Modernizing networks for the AI-native era

kyndryl

Contents

PAGE

Networks are the hidden catalyst for AI leadership

Behind the scenes of the AI revolution, a quiet engine drives innovation: network infrastructure. Network readiness is the decisive enabler of cloud innovation, AI maturity, and operational excellence. Networks deliver the connectivity essential for powering AI at scale. And as AI becomes more sophisticated and deeply embedded in business-critical operations, it demands more from network infrastructure. Unless they prioritize modernizing their networks, organizations risk watching their AI strategies stall, their agility erode, and their competitive edge fade.

Today, just 56% of organizations believe their infrastructure can support enterprise AI, and 67% cite a lack of network infrastructure as a blocker to cloud strategy.[1] Organizations whose networks can handle real-time, distributed workloads are outperforming their peers.

Most organizations focus their optimization programs on applications and cloud platforms, assuming the network will naturally keep pace. Kyndryl's own experience as the leading operator of mission-critical networks globally is that the converse is true: network readiness is the leading indicator of whether AI and cloud investments will scale or stall. In operating critical infrastructure for global clients, Kyndryl Bridge technology tracks lifecycle and performance data across hybrid networks, enabling Kyndryl to detect failures before they appear in cloud dashboards.

As networks evolve toward AI-grade infrastructure — programmable, observable, and adaptive in real time — organizations should view network modernization as a strategic investment in business capability. Networks should be considered as growth infrastructure rather than cost centers, and their KPIs should be aligned with AI performance, customer experience, and innovation speed.

The key barriers to network modernization include the isolation of network teams from decision-making around cloud, security and AI, and a tendency to underestimate the stresses that AI places on network latency, throughput, and reliability.

By partnering with Kyndryl, organizations can overcome these barriers and transform legacy networks into innovation powerhouses. Combining deep expertise in mission-critical infrastructure, AI-driven intelligence, and global-scale delivery, we help you design networks for speed, agility, and trust. Together, we equip your business with the modern infrastructure foundations required to unlock continuous innovation and value in the AI-native era.

From accidental complexity to intentional network architecture

AI is quickly becoming the backbone of modern business operations. Yet, amid the race to embrace and scale this transformative technology, many organizations overlook a critical enabler: their network infrastructure.

Kyndryl research confirms this disconnect: only 38% of organizations have recently invested in foundational network infrastructure.[1]

Without network modernization, even the most innovative technology strategies risk being held back by the very connectivity meant to enable them. Most enterprise networks have evolved through accumulation rather than design, leaving them fragile, costly, and lacking agility. Some 70% of CEOs reached their current cloud environment by accident, and the same unplanned approach is now extending into hybrid and multi-cloud networks.[1]

To support modern AI workloads, network infrastructure must be designed for real-time responsiveness, high-throughput connectivity, and resilience under pressure. Increasingly sophisticated models demand vast data movement at high speeds, with near-zero latency. Such demands can easily overwhelm traditional networks, exposing their every architectural weakness. What's more, legacy networks often lack the granular visibility and zero-trust segmentation necessary to protect distributed data across cloud, edge, and partner platforms. As AI-powered cyberattacks ramp up, the security risks are growing fast.

If networks are not modernized with AI in mind, organizations expose themselves to performance bottlenecks, security vulnerabilities, and operational failures that compromise business efficiency and competitive advantage.

The key challenge lies in the unintentional nature of most enterprise IT architecture. With multiple overlapping network patterns, inconsistent security models, and the lack of an architectural "north star," most organizations are ill-prepared for the AI-first future.

Simplification by design

Leaders in the AI-first economy are not just modernizing faster — they are simplifying deliberately.

The future direction is intent-based, cloud-native network architectures that:

- → Span on-prem, cloud, and edge seamlessly
- → Are designed once, executed everywhere
- → Scale without adding complexity

Organizations looking to take leadership in this space should:

- → Re-architect networks around business intent rather than legacy topology
- → Standardize connectivity patterns across environments
- → Eliminate redundant overlays and point solutions

Achieving this will require them to overcome:

- → Organizational fear of disruption
- → Vendor and contract inertia
- → Years of “temporary” fixes that became permanent

Confidence in IT infrastructure depends on network investments and modernization approaches — key findings from Kyndryl's Cloud Innovation Survey[1]

AI maturity

- Only 56% of organizations are confident that their company's IT infrastructure can support enterprise-wide use of AI
- IT personnel see AI/Automation for IT operations as the most important cloud technology investment, while line-of-business personnel cite investment in the modernization of data analytics platforms as most important

Infrastructure strategy

- Organizations with greater cloud investment success are much more confident in their IT infrastructure's ability to support enterprise-wide AI than those with less success (74% versus 47%)
- 38% of organizations have invested in their foundational network infrastructure in the last two to three years
- For 74% of organizations, technical debt is a challenge to implementing the cloud infrastructure strategy, while 67% cite insufficient network infrastructure as a challenge
- Cloud modernization strategies most commonly (29%) follow pragmatic or iterative approaches, with infrastructure-first approaches in second place (19%)

Metrics

- IT infrastructure performance is the most common metric for the success of cloud investments, followed by operating model effectiveness and business impact
- While 41% of organizations have integrated observability across cloud and on-premises infrastructure, only 17% have unified full-stack observability with AI-driven insights

Modernize networks for innovation speed, not just cost efficiency

In the Kyndryl Cloud Innovation Survey:

- **64% of leaders** are accelerating infrastructure modernization
- **50% of leaders** are enhancing network per formance specifically for AI
- **Laggards invest reactively** — and fall further behind

In Kyndryl's experience, cost-focused network programs optimize for stability, while leader-focused programs optimize for change — specifically, to increase the speed at which the business can innovate.

Leaders measure success through the following metrics:

- Time to launch new digital services
- Ability to scale AI use cases
- Resilience under spikes in demand

By modernizing networks for innovation speed rather than cost efficiency, organizations can make their networks into business accelerators, enabling:

- Faster product cycles
- Real-time customer experiences
- Continuous innovation without re-architecture

To unlock these potential benefits, Kyndryl recommends that organizations:

- Link network investment to business velocity metrics
- Prioritize automation and AI-driven operations
- Fund modernization continuously — not in bursts
- Abandon ROI models that ignore speed and opportunity cost
- Stop seeing networks as "run" infrastructure and start viewing them strategically

Embed security in network modernization

Historically, many organizations have layered security onto their networks by deploying multiple disconnected tools in an unplanned, piecemeal way. This approach is now causing serious problems, with **82% of surveyed organizations reporting major outages**. As distributed work and AI combine to dramatically expand the attack surface, security outcomes increasingly depend on network design.

Kyndryl sees that security failures stem increasingly from architectural fragmentation rather than from inadequate or missing controls. The best outcomes emerge where:

- → Zero Trust is embedded into network design
- → Security and networking operate as a single architecture
- → SASE and micro-segmentation are foundational, not optional

The future vision is one of converged network and security platforms that deliver:

- → Consistent policy everywhere
- → Built-in compliance
- → Lower operational overhead

To enable this future vision, organizations should:

- → Modernize network and security together
- → Collapse overlapping tools into unified architectures
- → Design for identity, not location
- → Break down organizational silos between network and security teams
- → Reject perimeter-based thinking in favor of holistic approaches

Engineering networks for AI advantage

Kyndryl helps organizations modernize their networks to accelerate data flow, reduce latency, and increase resilience. Our modernization methodology centers on three core principles of transformation.

01.

Build trusted foundations infrastructure-up

For mission-critical and agentic workloads, taking an infrastructure-up approach establishes the architecture needed to enable safe deployment and orchestration. Key points to consider include:

- Security, identity, and access controls.
- Observability and governance frameworks to promote auditability and traceability.
- Integration and orchestration across infrastructure, applications, and data layers.
- Infrastructure resilience to support growing compute and data demands.

This infrastructure-up approach supports agentic workflows across the hybrid reality in which most enterprises operate: mainframe, distributed, and cloud. Agents can gather context where it lives and execute actions where they belong.

02.

Start from business applications and rules

Applications are where customers engage, employees work, and AI delivers value. Applications embody business capabilities and experience, so modernization must be application-led.

At the same time, execution must be rules-first. This is a critical inversion of traditional approaches, which move problems to new platforms without first addressing the underlying technical debt. Rules-first execution helps ensure that business and technical objectives, regulatory requirements, and security standards are incorporated at the outset of modernization.

This approach eliminates guesswork and preserves the required business logic while enabling faster, higher-quality, and more predictable modernization. The result is applications that are not just technically current, but adaptive, secure, and ready to host agent-driven experiences without reintroducing technical debt.

03.

Operate a continuous modernization model

A continuous modernization model sees operational spending continuously reinvested in agent-driven modernization. Rather than large, risky programs that take years, organizations modernize incrementally and safely in weeks and months, guided by business priorities and validated by agents at each step.

An infrastructure-up foundation is critical for supporting continuous modernization by ensuring observability (continuously assessing system health), governance (sustaining compliance through continuous change), orchestration (executing changes safely across layers), and resilience (maintaining business continuity during modernization).

Benefits

By moving from hardware-heavy, on-premises networks to cloud-native, software-defined hybrid networks, organizations can reduce time-to-market for AI initiatives while introducing stronger security, greater efficiency, and enriched experiences for employees and customers alike.

01

Accelerate AI initiatives

- → Enable real-time AI inference and training with high-bandwidth, low-latency connectivity.
- → Support agentic AI workloads by handling unpredictable data flows.
- → Optimize performance to cut AI deployment time and achieve higher ROI.

02

Strengthen security and resilience

- → Protect against AI-powered attacks and emerging quantum threats.
- → Reduce incident response times and simplify policy changes with unified security platforms.
- → Ensure resilient, always-on networks to prevent costly outages.

03

Elevate efficiency and cut costs

- → Automate network operations with self-healing capabilities to cut unplanned downtime.
- → Accelerate provisioning through intelligent SDN platforms.
- → Reduce infrastructure and operational costs via automation and simplified management, freeing capital for innovation.

04

Enhance connectivity and experience

- → Deliver seamless, secure connectivity for hybrid workforces with SASE and SD-WAN.
- → Enable real-time collaboration and productivity for distributed teams.
- → Maintain consistent, high-quality connections to reduce customer abandonment and improve satisfaction.

Kyndryl capabilities

As one of the largest global providers of IT infrastructure services, Kyndryl draws on decades of experience managing enterprise-grade systems across multiple industries. We bring a combination of expertise, technology, and methodology that no other provider can match.

We've built our best-in-class network modernization solution around three essential strengths, which enable CIOs to modernize with confidence and advance toward an AI-native enterprise.

01.

Mission-critical expertise

We understand, operate, and transform the systems the world depends on.

- Our experts have run and reimagined some of the world's most complex, highly regulated, always-on environments, from leading financial institutions and healthcare systems to energy grids and airlines.
- Our experience gives us unmatched visibility into how an entire IT estate behaves: the insights, dependencies, risks, and opportunities that exist across infrastructure, applications, data, and operations. It's why we can help CIOs modernize their environments with clarity, precision, and a deep understanding of what it takes to keep the business running.
- Kyndryl Bridge amplifies this expertise by analyzing billions of data points across customer estates, surfacing intelligence that accelerates modernization and enhances resilience at scale. For CIOs, this means modernization with fewer surprises, fewer disruptions, accelerated risk reduction, and shorter time-to-value.

02.

Proprietary technology and IP

A secure-by-design, agent-ready foundation for enterprise AI.

- Kyndryl's proprietary capabilities, including our Agentic AI Framework, agent ingestion tools, agent builder technology, and a growing catalog of validated AI agents, enable enterprises to orchestrate, secure, and scale AI across their most critical workflows.
- These technologies allow us to reverse-engineer an organization's existing estate, extract business logic and interdependencies, and forward-engineer modern, sovereign, cloud-native systems with embedded AI agents.
- The Agentic AI Framework is open and interoperable by design, supporting multiple hyperscalers, data environments, and AI models. All are rigorously validated for safety, transparency, compliance, and policy alignment, with humans in the loop for oversight and control. This gives CIOs the architectural control and transparency they need to deploy AI responsibly and confidently.

03.

Proven modernization and co-creation methodologies

Designed for speed, scale, adoption, and continuous improvement.

- Kyndryl's Consult methodology, together with our Kyndryl Vital co-creation approach, helps CIOs define the outcomes that matter most and rapidly translate them into a production-ready future state.
- Our forward-engineering methods minimize the time between design and deployment, enabling faster modernization cycles and greater scalability across hybrid, multi-cloud, and mainframe environments. We combine industry expertise, reference architectures, and proven engineering patterns to accelerate transformation while reducing operational risk.
- As AI reshapes work, we support CIOs with organizational change management, workforce readiness, and hybrid workforce models. By enabling people and AI agents to collaborate effectively and responsibly, we help modernization efforts to scale, rather than stall at the pilot phase.

Kyndryl network modernization services

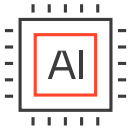
We apply modern skills, industry expertise, and IP to run and transform our customers' businesses. Our network modernization services span:

Network advisory and assessment

Evaluate your network with strategic advisory, lifecycle checks, compliance alignment, and cost optimization, building a roadmap for efficiency and future readiness.

Managed network and security services

Deliver 24/7 operations with integrated SNOC, proactive monitoring, and SLA-backed assurance for resilient, optimized network and security performance.



Intelligent and AI-driven networking

Embed AI for predictive analytics, automation, and self-healing networks, ensuring adaptive, always-on performance and real-time decision-making.

Secure and zero trust architectures

Modernize security with Zero Trust, SASE, and micro-segmentation, creating compliant, resilient networks that protect users, devices, and workloads everywhere.

Cloud and edge networking

Design cloud-first and edge-native architectures for low-latency performance, agile scaling, and near-real-time analytics across hybrid and multi-cloud environments.

Is your network ready for the AI-native era?

Contact Kyndryl to schedule a network modernization assessment and assess your network's readiness for AI transformation.

Learn more about our network modernization offerings by visiting: **https://www.kyndryl.com/us/en/services/network/modernization**

kyndryl

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Source:

1. Kyndryl Cloud Innovation Survey. 2025