alkira
A Lumen Connect® Solution

COMPARISON GUIDE

Modernizing Technology 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, Platform, and Network Teams

1 SCOPE

NIaaS is built for enterprise-wide connectivity across clouds, regions, data centers, edge locations, and partners under one operating scope.

Build-and-operate cloud networking overlays usually start cloud-first, then expand outward, requiring additional components and tools as scope grows.

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 team to design, deploy, patch, scale, and troubleshoot controllers and gateways per cloud, then keep them consistent as regions and environments multiply.

3 CHANGE MANAGEMENT AT SCALE

NIaaS standardizes how connectivity and segmentation changes are applied across domains using a single operating workflow. Day-2 changes follow repeatable workflows across environments.

Build-and-operate cloud networking overlays can work well, but as scope expands across clouds, regions, and adjacent domains, changes often require more cross-team coordination.

4 CONSISTENT SEGMENTATION

NIaaS lets you define segmentation policy once and apply it consistently across clouds and non-cloud environments through one operating model.

Build-and-operate cloud networking overlays can centralize segmentation across multiple clouds, but as scope expands beyond cloud networks, teams often manage policy across multiple enforcement points, which increases the chance of gaps and drift over time.

5 AI & DATA GRAVITY CHANGE THE LOAD PROFILE

NIaaS is designed to be hyper-agile and scalable for high-volume east-west flows and frequent connection changes across clouds and regions, managed through one operating workflow.

Build-and-operate cloud networking overlays can work well, but AI pipelines and SaaS dependencies create more high-traffic paths and more change events, which often increases day-2 operational burden across scaling, upgrades, troubleshooting, and keeping policy consistent over time.

Is Alkira NIaaS Right for You?

Best Fit For:

Platform and infrastructure teams that need **repeatable global connectivity** across clouds, regions, and services

Organizations expanding through **new regions, new clouds, acquisitions, or new partner ecosystems**

Teams that want **operational simplicity**, with fewer moving parts to deploy, patch, and troubleshoot

Security and networking leaders who need **consistent segmentation and governance** without translating policies across multiple systems

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	• Stand up new regions and connectivity through consistent UI/API workflows • Reduce time spent building/tuning control-plane components before teams can ship. Bring sites up within hours or days • Extend the same onboarding pattern to partners and non-cloud domains as needed	• Design and deploy multiple components per cloud (controllers, gateways, routing patterns) • Expansion often adds lead time, taking weeks or months, as you operationalize guardrails and standardize deployments • Expanding beyond cloud (partners, edge sites, or on-prem connectivity) often requires additional design and integration work.
Control & Visibility	• Central portal for policy, telemetry, and operations across cloud and non-cloud scope • End-to-end visibility across regions and domains without stitching multiple consoles • Faster path tracing and issue isolation when flows span clouds and environments	• Visibility spread across overlay tooling, cloud consoles, and third-party monitoring • Cross-cloud troubleshooting often becomes correlation across multiple systems • Longer mean time to isolate issues when paths span multiple domains and tools
Operational Model	• Network infrastructure delivered -aaS with standardized operations and SLAs • Lower day-2 burden for platform, cloud, and network teams as footprint expands • Operational workflows stay consistent as you add regions, clouds, and connections	• Your teams own lifecycle operations: upgrades, scaling, incidents, interoperability • Ops burden grows with each new region, cloud, environment, and connectivity type • Standardization becomes an ongoing effort across deployments and teams
Security Posture	• Centralized segmentation and policy enforcement designed to remain consistent over time • Easier to apply governance across clouds and non-cloud domains using one model • Fewer policy “hand-offs” as scope expands into partners and adjacent environments	• Can centralize segmentation across clouds, but enforcement consistency can drift as scope expands • Security posture often combines overlay policy plus cloud-native controls and tooling • Maintaining consistent outcomes across enforcement points increases ongoing effort
Deployment Speed & Complexity	• Fewer moving parts to deploy and maintain across expanding environments • Changes follow repeatable patterns, reducing misconfiguration risk • Better fit for frequent changes typical of technology orgs (new services/regions/partners)	• More components and integration points as environments grow • More coordination required across teams to keep deployments consistent • Complexity and misconfiguration risk increase as patterns multiply