

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

**HEAVY  
READING**  
**WHITE  
PAPER**

# **The Business Value of AI in Zero-Touch Network Monitoring**

*A Heavy Reading white paper produced for Anodot*



**AUTHOR: SANDRA O'BOYLE, ANALYST, HEAVY READING**

---

## INTRODUCTION

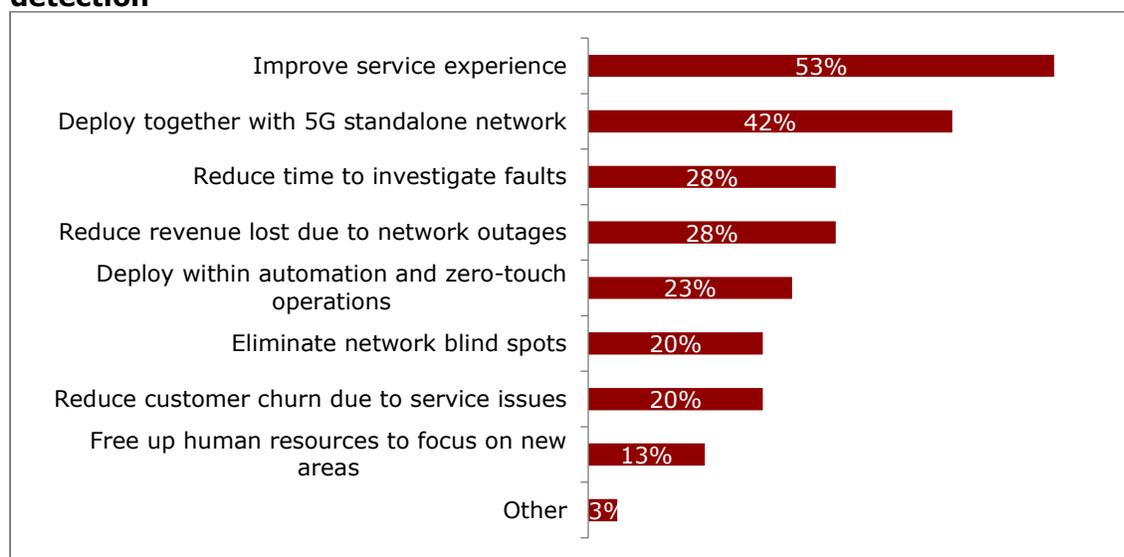
The number one driver for deploying AI-based network monitoring is improving the service experience. Customer experience and service delivery are becoming critical factors in communications service provider (CSP) businesses. Competition is fierce, and end users expect the type of frictionless service delivery and company interactions they get from web companies.

Artificial intelligence (AI) is expected to drive several capabilities for CSPs, including efficient network infrastructure and operations, automated service delivery, improved customer experience, and new revenue opportunities. Of these areas, the network operations domain is the most active, according to the public AI contracts tracked by Omdia. Of the 221 public telco AI contracts awarded between 1Q18 and 1Q21, 40% were related to network operations.

This market momentum is supported by the Anodot-sponsored Heavy Reading survey. Just over two-thirds (67%) of CSP respondents have deployed AI in their network. And more than 50% of those who have not yet deployed AI plan to do so within a year or two.

The momentum is driving the need for AI-based solutions that help network operations improve customer experience and accelerate troubleshooting when things do go wrong while also saving costs through automation and reducing opex.

**Figure 1: Primary drivers for deploying AI-based network monitoring and detection**



n=67 CSP respondents

Source: Heavy Reading global CSP survey, 3Q21

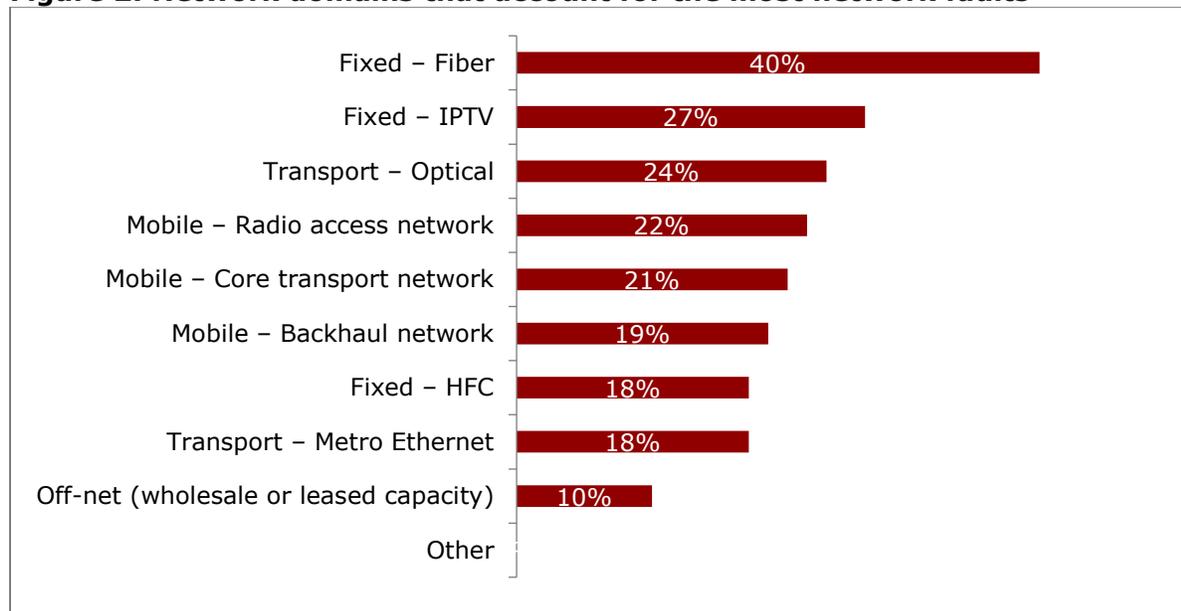
This paper looks at service provider plans and the drivers behind deploying AI for network monitoring and detection, key use cases that deliver cost savings, and the most important AI capabilities to drive zero-touch network monitoring. Research is based on a Heavy Reading global survey with 65+ key networking and IT decision makers in CSPs commissioned by Anodot in 3Q21.

## COST OF MAINTAINING STATUS QUO NETWORK OPERATIONS

While most CSPs will continue to aggressively seek top-line growth, the most likely way they will improve profitability is through reducing cost. Network operations represent a ripe area for transformation and finding more efficient ways of managing networks. Network traffic is growing year over year, but so too are the volume and diversity of connected devices. There will be 5x more machines connected to the mobile network than humans by 2025, according to the GSMA. The volume of data, alarms, and events will be too much for a human operations team to manage effectively. Due to the complexity facing telecom network operations today, AI and automation may be the only way service providers will be able to offer future network services and reduce costs to serve customers.

Service providers face challenges managing network performance issues across all network domains. Fixed fiber networks (40%) account for the most faults, followed by IPTV networks (27%), where network latency and jitter can affect video quality, and optical transport networks (24%). Mobile operators need better tools to gain visibility into faults across the RAN, core, and backhaul networks to understand the end-to-end service experience for customers (**Figure 2**).

**Figure 2: Network domains that account for the most network faults**



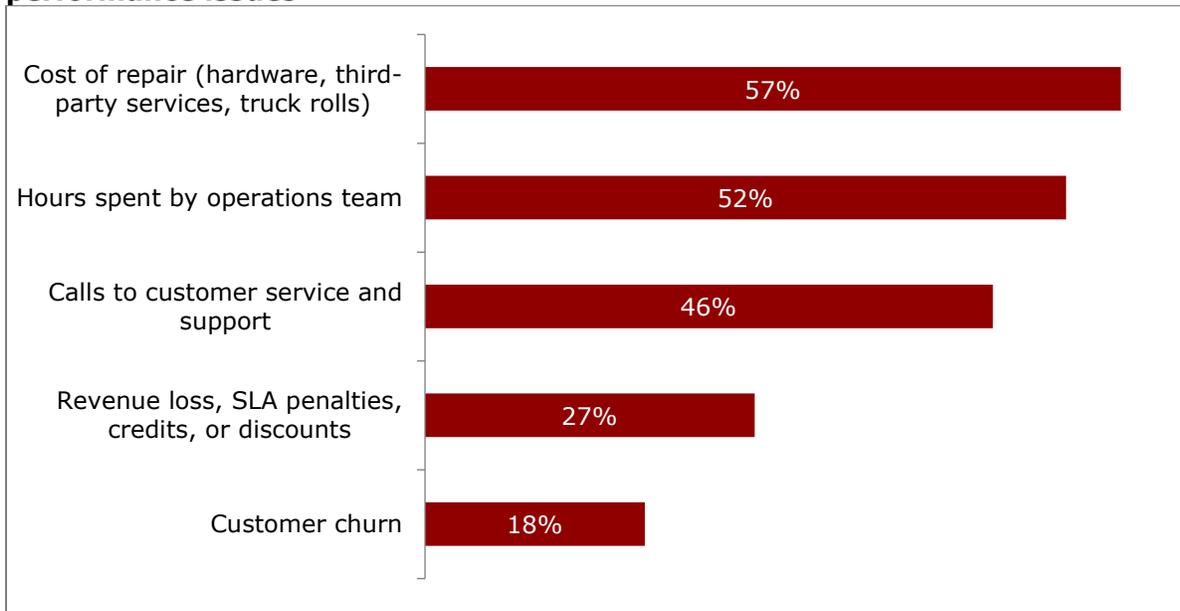
n=67 CSP respondents

Source: Heavy Reading global CSP survey, 3Q21

Manually trying to manage service degradations, customer reported issues, and trouble tickets no longer works for CSPs. This approach is reactive and takes too long, resulting in dissatisfied customers and higher labor and repair costs. More than half of CSPs (57%) identify repair costs, including truck rolls/site visits, replacing hardware, etc., as a significant cost drain. The second biggest cost area identified by CSPs (52%) is the number of hours spent by the operations team troubleshooting and manually trying to cross-check multiple silos of systems and network domains to determine what is causing problems.

Existing network monitoring tools are not capable of supporting complex networks, which is leading to long hours of investigation and analysis. CSPs have the potential to reduce costs and time spent on investigation, free up experienced staff to focus on new areas, and prevent expensive truck rolls with new tools that improve detection speed and quickly pinpoint the root cause of problems.

**Figure 3: Significant costs related to service degradation and customer performance issues**



n=67 CSP respondents

Source: Heavy Reading global CSP survey, 3Q21

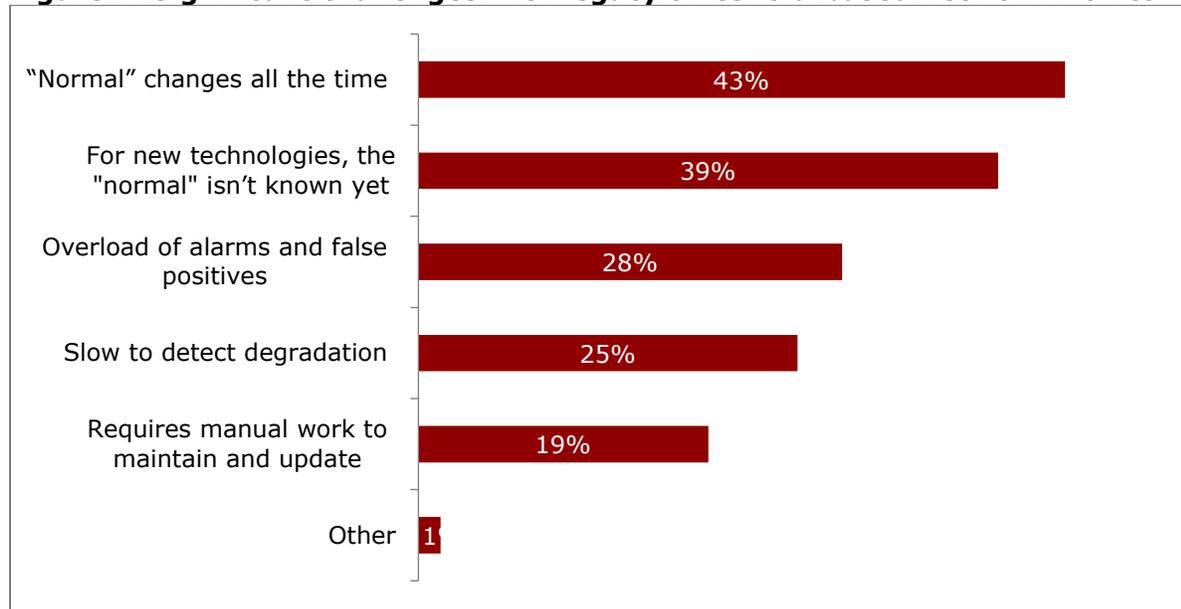
The most time-consuming aspects of troubleshooting cited by CSPs include detecting and identifying the issue (48%), isolating the fault domain (physical/virtual/network layer) (46%), and isolating and confirming the root cause (43%). Since CSPs deal with multiple systems and tools, diverse sources of data, and many network domains, vendors, and layers, they frequently lack end-to-end visibility into service performance. This makes it difficult to correlate data or add metadata to pinpoint the root cause of issues, which leads to inefficient manual processes and high labor costs.

Performance troubleshooting, early warning, and visibility into service degradations are important to avoid the third big cost center—calls to customer service and support, cited by nearly half of CSPs (46%). The ability to quickly pinpoint problems and detect anomalies and causes of recurring issues results in more predictive issue detection. This helps users to maintain customer experience, prevent revenue loss due to customer churn and service-level agreement (SLA) penalties, and avoid the cost of acquiring new customers.

## Moving away from threshold-based network monitoring

One of the challenges with the current approach of threshold-based network monitoring is that “normal” changes all the time (**Figure 4**). Human operations teams cannot keep up with the manual work of adjusting key performance indicator (KPI) parameters, detecting issues, and determining the root cause of issues in the network. This is particularly true with new technologies and services. Another big concern is that the overwhelming “noise” from alarms and events makes it difficult to detect real customer-affecting issues and performance degradations that should be prioritized.

**Figure 4: Significant challenges with legacy threshold-based network monitoring**



n=67 CSP respondents

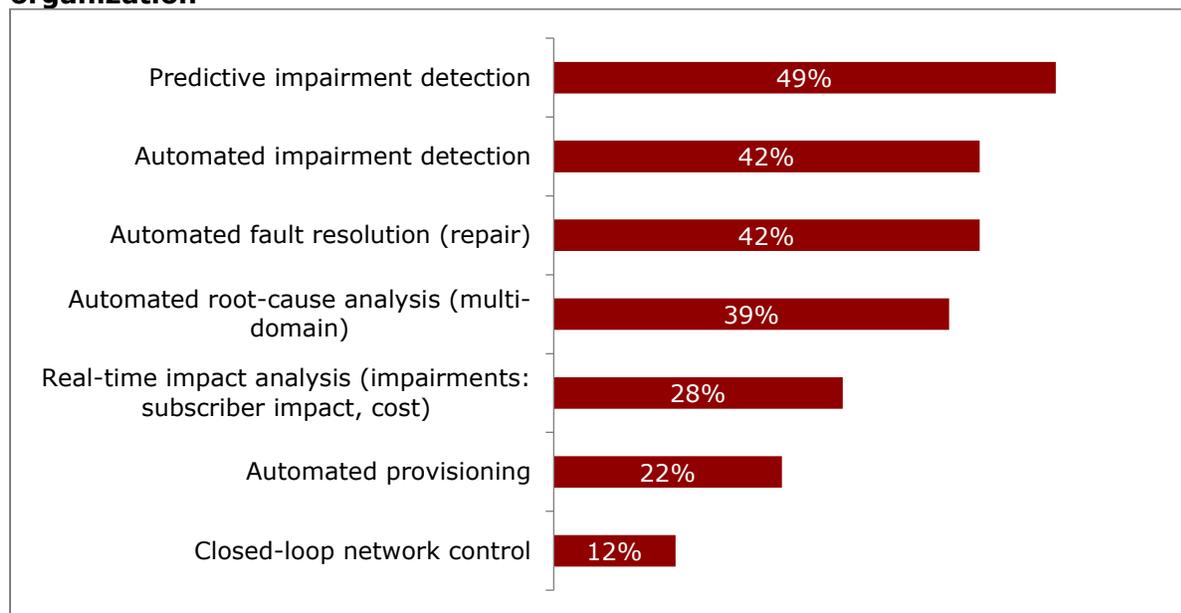
Source: Heavy Reading global CSP survey, 3Q21

## WHY NOW: THE VALUE OF AI-BASED NETWORK MONITORING

CSPs are building AI on top of their network and using self-learning at scale to continuously monitor and correlate network and service anomalies across the entire telco stack. This enables actionable alerts in their context, improving the time to detect and resolve incidents by as much as 30–50%.

AI-based network monitoring and anomaly detection will help manage the complexity of legacy networks and multiple silos of monitoring systems and tools. About half (49%) of CSPs expect AI-based network automation to save costs by automatically detecting and predicting issues and congestion *before* they cause an outage or performance issues (**Figure 5**).

**Figure 5: Network automation that delivers the biggest cost-savings for your organization**



n=67 CSP respondents

Source: Heavy Reading global CSP survey, 3Q21

## **CSP REQUIREMENTS: ZERO-TOUCH NETWORK MONITORING**

42% of CSPs surveyed cite integration with existing tools as the biggest barrier to deploying AI-based network monitoring and anomaly detection in networks. Service providers are looking for solutions that deliver a short time to value with easy integration and open APIs. They are also seeking solutions that are easy for teams to use and support without requiring significant investment in data science talent and professional services.

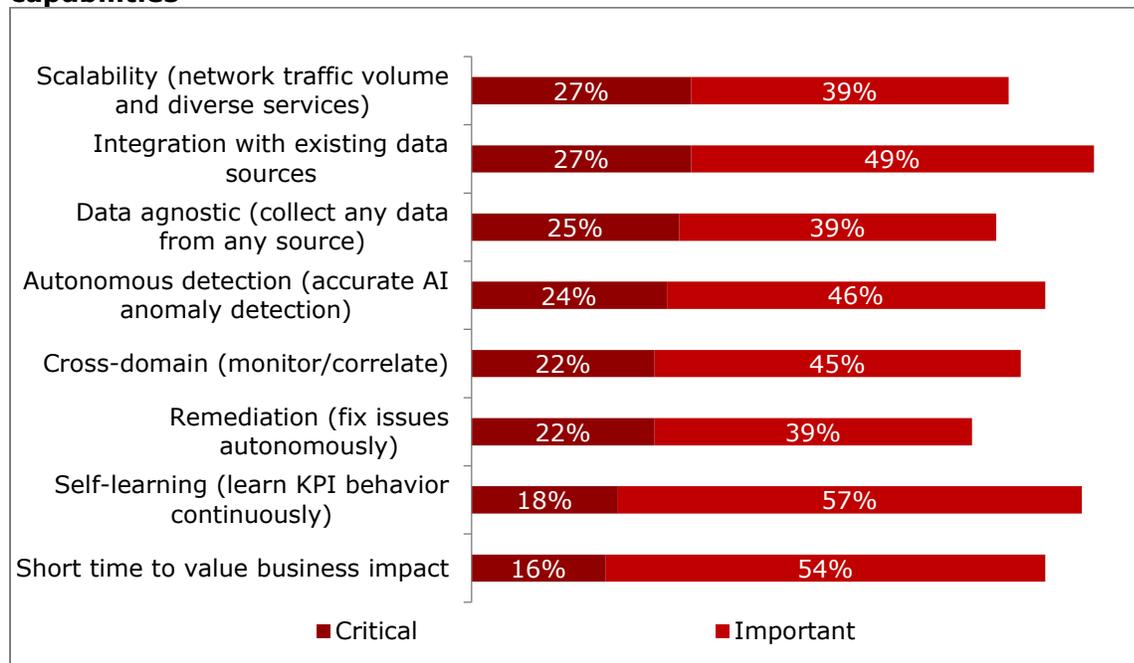
Proving business value and gaining early wins are important to build momentum and trust and gain support for wider adoption and investment. For integration with network automation and the supporting orchestration framework, AI solutions must be able to handle network data volume and diverse service KPIs. They must also be capable of self-learning KPI behavior on an autonomous and continuous basis. These capabilities enable users to avoid setting up and updating manual thresholds. Instead, AI algorithms learn the normal behavior of KPI metrics across domains and constantly monitor anomalies—without requiring configuration.

## Key requirements for service providers—percentage rated critical or important

**Figure 6** shows that CSPs have key requirements for AI-based network monitoring solutions:

- **Integrates with existing data (76%):** Collect all data types from all network types, layers, and domains at scale. Correlate data to uncover the root cause and drive fast time to resolution.
- **Self-learning (75%):** AI algorithms learn the normal behavior of KPI metrics across domains and constantly monitor anomalies without requiring configuration.
- **Short time to business impact (70%):** Results matter; AI-based solutions need to be easy and fast to implement and explainable with clearly defined use cases.
- **Accurate anomaly detection (70%):** Prioritizes anomalies based on customer impact, cutting through the noise and only focusing on what matters.
- **Autonomous (70%):** Automated; continuously monitors network and service anomalies across the network and service stack.
- **Cross-domain (67%):** All metrics are actively monitored, enabling CSPs to achieve full visibility into service degradation incidents.
- **Scalable (66%):** Can handle network volume, as well as diverse services and use cases.

**Figure 6: Zero-touch network automation and AI monitoring: Important capabilities**



n=67 CSP respondents

Source: Heavy Reading global CSP survey, 3Q21

---

## CONCLUSION

It is more a question of *when* rather than *if* CSPs should deploy AI-based network monitoring and anomaly detection. With the move to orchestrated software-defined networking and the ultimate goal of zero-touch operations, AI has a key role to play in managing volumes of network data, service KPIs, and alarms at scale and determining anomalies and service performance degradations before customers are affected to ensure the best service experience. From both a top-line (growth for new services) and bottom-line (cost reduction) perspective, AI can be seen as complementary to the operations team, a way of reducing manual labor and repair costs and speeding up time to detect and repair issues.

### Business benefits of AI-based network monitoring

- **Customer experience:** Find and fix customer experience issues before they affect usage, conversions, retention, and revenue.
- **Speed:** Spend less time looking through multiple systems, KPI dashboards, and reports. Reduce time to insight/resolution and reduce alarm noise/events.
- **Efficiency:** Identify the incidents that impact the bottom line, helping users detect issues up to 80% faster and cut incident costs by as much as 70%.
- **Opex reduction:** Reduce manual processes, save on labor costs, and automate network monitoring and anomaly detection.

### Recommendations

- **Start with specific use cases.** Once the first step is successful, enthusiasm for AI-based network monitoring in the organization will increase. Introduce AI-based network monitoring/anomaly detection solutions on top of the operations support system (OSS) to improve issue detection and resolution and then increase in complexity from there.
- **Consider vendors that bring solutions that can scale and are self-learning and simple to integrate** (with no need for professional services). Also look for proven and accurate AI algorithms/deployments along with demonstrated results in complex communications networks.
- **Measure the time to market and business value**, which are critically important. How long will it take to deploy? Focus on business value, as well—measure cost savings, process improvements, etc. in business terms.

## ABOUT ANODOT

[Anodot's](#) zero-touch network monitoring platform provides the ability to monitor cross-layer network performance and service experience in one platform. We collect all data types, at any scale, and use AI/ML to correlate anomalies across the entire telco stack. Our platform is the "brain" on top of the OSS that detects service-impacting incidents in real time. We help customers like T-Mobile and Megafon protect their revenue and improve service experience—reducing the number of alerts by 90% and shortening time to resolve incidents by 30%.