routing and connectivity constructs across AWS and Azure created significant architectural complexity. Without a unified control plane, network and cloud engineering teams were forced to maintain two distinct operating models, duplicating effort and increasing the risk of configuration errors. Connecting AWS regions to Azure environments required bespoke, fragile configurations that were difficult to troubleshoot and even harder to scale.

02 Insufficient East-West Security

The company has deployed chokepoint security or NGFWs within their cloud environments, but the architecture exposed critical limitations for modern cloud workloads. The NGFWs enforced policies based on static CIDR blocks, a model that worked reasonably well for traditional VM-based infrastructure but broke down rapidly as the environment evolved. Coverage gaps emerged across three dimensions:

- **CIDR-Based Policy Limitations:** As workloads scaled and cloud subnets were shared across multiple application tiers, CIDR-based rules became an unreliable proxy for workload identity. A single subnet could host dozens of distinct and ephemeral services, making it impossible to enforce least-privilege access without unacceptably broad rules that created lateral movement risk. This was especially problematic for the company's SAP environment, where sensitive supply chain and financial transactions required strict workload isolation that static CIDR policies could not reliably provide.

- **Kubernetes Namespace Blindness:** As containerized workloads and Kubernetes clusters were introduced, the NGFWs were unable to distinguish traffic by namespace, pod identity, or service account. East-west traffic between Kubernetes namespaces, which should be treated as distinct security domains, was effectively invisible to policy enforcement. This left a significant and growing attack surface uninspected.

- **Application-Type Coverage Gaps:** The diverse mix of application types across the cloud environment, including VMs, managed PaaS services, and containerized workloads, exceeded what the NGFW architecture could consistently protect. Each application type required different enforcement approaches, and the NGFW's reliance on network-layer constructs meant that workload-aware, identity-based Communication Governance was simply out of reach.

The result was a security posture with meaningful blind spots precisely where modern cloud environments are most dynamic and most at risk.

03 Supply Chain Operations Demanded Real-Time Network Visibility

Managing prescription fulfillment and supply chain operations for more than 100,000 veterinary practices worldwide requires rapid response when connectivity or security incidents arise. The company’s network and security teams had no single operational console for AWS and Azure, forcing context switching between separate cloud native tools for each environment. Troubleshooting a routing issue or investigating anomalous traffic required correlating data from multiple disconnected sources. For a supply chain platform where downtime translates directly to delayed prescriptions and disrupted patient care, the absence of centralized, real-time network visibility was an operational liability the business could no longer accept.

04 Availability and Redundancy Concerns

The company's cloud platforms support mission-critical services for veterinary practices worldwide. Chief among them is its SAP environment, which underpins global supply chain operations, financial reporting, and order fulfillment for tens of thousands of veterinary practices. Any degradation or outage in cloud network connectivity has a direct impact on the ability of veterinary professionals to access practice management tools, fulfill prescriptions, and manage patient care. The prospect of SAP downtime in particular drove a critical rearchitecting conversation: the existing cloud network lacked the enterprise-grade redundancy, Communication Governance, and visibility that a globally distributed SAP deployment demands. Native cloud redundancy mechanisms were insufficient to provide the high availability the business required, creating unacceptable risk for production workloads and ultimately serving as a catalyst for the decision to adopt Aviatrix.

Compounding the availability risk, the SAP environment also contended with overlapping IP address spaces across the multicloud environment, a common challenge in large, distributed deployments that had grown organically over time. The conflicting address ranges introduced routing ambiguity between AWS and Azure that native cloud tools could not resolve without a disruptive re-addressing project, adding significant complexity to an already strained architecture and making it even harder to establish reliable, consistent connectivity for SAP workloads.

Decision Making and the Aviatrix Solution

The company determined that leveraging first-party transit services was a long-term liability and that the gaps in its cloud security posture required a layer of enforcement that the existing NGFWs or chokepoint security could not provide. The SAP environment brought both problems into sharp focus simultaneously. As a workload requiring consistent, low-latency connectivity between AWS and Azure, strict workload-level network segmentation, and audit-ready security controls, SAP exposed every weakness in the existing architecture: the fragmented transit model, the NGFW's inability to distinguish workload identity across dynamic cloud environments, and the absence of centralized visibility.

After evaluating the landscape, the company selected Aviatrix to deliver a unified cloud network architecture. The Unified Cloud Network Fabric use case addressed connectivity fragmentation immediately, and the Distributed Cloud Firewall provided Zero Trust for their workloads by adding an identity-aware, workload-level enforcement and containment layer that works alongside the existing NGFW architecture to close the gaps that CIDR-based policies could not address.

The Aviatrix CNSF delivered the following core capabilities:

- **Unified Multicloud Transit Architecture:** Aviatrix delivered a single, repeatable transit architecture spanning both AWS and Azure across multiple regions, eliminating the fragmented connectivity models that had created operational debt. High Availability (HAGW) gateway pairs were deployed throughout, ensuring enterprise-grade redundancy for mission-critical applications.

- **Large-Scale Gateway Deployment Across AWS and Azure:** A multi-region gateway deployment was orchestrated across AWS and Azure, providing consistent connectivity and security enforcement at scale. The unified architecture replaced prior bespoke configurations and established a standardized operational model.
- **Distributed Cloud Firewall for Zero Trust East-West Security:** DCF was activated to begin enforcing Zero Trust policies for east-west traffic between cloud workloads. SmartGroups, dynamic workload groupings based on cloud native tags and attributes, enabled the security team to define granular, identity-aware policies without relying on static IP-based rules. The network and security teams, empowered by executive sponsorship from senior cybersecurity leadership, moved from DCF-enabled monitoring into active east-west enforcement, including consistent policy coverage for the SAP environment that CIDR-based NGFWs could not provide.
- **Centralized Visibility via CoPilot:** The unified platform gave the company's cloud, network, and security teams a single operational console for traffic visibility, policy management, and troubleshooting across both clouds, replacing the disjointed, cloud native toolset they had previously relied upon.
- **Overlapping IP Resolution for SAP:** Aviatrix resolved the overlapping IP address conflicts within the SAP environment through its network address translation capabilities, eliminating the need for a disruptive re-addressing project. By applying SNAT and DNAT policies at the gateway layer, the company was able to connect SAP tiers across AWS and Azure despite conflicting address spaces, enabling seamless communication without modifying the underlying network architecture of either cloud environment.
- **Infrastructure as Code and Automation:** The Aviatrix platform's support for Terraform-driven deployment enabled the company to manage gateway provisioning and policy updates programmatically, supporting DevSecOps workflows and reducing the manual overhead associated with operating a distributed multicloud environment.

Results and Business Value

The deployment of the Aviatrix Cloud Native Security Fabric delivered immediate and measurable outcomes for the company's cloud operations, security posture, and long-term scalability.

Key Result	Business Value
Unified Multicloud Networking	Replaced fragmented, cloud native connectivity constructs and chokepoint security with a single, repeatable Aviatrix transit architecture across AWS and Azure, eliminating technical debt and establishing a consistent operational model across both environments. Overlapping IP address conflicts in the SAP environment were resolved through Aviatrix SNAT and DNAT policies, enabling seamless cross-cloud SAP connectivity without a disruptive re-addressing effort.

Enterprise-Grade High Availability	Deployed HA gateway pairs throughout the environment, protecting mission-critical veterinary platforms from network-level outages and ensuring continuous availability for the 100,000+ practices the company serves globally.
Defense-in-Depth East-West Enforcement	The Aviatrix Distributed Cloud Firewall added an identity-aware enforcement layer alongside the existing NGFW architecture, closing the coverage gaps that CIDR-based policies could not address. SmartGroup-based Communication Governance delivered workload-aware policies across SAP environments, Kubernetes workloads, and mixed-workload subnets, establishing a defense-in-depth posture that the NGFW or chokepoint layer alone could not achieve.
Centralized Visibility and Operational Efficiency	Unified network observability across AWS and Azure through Aviatrix CoPilot, reducing troubleshooting time, improving audit capability, and enabling the network and security teams to operate from a single platform rather than disparate cloud native consoles.
Scalable Foundation for Growth	A multi-region architecture managed under a unified control plane, demonstrating the platform's ability to scale with the company's expanding cloud footprint without adding operational complexity. A 3-year strategic commitment reflects confidence in Aviatrix as a long-term infrastructure partner.

Key Takeaways

Category	Description
Company	Global Animal Health Technology Leader. Serves 100,000+ veterinary practices across North America, Europe, and Asia-Pacific. Approx $4.5B revenue, private company.
Core Challenges	1. Multicloud connectivity complexity across AWS and Azure with no unified control plane. 2. Insufficient east-west security: CIDR-based NGFW policies could not protect SAP, Kubernetes namespaces, or mixed workload types. 3. Supply chain operations visibility gap across disconnected cloud native tools. 4. SAP availability risk and overlapping IP address conflicts across cloud environments driving the decision to rearchitect.
Aviatrix Solution	Deployed a unified Aviatrix Cloud Native Security Fabric across AWS and Azure. HA gateway pairs across multiple regions established a scalable, reliable multicloud backbone. Aviatrix DCF activated for Zero Trust east-west enforcement via SmartGroup-based policies.

Key Security Wins	Aviatrix Distributed Cloud Firewall added an identity-aware enforcement layer alongside the existing NGFW architecture, closing gaps that CIDR-based policies could not address. SmartGroup policies delivered consistent east-west coverage for the SAP environment, Kubernetes namespaces, and mixed-workload subnets, establishing a defense-in-depth security posture across AWS and Azure.
Results	Unified multicloud transit architecture. Enterprise-grade HA for mission-critical applications. Zero Trust east-west enforcement. Centralized visibility via CoPilot.

About Aviatrix

Aviatrix® is pioneering the Cloud Native Security Fabric – the architecture the Containment Era requires. The Cloud Native Security Fabric governs every workload communication path across every cloud, every VPC, every Kubernetes cluster, and every serverless function, from a single policy plane. One rule. Universal propagation. Enforced at the workload, not at a chokepoint. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.