Data Assurance: Underpinning the Agentic AI Era

Author: Ruth Brown

February 2026

In partnership with:

RADCOM

Introduction

For years, telecom operators have automated basic tasks and optimized workflows. What they have not automated is authority. Network decisions still wait for human intervention, and this decision-making model no longer scales.

Agentic artificial intelligence (AI) is changing this; it offers multi-step workflow autonomy for complex scenarios, enabling systems to think, plan, execute, and reflect on decisions. But advancing beyond advisory roles requires trusted service assurance and reliable data. Proactive care and autonomous decision-making depend on continuous, real-time validation of network behavior, customer impact, and service quality.

Creating this vision goes beyond traditional service assurance or the capabilities of generative AI (GenAI) copilots. It requires robust data assurance foundations to guarantee accuracy and trust as telecoms progress toward AI-native networks.

The agentic evolution

The convergence of advanced AI, intent-based networking, and cloud technologies is driving telco-agentic AI development. These technologies collectively enable service providers to create more adaptive, intelligent, and autonomous systems for their networks and operations. In this early phase, agentic operations (AgenticOps) introduce many considerations, especially around network decision autonomy, trust, and operational changes, as outlined in **Table 1**.

Table 1: AgenticOps network considerations and benefits

	Considerations	Benefits
Decision autonomy	• Safe autonomy (human-in-the-loop vs. human-on-the-loop vs. closed-loop) • How to establish responsible AI (trust, explainability, transparency, governance) • Guardrail execution and thresholds	• Faster, real-time decisions • Reduced manual intervention and escalation • Resilient and self-healing behavior • Introduction of agent-led loops to low risk tasks to prove behavior and confidence
Architecture	• Modular operations/business support systems (OSS/BSS), event-driven, legacy support, and API compliant • Multiple specialized agents (standardized interfaces, open, interoperable, scalable) • Data-centric, context sharing	• Enhanced agility, scalability, and future-ready • Vendor-neutral, standardized design, faster capability integration via composable agents • Better multi-domain coordination (networks to IT to customer experience to partners)
Operational costs	• Investment in platforms, data, and skills • Model training, inference & scaling costs • Avoidance of intelligence duplication and agent sprawl • Lab-to-live process to ensure trust and scaling	• Opex reduction through automation and lower mean time to repair • Optimized network and IT resource utilization • Move from reactive to proactive/preemptive • Human roles shift toward exception handling, autonomy oversight, and complex issues
Customer-centric decisions	• Ensuring agents act in the customer's best interest, not for cost reduction • Managing consent, privacy, and ethical AI	• Hyper-personalized, context-aware interactions • Proactive resolution before customer impact • Increased net promoter score (NPS)

Source: Omdia

Data assurance foundations

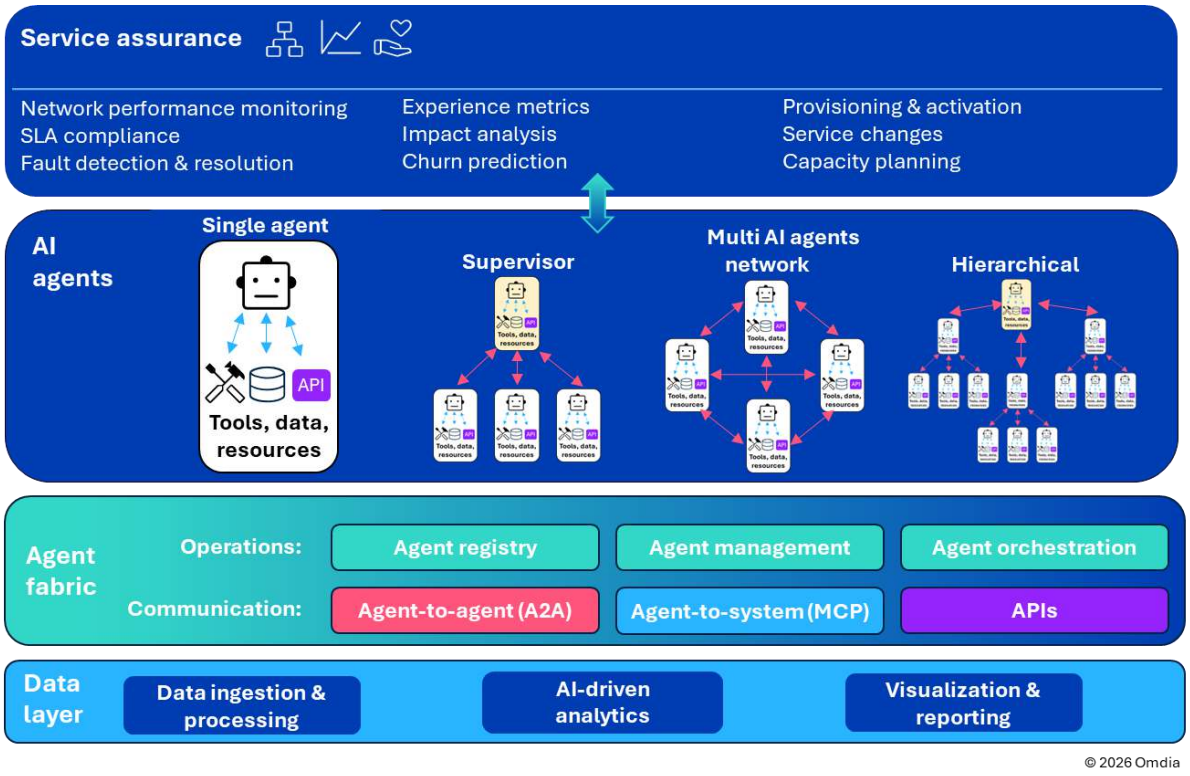
Accurate, reliable, and trusted network data is a prerequisite for the successful implementation of agentic AI. Service assurance delivers operational context to transform raw data into trusted intelligence, giving operators confidence that their AI agents are acting based on valid network conditions rather than assumptions. Data assurance foundations include the following:

- **Real-time end-to-end data pipelines:** Agentic AI will be more reliant on comprehensive data access, but the lack of new analytics tools, combined with massive volumes of network data and processing demands, continues to challenge operators. High speed processing, accelerated compute, and AI-assisted processing look to address scale and cost.
- **Subscriber-centric insights:** Network-centric metrics, such as throughput, latency, and packet loss, often fail to capture the true customer experience. To increase accuracy and understand the actual impact on applications and services, operators need new reference points that incorporate a deeper understanding of the real customer experience.
- **Data quality:** Inconsistent terminology, context, and cross-domain correlations undermine trust in AI decisions. Unifying datasets, establishing control, and adopting a standardized ontology shifts data from metric-centric to knowledge-centric, enabling unified analytics and interoperability across vendors and technologies.
- **Data stores:** Repositories for raw, processed, or intermediate data (e.g., relational databases, data lakes/lakehouses, distributed files) must handle diverse data types (structured, unstructured, hybrid) and support fast data processing and retrieval to meet real-time analytics requirements.

Agentic-powered service assurance

AI agents are advanced, autonomous, or semi-autonomous systems that evaluate, reason, and execute actions independently. They offer the potential to automate service assurance workflows by leveraging customer intent and predictive models (**Figure 1**).

Figure 1: Agentic service assurance



Source: Omdia

An agent fabric layer (the middleware or operational backbone) provides interface communication and manages key operations that interact with the data assurance functions within the data layer to power actions. Operational capabilities include the agent registry (identifying agent capabilities and owners), agent management (discovery, routing, security, observability, etc.), and agent orchestration.

Specialized telco frameworks (development toolkits) are increasingly surpassing general-purpose multi-agent AI application frameworks, such as JADE and Akka, in addressing the unique demands of the telecommunications industry. Emerging platforms such as LangGraph, AutoGen, and CrewAI are not as widely established as initial frameworks. Yet,

they offer distinctive telco service assurance and service management capabilities, enabling the creation of agents with advanced reasoning and natural language capabilities.

Agent connectors ensure interoperability and efficient collaboration across complex systems and between agents, tools, data sources, and AI models:

- **Agent-to-agent (A2A) protocol:** Direct communication between agents for collaboration (**Figure 2**, rose arrows).
- **Model context protocol (MCP):** Agent-to-system communication; e.g., AI models and LLMs to access external tools, systems, and data sources (**Figure 2**, blue arrows).
- **APIs:** Allow agents to connect to external software, tools, and data (e.g., database queries, email sending, etc.). TM Forum is standardizing telecom agent APIs for intent management (TMF921), copilot assistant (TMF785), and agent management (TMF939).

Depending on task complexity and network layers, service assurance systems can be orchestrated as single or multi-agent process architectures to fulfill and execute actions:

- **Single-agent:** Localized, independent tasks requiring minimal coordination (e.g., monitoring a specific network segment for performance issues, such as packet loss or latency spikes).
- **Multi-agents:** Specialized tasks or multiple tool integration have various architectures:
  - **Network architecture:** Collaborative agents with shared goals (e.g., QoS distributed network monitoring). For example, monitoring agents gather metrics, analysis agents detect anomalies, and action agents optimize traffic or bandwidth for seamless video streaming.
  - **Supervisor architecture:** Centralized oversight for large-scale tasks. For example, a supervisor agent manages 5G optimization, while worker agents at nodes like gNBs and edge servers collect data and perform tasks, such as frequency tuning and load balancing.
  - **Hierarchical architecture:** Tiered structure for distributed decision-making. For example, top-level agents analyze global data, mid-level agents address domain-specific issues, and low-level agents manage localized tasks, such as detecting configuration errors or hardware failures at nodes (e.g., gNBs and routers).
  - **Custom:** A hybrid or bespoke workflow that defines which agents may communicate.

Telco use cases

Agentic AI assurance enables a common intelligence layer that aligns AI-driven actions with real-time network conditions and end-user experience. **Table 2** describes agent scenarios, including how multi-agent predictive coordination is occurring.

Table 2: Industry use cases

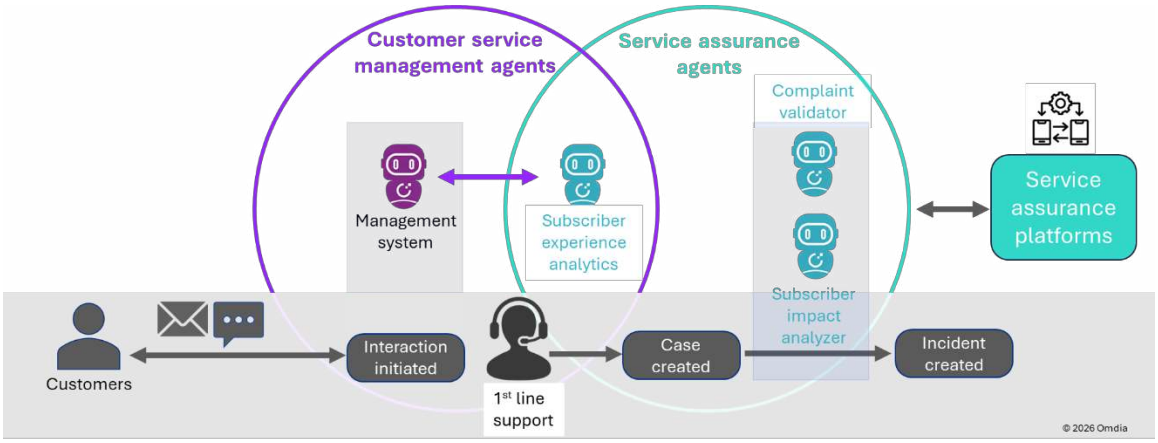
Use case	Description
Network optimization	Real-time and proactive optimization for enhanced network performance and user experience. • **Capabilities:** Agent-driven dynamic spectrum allocation, congestion management, and energy optimization leveraging real-time service assurance insights and intelligence. • **Outcome:** Energy efficiency, improved QoS, cost savings. • **Example:** DT's Multi-Agent RAN Guardian optimizes network performance.
Network fault management	Predict, detect, and resolve network issues and anomalies before customer impact. • **Capabilities:** Fault detection, root cause analysis (RCA), and preventative equipment failure using multi-agent systems that leverage predictive analytics and real-time monitoring. • **Outcome:** Increased network reliability/uptime, reduced network engineering efforts, and a shift of resources to advanced non-agent-controlled domains, and enhanced customer satisfaction. • **Example:** AT&T's AI agents manage network resilience, predicting faults before they disrupt services.
Customer engagement	Delivering personalized proactive assistance through multi-agent collaboration. • **Capabilities:** Agents cross-correlate customer sentiment with KPIs, delivering proactive notifications for service updates, billing issues, and outages—escalation of complex problems to a human operator. • **Outcome:** Operational cost savings, improved customer experience, and retention. • **Examples:** SK Telecom's AI assistant uses agents to deliver intelligent hyper-personalization.

Source: Omdia

Customer complaint and incident creation example

Figure 2 illustrates an AI agent complaint validation workflow. Built on an open framework, these agents enable seamless collaboration and tiered decision-making. In the OSS/BSS domain, customer service management (CSM), IT service management (ITSM), and mobile network agents collaborate to assist customers, schedule maintenance, and optimize operations.

Figure 2: Service management system workflow



Source: Omdia, RADCOM

In this scenario, mobile experience and CSM AI agents validate customer complaints by correlating natural language case descriptions with network KPIs. When a customer contacts the helpdesk, multi-agent collaboration begins as follows:

- The subscriber experience agent reports a subscriber's current network experience and complaint potential to the management system agent.
- The complaint validator agent verifies the subscriber's network experience KPIs and searches for evidence of the issue.
- The subscriber impact analyzer agent identifies current and potential subscribers impacted by the network issue.
- Now validated, an incident is created and agents identify all affected subscribers.

Conclusion: Data assurance is foundational to agentic AI

Agentic AI represents a clear route for telecom operators to achieve autonomy and realize intent-based networking. Operators need strong foundations, including comprehensive data assurance and real-time monitoring to ensure the accuracy of AI-driven decisions.

AI agent technology and development platforms should be open, interoperable frameworks with communication protocols and APIs able to leverage the full potential of cross-domain intelligence and support scalable decision-making for the future. Next-generation service assurance is already bridging this gap by leveraging real-time, reliable, operational end-to-end network intelligence and multi-agent predictive coordination.

The agentic AI era has begun, but it will only succeed if built on trusted, real-time data. Connected service assurance provides this base, unifying performance, observability, and experience to advance AI authority from the lab to the live environment.

Appendix

Methodology

This report and its findings are based on research and discussions with communications service providers (CSPs) and vendors. Omdia considered research from the Heavy Reading (now Omdia) *AIOps Network Operator Survey* (October 2025) in the course of writing this report.

Further reading

Heavy Reading (now Omdia) *AIOps Network Operator Survey* (October 2025)

Ruth Brown, Principal Analyst, Mobile Networks, GTM Telecom Insights and Advisory
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer