LiveAction

REPORT

Network Performance Monitoring Trends Report 2024

Executive Summary

For just about as long as there have been computer networks, there has been a need to monitor those networks and their performance. It's a must-have practice for IT and networking professionals. Without network performance monitoring, teams can't effectively optimize their networking environments for speed, availability, security, and other critical environments. That fundamental truth never seems to change.

What has changed is the network itself. The traditional corporate perimeter has evolved considerably to include far more distributed networking architectures — including cloud, hybrid cloud, and edge computing environments — plus a much more diverse set of devices, applications, and data connecting to and traveling over those networks.

As the complexity of modern networks expands, so too does the challenge of managing and monitoring them. The landscape of risks and threats has become more sophisticated and varied, outpacing the capabilities of legacy tools and manual processes that many organizations still rely on. These outdated legacy systems are not capable of supporting the agility and structure of modern network environments, elevating the risk of issues related to availability, performance, and security. Moreover, this reliance on antiquated methods can inflate costs and consume IT personnel with monotonous manual tasks, diverting valuable resources away from more strategic initiatives.

The good news: There is a sea change underway in how organizations manage their networks. Emerging innovations and capabilities that embrace AI, automation, and tighter integration with security solutions are enabling a shift from traditional network monitoring to network *intelligence*.

LiveAction partnered with 1105 Media to survey nearly 250 professionals — the majority (77%) of whom are actively involved in managing their company's networks — about current trends in networking monitoring and observability. Most of them said they see that shift already happening today or that they expect it to happen in the next 1-3 years.

In this eBook, we'll examine what that trend mean — and many other current trends in network performance monitoring.

What Is Network Performance Monitoring?

Understanding current trends, tools, and practices in network performance monitoring first requires defining the term itself.

Essentially, network performance monitoring (NPM) is about visibility. The ability to see and monitor *everything* on an organization's network — no matter how that network is architected or where it resides — to optimize performance while minimizing risks such as downtime or security breaches. That means you need the ability to see and monitor every IT asset on the network — every device, dataset, application, and more.

Network administrators and other IT pros use a mix of tools and best practices to keep tabs on networking performance and proactively identify and troubleshoot potential problems, wherever and whenever they may occur.

The essential goals of NPM include: accelerating the time to resolution (or repair) when issues do occur; bolstering network and application security; minimizing expensive outages and downtime; and generally ensuring the speed and availability of network resources to help achieve business goals.

4 Key Challenges IT Teams Face With NPM Today

The need for observability and monitoring is as great as ever, but so are the challenges today's networks pose for IT teams. Let's take a closer look at four common issues organizations face in terms of maximizing network performance while minimizing risks.

01 Networks have grown more diverse, distributed, and complex — especially during the last several years.

It's no longer simply a matter of monitoring and securing the traditional corporate network. Companies now commonly manage cloud footprints, hybrid cloud architectures, software-defined/WAN networks, edge computing environments, and more.

We see this reflected in our 2024 Network Performance Monitoring/Observability Trends survey, in which respondents were asked about the types of networking environments they managed and could select all that applied:

74%

of respondents said they manage on-premises networks, such as data centers, branch offices, and local-area networks (LANs).

61%

said they are running hybrid architectures that span on-premises environments with public and/or private cloud infrastructure.

70%

said they manage cloud environments, such as AWS or Azure.

43%

are managing WAN or SD-WAN networks.

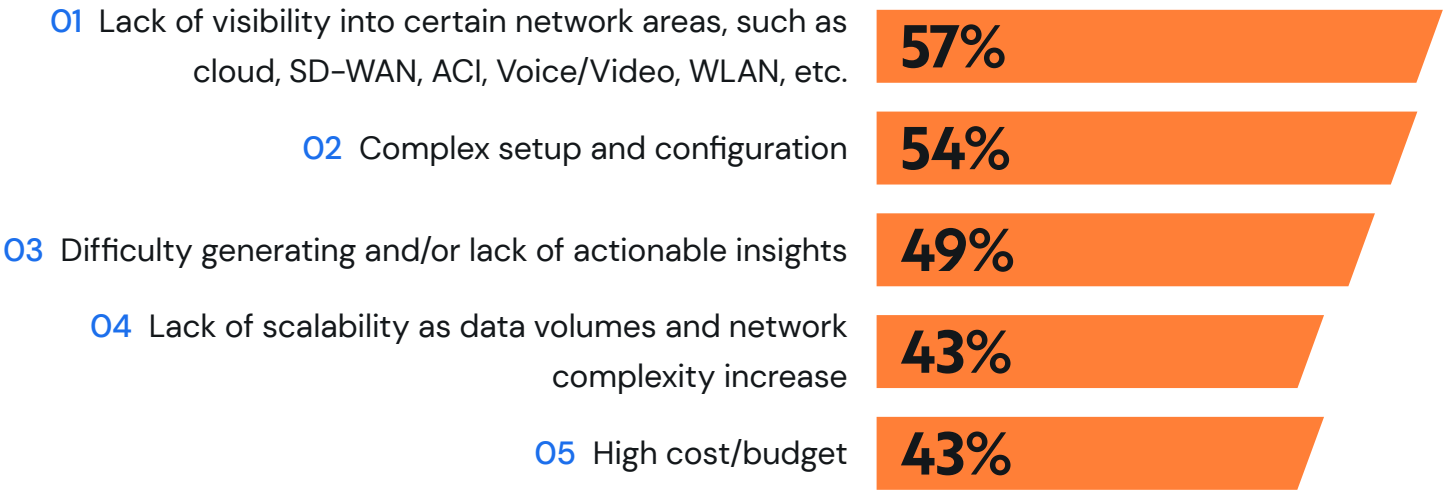
The high percentages reflect the reality that many teams are monitoring and managing multiple types of networks, a significant shift from the days of traditional, homogeneous corporate networks.

02 Networking teams are often still highly reliant on manual processes and repetitive effort.

These processes, and the tools that support them, have yet to embrace and integrate AI capabilities — along with a broader class of IT automation — to reduce operational overhead and complexity while improving performance.

03 Legacy NPM tools are not keeping up with the times.

As networks have grown more complex, some tools aren't innovating fast enough. This leads to a variety of issues for networking teams, including a patchwork of disparate tools — often four or five separate tools just for NPM tasks. Survey respondents indicated the five top challenges caused by their current NPM tools included:



Just one in three survey respondents reported being "very satisfied" with their current NPM tools, while a combined 63% said they were "somewhat satisfied" or "neutral," showing plenty of room for improvement.

04 The risks to network performance and security continue to grow more complex.

Security threats are constantly evolving, complex data and application architectures put new strains on performance, and increasing volumes of data pose additional problems when not adequately accounted for.

A specific challenge on this front is that many organizations continue to treat NPM and network security as distinct, siloed requirements — stretching resources and increasing operational complexity in the process. While 57 percent of respondents have integrated security with NPM, 30 percent are only considering it, and another 13 percent simply said "no."

6 Best Practices for Modern Network Performance Monitoring

Fortunately, the challenges can be readily mitigated with the right mix of best practices and technical capabilities. These include a mix of current and emerging capabilities that bridge the gap between traditional NPM strategies and the network intelligence approach.

Here are six key areas to prioritize:

01 Real-time monitoring

Some monitoring solutions are "near-time," in that they don't actually reveal the network's current state, only provide a historical view, or focus on synthetic transactions. Real-time monitoring is crucial in today's dynamic, rapidly changing environments.

78%

of survey respondents listed real-time monitoring and alerting as one of their top NPM priorities.

02 360-degree discovery and observability

It's not enough to acquire visibility and monitoring capabilities for some of your network. Optimal performance and risk management requires full visibility of the entire network and everything on it, whether on-premises, in a cloud, or across areas such as SD-WAN, ACI, Voice/Video, WLAN, and so forth. While networks are commonly thought of as infrastructure, it's also crucial to remember the applications that run on that network.

44%

of respondents said application performance monitoring was one of their top NPM priorities.

03 Automation & orchestration

The days of being able to effectively monitor and manage network performance manually are long gone. Network operations teams need to complement their natural abilities with superpowers, leveraging greater automation and orchestration of their NPM efforts.

57%

of respondents said automation and orchestration are important to their NPM strategies over the next 1-3 years.

04 Packet *and* flow analysis

Some network monitoring tools take an either/or approach to two popular network monitoring techniques, flow analysis and packet analysis. They both have benefits and challenges — and the best solutions incorporate both techniques in a complementary fashion, rather than picking one or the other. Get a detailed **breakdown of both approaches here**.

34%

of respondents listed the aggregation of multiple data sources (i.e. SNMP, FLOW, API, Packets, etc.) into a unified user interface as a top priority for their NPM solution.

05 Integration & interoperability with security solutions

Mitigating the complexity of today's networks and the security threat landscape requires a unified approach that brings data, insights, and intelligence into a single platform that includes robust capabilities for zero trust, identity management, and enforcement, and other security requirements.

87%

of respondents said it was either very important or important to them that their NPM solution was interoperable with their other network management and security tools.

06 AI and machine learning

The path to network intelligence is brightly lit by emerging **AI-based capabilities in network monitoring**. This is enabling a more automated approach to discovery and monitoring, as well as predictive insights and automated next-best-actions that reduce the manual toil required of network admins.

71%

of respondents said AI and machine learning will have the biggest impact on NPM over the next 1-3 years, by far the most popular answer.

The Future of NPM: Network Intelligence

It's an exciting time in network monitoring. The challenges have never been greater — but neither have the solutions. Emerging capabilities in AI, automation, interoperability, and data are enabling forward-thinking organizations to grow from their network monitoring roots into network intelligence.

This represents an evolution from network monitoring's reactive past to network intelligence's proactive future, one that is more predictive, more automated, higher performing, and more secure.

The overwhelming majority (84%) of professionals who responded to our NPM trends survey said the shift to network intelligence is either already underway or will happen within the next three years.

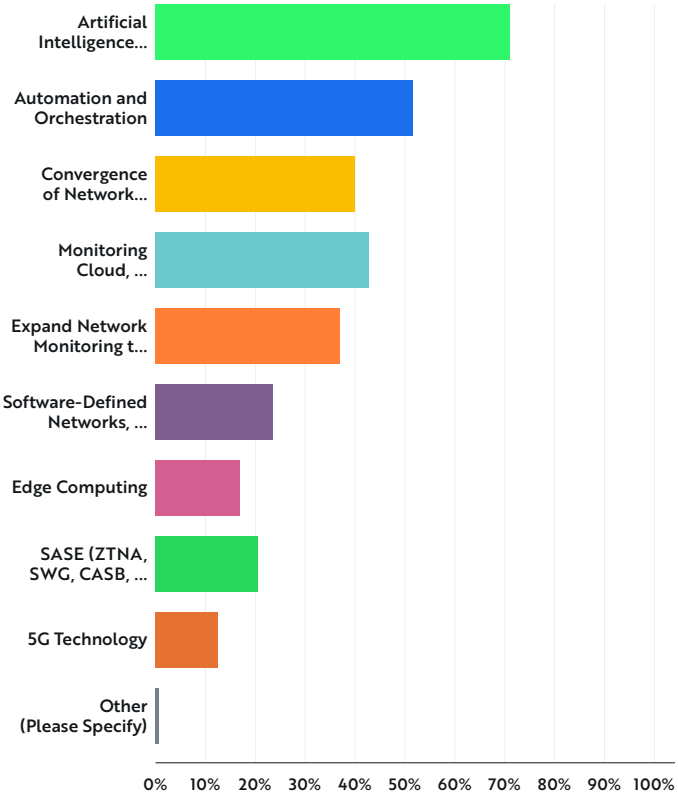
That's because this overarching trend aggregates the best of all worlds and capabilities in terms of network performance and security. Better still, it enhances the talent and abilities of IT teams while keeping costs in check as network complexity and data volumes continue to scale upwards.

Network monitoring is the minimum table stakes. Network intelligence is the path forward to smarter, faster, more secure networks. LiveAction can help.

Q14

What will have the biggest impact on network monitoring in the future?

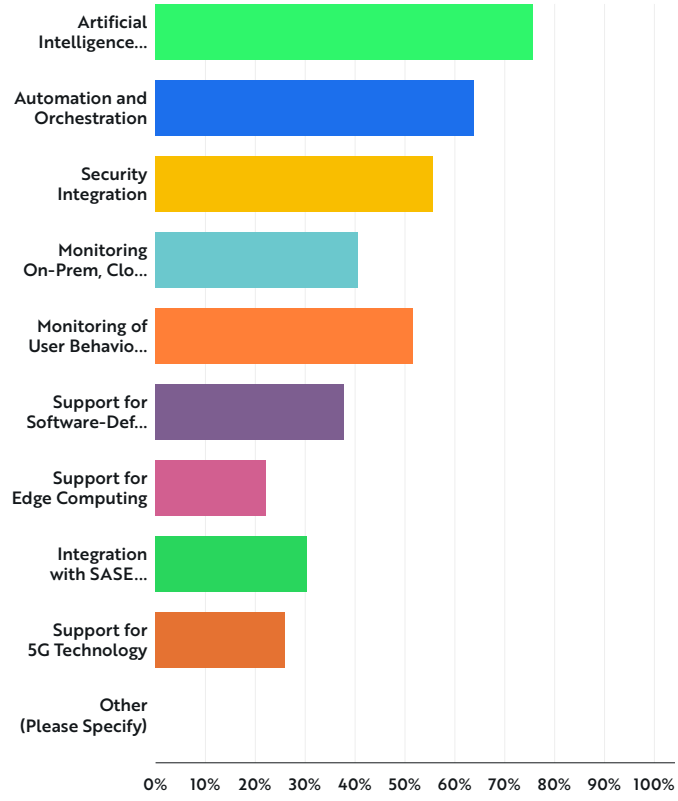
Answered: 135 Skipped: 113



Q15

What do you believe will be the key features of a network intelligence solution in 1–3 years?

Answered: 108 Skipped: 140



How LiveAction Can Help

LiveAction is at the forefront of the evolution from network performance monitoring to advanced network intelligence — delivering best-in-class solutions to maximize the potential of your network's performance while safeguarding your business from risks.

LiveAction equips IT administrators with deep, actionable intelligence for superior decision-making and significantly streamlines operational costs. By integrating and enhancing the analysis of network, application, and user data, LiveAction enables network professionals to proactively address, diagnose, and rectify challenges within increasingly sophisticated networks.

LiveAction continues to embrace and embed AI throughout its portfolio — from discovery to monitoring to security and more — to empower organizations on their journey to network intelligence.

Your network should never be a weakness. LiveAction helps make it one of your company's strengths.

Delivering Demonstrable Economic and Operational Impact

ROI

153%

Reduction in MTTR

50%

Payback

12 months

Learn More

Traditional network monitoring is no longer enough to maximize the potential of your valuable IT resources while protecting your business in the process.

It's time for network intelligence. Learn how LiveAction can help at https://www.liveaction.com/solutions/network-performance/.

LiveAction

901 Campisi Way, Suite 222
Campbell, CA 95008
(888) 881-1116

LiveAction provides end-to-end visibility for network security and performance. By relying on a single source of truth – the packets – LiveAction gives modern enterprises the confidence needed to ensure the network is securely meeting business objectives, providing full network visibility to better inform NetOps and SecOps, and reducing the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks.

To learn more about LiveAction, visit www.liveaction.com