Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
WHITE PAPER

AIOps Network Operator Survey: From Ambition to Action

A Heavy Reading (now part of Omdia) white paper produced for Amdocs and RADCOM

AUTHOR: RUTH BROWN, PRINCIPAL ANALYST, HEAVY READING (NOW PART OF OMDIA)

EXECUTIVE SUMMARY

Today's telco domains serve a range of diverse use cases. Over the past few years, the industry has been actively exploring and implementing AI-driven automation solutions to ensure high performance, reliability, and optimal efficiency. Operators recognize that maturing their artificial intelligence for IT operations (AIOps) capabilities is crucial and that this journey is intrinsically linked to their ongoing transformation of network data architecture and operational systems.

Heavy Reading (now part of Omdia) launched its first Analytics and Automation Market Leadership Program in 2023 to investigate the opportunities and challenges in 5G networks. Year 3 of this project focuses on the progress of mobile network automation and how AI will underpin telco networks and service operations.

This report presents the key findings of the Heavy Reading (now part of Omdia) **2025 5G AIOps Network Operator Survey**. It provides the latest outlook on operator strategies for analytics, automation, and AI. The report is structured as follows:

- AIOps adoption strategies
- Network data quality
- 5G user plane monitoring
- Automation and trust
- Agentic AI

The project partners for the **2025 5G AIOps Network Operator Survey** are Amdocs and RADCOM.

Key findings

- **Operators are closing the gap between AI ambition and implementation and making measurable advances in network automation.** 47% of respondents believe their network assurance operations are "operating autonomously for specific proactive use cases and domains, with minimal human oversight." Yet, 64% of respondents are unlikely to deploy closed-loop automation or plan to do so in two to three years, illustrating how immature advanced network autonomy still is.
- **Data quality underpins AIOps success and is a priority for foundational data models feeding AI systems.** Yet, 52% of operators operate with partially unified or siloed systems. While operators pursue data federation (48%) and hybrid cloud approaches (46%)—favored by larger providers—telcos must prioritize unified data architectures and standardized APIs to advance network autonomy and ensure AI trustworthiness.
- **Operators are eager to deploy AI agents; over 74% plan to deploy them across multiple network operations processes within two years.** Reactive and proactive service assurance and remediation recommendation/ open loop automation AI agents lead immediate adoption (42–45% within one year). Complex applications like closed-loop automation follow later. This is an optimistic outlook, and operators are likely to deploy low risk use cases to prove trust before full multi-agent systems with shared context begin to evolve over the next three years.

- **Operators will strategically diversify agentic AI approaches—38% favoring in-house development leveraging hyperscaler platforms, while the remainder is split between network equipment providers (NEPs, 18%), multi-vendor solutions (18%), and independent software vendors (ISVs, 17%).** This balanced strategy reflects operators' desire to partner with key agentic experts and avoid solution lock-in while addressing skills gaps.
- **Digital twins emerge as the cornerstone for establishing AI trust in autonomous networks.** Operators surveyed confirm that their primary methods to build trust are gradually increasing automation with human oversight and digital twins for monitoring (58%), while 55% use digital twins to simulate AI-triggered changes before implementation. This approach, already adopted by AT&T, Telefónica, and Vodafone Germany, provides essential validation in a zero-risk environment before live rollout.
- **While 98% of operators plan to implement 5G real-time user plane analysis, only 15% currently achieve full coverage.** The cost of systems integration and operational overhead, along with infrastructure costs (both 48%), are primary concerns, but data volume and compelling use cases remain barriers. Data collection innovation and AI-powered solutions will address these challenges, enabling deeper network insights for hyper-personalization and competitive advantage.
- **Operators identify three closely scoring, high value areas for AI-driven assurance integration: "fault and performance management" leads at 53%, while "customer care and subscriber platforms" and "service management systems/trouble ticketing" both score 49%.** The close scoring highlights how these interlinked domains offer the greatest AI opportunities for investment, customer experience, and performance. Customer experience enhancement also remains operators' top priority, consistent with 2024 survey findings.
- **Legacy integration and multi-vendor network elements remain a significant challenge for AIOps adoption and scaling.** Integration with existing operations support systems and business support systems (OSS/BSS) is cited by 55% of operators. Skills gaps in AI/machine learning (ML) and telecoms (40%) are the second leading concern. Operators are deploying modernization strategies: standardized interfaces or APIs, phased transformation, etc. Those who succeed will gain a substantial competitive advantage.

Survey demographics

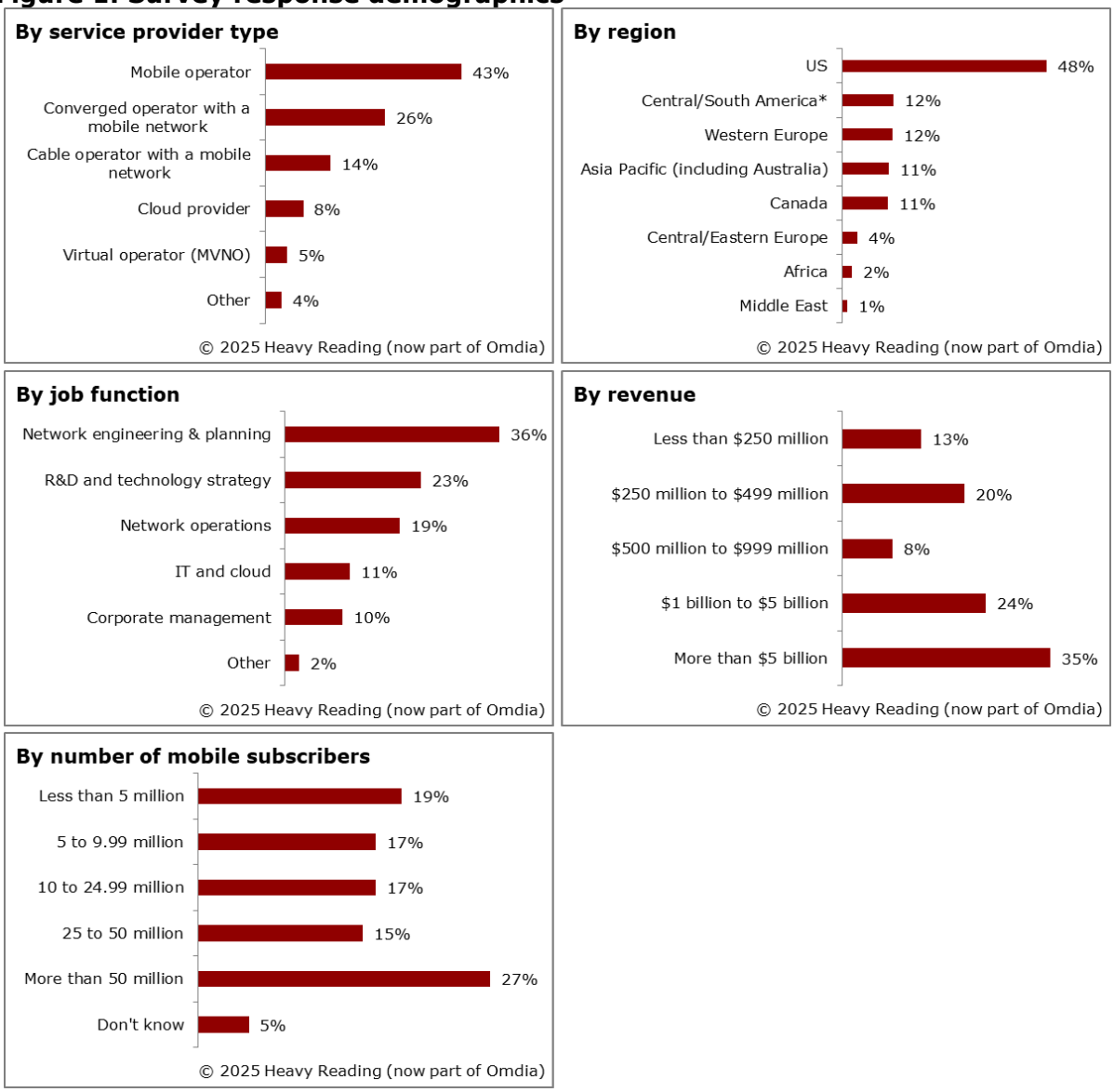
This report is based on a survey of 84 qualified individuals working at a verifiable network operator with mobile network businesses. The questionnaire was jointly developed by Heavy Reading (now part of Omdia), Amdocs, and RADCOM and fielded globally by corporate parent Informa TechTarget in July/August 2025.

All responses are confidential and only ever presented in aggregate form. Note: Heavy Reading (now part of Omdia) does not share individual or company names from the survey in the demographics.

Respondent demographics

Figure 1 shows the respondent demographics: 43% work at a mobile operator, 26% at a converged operator with a mobile network, and 14% at a cable operator with a mobile network. The remaining votes are spread across cloud provider, MVNO, and other.

Figure 1: Survey response demographics



Notes: Numbers in figures throughout this report may not total 100 due to rounding. (n=84)
Central/South America includes Mexico & the Caribbean.
Source: Heavy Reading (now part of Omdia), 2025

US respondents form the largest market, providing 48% of the responses. In this report, Heavy Reading (now part of Omdia) compares the US to the rest of the world (RoW), comprising the remaining global regions. Where demographic filters are used in the analysis, it is made clear in the report.

Network engineering and planning is the largest group of respondents by job function with 36%, followed by R&D and technology strategy (23%) and network operations (19%).

Service providers with more than $5bn in annual revenue (35%) lead the response, followed by 24% with $1bn to $5bn. These represent national-scale operators. However, the survey base also has a good representation of medium-sized service providers.

A plurality of respondents (27%) represented service providers with over 50 million mobile subscribers, followed by a fairly even spread across other groups by number of subscribers.

AI STRATEGY AND ADOPTION

Last year, the 2024 Heavy Reading (now part of Omdia) survey highlighted enthusiasm for AI integration into service providers' operational processes. This year's survey re-examines the use case priorities and ongoing challenges to adopting and scaling AIOps.

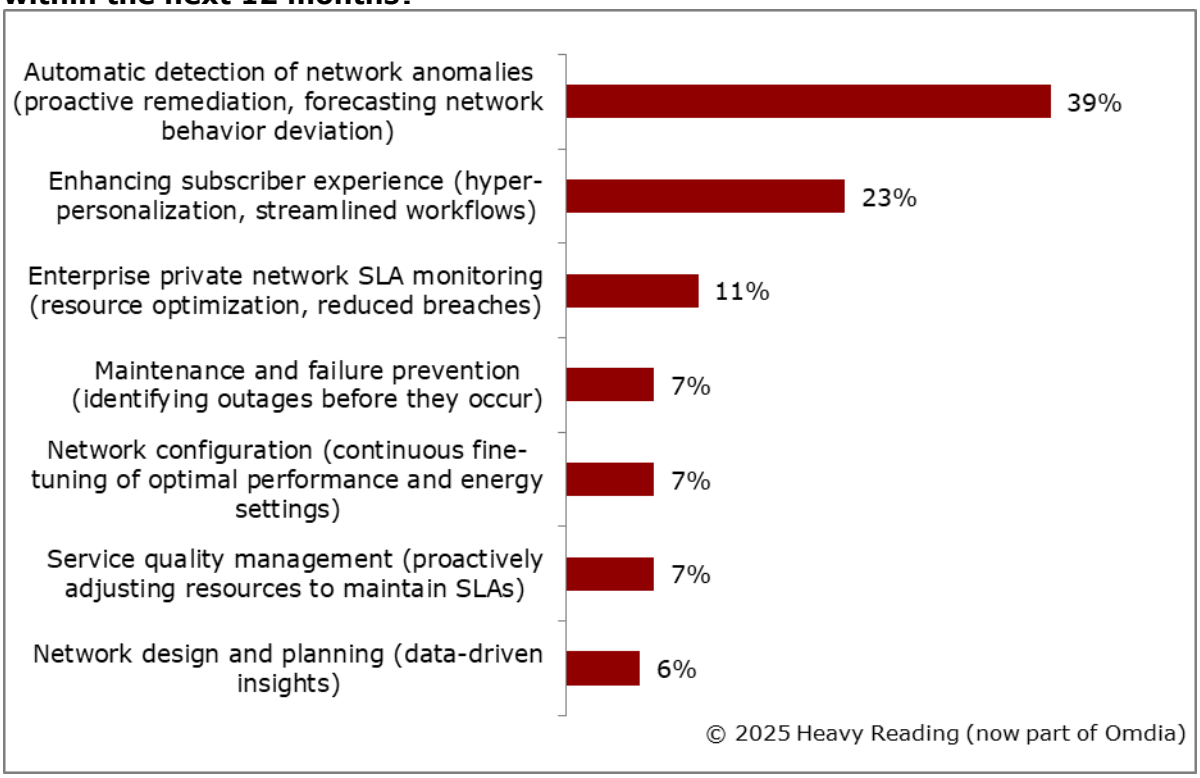
AI use case priority

More than a third of operators (39%) believe automatic detection of network anomalies will be the highest priority use case for AI transformation within the next 12 months, according to **Figure 2**. This reflects efforts across the industry to experiment with anomaly detection, root cause analysis, and remediation. Almost a quarter (23%) will prioritize enhancing subscriber experience, highlighting the growing importance of hyper-personalization, reliability, and performance to support customer retention and higher satisfaction.

Enterprise private network service-level agreement (SLA) monitoring (11%) ranks in third place. It is worth noting that this question lists "service quality management (proactively adjusting resources to maintain SLAs)" in another category for public networks, giving a combined total of 18% for SLAs overall.

The remaining options score almost identically in fourth place: maintenance and failure prevention (6%); and network configuration, service quality management and network design and planning (6%). These use cases are more complex and require higher trust and autonomy than the leaders. The close scoring also reveals several use case strategies and the desire to build AI and automation capabilities as technical and organizational readiness allows.

Figure 2: Which use case will your organization prioritize for AI transformation within the next 12 months?



n=84

Source: Heavy Reading (now part of Omdia), June 2025

AIOps adoption challenges

Many service providers operate hybrid networks, supporting multiple vendors, systems, and network generations. **Figure 3** illustrates the factors challenging the adoption and scaling of AIOps capabilities. Results reflect some maturing of AIOps, with operators identifying fewer "significant challenges" than factors considered "somewhat of a challenge" across every category, except for integrating with existing legacy OSS/BSS systems and multi-vendor network elements.

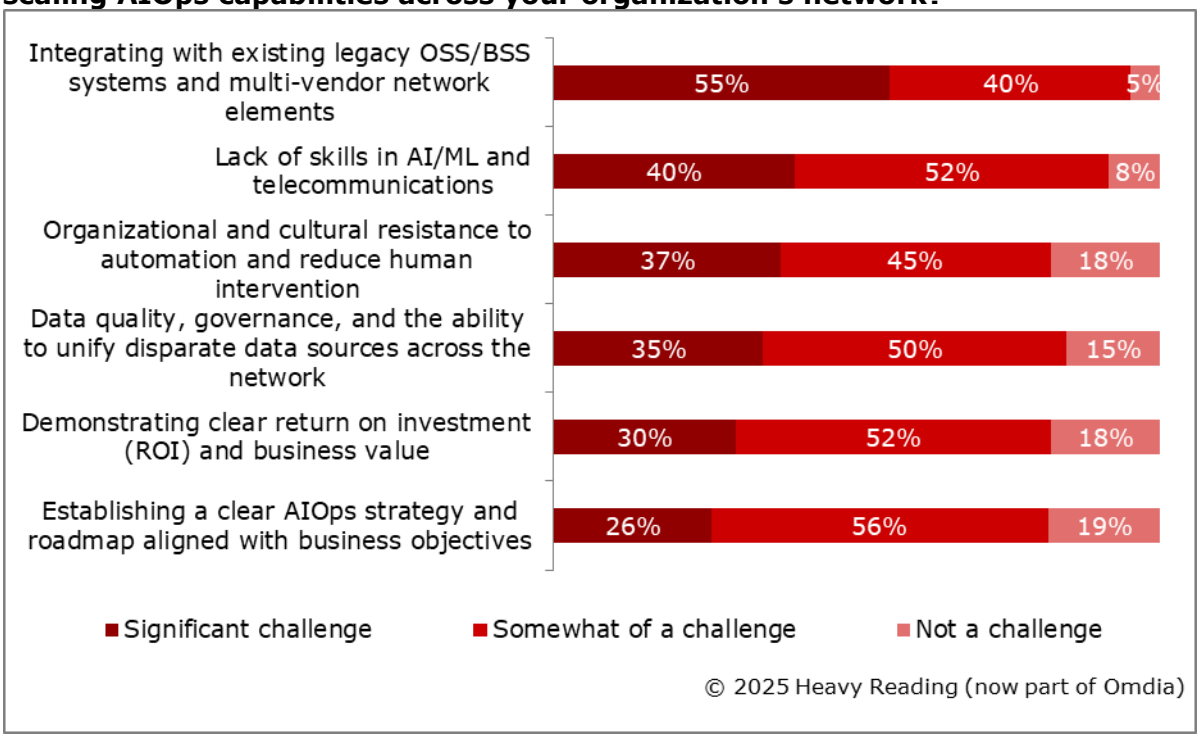
Integrating existing legacy OSS/BSS and multi-vendor network elements was cited by 55% of operators as the leading significant challenge to adopting and scaling AIOps capabilities. Lack of skills in AI/ML and telecommunications (40%) ranks second as a significant challenge, reflecting the recognition that substantial gaps remain.

Organizational and cultural resistance to automation and reduced human interference (37%), and data quality, governance, and the ability to unify disparate data sources across the network follow closely in third and fourth. While data remains a significant challenge for many operators, its lower ranking in fourth at 35% signifies the progress underway to unify and resolve the many challenges in this area. Demonstrating ROI (30%) and establishing a clear strategy and roadmap (26%) score lowest in terms of significant challenges.

Respondents from RoW have a greater challenge with integrating OSS/BSS systems and multi-vendor network elements, as 66% determine this is a significant challenge compared to only 44% of their US counterparts. To reduce these challenges, operators should cooperate with partners and the ecosystem and implement industry guidelines and best practices.

Integrating existing legacy OSS/BSS remains the most significant challenge for adopting and scaling AIOps and is cited by 55% of operators. Operators are deploying several strategies to bridge legacy and modern systems: standardized interfaces or APIs; phased transformation; and data strategies to uplift, verify, and curate data. Those who succeed will gain a substantial competitive advantage through improved efficiency and enhanced customer experience.

Figure 3: To what extent are the following factors a challenge to adopting and scaling AIOps capabilities across your organization's network?



n=81–84

Source: Heavy Reading (now part of Omdia), June 2025

DATA QUALITY

Many telco service providers are engaging with AI processes, tools, and workloads. Yet for many service providers, data remains fragmented across organizational and network domains. Legacy equipment and infrastructure also impede AI integration. This section explores the current state of service providers' data layer and their challenges in aligning it.

Today's telco data layer

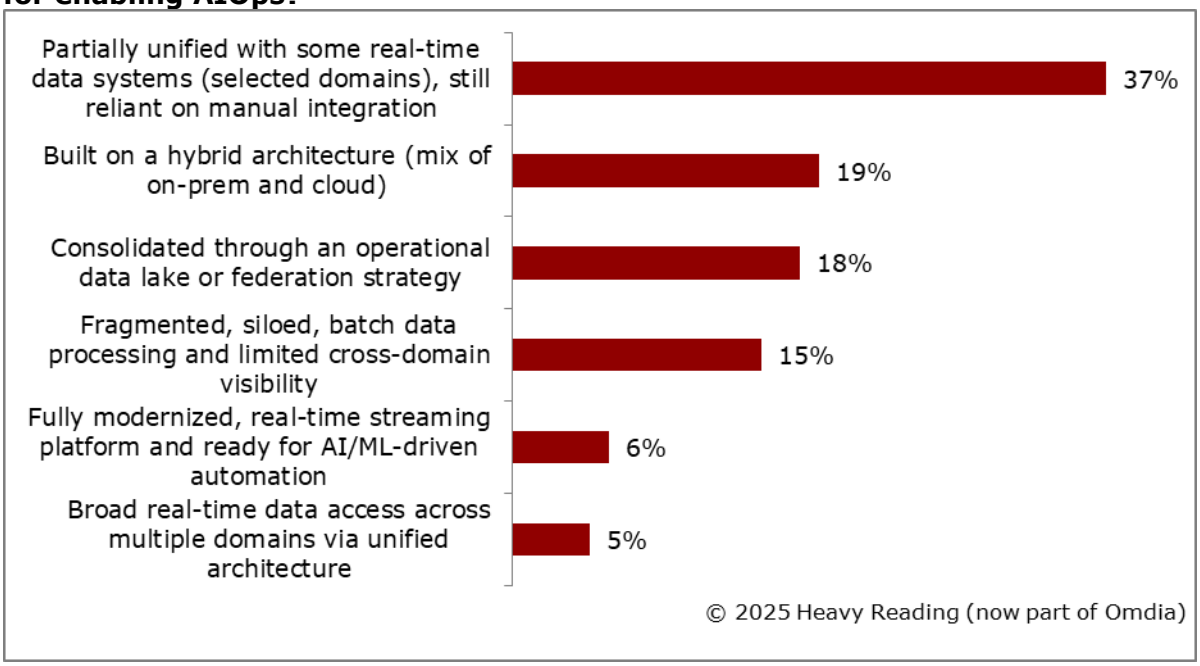
Operators have struggled for many years with unifying disparate and siloed data sources. Legacy systems, network domains, and organizational boundaries have added complexity. As network automation and AI demands increase, data integration strategies become more urgent to ensure data quality and support AIOps.

Figure 4 examines the current state of service providers' data layer for enabling AIOps. "Partially unified with some real-time data systems (selected domains), still reliant on manual integration" emerged as the leading state for over a third of the respondents (37%). "Built on hybrid architecture" (19%) and "consolidated through an operational data lake or federation strategy" (18%) follow, scoring almost identically ahead of "fragmented, siloed, batch data processing and limited cross-domain visibility" (15%).

In contrast, very few respondents have completely unified their data layer. Only 6% report their organization's current state as "fully modernized, real-time streaming platform and ready for AI/ML-driven automation," and only 5% can boast "broad real-time data access across multiple domains via unified architecture."

Survey data confirms operator progress toward consolidating network data has begun. Yet half (52%) have either only partially unified (37%) or fragmented, siloed, batch data processing (15%), suggesting considerable work and modernization remains to standardize processes, APIs, and data models.

Figure 4: What best describes the current state of your organization's data layer for enabling AIOps?



n=84

Source: Heavy Reading (now part of Omdia), June 2025

Strategies to overcome data quality and silos

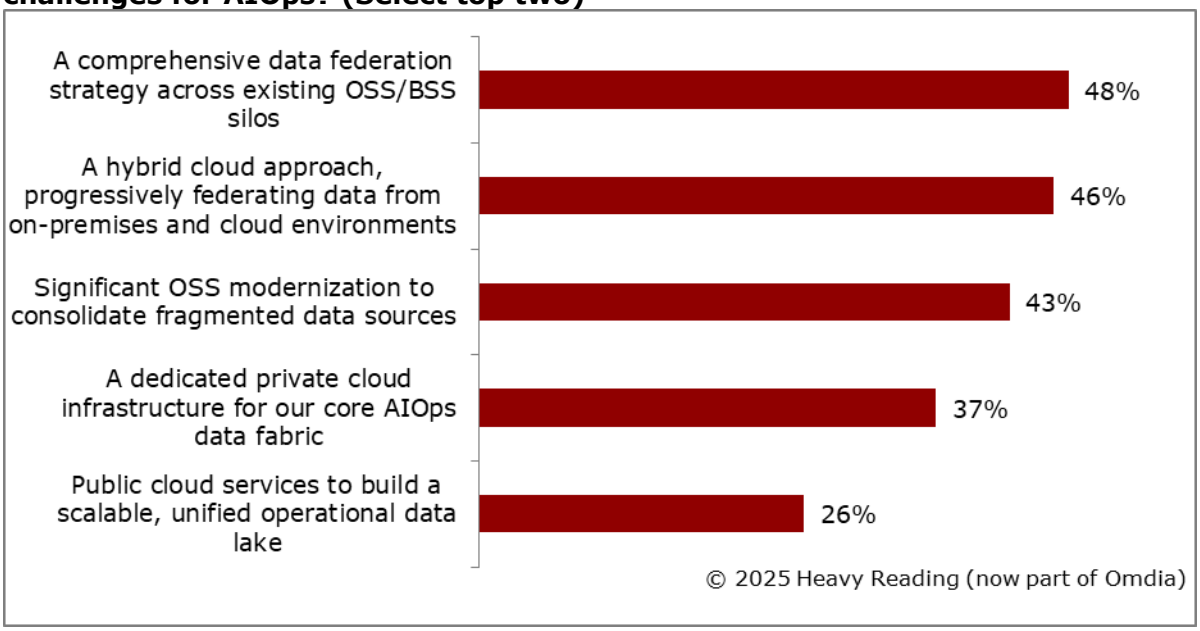
Operators have mixed strategies to overcome data quality and silo challenges for AIOps (**Figure 5**). Leading approaches include: a comprehensive data federation strategy across existing OSS/BSS silos (48%); and a hybrid cloud approach, progressively federating data from on-premises and cloud environments (46%).

The survey also confirms that operators expect significant OSS modernization to consolidate fragmented data sources (43%), ranking third. A dedicated private cloud infrastructure for core AIOps data fabric (37%) and public cloud services (26%) score lowest.

Respondents from organizations with revenue over $1bn are far more likely to use a hybrid cloud approach (59%) as their primary strategy, ahead of OSS modernization (47%) and a comprehensive data federation strategy (43%) in second and third, respectively. Organizations with annual revenue of less than $999m cite a comprehensive data federation strategy (54%) as their top choice, slightly ahead of dedicated private cloud infrastructure (49%) in second.

Heavy Reading (now part of Omdia) believes the contrasting data strategies reflect a balance between innovation, security constraints, cost, and reliability. As operators continue to transform their data architectures, ensuring their strategies are future-proofed for AI operations is vital.

Figure 5: How does your organization plan to overcome data quality and silo challenges for AIOps? (Select top two)



n=84

Source: Heavy Reading (now part of Omdia), June 2025

Data integration challenges

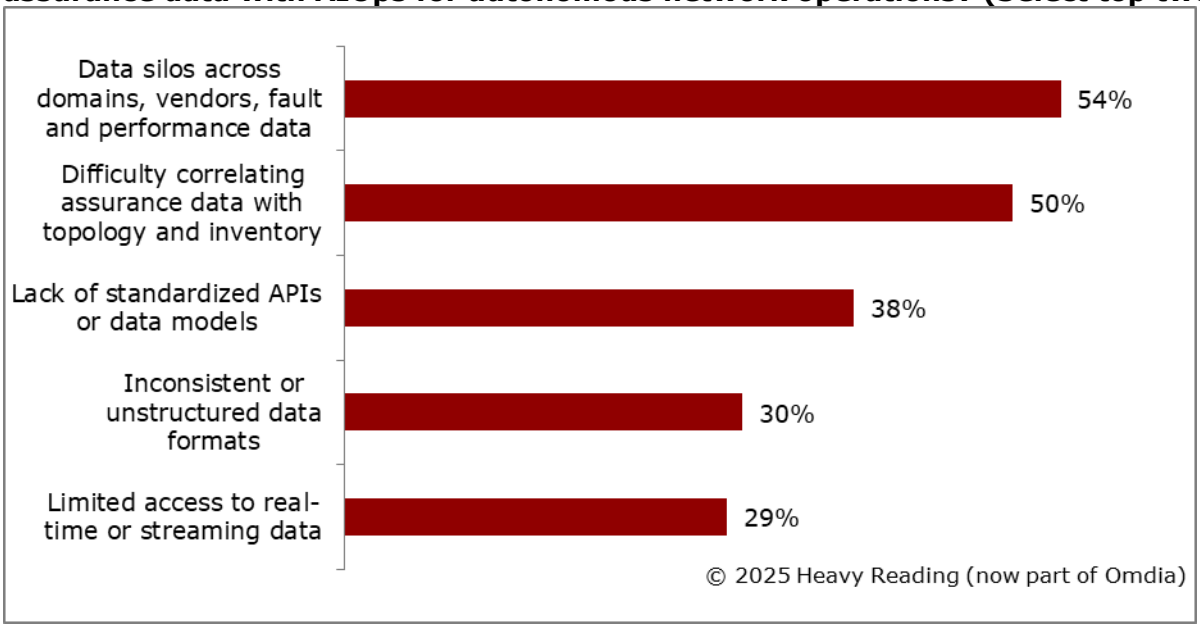
Data and its quality are central to AIOps; challenges with acquiring and curating it hamper the accuracy and effectiveness of network tools and decisions. **Figure 6** addresses data quality and accessibility issues, asking operators to select the top challenges faced when integrating assurance data with AIOps. The wide distribution of operator opinions across multiple categories emphasizes the many challenges.

Data silos (54%) and difficulty correlating assurance data with topology and inventory (50%) remain the top challenges for operators as they integrate service assurance data with AIOps. Despite transformation efforts over several years, legacy infrastructure, multi-vendor environments, domain-specific data, quality, and governance concerns (also confirmed in **Figure 3**) all add complexity.

Lack of standardized APIs or data models (38%) places third. Inconsistent or unstructured data formats (30%) and limited access to real-time or streaming data (29%) score almost equally in fourth. These problems are well-known, and industry projects for open APIs and collaborations between vendors and operators are working to define common, standardized data structures for assurance data and open APIs for data exchange.

Operators must continue to invest in their data layer, unifying data architectures and implementing long-term strategies to both ensure accuracy and readiness for AI workloads and increase network autonomy.

Figure 6: What challenges does your organization face when integrating service assurance data with AIOps for autonomous network operations? (Select top two)



n=84

Source: Heavy Reading (now part of Omdia), June 2025

Network inventory

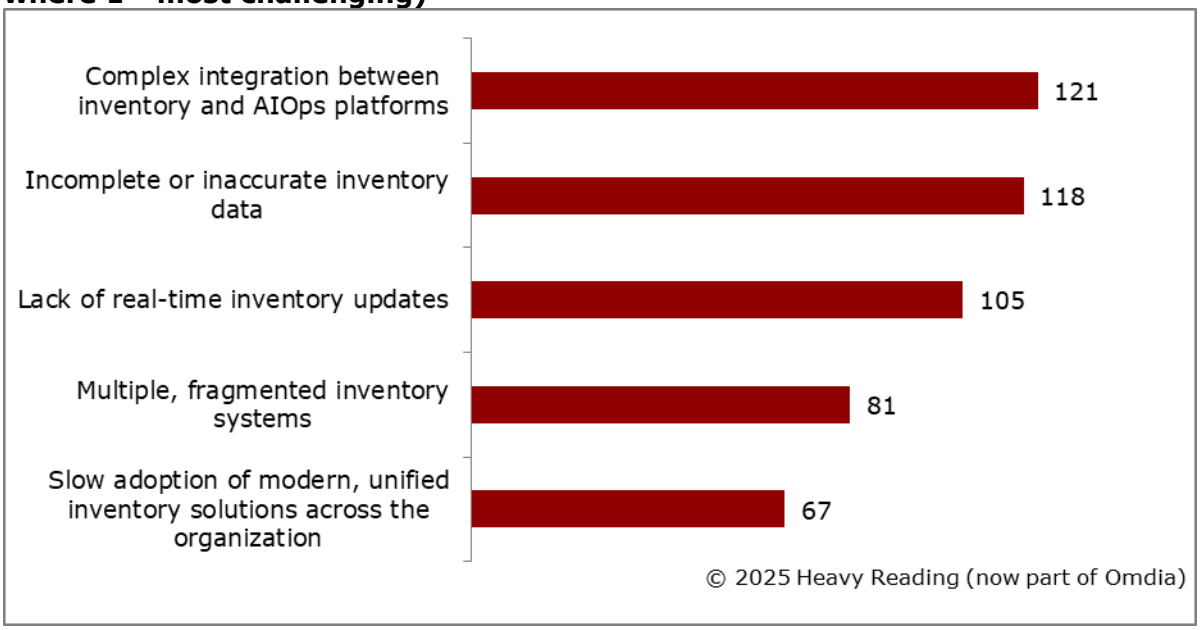
Establishing a real-time view of the network, its services, and its functions is essential for performance, quality of experience (QoE), and operational efficiency. **Figure 7** ranks the top three challenges operators face in leveraging network inventory as the key source of network topology data for AIOps.

Operators rank "complex integration between inventory and AIOps platforms" first, scoring highest with operator respondents, followed closely by "incomplete or inaccurate inventory data" (second). Lack of real-time inventory updates places third. Traditional static inventories are no longer sufficient for dynamic environments, requiring a real-time view of resources to support automation of service fulfillment, assurance, network orchestration, etc.

Multiple, fragmented inventory systems and slow adoptions of modern unified inventory solutions across the organization score lower in fourth and fifth, respectively, but indicate the breadth of current issues.

As the scope and complexity of today's networks expand with multi-generational networks, IoT, and cloud technology, accurate inventory data is a foundational layer to navigate topology, enhance fault management, and optimize network resources and services.

Figure 7: What challenges does your organization face in leveraging network inventory as the key source of network topology data for AIOps? (Rank top three where 1= most challenging)



n=84

Source: Heavy Reading (now part of Omdia), June 2025

THE TELCO AI ASSURANCE MANDATE

Operators expect to invest heavily in AI as it becomes a strategic necessity to deliver enhanced performance, customer experience, and efficiency. This section examines the obstacles to achieving this transformation and the value operators can expect to gain.

AIOps implementation challenges

Figure 8 confirms the biggest obstacles for operators' AIOps implementation/AI strategy for assurance workflows. In a continuing survey trend (**Figure 3**), operators cite integration complexity (37%) as the leading obstacle.

In second place, a quarter (24%) of operators cite AI model accuracy, explainability, and trust as significant obstacles. Operators require absolute transparency and trust as AIOps assurance technology evolves from more established predictive AI use cases (e.g., root cause analysis and anomaly detection) to more complex GenAI applications (network config creation, co-pilots, etc.) and finally to dynamic multi-network system automation via agentic AI workflows. Without these elements, AIOps cannot achieve closed-loop automation or scale effectively. To build foundational trust, operators require accurate data, continuous validation processes, and innovative tools such as digital twins to ensure model precision and reliability.

Unsurprisingly, data challenges (18%) score toward the top, placing third. The final tier of responses is split closely between organizational challenges (12%) and deployment concerns (10%).

The industry has quickly embraced GenAI technology across efficiency tools (e.g., coding and knowledge services), customer service analytics, and other applications. However, to move into an era of more sophisticated, network- and context-aware AI-driven decisions, operators must transform their legacy assurance systems and data layer as a foundation for AI accuracy.

Figure 8: What is the biggest obstacle to your organization's AIOps implementation/AI strategy for assurance workflows?

n=84

Source: Heavy Reading (now part of Omdia), June 2025

The value of AI-driven assurance

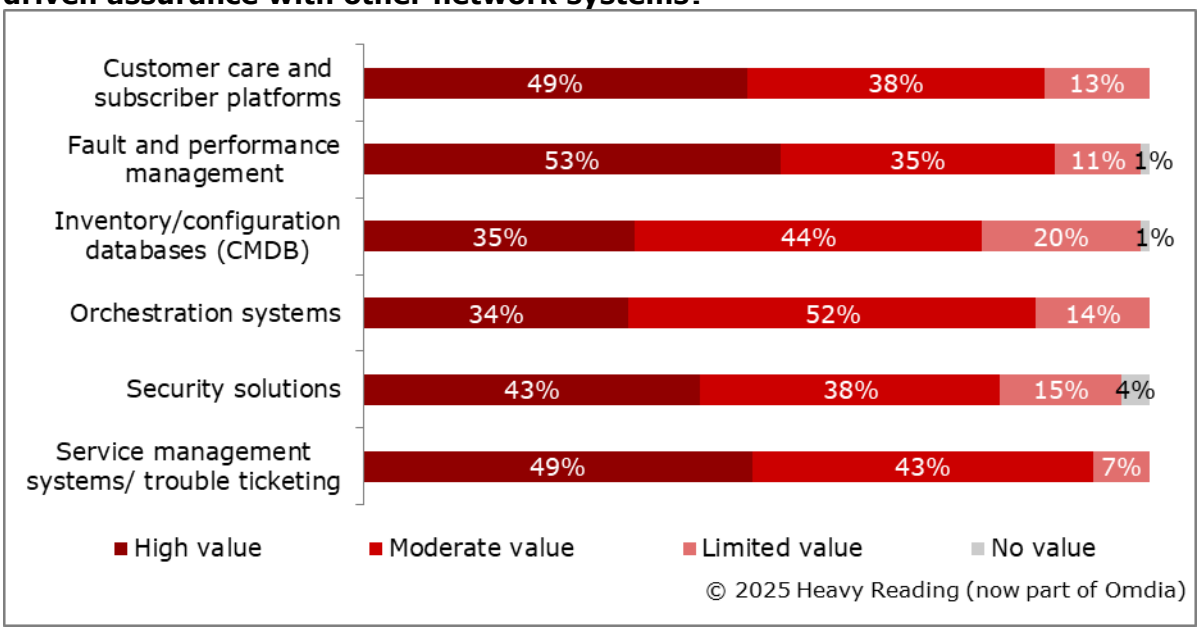
To remain competitive, operators need streamlined operations, increased reliability, and enhanced customer performance. **Figure 9** considers the business value operators expect to gain from AI-driven integration.

Unsurprisingly, operators confirm that "fault and performance management" (53%), followed closely by "customer care and subscriber platforms," and "service management systems/trouble ticketing," both with 49%, are high value. The results reflect the efforts and early inroads made to reduce time and cost and drive up performance by transforming fault resolution as well as service and performance management. In last year's survey, respondents also confirmed that enhancing customer experience was at the top of operators' agendas, along with integrating AI-driven automation to enhance both subscriber interactions in the call center and customer analysis.

While security solutions are always a top priority for operators, a nearly equal number of respondents deem the value of AI-driven integration to be high (43%) and moderate (38%). Heavy Reading (now part of Omdia) believes the split opinion reflects unclear value given current data privacy and ethical concerns surrounding collecting and analyzing large volumes of data while adhering to regulations such as GDPR, CCPA, and others.

Operators deem inventory/configuration databases (CMDB) and orchestration systems as less likely to offer "high value" than the other categories. Yet they lead the moderate value scorings with 44% and 52% respectively. The lower prioritization of inventory/CMDB and orchestration may reflect the associated costs to transform these systems and improve the data quality feeding them.

Figure 9: What value does your organization expect to gain from integrating AI-driven assurance with other network systems?



n=82–84
Source: Heavy Reading (now part of Omdia), June 2025

AI assurance integration timelines

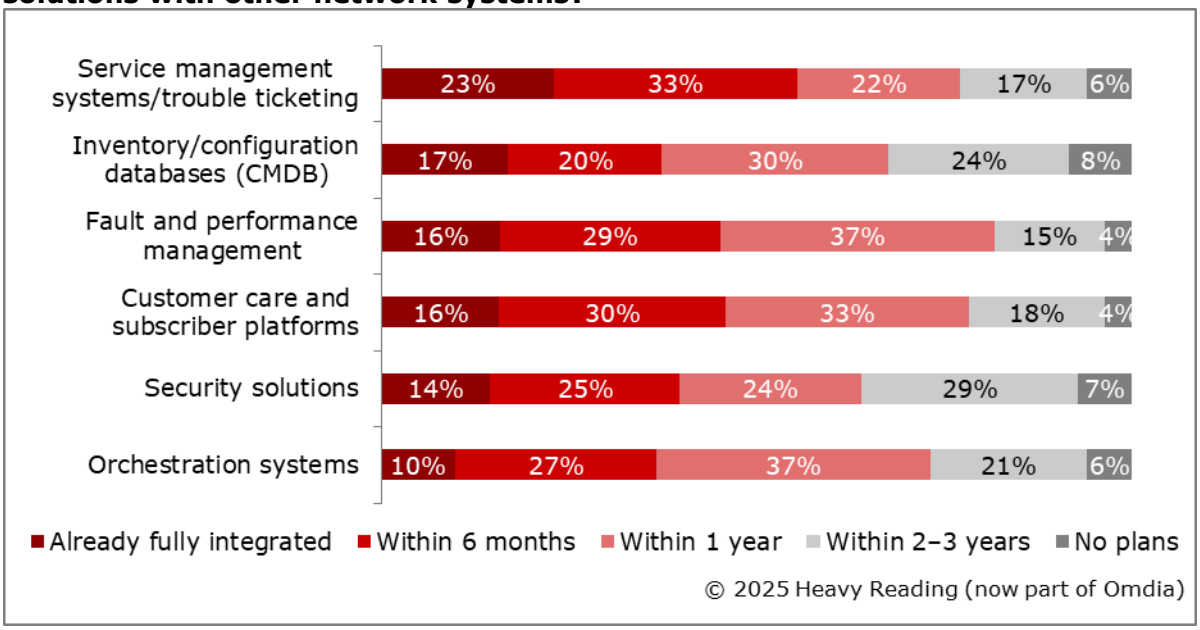
Following the last question, the survey asks operators to determine timescales for fully integrating AI-driven assurance with their network systems (**Figure 10**). Overall, survey data reflected enthusiastic timeframes, with approximately 60–80% of respondents stating they would have fully integrated AI-driven assurance solutions with other network systems within a year (combining "already fully integrated," "within 6 months," and "within 1 year" responses).

Operators indicate AI integration progress across all categories, with the survey showing that "service management systems/trouble ticketing" is the most mature. A full 23% of respondents have "already fully integrated" AI into such systems, and a further 33% expect to do so "within 1 year." All other categories follow closely in a second tier of 14–17% "already fully integrated" except orchestration systems (10%), which lag behind in AI support.

Timescales for integrating inventory/configuration databases (CMDB) and orchestration systems, which operators deemed to offer moderate value (**Figure 9**), have slightly longer horizons, with 54% and 58%, respectively, indicating this will occur within one to three years. This timeline also points to the complexity of legacy systems and the multiple components associated with them.

While this question demonstrates operators' eagerness to integrate AI-driven assurance, it is likely that integrations within a year or less will be heavily supported by human oversight, since the majority of operators still only support lower levels of automation. For example, Omdia's *Telco Network and Service Automation Market Tracker Report – 2025* (May 2025) reported that most network domains have a weighted average automation level of 2.4 (representing partial to conditional autonomous network ability), according to the TM Forum's Autonomous Network Level standard (see ***Appendix***).

Figure 10: When will your organization fully integrate AI-driven assurance solutions with other network systems?



n=82–83

Source: Heavy Reading (now part of Omdia), June 2025

AIOps maturity

To achieve greater operational efficiency and enhance customer experience, service providers must continue to evolve manual operations toward fully autonomous networks by strategically implementing AIOps capabilities. Low risk repetitive tasks are often the starting point for network autonomy with human oversight before a transition to greater levels of AI-driven reactive operation and a level of autonomy that incorporates predictive AI techniques to allow proactive network management.

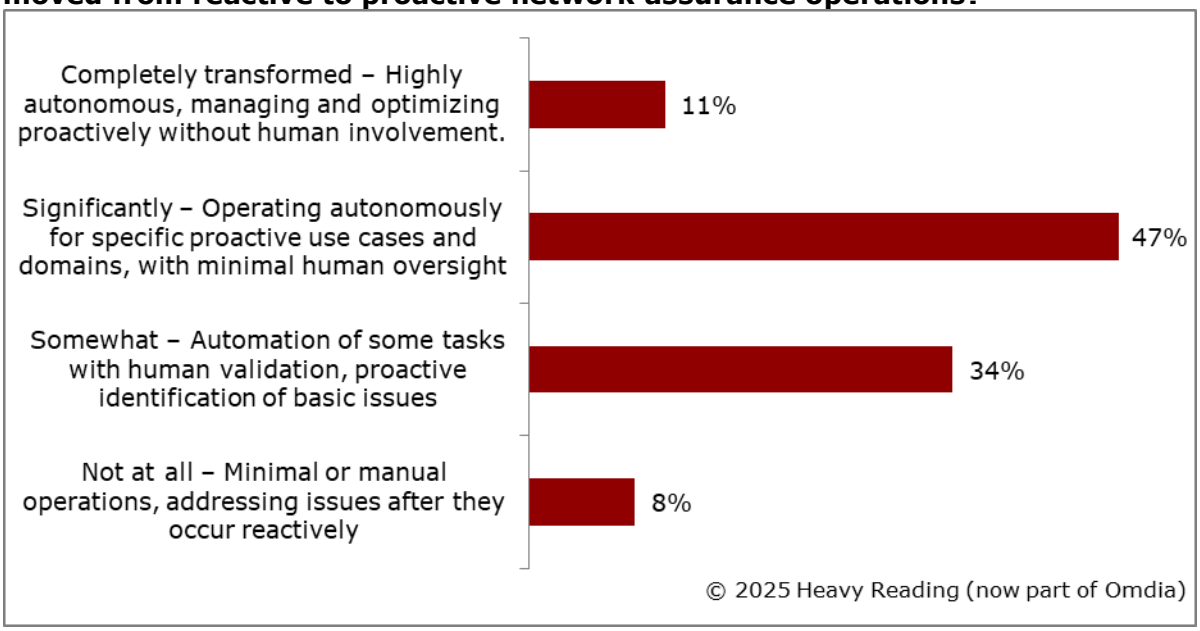
Operators are at differing stages of autonomy and AIOps maturing, as shown in **Figure 11**. Almost half of the respondents (47%) believe their network assurance operations are "operating autonomously for specific proactive use cases and domains, with minimal human oversight." A third of respondents (34%) are less advanced, confirming "automation of some tasks with human validation, proactive identification of basic issues."

A smaller group (11%) believes they have completely transformed their network assurance operations to be "highly autonomous, managing and optimizing proactively without human involvement." The smallest group of respondents reports "minimal or manual operations, addressing issues after they occur reactively" (8%).

Operators are impatient to close the gap between AI ambition and implementation to increase autonomy. Despite the 47% of respondents who believe their network assurance operations are "operating autonomously for specific proactive use cases and domains, with minimal human oversight," almost two-thirds (64%) of respondents are unlikely to deploy closed-loop automation, or plan to do so in two to three years (**Figure 19**), illustrating the persistent immaturity of advanced network autonomy.

Readers should view this result cautiously. While operators such as China Mobile, Orange, and Telefónica have achieved or aim to achieve "highly autonomous network" (Level 4) automation by the end of 2025, many are only reaching lower autonomy levels.

Figure 11: In terms of AIOps maturity, to what extent has your organization moved from reactive to proactive network assurance operations?



n=83

Source: Heavy Reading (now part of Omdia), June 2025

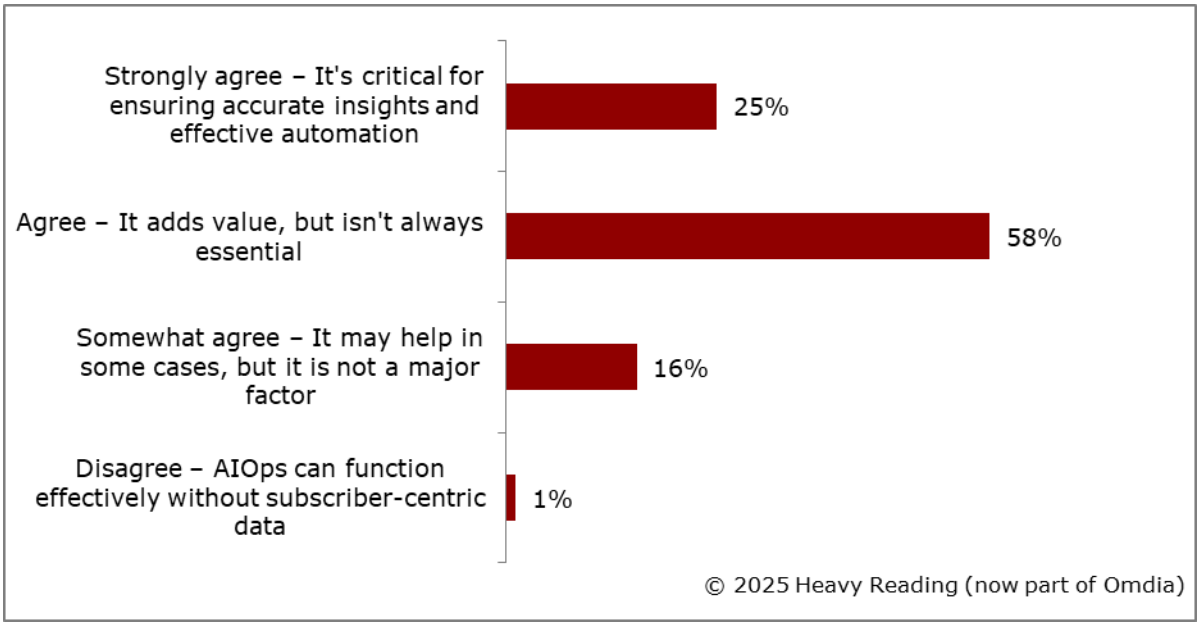
Subscriber-centric data

Figure 12 asks service providers to what extent AIOps should be driven by subscriber-centric data. A combined group of 83% of service providers either strongly agree (25%) or agree (58%). Reinforcing this view, only 1% of respondents believe AIOps can function effectively without subscriber-centric data.

A smaller group of 16% "somewhat agree – it may help in some use cases, but is not a major factor." Traditional NetOps feedback is a bottom-up approach, with many alarms triggered by network events. Evolving to top-down, customer-centric insights remains challenging. Operators must navigate data volume and quality issues, privacy and compliance, and integration complexities. However, utilizing customer usage patterns, service reliability, and customer data can provide additional context for technical issues.

As operators aim to provide a better customer experience and hyper-personalization, shifting from network-centric data to incorporating customer-centric information is vital.

Figure 12: To what extent do you agree that AIOps should be driven by subscriber-centric data?



n=83
Source: Heavy Reading (now part of Omdia), June 2025

USER PLANE MONITORING

As operators strive to improve customer experience, reduce churn, and hyper-personalize, they must maintain a deep understanding of real-time service performance. This section investigates current levels of insight, cost factors, and barriers for user plane traffic analysis.

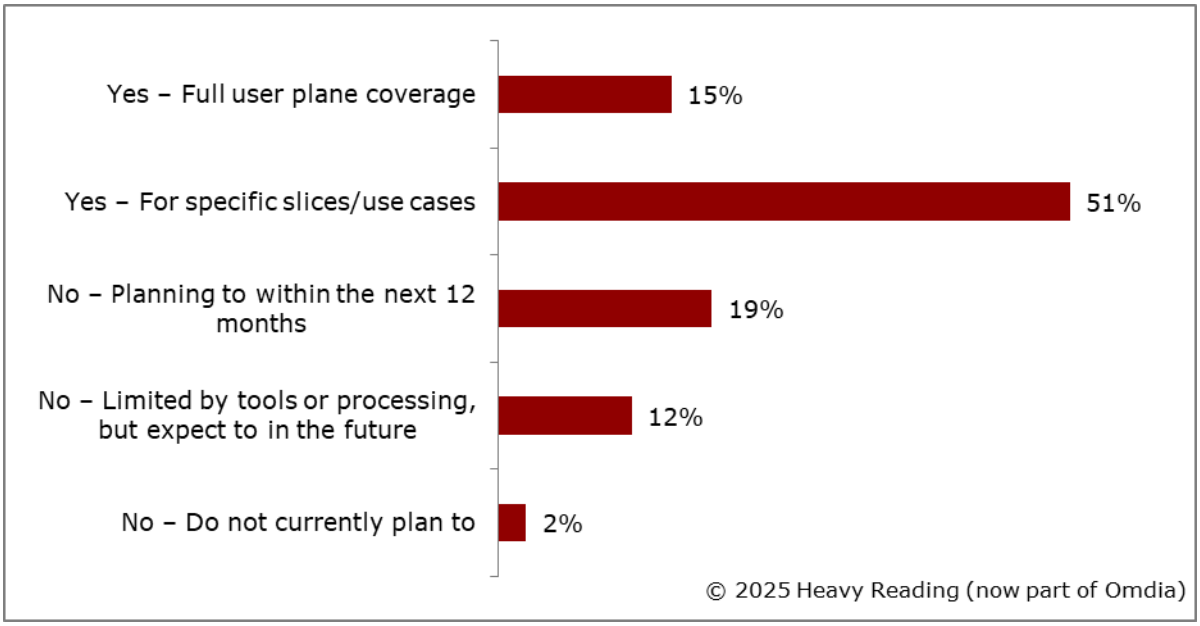
Real-time user plane analysis today

Real-time user data plane monitoring provides visibility into key performance indicators (KPIs) such as latency, jitter, throughput, and packet loss, and supports proactive anomaly detection and congestion prediction. The vast majority of operators (98%) confirm that they currently analyze real-time user plane coverage for 5G subscribers or plan to in the future, while only 2% currently do not plan to (see **Figure 13**).

Survey data confirms that most operators (51%) surveyed analyze "specific slices/use cases" for real-time user plane traffic. A further 19% are "planning to within the next 12 months," and 12% are "limited by tools or processing, but expect to in the future."

Only 15% of operators currently analyze "full user plane coverage." The most likely reasons for limited user plane coverage support include cost (as discussed in **Figure 14**), 5G network and tool maturity, levels of SLA, and lack of a compelling use case. 5G visibility is not fully mature, and many operators are still building out their 5G observability while focusing initially on RANs, selected services and domains, or currently operating with partial coverage.

Figure 13: Do you currently analyze real-time user plane traffic for all 5G subscribers?



n=84
Source: Heavy Reading (now part of Omdia), June 2025

The cost of user plane analysis

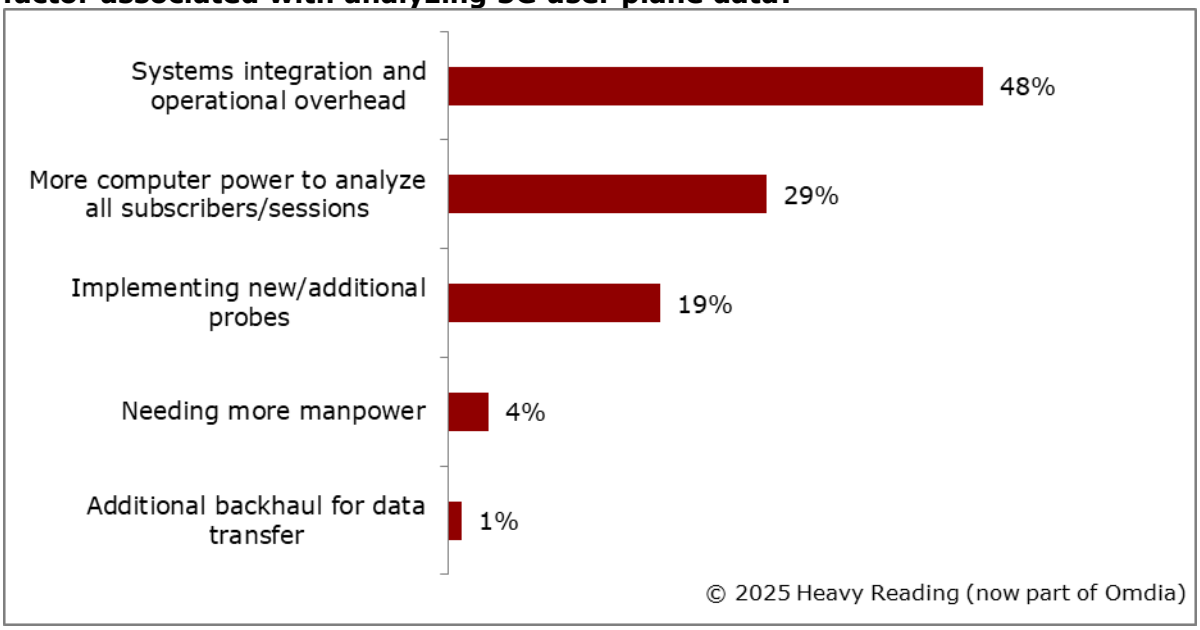
Monitoring the entire 5G user plane is not economically viable for many operators. For example, rising traffic growth and numbers of connected devices, infrastructure costs (compute, additional probes, manpower, and data center power), and technical complexity all increase costs. **Figure 14** queries what operators consider the most significant cost-related factor for analyzing the 5G user data plane.

Operators view the most significant cost of 5G user plane data analysis to be systems integration and operational overhead (48%), though an equal share cited infrastructure concerns (48%, based on a combined group of computer power [29%] and probes [19%]). Few are concerned about additional manpower (4%) or additional backhaul for data transfer (1%).

The industry is already developing multiple approaches to address the cost challenges of data collection and analysis. These include leveraging AI to reduce the volume of data requiring processing, hardware acceleration and data processing unit-based (DPU-based) solutions to optimize compute resources, selective monitoring approaches (dropping and forwarding traffic based on subscriber, device, RAN, network slice), and centralized vs. edge-based monitoring.

As data analysis, innovation, and techniques mature, the cost of user plane data analysis will fall. However, Heavy Reading (now part of Omdia) expects operators to prioritize use cases (as confirmed by **Figure 13**) in the short term.

Figure 14: What does your organization consider the most significant cost-related factor associated with analyzing 5G user plane data?



n=84
Source: Heavy Reading (now part of Omdia), June 2025

Barriers to 5G user plane monitoring

5G user plane monitoring presents significantly greater challenges than previous generations due to fundamental architectural changes, cloud technology, the sheer volume of connected devices generating traffic, and diverse use cases. **Figure 15** shows which factors operators consider the biggest barriers when evaluating 5G user plane monitoring for all subscribers.

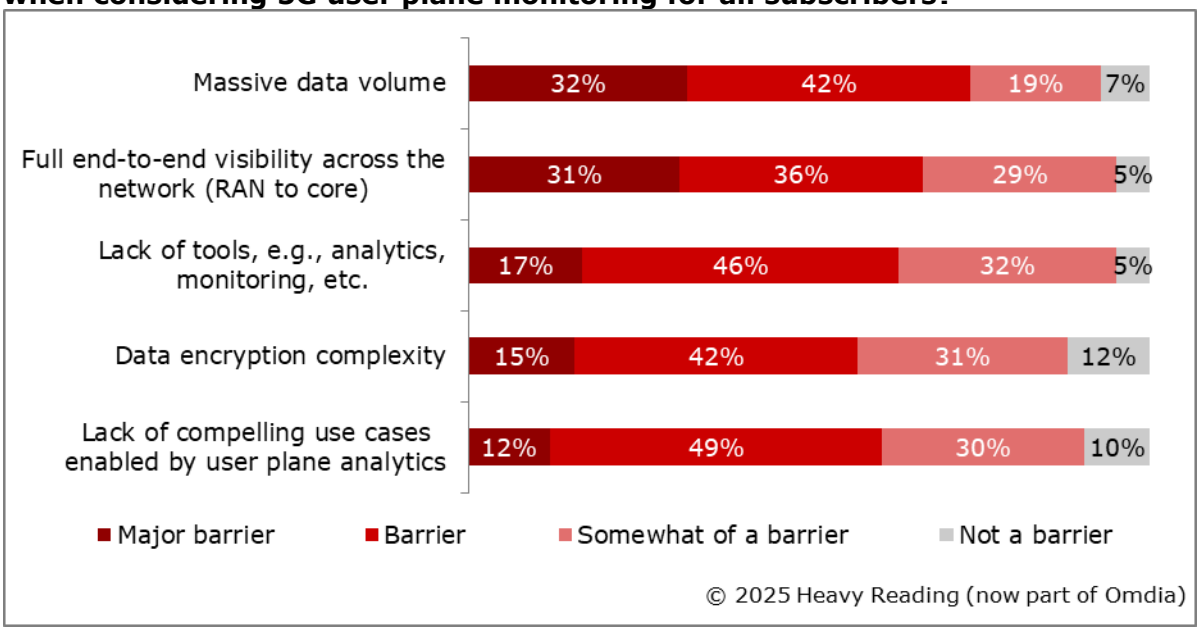
The survey reveals that operators cite more "barriers" than "major barriers" to monitoring, suggesting some progress with strategy and a clearer understanding of 5G data plane priorities. Massive data volume (32%) and full end-to-end visibility (31%) lead as the most frequently cited major barriers.

Operators also continue to struggle with "lack of compelling use cases" (49%) and "lack of tools" (46%), which rank as the most commonly cited barriers. 5G has diverse use case requirements, making it challenging to support varying performance, security, and analytical needs. Additionally, justifying return on investment remains difficult as operators continue to wrestle with monetization strategies.

Much of the mobile data consumed today is encrypted; for example, video content from popular streaming platforms using HTTPS or QUIC protocols remains invisible to conventional monitoring tools. The survey data indicates that while data encryption complexity scores lower than other categories overall at 57% (combining "major barrier" [15%] or "barrier" [42%]), it remains a significant concern. AI analytics offer a promising solution by interpreting encrypted traffic patterns to characterize behaviors, such as video buffering frequency, resolution changes, and other quality indicators.

5G user plane analysis is not fully mature. There has been significant progress, but operators are still determining customer needs and usage in the 5G environment. As we move into the mid-term of the 5G era, Heavy Reading (now part of Omdia) expects user plane monitoring to mature significantly as gaining deeper network insights becomes critical for hyper-personalization and maintaining competitive advantage.

Figure 15: To what extent are the following factors a barrier for your organization when considering 5G user plane monitoring for all subscribers?



n=84

Source: Heavy Reading (now part of Omdia), June 2025

ESTABLISHING HIGHER LEVELS OF AUTOMATION AND TRUST

To reap the rewards of full network autonomy (operational efficiency, performance gains, and greater personalization), operators must establish higher levels of trust. Operator initiatives, tools, and the journey to multi-agent technology will support this.

Autonomous network initiatives

Operators are actively pursuing network automation initiatives to help them increase network automation and leverage greater AIOps capabilities (**Figure 16**). When asked to select all initiatives that apply, operators reported undertaking a mean of 2.3 initiatives. The distribution of results also confirms that many strategies are under consideration.

"Evaluating AIOps solutions from traditional OSS/network vendors" (68%) scores highest, with "executing a broad OSS transformation program involving multiple systems" (54%) in second. Operators have differing automation approaches, but a flurry of industry catalyst projects, PoC, and evaluation activity has been underway.

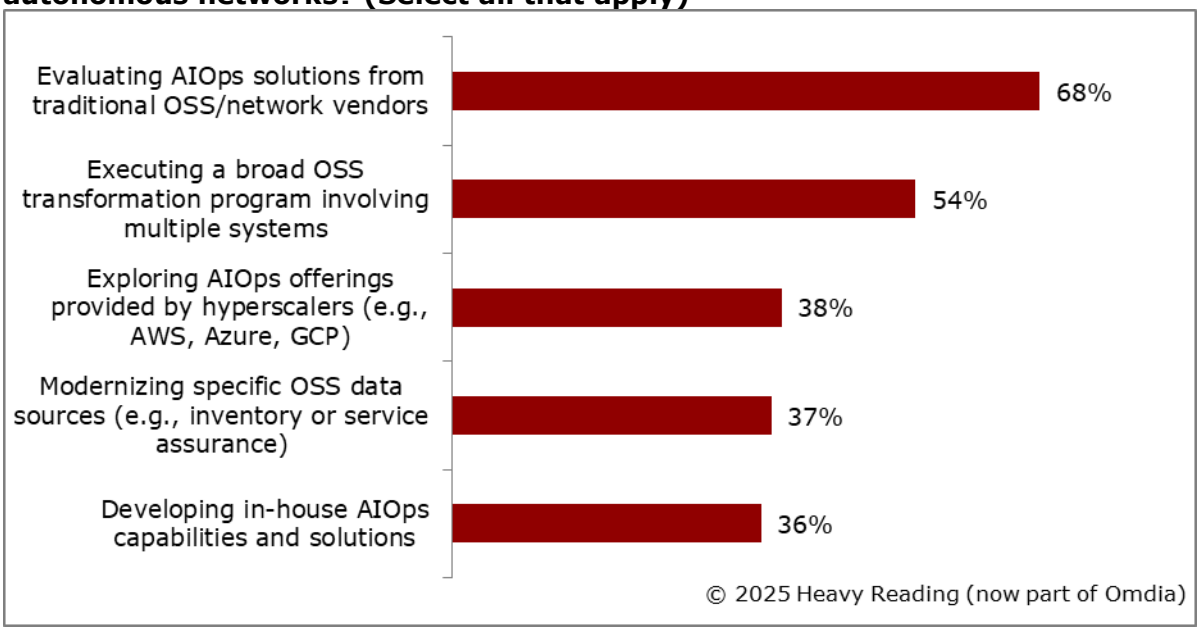
A second tier of initiatives includes:

- Exploring AIOps offerings provided by hyperscalers (38%)
- Modernizing specific data sources (37%)
- Developing in-house AIOps capabilities (36%)

Telcos are already pursuing multicloud strategies (see **Figure 4** in this survey). A number of them are already working with public cloud providers for telco OSS/BSS, including Orange, AT&T, Telefónica, etc. Hyperscalers have extensive knowledge of AI and automation and huge resources to ingest and store large volumes of network data.

Other operators, such as DT, are looking toward in-house developed AIOps capabilities, leveraging open source components.

Figure 16: What initiatives is your organization undertaking to advance its level of autonomous networks? (Select all that apply)



n=84

Source: Heavy Reading (now part of Omdia), June 2025

Digital twin and AI trust

For operators to increase levels of network autonomy, AI-driven decisions must be secure, reliable, and transparent. As AI technology moves toward agentic systems designed to work through complex networking problems and create an action plan before using tools to execute an action, operators must guarantee accuracy and establish decision-making boundaries.

To understand how operators will establish AI trust, the survey asked respondents what methods they use for AI decisions and advancing network autonomy (**Figure 17**).

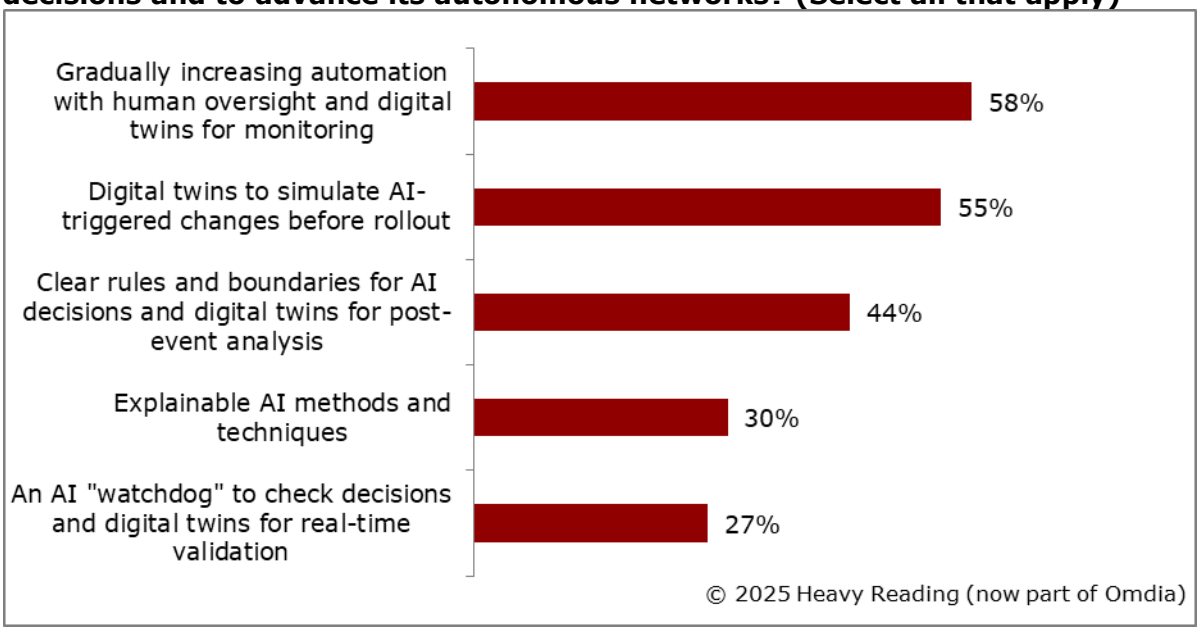
Operators were instructed to select "all that apply," and respondents chose on average 2.1 methods. Survey data confirmed that "gradually increasing automation with human oversight and digital twins for monitoring" (58%) was most common, followed closely by "digital twins to simulate AI-triggered changes before rollout" (55%). The results support well-recognized and established working methods for improving AI trust and the proven inroads of the digital twin method. For example, large operators such as AT&T, Telefónica, and Vodafone Germany use digital twins to verify processes and improve efficiency and customer experience.

"Clear rules and boundaries for AI decisions and digital twins for post-event analysis" (44%) places third. Post-event analysis will become increasingly useful for incident investigation, impact analysis, and enhancing customer experience, as well as for future network planning and optimization.

"Explainable AI methods and techniques" and "An AI 'watchdog' (30%) to check decisions for digital twins for real-time validation" (27%) score lowest. Explainable AI is an active field aiming to establish AI transparency and accountability. It is likely that challenges around subjectivity of explanations, complexity, and compute resource overheads currently make this a less attractive method for operators. Data protection laws and AI regulation are still maturing, explaining the lower placing of "watchdog."

Digital twin monitoring is instrumental to establishing AI trust. Operators surveyed confirm that their primary methods to build trust are digital twin monitoring with human oversight and simulating AI-triggered changes before live rollout to verify and validate AI decisions and advance network autonomy.

Figure 17: What methods are your organization using to establish trust for AI decisions and to advance its autonomous networks? (Select all that apply)



n=84

Source: Heavy Reading (now part of Omdia), June 2025

Agentic AI deployment strategies

Rapidly evolving agentic AI systems will transform network operations by enabling multi-step task completion with minimal human oversight. Instead of merely identifying an anomaly and its root cause, these advanced agents can autonomously execute remediation steps—maintaining customer experience and performance.

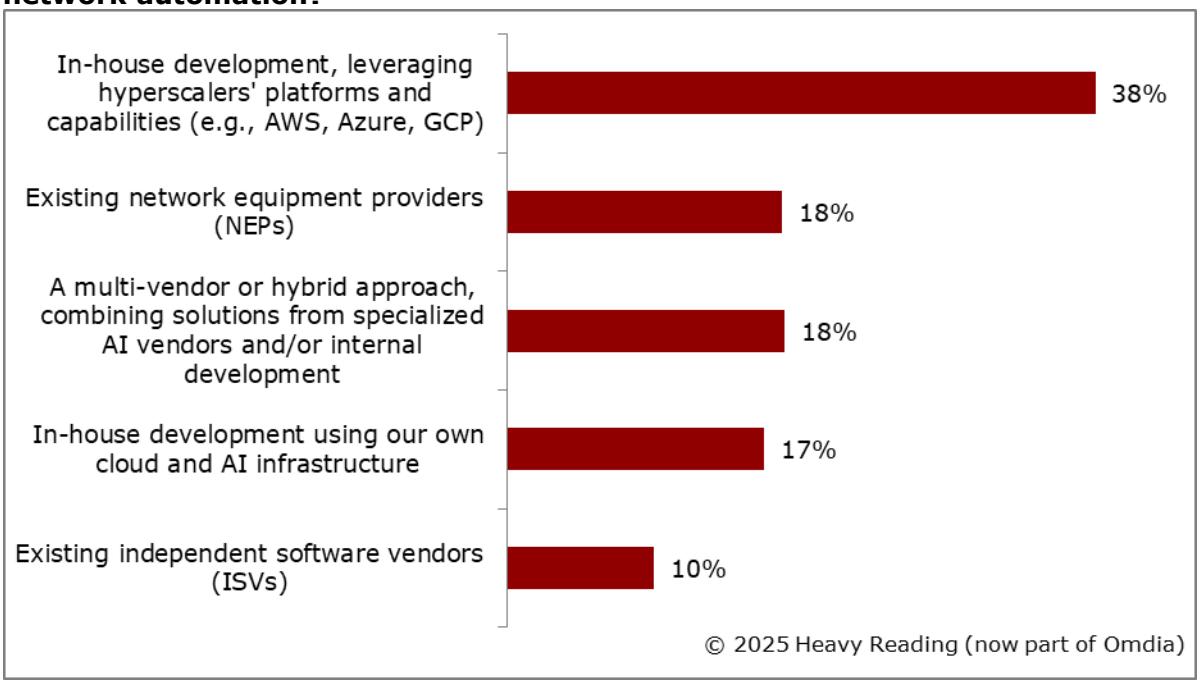
Service providers will primarily use "in-house development, leveraging hyperscalers' platforms and capabilities" (38%) to deploy agentic AI for network automation. This reflects a desire to leverage the leading-edge skills of the hyperscalers while growing in-house expertise, which was lacking in **Figure 18**.

A secondary tier of close responses includes "existing network equipment providers (NEPs)" and "multi-vendor or hybrid approach" scoring equally at 18%, about the same as "in-house development using own cloud and AI infrastructure" (17%). Existing independent software

vendors (ISVs) score lowest with 10%, possibly due to service providers' belief that others, such as hyperscalers, have stronger agentic experience.

Operators reveal mixed agentic AI strategies. Responses indicate almost an even split between in-house development (either with or without partner support) and provider solutions (NEPs, ISVs, multi-vendor). Many are partnering with hyperscalers to leverage experience and platform resources and to build AI competence. Existing NEPs will also support operators' ambitions for automation. This balanced strategy reflects operators' desire to partner with key agentic experts and avoid solution lock-in while addressing skills gaps.

Figure 18: What is your organization's strategy for deploying agentic AI for network automation?



n=84

Source: Heavy Reading (now part of Omdia), June 2025

AI agent deployment timescales

An AI agent is the next evolution from GenAI. They can reason, have memory, and use external tools to plan next steps and adapt based on feedback. These capabilities allow them to automate complex workflows and operate semi-autonomously. Moving to the next stage—multiple agents with shared context, coordinated tasks, and continuous adaptation—moves toward full process automation.

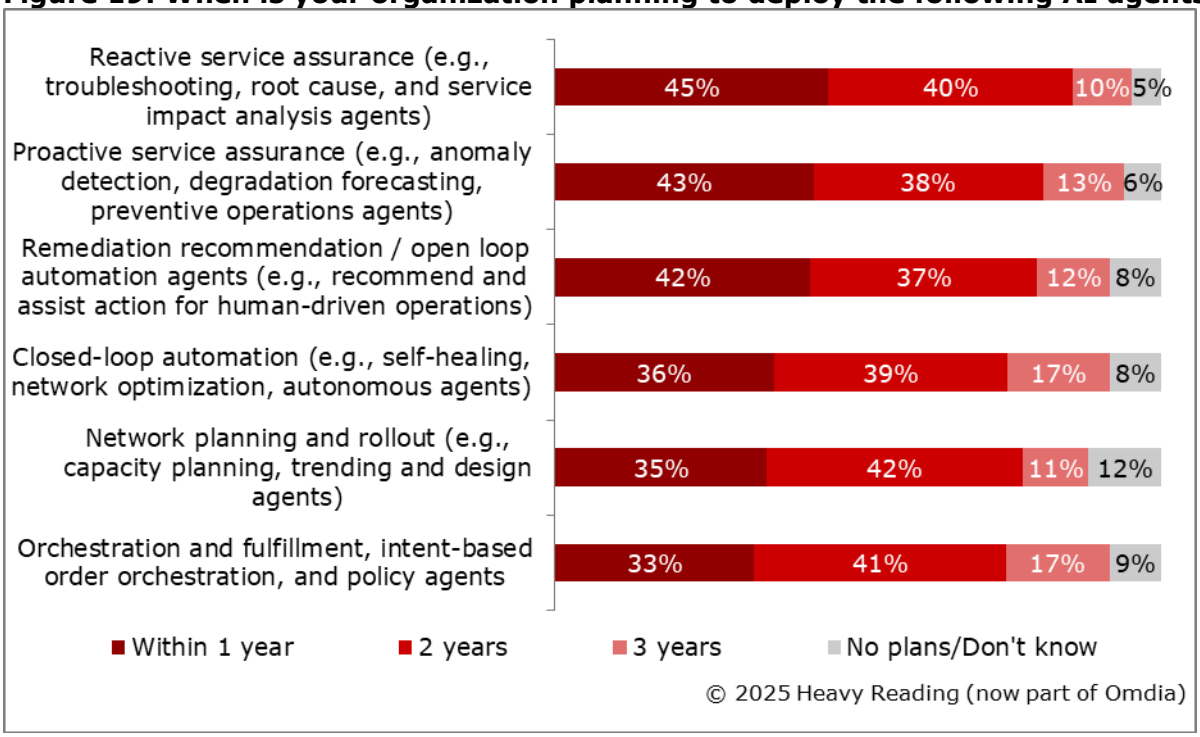
The interest and expectation of telco agent technology is vast. NetOps environments depend on and interlink multiple systems and tasks, making them ideal for agent AI-driven workflows. To determine how AI agents are likely to be adopted across various NetOps and assurance tasks, the survey asks respondents about their plans to deploy AI agents (**Figure 19**).

The survey data confirms great enthusiasm for AI agents. Over 74% of operators plan to deploy AI agents across all NetOps survey categories within two years (representing combined responses of within one year and two years). Reactive service assurance, proactive service assurance, and remediation recommendations/open loop automation agents are cited as the most likely use cases to deploy AI agents within one year, with around 42–45% of respondents agreeing.

Fewer respondents (33–36%) expect to deploy AI agents within a year to take on the tasks of closed-loop automation, network planning and rollout, or orchestration and fulfillment. However, they have slightly more confidence in doing so within two years (39–42%). These tasks are more likely to require multiple agent systems; this lower score, while still optimistic, acknowledges the complexity, trust, and supporting systems required to achieve this goal.

The survey data indicates operators are eager to introduce AI agents. This optimistic outlook means operators are likely to deploy low risk use cases to prove trust before full multi-agent systems with shared context begin to evolve over the next three years.

Figure 19: When is your organization planning to deploy the following AI agents?



n=82–83

Source: Heavy Reading (now part of Omdia), June 2025

Deployment of agentic AI

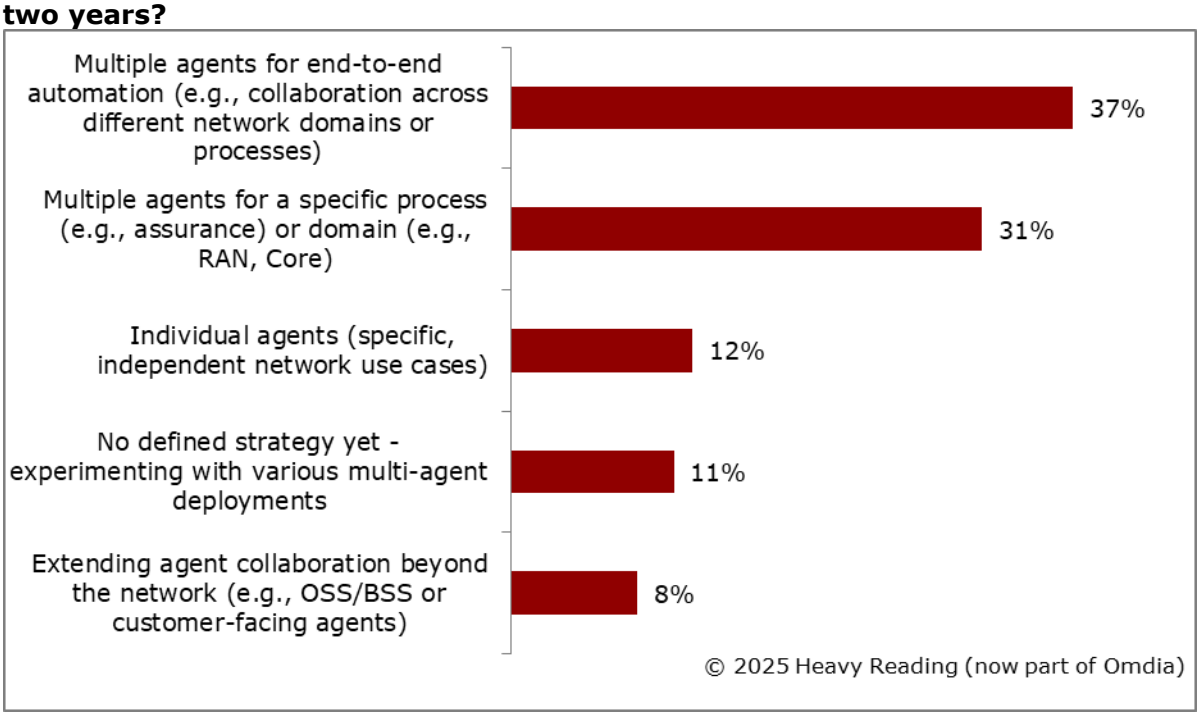
As operators plan to deploy AI agents, determining how their AI systems will integrate with their workflows and make decisions is vital:

- Connect individual agents using the Model Context Protocol (MCP) to connect to tools, APIs, and databases.
- Deploy multiple specialized agents to a single source and use agent-to-agent (A2A) protocols to coordinate.

Deployment model architecture can be likened to the telco hub and spoke routing model (individual agent) vs. a distributed network of peers (A2A). AI systems can use either individual or multiple agents, so the use case will likely determine the choice.

Service providers are eager to deploy agentic AI throughout their networks (see **Figure 19**), and **Figure 20** also confirms that the majority (89%) have a defined strategy.

Figure 20: How does your organization plan to deploy agentic AI within the next two years?



n=83

Source: Heavy Reading (now part of Omdia), June 2025

Multiple agent strategies are desirable. Respondents confirm that "multiple agents for end-to-end automation" (37%) is the leading approach, followed by "multiple agents for a specific process (e.g., assurance) or domain (e.g., RAN, core)." Service providers are less likely to implement "individual agents" (12%) or extend agent collaboration beyond the network (8%). Operators may determine that a multi-agent strategy is preferable due to the scope of larger processes, domains, end-to-end tasks (e.g., ability to fine-tune agents to specific tools, workflows for accuracy), resilience (avoiding individual agent failure disruption), or scalability.

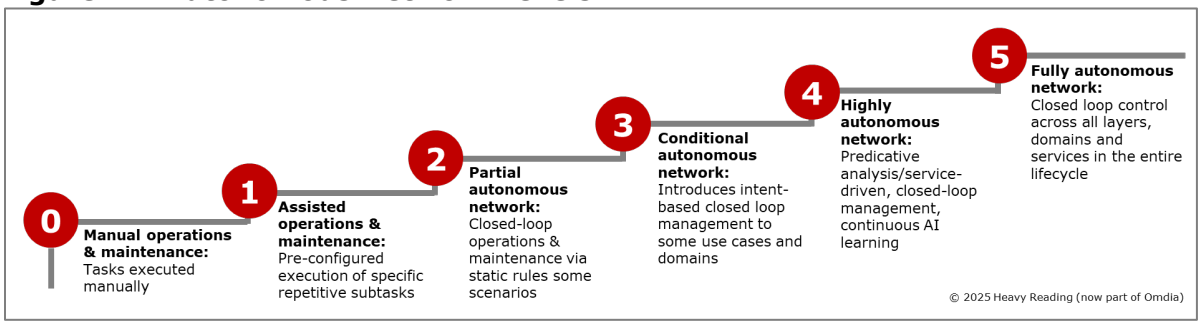
The RoW group of respondents has slightly differing opinions from the combined worldwide group, as 42% confirm their plan to deploy "multiple agents for specific processes," then multiple agents for end-to-end collaboration (28%), with individual agents and extending agent collaboration jointly scoring 12%.

The choice between multiple agent approaches vs. individual agents—or a hybrid approach—will likely differ across organizations and depend on the network use case. Operators must ensure their future AI deployments are scalable and adaptable to remain future-proof.

APPENDIX

The TM Forum classifies the autonomous levels (shown in **Figure 21**) into six steps.

Figure 21: Autonomous Network Levels



Source: Heavy Reading (now part of Omdia), TM Forum