

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

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

1

RETAIL SCOPE IS NOT “CLOUD-ONLY”

NlaaS is built for retail and e-commerce’s end-to-end scope, connecting clouds and regions with stores, warehouses and DCs, contact centers, SaaS, marketplaces, payment providers, and 3PLs.

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

PEAK SEASON EXPOSES OPERATIONAL OVERHEAD

NlaaS 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 everything consistent as footprint and traffic surge.

2

3

STORE, DC & PARTNER ONBOARDING REPEATABILITY

NlaaS standardizes how you onboard new stores, pop-ups, DCs, and partners with consistent connectivity and policy workflows.

Build-and-operate cloud networking overlays typically require an increase in coordination across multiple systems (overlay + cloud consoles + third-party tooling) as you add non-cloud environments and partner paths.

SEGMENTATION CONSISTENCY = STRENGTH

NlaaS supports strict retail isolation by letting you define segmentation intent once and enforce it consistently across domains for POS and payment flows, corporate apps, guest Wi-Fi, IoT, and vendor access.

Build-and-operate cloud networking overlays can centralize some policy, but enforcement often becomes a multi-domain translation exercise, which increases drift and audit effort over time.

4

5

AI & REAL-TIME COMMERCE SPEED UP CHANGE

NlaaS keeps change manageable as you add personalization, fraud controls, real-time inventory, and ship-from-store, because more services must communicate across clouds, regions, stores, and partners, which drives more connections to deploy, more segmentation rules to keep consistent, and more changes during tight windows, and NlaaS reduces the operational load with fewer components to deploy and maintain so updates and expansions stay repeatable as scope grows.

Build-and-operate cloud networking overlays can work, but as you add regions and edge sites, your team typically ends up managing more gateways, upgrades, and policy translation, which increases day-2 effort.

Is Alkira NlaaS Right for You?

Best Fit For:

Teams expanding across **stores, fulfillment centers, and cloud regions** that need repeatable rollout and change

Organizations integrating **marketplaces, payment providers, and 3PLs** and want simpler governance and troubleshooting

Security and network leaders who need **consistent segmentation** for POS/ payment environments and vendor access paths

Lean platform and NetOps teams that want **as-a-service operations** with fewer components to deploy, patch, and scale

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



Expanded Operating Model Comparison

Consideration Points	NlaaS	Build-and-Operate Cloud Networking Overlays
Speed to Value	- Bring new regions, stores, DCs, and partners online with consistent UI/API workflows - Expansion happens in hours or days	- Design and deploy can require multiple components (controllers, gateways, etc.) per cloud - Expansion often adds weeks or months
Control & Visibility	- Centralized portal for policy, telemetry, and operations across cloud and non-cloud scope - Trace paths end-to-end without stitching tools	- Visibility split across overlay tooling, cloud consoles, and third-party monitoring - Troubleshooting often requires manual correlation across systems
Operational Model	- Network infrastructure delivered -aaS with standardized operations and SLAs - Day-2 work scales more predictably as footprint grows	- Your teams own lifecycle management for controllers and gateways - Manage upgrades, scaling, incidents, and interoperability across domains - Ops burden increases as clouds and adjacent scope expand
Security Posture	- Centralized segmentation and consistent enforcement across domains - Supports isolation for POS and payment, corporate apps, IoT, guest, and vendor access - Governance stays scalable as stores, partners, and services change	- Security posture becomes a blend of overlay policy, cloud-native controls, and additional tooling - Maintaining equivalent controls across clouds and sites is labor-intensive - Drift and inconsistent enforcement become more likely at enterprise scale
Deployment Speed & Complexity	- Fewer moving parts to deploy and operate - Changes follow repeatable patterns - Reduced misconfiguration risk during peak season freezes and tight change windows	- More components and more coordination across teams and environments - Complexity rises as you add clouds, regions, stores, DCs, and partners - Misconfiguration risk increases with scope