alkira

COMPARISON GUIDE

# Modernizing Healthcare Connectivity

Comparing Network Infrastructure-as-a-Service (NIaaS) and Build-and-Operate Cloud Networking Overlays

## 5 Things to Know: NIaaS vs. Build-and-Operate Cloud Networking Overlays

A Practical Model Comparison Guide for Infrastructure, Cloud, and Network Teams

### 1 SCOPE

**NIaaS** supports enterprise-wide connectivity with a unified policy model across clouds, data centers, clinics, and partners.

**Build-and-operate cloud networking overlays** typically focus on cloud environments and may require additional tools for non-cloud needs.

### 2 WHO RUNS IT

**NIaaS** is delivered as a service with centralized control through a SaaS portal. Zero hardware or software to deploy.

**Build-and-operate cloud networking overlays** require your teams to design, deploy, patch, scale, and troubleshoot controllers and gateways per cloud, which increases operational burden as scope grows.

### 3 POLICY MODEL

**NIaaS** centralizes segmentation intent and enforcement across domains, reducing translation gaps that lead to drift.

**Build-and-operate cloud networking overlays** often depend on per-cloud primitives and overlay constructs, which can be hard to keep consistent across clouds, sites, and partner paths.

### 4 BEYOND PUBLIC CLOUD

**NIaaS** is designed to connect hospitals, clinics, DR sites, SaaS, and partner networks as a single operating scope.

**Build-and-operate cloud networking overlays** are optimized for public cloud connectivity and can become a multi-tool design when you add clinics, medical device networks, or partner exchange.

### 5 DESIGN APPROACH

**NIaaS** prioritizes operational simplicity, repeatable change, and consistent segmentation at enterprise scale.

**Build-and-operate cloud networking overlays** add components and coordination overhead, which increases misconfiguration risk and change friction in regulated, uptime-sensitive environments.

## Is Alkira NIaaS Right for You?

**Best Fit For:**

Healthcare networks that need **consistent PHI segmentation** across hospitals, clinics, clouds, SaaS, and partners

Teams that want **as-a-service operations** with fewer infrastructure components to deploy, patch, and manage

Organizations optimizing for **clinical uptime** and faster, safer change windows

Health systems that regularly onboard **new sites, acquired practices, and external partners** and need repeatable connectivity and audit evidence

*Not sure? Talk to our team. We'll help you map fit and value across your environment.*

# Expanded Operating Model Comparison

| Consideration Points | NIaaS | Build-and-Operate Cloud Networking Overlays |
|---|---|---|
| **Speed to Value** | • Delivered as a service with a cloud-delivered global fabric<br>• Bring new regions, clinics, and partner connections online within hours or days via repeatable workflows<br>• Faster onboarding for acquisitions, new ambulatory sites, and DR readiness | • Requires architecture design plus deployment of multiple components per cloud/environment<br>• Expansion typically adds more build steps, integration, and validation<br>• Timelines often extend as you add clinics, non-cloud sites, and third-party connectivity. Bringing up sites can take weeks or months |
| **Control & Visibility** | • Centralized SaaS portal for policy, telemetry, and operations<br>• End-to-end visibility across cloud and non-cloud scope<br>• Easier to generate unified evidence for audits and incident response | • Visibility split across overlay tooling, cloud consoles, and monitoring systems<br>• Cross-domain troubleshooting becomes manual correlation across tools<br>• Audit reporting often requires stitching data from multiple sources |
| **Operational Model** | • Network infrastructure delivered -aaS with SLAs and standardized operations<br>• Reduces day-2 load across cloud, network, and security teams<br>• Operational overhead scales more predictably as footprint grows | • Your teams own lifecycle management for controllers, gateways, routing, upgrades, and scaling<br>• Incident handling and interoperability are on you<br>• Ops effort rises with every new region, cloud, site, and partner path |
| **Security Posture** | • Centralized segmentation and policy enforcement across domains<br>• Supports PHI isolation and least-privilege access patterns<br>• Repeatable controls across hybrid scope with fewer drift points | • Security posture becomes a blend of overlay policy, cloud-native controls, and third-party tooling<br>• Equivalent controls across clouds/sites are harder to maintain consistently<br>• Drift risk increases as policies are translated across multiple systems |
| **Deployment Speed & Complexity** | • Fewer moving parts for clinics and partner connectivity<br>• Changes follow consistent workflows via UI, API, or MCP Server<br>• Reduces change risk during tight maintenance windows | • Requires deploying and linking components in each cloud<br>• Additional design work for clinics, partner exchange, and DR paths<br>• Complexity and misconfiguration risk increase as scope expands |