



ARMATURE
SYSTEMS

CASE STUDY

From Legacy to Zero Trust: How a Cell & Gene Therapy Innovator Modernized Its Global Network and Security

Industry: **Biopharma**
February 2026

The Challenge

As the client's clinical pipeline matured from discovery toward pivotal trials, their legacy perimeter based security model became an obstacle to growth.



The VPN Bottleneck: When Security Slows Science

Traditional VPNs forced international research teams to backhaul massive sequencing files through a central data center. This "tromboning" introduced high latency and hindered real-time collaboration on the large-scale genomic datasets essential to modern diagnostics.



A Complex Regulatory and Data Sovereignty Landscape

Operating across the US and EU, the client faced mounting pressure to demonstrate data sovereignty, ensuring patient genomic data remained within specific jurisdictions while still enabling global analysis. Meeting this requirement was a manual, audit-heavy burden.



Securing Automated Manufacturing

The integration of automated lab equipment and cell-processing hardware introduced new IoT vulnerabilities. A lean IT team found itself overwhelmed by disconnected alerts spanning both cloud environments and the lab floor.



Slow Affiliate Onboarding

Following a hub-and-spoke model, onboarding new research affiliates often took months, the result of incompatible legacy network stacks and a fragmented security toolset.

The Partnership

The client is a cell and gene therapy innovator with R&D hubs spanning the US and Europe, running decentralized clinical trial sites and specialized cell therapy manufacturing facilities. As their clinical pipeline matured toward pivotal trials, they needed a security partner who could keep pace with the science, not slow it down.

Armature Systems served as that partner, transitioning them from a fragmented, legacy infrastructure to a unified, identity-centric security model. By implementing a SASE framework alongside a 24/7 MDR program, Armature enabled the client to meet stringent FDA and GDPR requirements without slowing the pace of scientific discovery.

Our Solution

Armature Systems implemented a strategy centered on operationalizing security: ensuring that technology accelerated the business rather than constrained it.

1

EVOLVING BEYOND VPN WITH SASE

Armature redesigned the network using a SASE model, converging networking and security into a single cloud-delivered service:



Direct-to-Cloud Access

SASE allowed global scientists to connect securely to cloud-based R&D environments via the nearest Point of Presence (PoP), cutting the “VPN lag” that stalls data-heavy analysis.



Zero Trust for Affiliates

Using Zero Trust Network Access (ZTNA), the client can now grant specific, identity-based access to third-party Contract Research Organizations (CROs) or newly integrated research teams without exposing the entire corporate network.

2

REGULATORY ALIGNMENT & DATA INTEGRITY

Armature moved compliance from a “check-the-box” activity to an automated baseline:



Automated Evidence Collection

By centralizing security at the edge, the client gained a “Single Source of Truth” for access logs, essential for proving data integrity during regulatory audits.



Geofencing & Sovereignty

SASE policies were configured to ensure sensitive patient data stayed within designated regions, satisfying global privacy laws automatically.

3

24/7 MANAGED DETECTION AND RESPONSE (MDR)

To protect intellectual property (IP) and clinical manufacturing lines, the client onboarded to Armature’s MDR service:



Proactive Threat Hunting

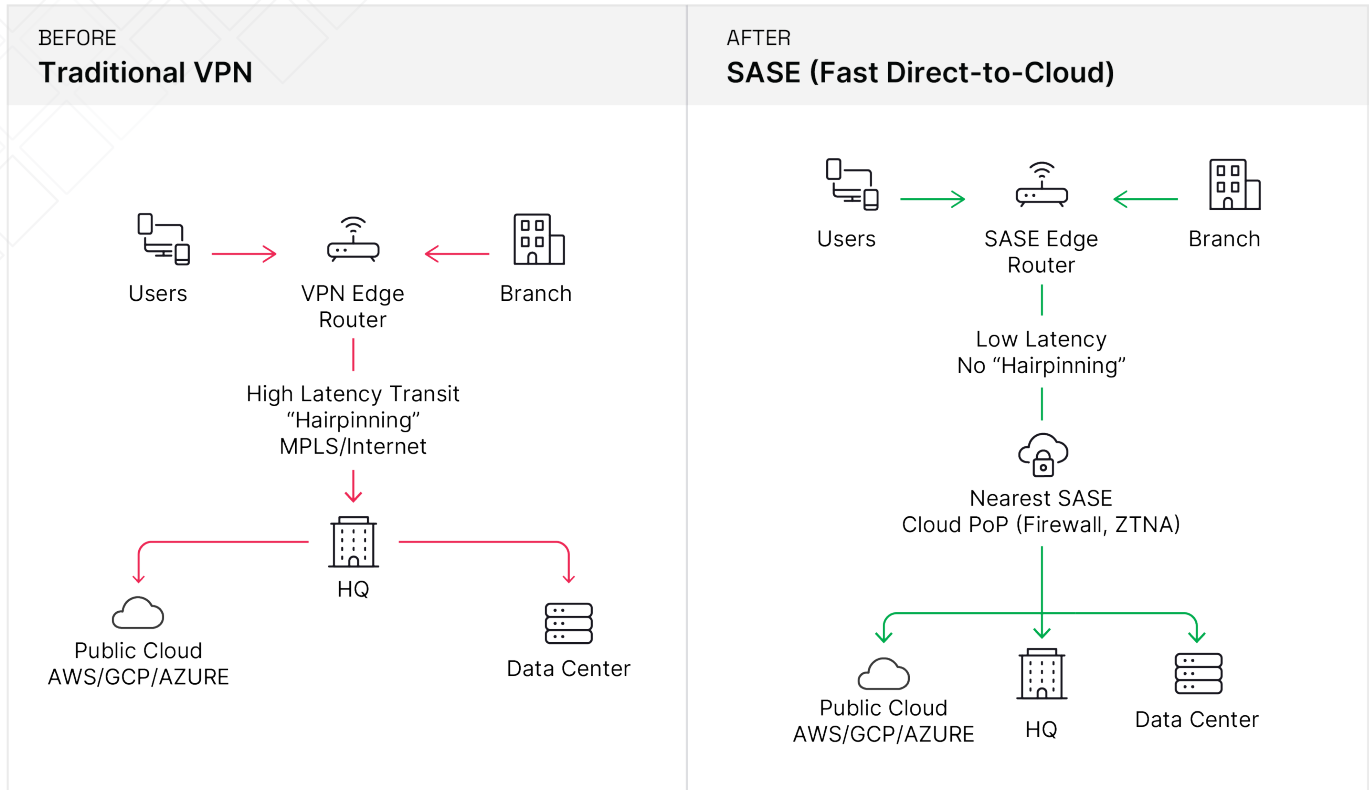
SOC analysts search for threats targeting proprietary genetic sequences or therapeutic platforms.



Clinical-First Response

Incident playbooks were customized to ensure security actions (like isolating a workstation) never inadvertently disrupt a live, time-sensitive cell-processing run.

The Outcomes



Accelerated Data Velocity

Replacing legacy VPNs with SASE reduced network latency enabling near-instantaneous sharing of large-scale data across global sites.

Faster Affiliate and Partner Onboarding

The time to value for on-boarding new research groups dropped from weeks to days through unified cloud-edge policies.

Continuous Compliance Posture

The client transitioned to a continuous audit state, with automated reporting satisfying global regulators and internal stakeholders alike.

Focus on the Pipeline

With Armature's SOC monitoring the environment 24/7, the internal IT team was freed from firefighting to focus on high-value initiatives like Bio-IT and lab automation.



ARMATURE
S Y S T E M S



ABOUT ARMATURE SYSTEMS

Armature Systems is a cybersecurity systems integrator that helps organizations design, build, and operate network and security programs across the full lifecycle.

We work hands-on alongside internal teams to deploy the right technology, build effective processes, and deliver measurable security outcomes across network, cloud, identity, compliance, and threat response.

Ready to modernize your security program? Visit armaturesystems.com