ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 13, Issue 2, pp: (5-7), Month: April - June 2025, Available at: www.researchpublish.com

AI-DRIVEN NETWORK MONITORING: MARKETING HYPE VS. OPERATIONAL REALITY

Marek Zidek

Affiliation: Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.15669580

Published Date: 15-March-2025

Abstract: **This article aims to compare the marketing promises of AI-driven network monitoring (AIOps) with its operational reality. While AI provides benefits like noise reduction and behavioral analysis, it requires ongoing tuning, customization, and human oversight, far from the plug-and-play solutions often advertised.**

Keyword: **network monitoring, AI, artificial intelligence, IT, internet, network, AIOps.**

I. INTRODUCTION

Artificial Intelligence (AI) is redefining the landscape of enterprise IT operations—and nowhere is the impact more hyped than in the field of network monitoring. Marketing brochures from vendors promise a paradigm shift: networks that predict outages before they occur, autonomously diagnose issues, and even self-heal without human intervention. “Let AI run your network,” they claim.

However, as many network engineers, operators and architects are discovering, the real-world implementation of AI-driven network monitoring is more complex. This article examines the differences between vendor expectations and actual operational experiences, offering a grounded perspective on what AI can and cannot deliver in modern network environments.

II. THE VISION: A SELF-DRIVING NETWORK

At a high level, AI-powered network monitoring is built around several core capabilities, often marketed as pillars of the “self-driving network”:

Predictive Analytics: Identify network anomalies and impending failures before they cause disruption.

Real-Time Anomaly Detection: Continuously scan telemetry data for deviations from established behavioural baselines.

Automated Root Cause Analysis (RCA): Correlate events across layers and domains to isolate the root of a problem.

Self-Healing Mechanisms: Automatically trigger remediation workflows based on identified issues.

Scale and Flexibility: Process millions of data points per second across hybrid, multi-cloud infrastructures.

These claims are compelling, especially for enterprises managing complex and hybrid networks. The pitch is simple: reduce operational workload, minimize downtime, and gain actionable intelligence, all without increasing headcount.

III. THE REALITY: PROMISING, BUT NOT PLUG-AND-PLAY

Data Quality Remains the Achilles' Heel

Marketing promise: “AI learns from your data and delivers insights immediately.”

Reality: AI is only as smart as the data you feed it.

Network telemetry is often inconsistent, redundant, or incomplete. Many enterprises lack a unified observability strategy, leading to fragmented datasets. This fragmentation inhibits effective machine learning, which depends on normalized, context-rich input.

Contextual Awareness Is Limited

Marketing promise: “AI understands your environment.”

Reality: AI lacks domain-specific context unless you provide it manually.

Effective correlation and RCA depend on understanding the topology, service relationships, and business impact of infrastructure elements.

Root Cause Analysis Is Probabilistic, Not Deterministic

Marketing promise: “AI isolates root causes instantly.”

Reality: RCA often delivers “most likely” causes that require human validation.

AI models lack context about the specific enterprise environment, which varies across networks, infrastructures, configurations, and operational practices. Root cause in one environment might be a false positive in another. As a result, RCA systems must be adapted and refined by human.

Closed-Loop Automation Is Rare

Marketing promise: “Networks heal themselves.”

Reality: Most organizations don't trust automation to act autonomously.

Even when closed-loop automation is technically implemented, it is usually deployed in a “human-supervised” model, where a human operator typically approves and monitors the actions. This cautious approach reflects the high stakes involved in enterprise environments, where uptime and service reliability are critical. In practice, full closed-loop automation is limited to non-essential services that have no impact on core enterprise infrastructure.

Training, Tuning, and Governance Are Ongoing Tasks

Marketing promise: “Intelligent monitoring out of the box.”

Reality: AI needs customization, tuning, and governance.

AIOps systems are promoted as plug-and-play and should be ready to deliver insights immediately after deployment with minimal customizations. However, enterprises quickly realize that this is not the case. AI-driven monitoring platforms typically require training, tuning, and adaptation to understand the specific characteristics of their environment. Existing alerting thresholds, correlation rules, and business logic don’t automatically carry over. Instead, teams must invest time to rebuild context, fine-tune models, and define new logic aligned with operational goals.

IV. WHAT AIOPS MONITORING DOES DELIVER WELL

Despite the operational limitations, it does offer several high-value capabilities that provide measurable operational benefits. When properly implemented and tuned, AIOps platforms can significantly enhance visibility, reduce manual workload, and support decision-making.

AIOps Key strengths:

Alert Noise Reduction: AI excels at correlating related events and suppressing false positives using simple logic. It helps with initial noise reduction and enables IT teams to fine-tune and customize more complex rules.

Trend Analysis and Capacity Planning: By continuously analysing historical and real-time data, AIOps tools help identify usage trends, forecast capacity needs, and support long-term infrastructure planning with data-driven insights.

Behavioural Baselines: AI establishes normal operating patterns for systems and services, allowing it to detect subtle anomalies that would be difficult to identify with static thresholds alone.

Multi-Domain Visibility: AIOps platforms integrate data across infrastructure, applications, and networks, providing a unified view that breaks down operational silos and improves cross-domain troubleshooting.

V. CONCLUSION

AI-driven network monitoring (AIOps) is a significant transformation of the operational monitoring, but it is not a miracle. The path from data collection to actionable insights is complex, requiring effort, continuous customizations, and organizational alignment. Enterprises must invest in configuring, training, and tuning AI systems to reflect the realities of their unique environments. Success depends not just on the technology, but on the people and processes that support it. Patience, governance, and domain expertise are essential to move from noise to clarity, from detection to effective action. Organizations promote AI as a strategic tool that enhances human decision-making and helps unlock the full potential of AI technologies. With the right approach, AI can drive tangible improvements in network resilience, operational efficiency, and service quality, enabling IT teams to shift from reactive to proactive monitoring.

REFERENCES

[1] https://www.ibm.com/cloud/watson-aiops.

[2] https://www.gartner.com/