alkira
A Lumen Connect® Solution

COMPARISON GUIDE

# Modernizing BFSI 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 MATTERS

**NIaaS** supports enterprise-wide connectivity with unified policy across clouds, data centers, branches, 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 a fully managed service where network infrastructure is deployed on demand and operated through a centralized SaaS portal. Zero hardware or software to deploy and manage.

**Build-and-operate cloud networking overlays** require internal teams to design, deploy, and maintain the entire control plane. This includes managing controllers, gateways, and routing across each cloud, which increases operational effort, demands specialized expertise, and introduces more risk as the environment grows.

### 3 POLICY MODEL

**NIaaS** offers an abstracted, centralized policy model that spans clouds, regions, and sites.

**Build-and-operate cloud networking overlays** rely on managing cloud-native constructs like route tables and security groups within each environment, which can be complex to maintain and difficult to standardize consistently at scale.

### 4 BEYOND PUBLIC CLOUD

**NIaaS** supports non-cloud environments like DR sites and partner interconnects by offering a single fabric, delivered -aaS.

**Build-and-operate cloud networking overlays** are designed primarily for public cloud environments. Extending connectivity to data centers, branches, or partner networks often requires separate tools or additional design effort.

### 5 DESIGN APPROACH

**NIaaS** prioritizes simplicity and speed with a unified network fabric, with sites brought up within hours or days.

**Build-and-operate cloud networking overlays** involve more components and coordination, which can increase complexity and operational risk at scale. New sites may take weeks or months.

## Is Alkira NIaaS Right for You?

**Best Fit For:**

Teams seeking **as-a-service** simplicity with no infrastructure to deploy or manage

Organizations needing **uniform security and segmentation** across cloud, data center, and edge

Enterprises that value **fast deployment, built-in resilience, and predictable OpEx pricing**

BFSI leaders aiming to streamline compliance and connectivity without deep networking overhead

*Not sure? Talk to our team.*

# Expanded Operating Model Comparison

| Consideration Points | NIaaS | Build-and-Operate Cloud Networking Overlays |
|---|---|---|
| **Speed to Value** | • Delivered as a service over a private, global backbone fabric<br>• Connect new clouds, branches, or acquisitions in minutes or hours<br>• Enables faster execution for M&A, cloud migration, and regulatory onboarding | • Internal teams must design and deploy components in each cloud<br>• Long project cycles delay time-to-value, taking weeks or months<br>• Slower response to compliance, M&A, or business expansion needs |
| **Control & Visibility** | • Centralized SaaS portal for real-time telemetry and policy<br>• Unified view across cloud, data center, and edge sites. No need to maintain or switch between multiple tools | • Visibility split across multiple UIs, consoles, and plugins<br>• Requires manual correlation for troubleshooting and audits |
| **Operational Model** | • Network infrastructure delivered -aaS with standardized operations and SLAs<br>• Zero infrastructure to manage or deploy, Day-2 work scales more predictably as footprint grows | • Customer-managed architecture with controller and gateways<br>• Day-to-day upkeep requires skilled engineering effort<br>• Increased operational risk from human error or misconfiguration |
| **Security Posture** | • Zero-trust segmentation built into the platform<br>• Centralized policy enforcement across hybrid environments<br>• Integrated security services without rip-and-replace<br>• Supports BFSI compliance, isolation, and access control | • Policy managed through cloud-native tools and third-party firewalls<br>• Manual effort to enforce consistent controls across clouds<br>• Extending to non-cloud environments often requires separate tooling |
| **Deployment Speed & Complexity** | • No hardware or software to deploy<br>• Cloud, site, and partner connectivity via UI, API, or MCP Server<br>• Simplifies expansion and audit-readiness | • Components (controllers, gateways, etc.) must be deployed manually in each cloud/region<br>• Scaling increases configuration overhead and risk<br>• Requires deep knowledge of cloud-specific networking constructs |
| **Segmentation & Policy Management** | • Built-in segmentation with support for overlapping IPs<br>• Centralized control for tenant isolation and segment-level policy<br>• Ideal for M&A, line-of-business separation, and compliance zones | • Segmentation via domains and policies with per-cloud tuning<br>• Overlapping IPs not supported in a single transit<br>• Policy enforcement varies by cloud and must be managed individually |