AVIATRIX®

CASE STUDY

Leading Academic Medical Center Closes HIPAA Encryption Gap and Builds a Secure Multicloud Foundation for Clinical AI and Digital Pathology with Aviatrix

A Leading Academic Medical Center and Top-50 Integrated Delivery Network (IDN) operates more than 200 care locations across its metropolitan area, including six inpatient facilities and a broad network of outpatient and physician practice sites. The organization has built one of the most ambitious clinical innovation programs in U.S. healthcare: more than 30 AI models in active clinical and operational use, a large language model trained on over a decade of inpatient clinical notes to support predictive care workflows, and more than 40 million medical images in cloud storage supporting its digital pathology and radiology programs. Epic EHR anchors clinical operations, with telemedicine, digital pathology, and AI-assisted workflows all built on top of it.

To support this level of innovation, the organization built a multicloud environment with AWS as its primary platform and largest workload footprint, Azure as a secondary environment, and GCP for emerging workloads, alongside two on-premises datacenters that continue to host core systems including Epic. As new technology leadership took the helm and clinical workloads including digital pathology and AI/ML applications accelerated their migration to cloud, the gaps in the existing architecture became critical: no end-to-end encryption across cloud environments, fragmented operations across three hyperscalers with no unified model, security loopholes in Azure, and no consistent visibility for compliance.

To close these gaps, the organization selected Aviatrix and its Cloud Native Security Fabric (CNSF), delivering end-to-end encryption across AWS, Azure, GCP, and on-premises environments to meet HIPAA requirements, unifying multicloud and datacenter connectivity under a single architecture, and integrating Palo Alto firewall service insertion to close Azure security loopholes as part of a defense-in-depth posture.

A Growing Clinical Innovation Agenda Exposed Critical Gaps in Cloud Architecture

As the medical center accelerated its migration of clinical workloads to cloud, the limitations of its existing architecture became a constraint on both compliance and innovation. Private circuits without end-to-end encryption, three separate cloud environments with no unified operating model, security gaps in Azure, and the operational burden of managing a complex multicloud environment without automation created compounding risk for an organization handling some of the most sensitive data in healthcare.

01 Strengthening End-to-End Encryption Across the Multicloud

The organization's cloud environments were connected through private circuits from cloud service providers. These circuits were complemented by application-level encryption and point-to-point encryption capabilities that protected sensitive data in transit. As workloads including digital pathology applications, medical image repositories containing tens of millions of images, and AI model training pipelines continued to expand across AWS, Azure, GCP, and on-premises datacenters, the organization determined that establishing a consistent, uniform encryption layer across all environments was the next step in maturing their security posture – ensuring that HIPAA requirements for data in transit were met comprehensively and at infrastructure scale, rather than relying solely on application and point-to-point controls.

02 Three-Cloud and Multi-Datacenter Complexity Without a Unified Operating Model

AWS served as the organization's primary cloud with the largest workload footprint, followed by Azure as a secondary environment, and GCP for emerging workloads. Two on-premises datacenters, including the one hosting the Epic EHR environment, required reliable connectivity to all three clouds as workloads migrated. Each cloud and datacenter connection was managed independently, with no shared architecture, no consistent routing model, and no unified control plane. Teams operated across multiple toolsets, and the absence of a single operational model made it difficult to enforce consistent policies, troubleshoot issues efficiently, or support the pace of application migration the organization required.

03 Security Loopholes in Azure Required Firewall Service Insertion

The organization had deployed Palo Alto firewalls as part of its security architecture but had identified specific security loopholes within the Azure environment that the existing configuration could not close. Routing and traffic inspection gaps in Azure meant that certain east-west traffic paths were not being inspected by the firewall, creating blind spots in an environment hosting sensitive clinical and research workloads. The organization needed a way to ensure all Azure traffic was routed through the Palo Alto firewalls consistently, without requiring a manual reconfiguration of every workload or relying on native Azure constructs that had already demonstrated their limitations.

04 Skills Gap and Operational Complexity Slowed Cloud Migration

The cloud networking team faced a skills gap that made operating a three-cloud, multi-datacenter environment increasingly difficult to sustain. Application migration was hampered by the complexity of configuring cloud networking for each workload, and the absence of Terraform-driven automation meant that every new application required significant manual effort. App owners across the organization struggled to provide the network and security requirements their workloads needed, slowing migrations and creating a backlog of clinical applications waiting to move off legacy infrastructure. The team needed a platform that could simplify operations through Infrastructure as Code and reduce the per-application overhead of onboarding workloads to cloud.

Decision Making and the Aviatrix Solution

The organization's technology leadership defined a clear set of requirements: end-to-end encryption across all cloud and on-premises environments to satisfy HIPAA obligations, a unified networking architecture spanning AWS, Azure, GCP, and two datacenters under a single operating model, consistent Palo Alto firewall service insertion in Azure to close the security gaps the existing configuration had left open, and Terraform-driven automation to reduce the operational burden on the cloud networking team. A partner introduced Aviatrix as the platform best positioned to address all four requirements simultaneously. After evaluation, the organization selected Aviatrix and deployed the Cloud Native Security Fabric across its full multicloud and on-premises environment.

The Aviatrix CNSF delivered the following core capabilities:

- **End-to-End Encryption Across AWS, Azure, GCP, and On-Premises:** Aviatrix established encrypted tunnels across all cloud environments and the on-premises datacenters, closing the HIPAA encryption gap that private circuits alone could not address. All traffic traversing the Aviatrix fabric, including data in transit between cloud workloads and between cloud and datacenter environments, is encrypted end-to-end, providing the compliance posture required for clinical and research data at scale including digital pathology, medical imaging, and AI model workloads.

- **Unified Multicloud and Datacenter Transit Architecture:** Aviatrix delivered a single, repeatable transit architecture spanning AWS, Azure, GCP, and two on-premises datacenters, replacing independent configurations with a consistent operational model. HA gateway pairs were deployed throughout, providing enterprise-grade redundancy for Epic EHR connectivity and ensuring reliable, encrypted access to cloud-hosted clinical workloads.

- **Palo Alto Firewall Service Insertion for Defense-in-Depth:** Aviatrix resolved the Azure security loopholes by enabling consistent Palo Alto firewall service insertion across the Azure environment. By routing all east-west and north-south traffic through the Palo Alto firewalls via the Aviatrix data plane, the organization closed the traffic inspection gaps that native Azure routing had left open, establishing a defense-in-depth security posture without requiring workload-level reconfiguration.

- **Terraform-Driven Automation to Address the Skills Gap:** The Aviatrix platform's native Terraform support enabled the team to manage gateway provisioning, policy configuration, and network changes programmatically. Automating cloud networking through Infrastructure as Code reduced the per-application overhead of migrations, allowed the team to operate a complex multicloud environment with existing skill sets, and established a repeatable process for onboarding clinical workloads to cloud.

- **Centralized Visibility via CoPilot for Compliance and Operations:** Aviatrix CoPilot provided a unified operational console for traffic visibility, policy management, and troubleshooting across all three clouds and the on-premises environment, replacing disconnected cloud native toolsets with a single audit-ready platform that supports ongoing HIPAA compliance validation.

Results and Business Value

The deployment of the Aviatrix Cloud Native Security Fabric addressed each of the organization's critical infrastructure challenges, delivering HIPAA-compliant encryption, unified multicloud operations, and a secure foundation for its clinical innovation agenda.

Key Result	Business Value
HIPAA-Compliant End-to-End Encryption	Aviatrix closed the encryption gap across AWS, Azure, GCP, and on-premises environments, providing end-to-end encrypted connectivity for all workloads in transit. The organization can now demonstrate HIPAA compliance for data in motion across its full cloud and datacenter footprint, including digital pathology, medical imaging, and AI/ML workloads.
Unified Multicloud and Datacenter Architecture	A single Aviatrix transit architecture spanning AWS, Azure, GCP, and two on-premises datacenters replaced fragmented, cloud native connectivity configurations, establishing a consistent operational model and reliable encrypted connectivity between cloud environments and the Epic EHR datacenter.
Azure Security Loopholes Closed via Firewall Insertion	Aviatrix enabled consistent Palo Alto firewall service insertion across the Azure environment, closing the traffic inspection gaps that native routing had left open. Combined with existing perimeter controls, the organization achieved a defense-in-depth security posture across its full cloud environment.
Operational Simplification Through Automation	Terraform-driven deployment and configuration management reduced the per-workload overhead of cloud networking, accelerated application migrations, and allowed the team to operate a three-cloud, multi-datacenter environment with existing skill sets without manual per-application network configuration.
Secure Foundation for Clinical Innovation	With end-to-end encryption, unified connectivity, and consistent security enforcement in place, the organization established the secure cloud foundation required to migrate and scale its most sensitive clinical workloads, including digital pathology applications, medical imaging repositories, AI model training pipelines, and Databricks analytics environments.

Key Takeaways

Category	Description
Company	Leading Academic Medical Center and Top-50 IDN. Operates more than 200 care locations including 6 inpatient facilities. 30+ AI models in production, 40M+ medical images in cloud storage, digital pathology and telemedicine integrated with Epic EHR. Multicloud across AWS (primary), Azure, and GCP, plus two on-premises datacenters.
Core Challenges	1. No end-to-end encryption across cloud environments, creating a HIPAA compliance gap. 2. Three-cloud and multi-datacenter complexity with no unified operating model. 3. Security loopholes in Azure requiring consistent Palo Alto firewall service insertion. 4. Skills gap and operational complexity slowing clinical workload migration to cloud.
Aviatrix Solution	Deployed Aviatrix Cloud Native Security Fabric across AWS, Azure, GCP, and two on-premises datacenters. End-to-end encrypted tunnels closed the HIPAA compliance gap. Palo Alto firewall service insertion closed Azure security loopholes in a defense-in-depth model. Terraform-driven automation reduced per-workload migration overhead.
Key Security Wins	End-to-end encryption enforced across all cloud and datacenter traffic, satisfying HIPAA requirements for data in motion across digital pathology, medical imaging, and AI/ML workloads. Palo Alto firewall service insertion via Aviatrix closed Azure traffic inspection gaps, establishing a consistent defense-in-depth posture.
Results	HIPAA-compliant E2E encryption across the full multicloud and on-premises environment. Unified transit architecture across AWS, Azure, GCP, and two datacenters. Azure security loopholes closed via Palo Alto service insertion. Terraform automation accelerating clinical workload migrations. Secure foundation for digital pathology, medical imaging, and AI/ML at cloud scale.

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.com.