SOLUTION BRIEF

Modernizing Financial Services Networks: Exiting the Colocation Era

Delivering a network operating model for secure, compliant connectivity across branches, clouds, and partners, without colo hubs.

Executive Overview

Banks, insurers, and capital markets firms are under pressure to ship digital capabilities faster while meeting strict security, resiliency, and compliance requirements. Many financial services networks were built around colocation hubs to aggregate private connectivity, terminate security controls, and serve as early on-ramps to public cloud.

That model is now colliding with modern traffic patterns and operating realities. Critical applications and data move cloud to cloud, site to cloud, and across regions. Partner connectivity has expanded across fintechs, payment processors, market data providers, and outsourced services. M&A and divestitures demand repeatable integration playbooks. At the same time, teams are facing colo renewals, hardware refresh cycles, and operational fragmentation that slows change and increases risk.

This solution brief outlines an alternative approach. Reduce or replace colocation hub dependence with ***Network Infrastructure-as-a-Service (NIaaS)***, a cloud-delivered operating model that scales connectivity across clouds, data centers, sites, and partners while keeping segmentation and policy consistent.

The Financial Services Network Problem: Colo-Era Hubs Cannot Keep Up

Financial services environments have unique constraints: regulated data handling, high availability expectations, third-party connectivity at scale, and constant change. Colo-centric architectures introduce structural friction:

- ✓ **High fixed costs and refresh cycles:** cages, cross-connect fees, power and cooling, hardware lifecycle planning, and capacity expansion projects.
- ✓ **Slow change velocity:** new connections, segmentation changes, and capacity increases require physical work, long lead times, and multi-vendor coordination.
- ✓ **Operational fragmentation:** siloed tools and per-site configuration patterns create inconsistent outcomes, higher change risk, and slower troubleshooting.
- ✓ **Inconsistent segmentation and policy enforcement:** controls concentrated in hubs create blind spots as traffic shifts to cloud-to-cloud and partner-heavy flows.
- ✓ **Resiliency complexity:** active-active designs, DR connectivity, and multi-region architectures become harder to operate when policy and routing are distributed across devices and locations.

What Modern Financial Services Networks Require

To support digital banking, real-time risk and fraud analytics, and increasing third-party ecosystems, BFSI organizations need an operating model that can deliver:

- **Any-to-any connectivity** across branches, offices, data centers, and multiple clouds
- **Consistent segmentation** for regulated workloads and sensitive data flows across hybrid and multi-cloud environments
- **Fast onboarding** for partners, new sites, and acquisitions without redesigning the network each time
- **Centralized policy and visibility** to reduce change risk and operational toil
- **Predictable consumption economics** aligned to demand variability and growth

How Alkira Fits: Network Infrastructure for Financial Services Organizations

The Alkira Platform delivers NIaaS as a cloud-delivered network fabric operated through a centralized control plane. Financial services organizations can use the platform to connect sites, data centers, clouds, and partners in a unified topology, with consistent segmentation and governance. This shifts network operations away from hardware refresh cycles and manual change workflows toward on-demand connectivity, standardized policy, and centralized control.

Core capabilities

Cloud-delivered fabric with global reach
Deploy connectivity where you need it without standing up new colo hubs or re-architecting per region.

Connect sites, data centers, clouds, and partners in a unified topology
Support hybrid and multi-cloud connectivity patterns and enable controlled partner access without forcing traffic to hairpin through centralized hubs.

Central policy, segmentation, and governance
Define segmentation intent once and apply consistently across environments to reduce drift and gaps across regulated and non-regulated zones.

Operational simplicity with a single control plane (console + API)
Standardize provisioning, change management, and visibility across the network to reduce operational burden and improve troubleshooting consistency.

On-demand consumption model
Shift from fixed, hardware-tied capacity planning to scalable service consumption that aligns with real utilization and business priorities.

Outcomes that Matter in Financial Services

Financial services leaders evaluate networking by risk exposure, audit readiness, resiliency, and speed of change. It is no longer just bandwidth.

- ✓ **Accelerate site and service rollout**
  Bring new branches, offices, cloud environments, and digital services online faster by provisioning connectivity through software rather than physical hub expansion.
- ✓ **Improve segmentation consistency for regulated data flows**
  Reduce policy drift across clouds and sites by centralizing segmentation and governance. This supports compliance-aligned architectures and improves audit readiness.
- ✓ **Reduce operational overhead and change risk**
  Consolidate control, visibility, and configuration patterns to cut manual effort and reduce the likelihood of inconsistent configurations across environments.
- ✓ **Scale partner connectivity with stronger controls**
  Onboard fintechs, payment providers, market data services, and other third parties faster with standardized segmentation and controlled access patterns.
- ✓ **Support latency-sensitive and multi-region architectures**
  Enable connectivity patterns designed for modern cloud-to-cloud and hybrid traffic flows, while supporting availability and DR requirements across regions.

Representative Financial Services Use Cases

1. **PCI-aligned segmentation for payments environments**
   Isolate payment processing and sensitive workloads across sites and clouds with consistent segmentation and governance.
2. **Fintech and third-party connectivity at scale**
   Standardize onboarding for partners and providers while controlling access to specific applications, environments, and data zones.
3. **M&A integration and divestiture readiness**
   Connect acquired entities faster using repeatable network and segmentation patterns, reducing time-to-synergy and integration risk.
4. **Multi-cloud risk analytics and fraud pipelines**
   Support high-volume data movement across clouds and regions with connectivity patterns aligned to modern data flows.
5. **Resilient multi-region application delivery**
   Connect active-active and DR environments with consistent policy and visibility across regions.

Next Steps

If you are approaching colo renewals, hardware end-of-life, expanding multi-cloud initiatives, or scaling partner connectivity, Alkira can help you modernize the network operating model without inheriting more hubs, appliances, and fragmented operations.

Visit alkira.com to learn more about the Alkira Platform.