Publication date:
02 Jul 2021
Author:
Adaora Okeleke
Roy Illsley

Transforming Telco Operations with AIOps

Moving from reactive to proactive operations

Brought to you by Informa Tech

Omdia commissioned research, sponsored by IBM

Contents

Summary

Operational transformation is inevitable

Communications service providers (CSPs) face several challenges including increasing customer expectations, reduced revenue growth, and high operational costs. The growing complexity of their network and IT landscapes and continual mergers and acquisitions (M&A) are some of the factors that have contributed to these challenges. While CSPs are still in the early stages of transitioning to cloud-native networks and IT environments to drive more innovation and agility, this change will further heighten the issues they currently face, especially with operations and management. To meet business imperatives, CSPs need to transform current operational practices from being reactive to being more proactive.

Artificial intelligence for IT operations (AIOps) presents opportunities for CSPs to transform to more proactive operational practices. Omdia defines AIOps as the overarching technology that can bring all the management practices in IT together. It is a multilayered technology that automates and enhances network and IT operations. It leverages big data and AI technologies such as machine learning (ML) to analyse data across multiple data silos in networks and IT. With this capability, CSPs can gain deeper visibility into their networks and IT systems and use this insight to drive efficient and effective operations. It is particularly crucial to managing hybrid network environments, which in the future will become more cloud native and will therefore require advanced capabilities beyond those provided by traditional monitoring tools.

Proactive customer service, network fault prediction and prevention, anomaly detection in system performance, and network security are examples of use cases where CSPs are currently exploring the use of AIOps. CSPs such as Hong Kong Telecom and Smart Communications have performed proofs of concept (POCs), generating results such as early detection of network failures and triggering actions such as site visits in advance to mitigate risks associated with the failures. A South African CSP found that by applying AIOps capabilities it was able to reduce mean time to detect (MTTD) and mean time to repair (MTTR). MTTR was reduced by a factor of 17.

Successful implementation of AIOps is not just a technology play: it requires changes in organisational culture and practices. Existing barriers between teams need to be broken down to allow easy exchange of data. Processes also need to be restructured to allow the recommendations provided by AIOps solutions to be acted on. Effective data management and governance practices must be established and baked into day-to-day operational activities to ensure that high-quality data is available to drive AIOps use cases. Most importantly, C-level executives have a role to play in educating teams on the benefits that AIOps will bring to enhancing operations. Vendors, on the other hand, need to work closely with CSP customers to develop impactful use cases that can address their most critical challenges. Their expertise in data science will accelerate CSPs' adoption of AIOps. Engagements with standards organisation such as the Tele Management Forum (TM

Forum) will also foster developments around AIOps because they provide a platform for CSPs and vendors to collaborate in developing use cases and establishing best practices.

Introduction

More complexity for the CSPs

CSPs are under pressure to grow revenue and reduce costs. They also need to counter growing competition from peers and other digital service providers. CSPs look to address these challenges by delivering new services via technologies such as 5G, the Internet of Things (IoT), and edge computing, improving customer experience and operational efficiency.

However, network and IT landscapes are becoming more complex. Networks are changing from pure physical network infrastructure to a mix of physical, virtualised, and containerised network functions. Technology environments are being re-architected as cloud native and deployed to all cloud types. Delivering and managing services in these environments is very challenging. Service portfolios have also evolved from being voice and data services to including digital services with low tolerance to service quality issues. Network migration to 5G will drive further complexity as capabilities such as network slicing add further difficulty in managing the network and meeting service level agreements.

M&A activities also drive huge complexity. Omdia's Communications Provider M&A report indicates that mobile and wireless CSPs have dominated M&A deals. In the last five years, wireline and mobile segments saw 392 and 191 deal announcements respectively. The resulting IT landscape is complicated and difficult to consolidate and manage. As a result, there are siloed IT stacks still in operation.

Because of the growing complexity in network and IT environments, more services, network entities, IT systems, and KPIs need to be monitored. CSPs' current reactive approaches to managing networks and operations must change to support business priorities. They are manual and dependent on human expertise and so are time consuming, prone to errors, and do not scale well. Current tools are also not fit to support changes in the network and IT. Average handling time for failures is high, leading to increased operational costs. Delivering impactful customer experience and achieving operational efficiency will be challenging.

In his 2020 Digital Transformation World Series keynote address, Orange CEO and GSMA chair Stephane Richard said, "CSP debt is so heavy," highlighting the need for CSPs to transform to automated operations. This would enable them to save costs and be more responsive and proactive. The target is to have the ability to detect events of interest before they start having an impact on customers and operations. This approach can drive high-quality service delivery to customers and reduce operational costs.

AIOps to enable proactive and efficient telco operations

What is AIOps?

Artificial intelligence for IT operations (AIOps) is a term that has been adopted by the market to define the way IT operations needs to perform in digital enterprises. Omdia defines AIOps as the overarching technology that can bring all the management practices in IT together. It is a multilayered technology of platforms that automate and enhance IT operations through AI technologies.

While AIOps was developed to scale the manageability of IT systems, it can also be applied in the telecoms operations space beyond IT support. This application is driven by several factors including the changing landscape of the network as it becomes more software driven with virtualisation and software-defined networking (SDN). The demarcation of responsibilities between network and IT support is increasingly blurred, so IT capabilities are becoming increasingly relevant to the network environment.

AIOps platforms combine big data and AI technologies such as ML to analyse data across multiple data silos. Application, service, and network performance are monitored to find related triggers that indicate an issue is likely to occur. Based on the correlation of these triggers (including metrics, time series data, and events), root causes can be determined and resolved accordingly.

The role of AI in AIOps

The key role of AI in AIOps is to automate analysis of data at scale. As data sources and volumes increase, analysing data manually becomes challenging. Using AI technologies such as ML, models are trained using supervised, semi-supervised, and unsupervised learning to recognise patterns in multiple large datasets. Leveraging this capability, AIOps solutions can achieve the following:

- **Dynamic baselining of KPIs.** AI models can determine normal behavioural patterns of KPIs and automatically set adaptive thresholds based on current system performance. Deviations occurring outside of learned patterns are flagged as anomalies and further investigated to determine whether a likely failure is about to occur.

- **Predictive analytics.** Given AI's strong pattern recognition capabilities, models running within AIOps can be used to predict the likelihood of events such as application or network failures, enabling better assurance of customer and network services.

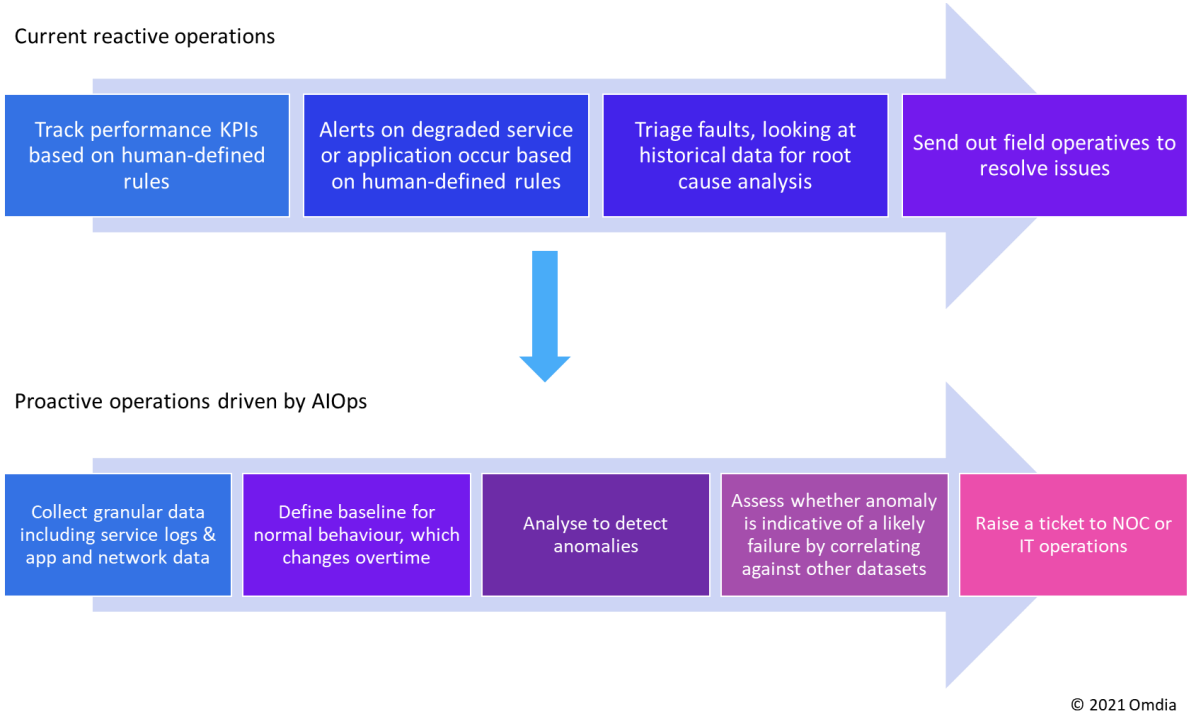
- **Multivariate analysis.** This involves the analysis and prediction of a single variable (dependent variable) based on the performance of multiple independent variables. Once a model is trained to determine the relationship between these variables and baselines are established, anomalies that occur are flagged to engineers to investigate and resolve. The correlation between variables can provide insights into probable root causes.

- **Recommend next best actions**. ML models can also be trained to recognise remedial actions to take based on previous actions taken to correct similar failures. These recommendations can either be activated through closed-loop automations or communicated to network and IT operations teams to implement.

Why AIOps is critical to CSPs

With AIOps, CSPs can achieve their ambitions to transition from current reactive to more effective and proactive ways of operating and managing network and IT. Instead of monitoring KPIs for degradation before troubleshooting a network failure, CSPs can use AIOps to help them spot issues before they begin to affect operations or customer experience and take preventive steps to correct or avert the failure. **Figure 1** summarises how AIOps delivers this change.

Figure 1: Moving to proactive operations using AIOps



Source: Omdia

AIOps is especially relevant in gaining deep visibility into the network, which is necessary to being more proactive. As network functions and IT systems become cloud native and disaggregated, their components (as microservices) increase in number and become smaller and shorter lived. Consequently, several unknown events and patterns may occur that can affect service quality, and failure to detect or resolve them quickly can affect customer experience, revenue, and costs.

Traditional monitoring tools are equipped to detect known events (including failure events). Therefore, CSPs need to analyse more-granular datasets to detect both known and unknown events. They also need to locate root causes amongst containers in multiple Kubernetes clusters and take preventive steps to resolve them before the failure affects customers and the business. This is where the concept of observability becomes critical.

Observability provides deep visibility into distributed system performance and ties this view to business performance metrics. This is achieved by collecting, correlating, and analysing metrics, events, logs, and traces. While monitoring tools track metrics, the ability to correlate these metrics and events with the more granular details from logs and traces (record the flow of events in software) will enable faster reporting and prevention of or recovery from failures. However, the sheer volume of these datasets demands that a more robust and scalable solution is implemented to analyse them. The fast compute capabilities of AI within AIOps makes it an ideal solution to achieving observability and managing these environments at scale.

Therefore, CSPs that do not adopt AIOps risk not achieving operational efficiencies and will continue to face challenges such as the following:

- **Declining productivity levels in the operations workforce.** With so many datasets and metrics to track, operators will not be effective at performing their tasks. Consequently, operations teams will not be able to get ahead of network incidents and outages.

- **High opex.** An inability to address network issues efficiently through automation or through preventive maintenance activities enabled by the predictive capabilities of AIOps will lead to increased operational costs.

- **Increased exposure to security threats.** With more software driving the functions of the network and, thanks to IoT, more devices running on the network, security has become a key concern. CSPs need to be resilient in securing their networks, because the scope, variety, and complexity of cyberattacks such as distributed denial-of-service (DDoS) attacks are increasing. Without AIOps to detect unknown or unexpected activities on the network or operating systems, the network is exposed to high security risks.

- **Slow and inefficient delivery of services.** With increased service offerings, CSPs must ensure that crucial IT systems such as order management do not fail. Without effective order management systems, the CSPs' ability to complete orders, deliver solutions, and capture revenue would be damaged.

- **Stifle operational change.** If AIOps is not adopted, siloed teams and operations will persist, making it difficult to implement the changes needed to achieve operational efficiencies.

AIOps use cases in telecoms

Use cases are evolving

AIOps use cases in telecoms spans several areas primarily focused on improving network and IT operations. These use cases cover business imperatives such as improving customer experience, operational efficiency, and secured operations.

Proactive customer support

This use case can be achieved by predicting the likelihood that a customer's service quality will decline and identifying the root cause. The implementation of this use case can prevent customer complaints and reduce churn. By analysing data such as call and packet data records (xDRs), customer trouble tickets, and application and performance data, CSPs can take proactive steps to ensure customer experience is not impaired.

Hong Kong Telecom is an example of a CSP that has implemented a POC where AI models are implemented when network-related trouble tickets are processed. Once a customer complaint is received, ML models are applied to discover other users likely to be affected by this failure. Customer care actions and network improvement activities for these users are then prioritised. This example reflects how AIOps accelerates problem identification, root cause analysis, and remediation. By highlighting other customers likely to be affected by similar faults, AIOps enables the CSP to deliver more proactive operations.

Network fault prediction and prevention

The remit of CSPs' network operations centres (NOCs) is extending beyond keeping the lights on in the network. Network faults have a direct impact on CSP revenue and costs, so the NOC activities also centre around reducing operating costs and revenue losses. Being able to detect a service-impairing network fault early and take preventive steps using AIOps will not only enhance NOC productivity levels but will reduce operational costs and improve service quality.

Smart Communications is one CSP that has used AIOps to predict and prevent faults in base station systems (BTS). The CSP trained ML models using data such as network logs, performance metrics, configuration parameters, alarms, and other events to recognise normal network behaviour and detect anomalies. Algorithms such as random forests and decision trees were used for this implementation. Following the training of the models, the CSP applied them to real-time data from the BTS and other data sources and was able to detect network failures in advance and trigger pre-emptive actions such as site visits to mitigate risks associated with the failures.

Anomaly detection of BSS performance

AIOps capabilities such as adaptive baselining and multivariate analysis can be applied to network and IT operations to prevent failures and accelerate resolution. A CSP based in South Africa with more than 120 million customers and 7,500 employees performed a POC to implement an AIOps solution to reduce MTTR. If employees were unable to connect to a customer service application,

this led to poor customer service delivery and customer experience. Such incidents were resolved using manual processes for incident detection and root cause analysis. This took time and increased the cost of operations. The CSP decided to implement an AIOps solution to reduce MTTR. The first iteration involved the use of system logs to train ML models to detect known and unidentified anomalies. Logs from multiple sources were analysed and correlated in a second iteration of the exercise. Once the fast compute capabilities of the AIOps solution were leveraged, resolve failures were reduced and MTTD fell by two hours.

Network and IT security

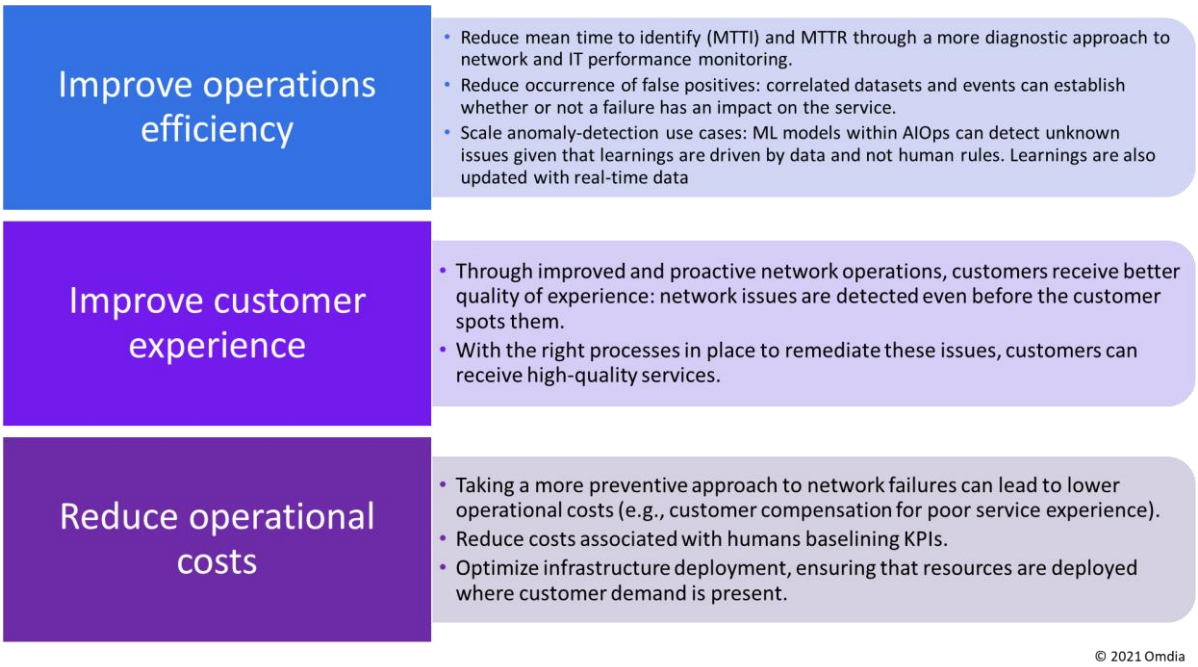
AIOps can be applied to IT and network security to protect the network against malicious attacks, especially those from DDoS. With its anomaly detection capabilities, early signs of traffic anomalies can be detected, root cause determined, and immediate action taken to shut down affected network nodes. This use case can avoid the potentially severe impact of such attacks and reduce costs associated with customer compensations and network repair.

A CSP based in North America leveraged AIOps to analyse the performance of 80,000 KPIs. An unknown DDoS service attack targeting its firewall and slowing down the network was detected. Using the multivariate analytics capabilities of AIOps, the root cause of the DDoS was detected four hours before the incumbent monitoring system detected the problem.

Benefits of AIOps to CSPs

Benefits of AIOps solutions span several areas including improved operational efficiency and improved customer experience as shown in **Figure 2**. Other benefits include enabling observability, delivering secure operations, and automating end-to-end network lifecycle management.

Figure 2: Benefits of AIOps



Source: Omdia

Recommendations

AIOps will play an important role in achieving CSPs' ambition to transform operations. There are, however, key challenges and best practices that CSPs should bear in mind to successfully implement and enjoy the benefits of AIOps.

Omdia's *OSS/BSS Evolution Survey – 2021* indicated that 42% of CSPs see limited access to data science skills as the biggest challenge they face regarding the use of AI. Other challenges include limited access to data, poor-quality data, a lack of compelling use cases, and scepticism around AI amongst employees. Partnering with vendors with expertise in developing and implementing AIOps solutions can address the issue with access to data science skills. Access to high-quality datasets will require strong data management and governance to establish specific guidelines on how data is collected and stored. CSPs can also address some of these challenges by engaging with industry standards organisations such as TM Forum. The forum's AIOps service management programme provides a platform for CSPs and vendors to explore AIOps use cases and develop industry standards and best practices to facilitate deployment of AIOps within the CSP environment.

AIOps solutions will need to fulfil key requirements. The top three, according to Omdia's recent OSS/BSS survey, are data collection, aggregation, and correlation; the ability to automate tasks across telco operations; and the use of open APIs and SDKs to extend the capabilities of the platform. The data collection, aggregation, and correlation capability is particularly critical given how distributed network functions and IT infrastructure are today. Being able to leverage intelligence from AI to automate operations highlights the need for processes to be restructured to embed insights from AI. Technology is only effective when it is used to transform processes.

Changing organisational culture and structure is the most crucial but the most challenging. Current processes, tools, and operational practices are siloed and focused on human effort to execute most functions. This needs to change to release the full potential of AIOps. Cross-functional teams within operations need to collaborate, particularly with respect to sharing disparate data, because this is critical to the functioning of AIOps solutions. Education is also important to emphasise the benefit that AIOps will bring in terms of increased productivity and the quality of services delivered to customers. Operational practices need to be restructured so that action is taken on recommendations provided by AIOps solutions. However, for this to occur, recommendations from AIOps solutions need to be stress tested to ensure that they align with operational policies.

Having C-level executives and departmental heads (especially within operations teams) champion AIOps-related projects and facilitate required organisational changes, such as breaking down silos and encouraging interactions between teams, will go a long way to ensure AIOps increases efficiencies in telco operations.

Appendix

Methodology

This report was produced in association with IBM. All analysis and conclusions have been independently produced by Omdia.

The information included in this report is based on primary research gathered through interviews, discussions, and inquiries with CSPs and IT vendors. Information in the report also includes survey insights from Omdia's *2021 ICT Enterprise Insights* survey, and *OSS/BSS Evolution Survey – 2021*. Secondary research from publicly available content and announced contracts, partnerships, and previously published research including Omdia's reports on AI and network automation were also used in the development of this report.

Further Reading

IBM, "Achieve zero-touch network operations," ibm.com/cloud/cloud-pak-for-network-automation

Author

Adaora Okeleke
Principal Analyst, Service Provider Ops and IT
customersuccess@omdia.com

Roy Illsley
Chief Analyst, IT Ecosystem and Ops
customersuccess@omdia.com

Get in touch

www.omdia.com
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 Tech, 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.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.