alkira
A Lumen Connect® Solution

COMPARISON GUIDE

Modernizing Manufacturing 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 designed for enterprise-wide connectivity across plants, warehouses, offices, clouds, data centers, and suppliers, with one operating scope.

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.

Build-and-operate cloud networking overlays require your teams to design, deploy, patch, scale, and troubleshoot controllers and gateways per cloud, then extend that model to sites and partners, which increases day-2 load as footprint grows.

3 CHANGE WINDOWS AND AGILITY

NIaaS makes change safer in manufacturing environments with tight maintenance windows and high downtime cost by using repeatable workflows and fewer moving parts.

Build-and-operate cloud networking overlays add components and coordination overhead, which can slow change and increase misconfiguration risk when you expand scope.

4 SEGMENTATION CONSISTENCY

NIaaS centralizes segmentation intent and enforces it consistently across domains, helping keep IT and OT access paths stable as plants and partners change.

Build-and-operate cloud networking overlays often translate intent into different per-cloud and per-site constructs, which increases drift and audit effort over time.

5 SUPPLIER AND PARTNER CONNECTIVITY

NIaaS standardizes how suppliers, OEMs, and 3PLs are connected and governed with consistent policy and onboarding workflows.

Build-and-operate cloud networking overlays often turn partner access into a custom, multi-system pattern that's harder to scale.

Is Alkira NIaaS Right for You?

Best Fit For:

Manufacturers onboarding new plants, lines, or acquired sites and needing repeatable connectivity in hours to days

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

Organizations that need consistent segmentation across IT, OT, cloud analytics, and supplier access paths

Networks that rely on third-party connectivity (OEMs, 3PLs, suppliers) and want simpler governance and troubleshooting

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	• Onboard plants, clouds, and suppliers through consistent workflows via UI or API • Simplify supplier onboarding without building a new control plane per environment • Accelerate new line rollouts, edge-to-cloud analytics, and M&A integration to days or hours	• Design and deploy multiple components per cloud • Extend the architecture to sites and partner paths as a separate effort • Expansion often takes weeks to months, slowing plant rollouts and delaying operational initiatives
Control & Visibility	• Centralized portal for policy, telemetry, and operations across cloud and non-cloud scope • Easier end-to-end troubleshooting across plant, WAN, cloud, and partner networks • Less need to stitch together multiple consoles and tools	• Visibility split across overlay tooling, cloud consoles, and third-party monitoring • Troubleshooting across plants and partner paths often requires manual correlation • More operational overhead to get end-to-end insight
Operational Model	• Service-delivered operations with standardized workflows and support • Reduces day-2 load on lean network teams as footprint grows • Supports consistent change workflows across global sites	• Your teams own lifecycle management for controllers, gateways, and routing • You manage upgrades, scaling, incidents, and interoperability • Operational burden grows with every new region, cloud, plant, and partner connection
Security Posture	• Centralized segmentation and enforcement across hybrid scope • Supports IT/OT isolation and least-privilege access (engineering, OEM support) • Helps keep controls consistent as environments evolve	• Security posture becomes a mix of overlay policy, cloud-native controls, and extra tooling • Maintaining equivalent controls across clouds, plants, and suppliers is labor-intensive • Higher likelihood of policy drift over time
Deployment Speed & Complexity	• Fewer moving parts to connect plants and partners • Repeatable connectivity and policy changes reduce misconfiguration risk • Better fit for tight maintenance windows	• Deploy and integrate components in each cloud first • Extend to sites with more appliances, tunnels, and coordination • Complexity and misconfiguration risk increase as scope expands beyond cloud-only
Segmentation & Policy Management	• Segmentation that is consistent and scales across domains • Supports isolation across plants, lines of business, and supplier networks • Helps handle overlapping IPs from acquisitions with simpler governance	• Segmentation becomes a per-domain, per-cloud exercise with more translation points • Overlapping IP support and consistent enforcement are harder across sites and partners • Policy consistency becomes harder to maintain as the environment grows