

Telcos are advancing toward autonomous networks powered by agentic AI, but achieving this goal requires robust real-time observability and unified data across diverse partners and platforms.

Closing the Observability Gap for Autonomous Networks and Agentic AI Services

December 2025

Written by: Chris Silberberg, Research Manager, Global Telecom Operations and Monetization

Introduction

Network service providers face a technology landscape of increasing complexity, significant cost pressures, meager revenue growth in their core connectivity products, shareholder mandates to innovate more, and escalating security threats. These challenges are coming together to make service providers accelerate their pursuit of autonomous networks to realize network efficiencies, enable new services, and respond faster to competitive forces and cybersecurity threats. Autonomous networks are able to optimize performance, resolve faults, and maintain and manage complex network services with minimal human intervention.

Observability is a foundational capability for delivering truly autonomous networks, especially as the costs of significant network disruptions continue to increase. Network outages can result in millions of dollars in economic losses and disrupt mission-critical services like healthcare and public safety. In IDC's 2025 *Telco Digital Transformation Survey*, 68% of service providers identified fragmented data silos as a top barrier to achieving real-time observability and automation. Overcoming data fragmentation through robust observability capabilities will enable service providers to proactively understand the impact of automated actions to optimize network configurations, resolve outages, and manage security threats. Over time, this observable positive impact will build service provider confidence in autonomous capabilities, empowering them to progressively automate more network functionality.

This progressive automation will rely on the development of network AI agents. Network agentic AI solutions depend on a diverse ecosystem of partners, including cloud providers, software vendors, and network equipment vendors. Again, observability is foundational to building this capability. Agentic ecosystems require shared real-time visibility into network and business operations to facilitate agents operating within and across domains. Observability de-risks these implementations by providing a single source of truth for these autonomous AI agents, ensuring they work for the benefit of the entire service, rather than the benefit of one domain to the detriment of the whole.

AT A GLANCE

KEY STATS

According to IDC's research:

- » 68% of telcos cite fragmented data across networks and IT as a key barrier to achieving real-time observability and automation.
- » 72% of telecom operators identify hyperscalers as strategic partners for AI, and 62% plan to increase their use of hyperscalers to support emerging AI workloads.
- » IDC forecasts that telcos will increase spending on service assurance and observability by 25% from 2024 to 2029.

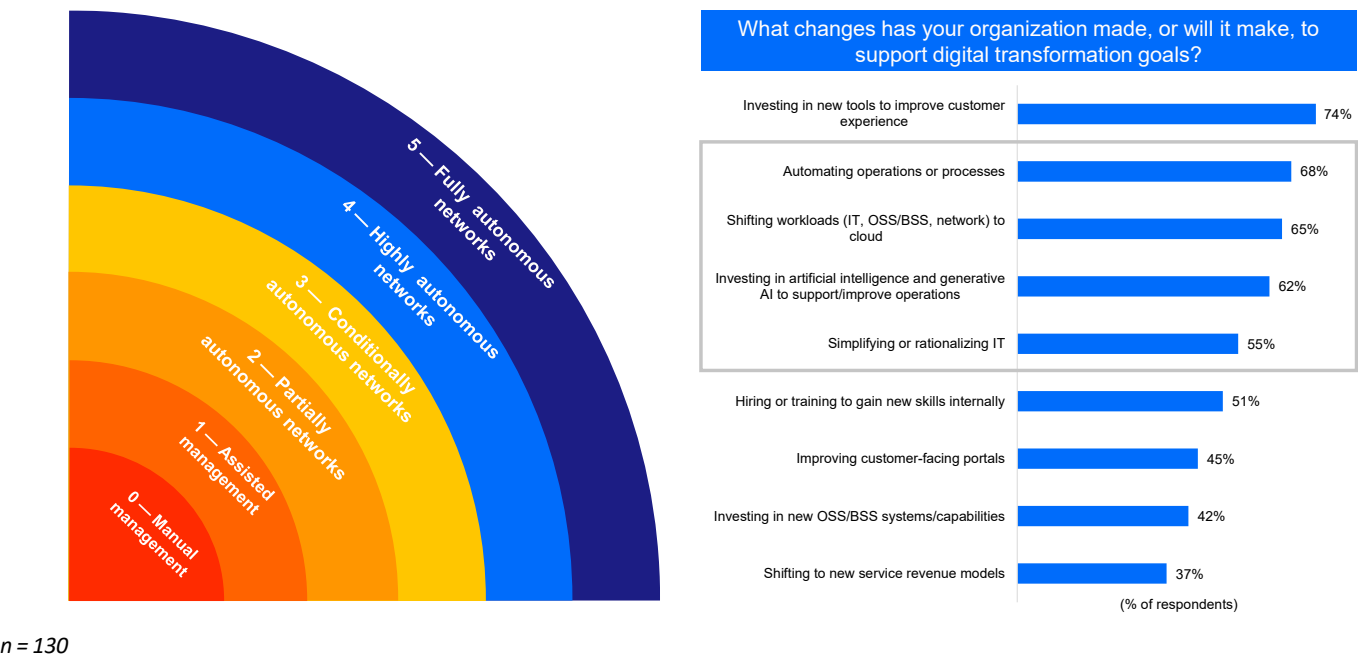
Automating Blind Is Not an Option

Telecoms have long focused on delivering five-nines reliability by deploying carrier-grade solutions, doing rigorous testing, and employing engineering teams to constantly monitor and manage their networks. This model was sustainable in a technology landscape where networking elements were closely tied to physical hardware nodes. Over the past decade, however, the complexity of monitoring and managing networks has grown exponentially as service providers adopted network virtualization, software-defined networking, and standalone 5G. These environments are highly complex, and severe service impacts can result from unanticipated and seemingly small factors.

When something goes wrong, fault alerts flood network operations teams, making it challenging to quickly isolate root causes and implement fixes. When applying a fix, network engineers must have confidence that the applied change will improve the network's condition and not exacerbate the current incident. The longer the outage, the higher the associated economic and societal costs. It is little surprise that this is a high-priority area for service providers to develop agentic AI capabilities. Already 69% of EMEA service providers are investing in agentic AI network performance monitoring and self-healing capabilities, according to IDC's August 2025 *EMEA Telco Transformation Survey*.

Many service providers seek to increase their network automation in line with the TM Forum Autonomous Network model. Starting from minimal automation, the model provides guidance on how service providers can progress from manual management (level 0) to highly autonomous (level 4) and fully autonomous (level 5) networks. With each level of progression, more processes such as execution, awareness, analysis, and decision-making are automated. In 2025, most operators self-report as being between level 1 and level 2: Many execution processes are automated, and network monitoring is alert driven with deeper insights and analysis available but requiring manual effort. To increase maturity requires a spectrum of investments, including projects that simplify legacy systems; deployment of cloud-native OSS; investments in data models, infrastructure, and governance; and organizational and technical AI capabilities (see Figure 1).

FIGURE 1: *Progress Toward Higher Autonomous Network Levels*



n = 130

Note: The left-hand side figure shows TM Forum's Autonomous Network Levels.

Source: IDC's Telco Digital Transformation Survey, April 2025, and TM Forum, 2025

To progress from levels 1 and 2 capabilities toward levels 3 and 4 requires concrete steps to increase network observability. Observability is a discipline that moves beyond traditional passive infrastructure monitoring to encompass end-to-end, real-time operational insights that guide decision-making, even in complex network environments. These insights are provided by interrelated metrics, events, logs, and traces generated by applications and network infrastructure deployed across on-premises, cloud, and edge platforms. In addition, predictive, AI/ML-enabled analytics rapidly correlate and mine data to identify anomalies, root causes, and recommended remediations.

Granular observability is foundational for higher levels of network autonomy, as it provides the contextual real-time data and insights needed for AI-driven decision-making and closed-loop operations. Humans need to be confident that their changes will not cause or worsen network outages. This concern is magnified when decisions on how to configure network elements are passed to AI agents that can make decisions, which will affect the network state. As a result, IDC forecasts that service providers will increase spending on service assurance and observability by 25% from 2024 to 2029, as they seek to increase both network autonomy and network performance transparency for customers.

The process of empowering AI to take on greater network management is as much cultural as it is technical. Service provider operation teams must first trust they have the capability to autonomously detect and correctly diagnose network issues. Once a suitable confidence threshold is met, diagnosis can be augmented with recommendations for optimizing network configuration and resolving network faults, supported by explanations as to why these recommendations are the optimal way to manage particular incidents. With recommendations, service providers can

empower AI agents to completely manage common network issues; eventually, human intervention will only be required in the most severe circumstances. Observability is critical at each stage in this evolution to ensure that AI agents can make accurate diagnoses, take the right actions, deliver tangible operational benefits such as reduced mean time to repair, and have their actions positively validated to build the cultural confidence required to empower autonomous decision-making.

The Ecosystem for Agentic AI in Telecoms

Implementing agentic AI capabilities at scale takes an ecosystem of partners, including cloud providers, software vendors, network equipment providers (NEPs), and industry alliances. Cloud providers are often foundational, offering scalable infrastructure, advanced data management, and AI platform services. According to IDC's 2025 *Telco Digital Transformation Survey*, 72% of telecom operators identify hyperscalers as strategic partners for AI, and 62% plan to increase their use of hyperscalers to support emerging AI workloads. This partnership is essential not only for compute resources but also for robust data governance and integration across distributed networks and data sources. As cloud providers also often act as the access point, host, and even provider of AI models to support agentic capabilities, their technical expertise, partner ecosystem, and learnings from their broad customer base make them strategic partners in the development of service provider agents for autonomous networks.

NEPs and software providers offer the deep domain expertise required to develop agentic solutions within their portfolio footprint. They can provide internally developed agentic capabilities to manage network operations; they also can offer guidance to service providers looking to develop their own agentic capabilities across vendor deployments, providing input on governance, dataflows, and how to achieve the desired impact from agentic AI investments.

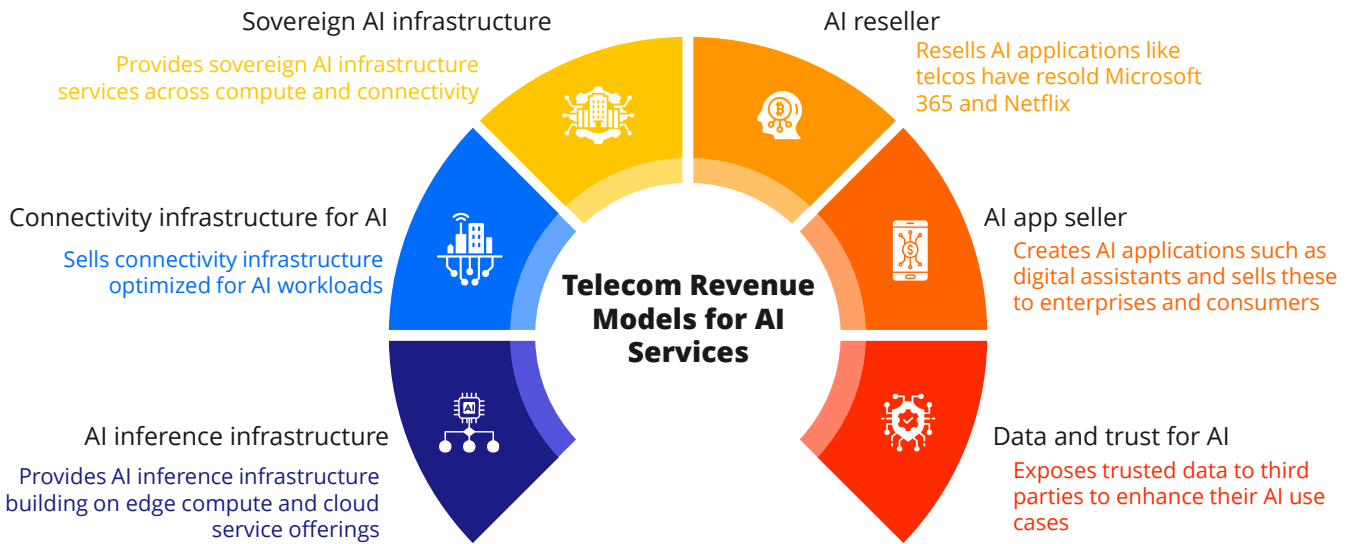
Standards-developing organizations provide forums for creating beneficial standardized interfaces and taxonomies that can accelerate development and reduce integration costs for new capabilities. The Model Context Protocol (MCP) is one example. Originally introduced by Anthropic in November 2024 to help its Claude model integrate and share data with external tools, systems, and data sources, MCP has quickly become a standard that model providers, NEPs, and software suppliers are integrating into their solutions.

With so many different stakeholders in the creation and scaling of AI agents, real-time observability across the ecosystem is vital to ensure that agentic solutions from different sources act in cohesion with each other in a shared understanding of the network state. Without comprehensive observability, the risks of unintended consequences or degraded service quality increase as agents take actions that may benefit their goals but are detrimental to the overall service. For example, one agent from provider A powers down a low-traffic basestation to manage energy efficiency, which could conflict with a congestion management agent from provider B that is trying to shift traffic to ease congestion in an adjacent basestation. If the agents share an understanding of the network, supported by embedded agentic observability capabilities such as intelligent alerting or automated remediation, they can work together to ensure that both goals are achieved without degrading the overall quality of service provided.

Supporting AI Value Creation for Service Provider Customers

Agentic AI is not just a driver of value for service providers through autonomous networks. It is also an enabler for new network services and new enterprise needs for connectivity solutions from telecom operators. Figure 2 highlights business model areas where service providers currently seek to grow revenue from AI services. Broadly speaking, they break down into infrastructure-based services and application-based services.

FIGURE 2: **Routes to Telecom Monetization of AI**



Source: IDC, 2025

Connectivity is critical for several agentic AI use cases IDC sees emerging across industries, such as asset tracking and monitoring in logistics and utilities verticals, real-time fraud detection and prevention in financial networks, and assurance of quality connections for payment devices during large sporting and cultural events. In some cases, such as support for drone operations, optimized connectivity requiring AI agents to support higher levels of network quality will enable enterprises to develop new capabilities to manage their business. In others, the role of the service provider will be to protect and guarantee the transmission of data that supports an industry's agentic operations, such as managing fraud in real time for financial transactions.

Observability remains key in facilitating these new agentic workflows. In use cases like mobility management, customers and service providers need visibility into the operational health of the network so that when issues are detected, they can be mitigated at speed — no one wants a drone carrying medical supplies falling out of the sky in a populated area. In situations where service providers facilitate customers' use of agentic AI, observability and security monitoring are critical for customers to ensure the efficacy and security of their AI workloads, especially as these will be high-value targets for threat actors to disrupt.

Considering Splunk, a Cisco Company

Cisco acquired Splunk in 2024, further strengthening its ability to help communications and media organizations build resilience across their entire digital footprint. Today, many of the world's largest and most complex communications and media organizations rely on Cisco and Splunk to keep their mission-critical systems secure and reliable.

Splunk Observability aims to enable deeper and broader visibility and insights across the entire network footprint. The platform supports [cross-stack](#) visibility that delivers monitoring, anomaly detection, and root cause analysis. This unified approach means that AI and ML tools can access the data needed for proactive incident management and network performance optimization. Service providers can leverage the AI, GenAI, and data ingestion capabilities offered by the Splunk platform and benefit from its broader SIEM, SOAR, and network capabilities.

AI assistants specialized in supporting issue detection, investigation, response, and prevention augment network operation and security teams to accelerate time to issue discovery and resolution. In observability, Splunk Observability Cloud unifies telemetry data from networks, infrastructure, and applications. This enables AI agents to proactively detect anomalies, perform root cause analysis, and execute self-healing actions, such as automated fixes for performance issues, all of which are crucial for maintaining network reliability and reducing downtime. Integrations with Cisco ThousandEyes and PCA further correlate network impacts on user experiences, supporting telco-specific use cases like predictive network optimization and end-to-end process automation from fault detection to resolution.

For security, agentic AI features in Splunk Enterprise Security, such as the Triage Agent for alert prioritization, Malware Reversal Agent for threat analysis, and AI Playbook Authoring, enable faster threat detection and autonomous responses, addressing telco challenges like adaptive fraud detection and real-time traffic monitoring to counter evolving cyberthreats amid expanding attack surfaces.

A key capability is Splunk's AI Toolkit, which allows organizations to customize the existing Splunk model or bring their own models to operationalize more advanced AI use cases. This empowers service providers to extend Splunk's capabilities to further enhance competitive differentiation. Splunk's road map includes tighter integration with Cisco's portfolio, expanded AI assistant skills, improved detection and investigation capabilities, and enhancements to the company's AI Toolkit, empowering telecom customers to further customize models using their own expertise and data.

Challenges

The adoption of agentic AI in telecom networks brings a fresh impetus to service provider efforts to rationalize, model, and connect their data footprint across their organization. This is no mean feat and takes a large amount of organizational effort. For vendors like Splunk, this is a challenge where it is often several steps ahead of its customers. To close this gap, Splunk must ensure that it is engaging with its customers closely on how they develop their data strategy, acting as a strategic partner on the best way to federate, consume, and secure diverse telecom data sources. Second, interoperability standards like TM Forum APIs and MCP are crucial in making it easier for Splunk and its customers to move at speed in connecting up these data sources when a road map to autonomous networks is decided.

Conclusion

Robust real-time observability is the cornerstone for service providers advancing toward agentic AI and highly autonomous networks. It enables safe and effective automation, supports collaboration across a diverse partner ecosystem, and ensures AI agents act with a unified network view. As service providers and other industries increasingly rely on agentic AI for mission-critical operations, comprehensive observability will be essential to maximize value, minimize risk, and deliver resilient, AI-driven services that meet evolving business and societal needs.

About the Analyst



Chris Silberberg, Research Manager, Global Telecom Operations and Monetization

Chris leads IDC's Global Telecom Operations and Monetization research, including the evolution of telco monetization, customer experience, orchestration, and assurance capabilities. Telcos are at a crossroads: double down as utility providers or become digital service powerhouses. Both strategies demand communication service providers fundamentally transform their IT capabilities to enable customer-first experiences, autonomous operations, and the capacity to innovate monetization models at scale.

MESSAGE FROM THE SPONSOR

Digital resilience is the ability for an organization to keep their business securely up and running in the face of any disruption. This involves proactively preventing, detecting, investigating, and responding to potential issues. Splunk, a Cisco company, helps service providers build digital resilience by providing visibility and insights across the entire digital footprint, uniquely combining the power of the network with security, observability, and assurance.

With Splunk, service providers are able to prevent incidents from becoming major issues, remediate quickly if something does happen to minimize business impact, and be in a position to adapt to anything and take advantage of new business opportunities.

Learn more about [Splunk for Service Providers](#).



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)