WHITEPAPER

Why Enterprises Must Rethink Managed Network Services for the Autonomous Era

netOps.ai:
Our Service Delivery Platform Transforming Enterprise Networks from Operational Infrastructure into Strategic Platforms

Authors

Kumkum Datta
Competency Head,
Network Services

Nikhil Anand
Principal Consultant &
Function Head Marketing,
Network Services & CSRM

TECH mahindra

Scale at Speed™

Executive Summary

With enterprise networks becoming the operating backbone for digitally connected businesses, network performance directly determines application availability, manufacturing continuity, workforce productivity, AI scalability, and regulatory resilience. When networks fail, enterprises risk connectivity and revenue loss, compliance breaches, and declining customer trust.

However, traditional managed network service models remain rooted in siloed operations and centralized architectures that no longer align with distributed enterprise environments.

This whitepaper examines the structural shifts reshaping managed network services, including AI-led operations, Zero Trust, converged netOps and SecOps, and consumption-based models. It also explores the emergence of intelligent orchestration and how Tech Mahindra's netOps.ai repositions networks as engines of growth for the enterprise, through a phased transition that eliminates the risk of rip-and-replace-induced business disruption.

Table of **Contents**

Introduction

Enterprise networks span cloud, edge, SaaS, private infrastructure, and distributed workforces, while supporting AI adoption, real-time operations, regulatory compliance, and digital customer experiences. As a result, network performance and resilience directly influence business continuity, operational agility, and enterprise growth.

However, many managed network service models still operate on assumptions built for an earlier era of IT. Siloed operational structures, perimeter-centric architectures, static delivery models, and fragmented visibility are increasingly difficult to sustain in highly distributed environments amid growing demands for security, sovereignty, and performance. At the same time, enterprises are under pressure to align network investments more closely with business outcomes, operational flexibility, and user experience expectations.

They are increasingly questioning whether traditional managed network service models can support the resilience, agility, visibility, and business alignment required in modern digital environments.

The Forces Reshaping Managed Network Services

1. Network Resilience is Now a Board-level Priority

Modern-day network failures shut down businesses across industry verticals globally, significantly affecting payment systems, trading platforms, retail checkout operations, manufacturing, remote workforces, and healthcare delivery.

The CrowdStrike incident in July 2024 highlighted the scale of this risk. A faulty update caused crashes on 8.5 million devices globally, disrupting airports, hospitals, banks, retailers, and manufacturers.[1] Fortune 500 losses alone were estimated at $5.4 billion, with healthcare and financial services among the hardest hit sectors.[2] Delta Airlines alone is estimated to have lost $500M.[3] More than a cyberattack, the incident stemmed from a network control-plane governance failure that let an unbounded update propagate across a globally connected endpoint environment without segmentation, telemetry-driven containment, or rollback controls.

The frequency of these outages and their catastrophic impact on enterprises continues to rise. Splunk and Oxford Economics estimate that Global 2000 companies incur $400 billion in losses from unplanned downtime annually, translating to about $200 million per company (or 9% of profits), roughly $9,000 per minute or $540,000 per hour.[4] Network resilience now a boardroom priority.

2. Network Architectures are Fragmented and Distributed

Legacy network managed services models assume centralized, perimeter-centric networks. That assumption has collapsed. Modern enterprise network architectures are now distributed and fragmented across cloud, colocation, SaaS, and edge, with additional complexity introduced by sovereignty and data residency requirements.

This mix of distributed architecture and regulatory pressures presents new operational demands, including jurisdiction-aware routing, localized control planes, sovereign policy enforcement, cross-border governance, multi-cloud orchestration, and optimization across distributed traffic and cloud interconnects, beyond what traditional service providers enable.

3. Network and Security Have Converged

Distributed architectures and AI-driven threat vectors have expanded the attack surface for enterprises. Cyber incidents are now the most common cause of outages. AI-led vulnerability reconnaissance, rapid exploitation, and adaptive malware allow threats to propagate quickly across networks and security domains through lateral movement, identity compromise, and application-layer intrusion.

Hence, security needs to be intrinsically embedded in the network fabric to enforce policies, manage identity, and control access across human and non-human users, devices, APIs, and application workloads. Enterprises are increasingly adopting SASE, Zero Trust, and identity-centric models to effectuate integrated, intelligence-driven, converged NOC/SOC operations through shared telemetry, unified incident management, cross-domain workflows, AI-led detection and response, and integrated policy enforcement across users, devices, APIs, and workloads.

4. AI is Redefining the Network

AI is reshaping how enterprises manage operations by incorporating autonomous network operations and how they are structured. But scaling AI necessitates infrastructure capable of supporting model training and inference workloads. It will include GPU clusters, low-latency inferencing environments, multi-edge compute, private 5G networks, and high-bandwidth spine-leaf topologies for deterministic throughput.

5. Networking Economics are Moving to Consumption Models

Traditional network refresh cycles relied on CapEx-heavy infrastructure investments made every few years. Leasing models, which were introduced to address the recurring purchase burden, assumed that network demand would remain relatively stable over time. That assumption is no longer valid today. Enterprises must scale up networks quickly during acquisitions, geographic expansion, or AI adoption, and reduce capacity during divestitures, restructuring, or workforce changes.

Leasing models based on fixed subscription contracts lack the flexibility to efficiently support these shifts. Rising interest rates and changing business priorities are also pushing CFOs to question the viability of long-term lease commitments.

Network-as-a-Service (NaaS) models change this equation by aligning costs more closely to usage and demand. Enterprises can then scale network capabilities more dynamically, avoid long-term lock-in, and improve financial flexibility in increasingly unpredictable operating environments.

The Widening Value Realization Gap in Network Managed Services.

Traditional providers continue to differentiate themselves through global scale, operational maturity, vendor ecosystem breadth, and transformation expertise, capabilities largely optimized around cost-to-serve. However, enterprises increasingly prioritize cost-to-outcome, driven by demands for real-time visibility, cloud orchestration, private 5G, and AI integration, user experience accountability, sustainability, and financial flexibility. This creates a misalignment between how services are delivered and how enterprises realize value.

This is a structural gap. Legacy models measure success through standardization, labor arbitrage, SLA adherence, and siloed operational efficiency. Enterprises, on the other hand, measure it through business impact, including revenue growth, speed to market, customer experience, compliance, resilience, and risk reduction.

To address the gap, enterprises are shifting away from siloed operational models toward end-to-end orchestration through a unified control layer spanning network, security, cloud, and edge environments. They need to replace siloed operations with a cohesive, AI-driven service delivery platform that more directly aligns network operations with business outcomes.

The table below demonstrates the operational gaps in traditional managed services models and the orchestration capabilities enterprises are increasingly prioritizing to bridge the gap between cost to serve and cost to outcome.

Operational Gap	Severity	Enterprise Impact	What Enterprises Are Looking For
Limited real-time netOps execution	High	Slower root cause isolation with overreliance on escalations	AI native netOps execution, telemetry-based visibility, faster RCA, higher FCR, and multivendor runtime control across hybrid environments
Fragmented operational visibility	High	No single pane of glass view delays triage, and low confidence in results	Unified service delivery platform (SDP) with integrated observability, service intelligence, and end-to-end visibility across networks, security, cloud, and applications
Cost-to-Outcome Inefficiency	High	Manual, labor-heavy economics fixed-term leasing models lack flexibility and limit NaaS adoption	Platform-led service delivery with automation at scale, outcome-based pricing, and flexible service-based consumption models (NaaS)
Automation without outcomes	High	Siloed tooling results in uneven automation and an inability to realize business outcomes.	AI Ops and automation tied to business KPIs, SLA/XLA outcomes, and closed-loop, intent-driven execution across domains
SLA / customer employee experience mismatch	Medium	Static network uptime SLAs result in weak experience or outcome accountability	XLA-based assurance with app awareness, user experience-centric metrics, and contractual accountability to business outcomes
Siloed NetOps and SecOps	Medium	Fragmented threat visibility results in slow cross-domain correlation of threat vectors, propagating threats across the enterprise	Converged NOC/SOC operations enabled by shared telemetry and unified response workflows
AI claims without business impact	Medium	Dashboard-level AI comes with no measurable service or business outcome impact	AI (AIOps + GenAI + agentic AI) embedded into process workflows with clear maturity, governance, and outcomes linked to KPIs, enabling process and value stream efficiency
Limited compliance and sovereignty	High (regulated industries)	Overprovisioned infrastructure costs impact energy efficiency, net zero commitments, and ESG	ESG-aligned reporting integrated into network operations, leveraging AI-optimized capacity management to orchestrate network energy consumption
Limited sustainability integration	Emerging	Overprovisioned infrastructure costs impact energy efficiency, net zero commitments, and ESG	ESG-aligned reporting integrated into network operations, leveraging AI-optimized capacity management to orchestrate network energy consumption

Figure 1: Operational Gap Analysis — Where Traditional Models Fall Short

Intelligent Network Orchestration for Next Generation Managed Services

Enterprises are resetting contracts to align provider incentives with business value and integrating cost-to-outcome into their existing contracts, which is tied to operational efficiency and cost reduction. This shift forces a structural change that siloed service towers and manual operations cannot deliver. What enterprises increasingly need is a service delivery platform (SDP) that enables intelligent end-to-end orchestration across network, security, cloud, edge, private 5G, and AI infrastructure through an AI-native control layer, transforming siloed operations into a cohesive, AI-driven service delivery.

netOps.ai, Tech Mahindra's AI-native service delivery platform, is purpose-built to deliver intelligent network orchestration for next-generation managed services. It converges traditionally siloed domains, including networks, security, multi-cloud, edge, private 5G, AI infrastructure, and experience management into a single operational control plane.

The platform supports multitenant service delivery, single-pane-of-glass portal visibility, lifecycle orchestration across all phases, and managed/co-managed models.

The following matrix maps netOps.ai capabilities to enterprise operational requirements, business outcomes, and measurable KPIs. KPIs are reported through the platform's customer portal in near-real time, supported by monthly formal reviews and quarterly business reviews that link operational performance to business outcomes. Baselines are set during discovery and onboarding, with target outcomes aligned to the transformation roadmap and commercial engagement model.

Capability	Capability Description	Key Business Benefit	Measurement KPIs	Baseline KPI (Illustrated)	Target KPI (Illustrated)
A Unified Operational Control Plane	Unified control layer removing tool sprawl, end-to-end visibility across network, security, cloud, edge	Unified control layer removing tool sprawl, end-to-end visibility across network, security, cloud, edge	MTTR	6 to 12 hrs	< 30 mins (80%)
			Cross-domain correlation	Days	< 2 mins
			# Management consoles	8 to 15	Single platform
Integrated Service Lifecycle Mgmt	Orchestrate the full lifecycle from onboarding to optimization in one platform	Accelerate M&A integration, branch rollout, and digital launches with lower overhead and quicker time to market	Provisioning time	15 to 45 days	< 24 hrs
			Change success ratio	70% to 80%	> 98%
			M&A integration baseline stabilization	6 to 18 months	< 60 days
			New site onboarding	4 to 12 weeks	< 5 days
Automation and Closed-Loop Ops	AI-driven intent automation for self-healing and closed-loop operations	Shift operations from reactive to proactive, lowers cost, and improves resilience	Closed-loop remediation incidents	< 5%	60% to 80%
			Repeat incidents	25% to 40%	< 5%
			MTTC	Reactive	< 3 mins
AI-Native SDP Architecture	AI/GenAI automation for high-volume incidents; intelligent workflow orchestration	Cut costs, speed response, and free up teams for governance	FCR	30% to 50%	> 90%
			MTTA	15 to 45 mins	< 60 sec
			Alert to action time	Mins to hrs	< 2 mins
			Automation coverage	< 20%	> 80%
			RCA accuracy	50% to 65%	> 95%

Real-Time Visibility	Near real-time dashboards for SLA/XLA reporting	Enable continuous visibility with higher accountability and faster	Dashboard latency	24 to 48 hrs	< 5 mins
			SLA compliance rate	85% to 92%	> 99%
			Escalations per month	8 to 15/month	< 2 / month
			Insight lag for Stakeholders	Days <	10 mins
Converged NetOps + SecOps	telemetry, queues, workflows	correlation, and containment of cross-domain threats	MTTC	6 to 24 hrs	< 15 mins
			False positive rate	40% to 70%	< 5%
			Handoff time NOC/SOC	1 to 4 hrs	Eliminated
			Network context on security incidents	< 20%	100%
AI Infrastructure Enablement	AI workload support across GPU, low-latency, edge, and 5G environments with full observability and deterministic connectivity	Makes network AI-ready and ensures throughput, latency, reliability, and efficiency	AI training throughput rate	Variable	Sustained line rate
			Inferring endpoint latency	>200ms	< 10ms
			AI job failures	Not tracked	<0.1%
			Edge AI SLA	None	99.99%
Compliance, Governance, Sovereignty	Automated compliance (PCI, HIPAA, etc.), audit trails, sovereign routing	Maintains continuous compliance; lower audit cost, lower risk	Audit readiness	4to 12 weeks	< 4 hrs
			Violation detection time	Hours to days	< 60 sec
			Compliance score	NA	> 99.5%
			Sovereignty breaches	Unknown	Zero
			Reporting	2 to 6 weeks	On demand

Customer Experience (XLA)	Alignment of network performance with user experience and business outcomes	Balances cost and outcome, and protects experience and revenue	Application XLA score	Not tracked	>95
			DES score per cohort	Unavailable	>90
			Application response time	3 to 8s	<500ms
			Session success	Not tracked	>99.5%
			Impact incidents	Unknown	<0.5%
Sustainability and ESG	Energy-aware operations with optimized workload, capacity, routing, and built-in ESG reporting	Cuts energy, meets ESG goals, and removes manual reporting effort	Energy consumption /network workload	Not tracked	30% to 50%
			Network carbon emission	Unquantified	Net-zero aligned
			Network utilization rate	25% to 40%	70–85%
			ESG Report prep time	4 to 8 weeks	On-demand
			Renewables as % of energy	< 30%	80%+
Multi-Vendor Orchestration	Neutral layer integrating multi-vendor, hybrid cloud into one platform	Enables faster integration, avoids lock-in, and improves flexibility	Integration time	8 to 24 weeks	<2 weeks
			Correlation	< 15%	90%+
			Onboarding cost	High	60% reduction
			Consistency	Variable	Unified
Flexible Operating Models	Managed, co-managed, and hybrid models with shared control and visibility	Gives control, flexibility, and combines scale with governance control	% co-managed	<10%	40% to 60%
			Maturity	L1 to L2	L4+
			Hand back time for co-managed models	Unstructured	<4 weeks
			Satisfaction NPS/ CSAT	Not tracked	>4.5/5
			Strategic/ operational ratio	20:80	80:20

Figure 2: netOps.ai Capability Framework: Business Outcomes and Success Measurement

Transition Guidance: From Legacy to Intelligent Orchestration Platforms

The biggest barriers for enterprises moving from siloed service towers to a unified, platform-driven managed services model are the risk of operational failure, financial penalties for unfulfilled contractual obligations, and increased compliance scrutiny associated with such transitions. netOps.ai mitigates this risk by overlaying existing tools and service towers to create a unified control plane that integrates fragmented systems, separates orchestration from execution, and introduces automation in stages without disrupting operations or breaching SLAs/XLAs. The outcome is a controlled, low-risk transition, rather than a disruptive rip-and-replace overhaul.

An illustrative phased transition journey is described below:

Phase 1

Establishing Unified Visibility and KPI Baselines

The first step is to deploy netOps.ai across existing enterprise tools to establish unified visibility, monitoring, and management across the network landscape. Key performance indicators (KPIs) are then baselined to measure operational effectiveness, including mean time to repair (MTTR), first call resolution rates, tier 1 automation levels, and application-level experience level agreements (XLAs). These benchmarks support the transition to autonomous operations. Lastly, AIOps capabilities are also introduced for cross-domain correlation, anomaly detection, and root cause analysis.

Phase 2

Automation

With the foundation now established, AIOps capabilities are scaled across the network lifecycle, including provisioning, change management, and incident resolution for more autonomous operations. Shared telemetry, unified incident handling, and GenAI copilots support convergence between NOC and SOC operations with broader oversight across network and security environments.

Operational governance also shifts from traditional SLA tracking towards experience level agreement (XLA)-based assurance, tying performance metrics directly to user and application experience, and service quality to outcomes. Where required, co-managed operational models allow enterprise teams to maintain shared control and oversight during the transition.

Phase 3

Autonomy and Network-as-a-Service (NaaS)

The transition focuses on integrating agentic AI for policy-bound autonomous remediation, reducing manual intervention, and improving operational efficiency. Eligible services are migrated to a consumption-based NaaS model, while continuous compliance supports ongoing regulatory requirements and sovereign operations.

Infrastructure support for scaling AI workloads is also initiated to support the growing adoption of AI-driven applications and services. Co-managed operational models continue to evolve based on enterprise maturity, allowing enterprises to strike a balance between shared control and autonomy.

Operating Model Shift

As autonomous network maturity increases within the organization, tasks such as level 1 incident resolution, routine provisioning, and compliance monitoring are performed autonomously, reducing the operational workload of the enterprise network teams. The focus for these teams shifts from daily execution to a governance-centric role, with greater responsibility for managing vendors, ensuring outcome accountability, aligning operations with business objectives, and handling exceptions outside automated processes. This shift enables enterprises to maintain strategic oversight while benefiting from increased efficiency and automation-led reliability.

Hybrid Commercial Models for Distributed Networks

As networks become more distributed across on-premises, cloud, edge, and private mobile environments, organizations are moving away from rigid one-size-fits-all commercial models toward hybrid commercial models that integrate fixed outcome an consumption-based pricing. This approach helps enterprises balance between cost predictability, performance accountability, operational flexibility, and value realization.

Conclusion

Enterprise networks are undergoing a fundamental structural change. Modern networks now underpin digital business operations, support the scaling of AI-driven solutions, maintain regulatory compliance, and provide the agility enterprises need to adapt to changing market conditions.

In this new era, the benchmarks for success have evolved: organizations must prioritize intelligent orchestration, deepen their automation capabilities, advance in AI maturity, and deliver assurance based on the quality of user and application experience. netOps.ai exemplifies this approach by transforming traditional networks into programmable, secure platforms closely aligned with desired business outcomes.

End Notes

1. Reuters. (2024, July 20). Microsoft says about 8.5 million of its devices affected by CrowdStrike-related outage. Reuters.

https://www.reuters.com/technology/microsoft-says-about-85-million-its-devices-affected-by-crowdstrike-related-2024-07-20/

2. Sabin, S. (2024, July 24). Fortune 500 companies lost an estimated $5.4 billion from the CrowdStrike outage. Axios.

https://www.axios.com/2024/07/24/fortune-500-crowdstrike-outage-impact?

3. Torres, R. (2024, July 31). Delta grapples with $500M in CrowdStrike outage costs. CIO Dive.

https://www.ciodive.com/news/delta-crowdstrike-outage-costs/722970/

4. (2024, July 23). The hidden costs of downtime: The $400B problem facing the Global 2000. Oxford Economics.

https://www.oxfordeconomics.com/resource/the-hidden-costs-of-downtime-the-400b-problem-facing-the-global-2000/

About the Authors

Kumkum Datta

Competency Head,
Network Services, Tech Mahindra

Kumkum Datta is Global Competency Head for Enterprise Networks and leads the Growth Office for New Solutions and Partner-Led Business. She is responsible for shaping the intelligent network vision, building strategic alliances, and driving market-leading solutions across AI-powered operations, cloud networking, SD-WAN, SASE, network automation, and digital infrastructure transformation. She collaborates with customers, partners, and industry analysts to translate emerging technology trends into scalable business outcomes.

Nikhil Anand

Principal Consultant & Function Head Marketing,
Network Services & CSRM, Tech Mahindra

Nikhil is a seasoned technology leader with experience spanning telecommunications, satellite, and cloud industries. He combines deep domain expertise with strategic vision to drive innovation across the network transformation landscape. Nikhil actively collaborates with leading industry bodies, such as the TM Forum, and engages with analysts to shape forward-looking strategies and co-create solutions that address the evolving challenges of the communications and digital services sectors.

About **Tech Mahindra**

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 147,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.x.com/tech_mahindra