AVIATRIX®

The Healthcare Architectural Divide: Securing PHI at Software Speed

Healthcare cloud adoption has accelerated at unprecedented speed – 70% of U.S. hospitals now leverage cloud infrastructure for remote patient monitoring, AI diagnostics, genomic research, and disaster recovery.

Organizations have deployed EHR systems, telehealth platforms, pharma automation, and big data analytics across AWS, Azure, GCP, and hybrid environments – evolving from lift-and-shift to cloud-native architectures built on serverless functions and container-based microservices.

The bottom line: **Healthcare is modernizing at software speed. Security architecture is not.**

The Architectural Divide

Healthcare organizations are attempting to secure cloud-native workloads with data center-era tools. The result: PHI and other sensitive data are exposed across environments that teams can see but cannot adequately protect.

Legacy tools are creating the gap:

1. Perimeter firewalls designed for static networks – not ephemeral cloud workloads
2. VPN tunnels capped at 1.25 Gbps – throttling medical imaging and large-data workflows
3. Manual policies that cannot prove continuous compliance for dynamic applications
4. Separate control planes per cloud provider – no unified visibility or enforcement

The Problem: A Mismatch of Velocity and Trust

You are held accountable for protecting PHI across environments you cannot fully see, using controls designed for a perimeter that no longer exists.

What this looks like day-to-day:

Tool sprawl. Separate security stacks for AWS, Azure, GCP, and on-prem – each with different policy languages, logging formats, and enforcement mechanisms. You can't hire or train fast enough to master all of them.

Security bypass. Developers wait days for firewall rule changes, so they route around security to meet deadlines.

Compliance blind spots. Auditors demand proof of continuous encryption and per-session authorization. Your tools only show snapshots of static configurations – not real-time traffic flows.

When the Divide Becomes a Breach

- The anatomy is predictable: an attacker compromises a credential via phishing or a misconfigured identity policy. MFA stops external access – but once inside, the network is wide open. Identity systems lack network context; network controls ignore workload identity.
- The attacker moves laterally through IP-based trust, discovering PHI repositories your team didn't know were exposed. Your posture tool flags the misconfiguration in the next scan – but the exfiltration is already complete.

To learn more about how Aviatrix closes the Architectural Divide, visit aviatrix.ai

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.