

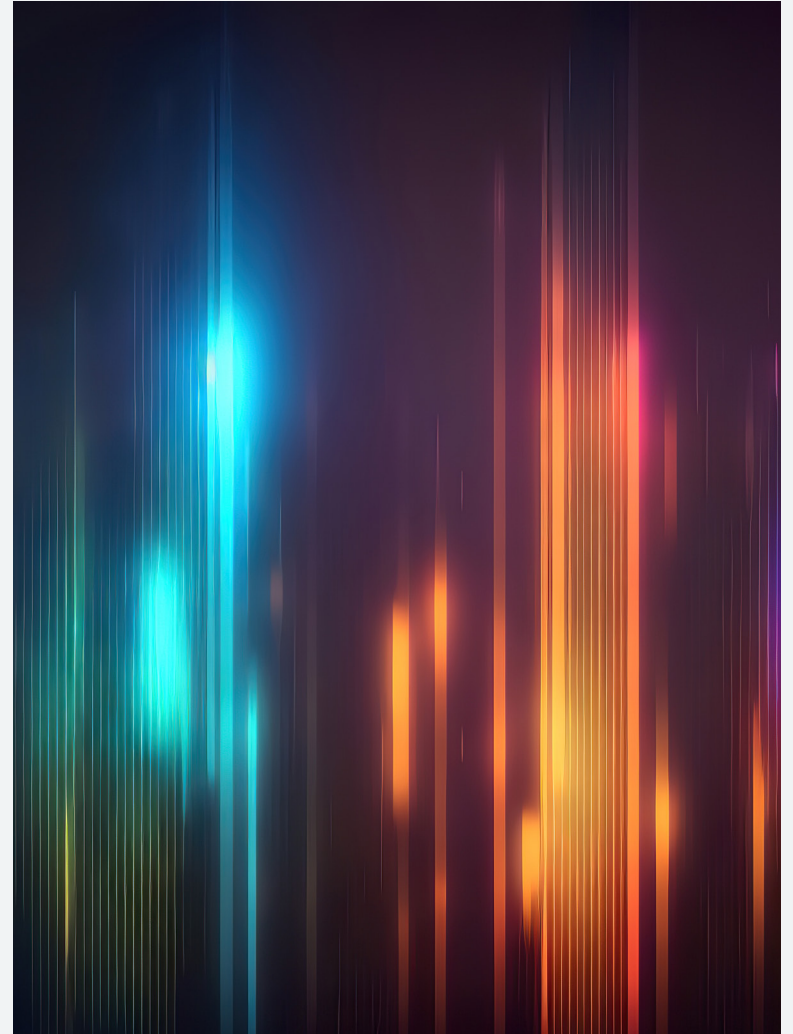
# Five Must-Haves for AI in Networking Operations

A handy guide for determining if a networking solution can deliver on the promise of AI.



# Contents

- 01** Why AI for network operations?
- 02** Must-have #1: Unified visibility and management
- 03** Must-have #2: High-quality, relevant data
- 04** Must-have #3: Accurate, actionable insights
- 05** Must-have #4: A scalable, cloud-based infrastructure
- 06** Must-have #5: Secure, trustworthy AI
- 07** Conclusion



# Why AI for networking?

Today's IT teams are under increasing pressure to deliver exceptional networking experiences with limited resources and multiple management tools that can't keep up with rising complexity, security concerns, and end user demands.

It probably comes as no surprise that AI is the answer.

AI for network operations refers to the subset of AI for IT operations (AIOps) specifically applied to networking. Leveraging AI and machine learning (ML) technologies to enhance network management allows organizations to transform operations and drive business growth. By applying intelligent algorithms to vast amounts of network data, enterprises can:

- Automate routine tasks
- Proactively detect anomalies
- Speed time to remediation
- Optimize performance in real time
- Proactively respond to threats
- Free time for more strategic initiatives

Streamline networking operations and optimize user experiences from client to cloud.

**Explore Juniper AIOps →**

Hold on though. As revolutionary as AI has been for network operations, the reality is that not all AI is created equal. Unfortunately, many vendors claim AI capabilities that are either superficial bolt-ons or simply fail to deliver meaningful outcomes. It turns out there's a vast difference between an AI-enhanced solution and a true, mature AI-native solution built from the ground up to leverage AI as a core capability.

So, how can you tell the difference? This guide lays out the five non-negotiables an AI for network ops solution must have in order to solve real-world challenges and deliver exceptional end user experiences.



# Key takeaways

In a recent survey by theCUBE Research and ZK Research<sup>1</sup>, respondents were asked to list the primary benefits of leveraging AIOps in their network operations. The top three responses are detailed here.



---

## 33%

### Increased operational efficiency

AI helps organizations free up network admins and architects to work on more strategic initiatives that drive business value.

---

## 31%

### Faster time to remediate issues

Automation ensures that AI insights are acted upon consistently and rapidly, minimizing downtime and improving reliability.

---

## 28%

### Faster time to identify issues

AI brings the intelligence to analyze vast streams of real-time data, identify patterns, and predict issues before they impact performance.

---

## 02 Must-have #1

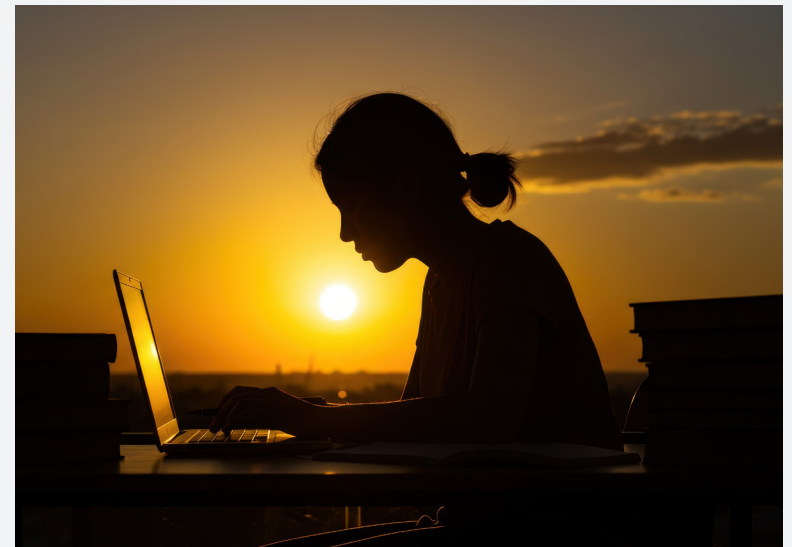
# Unified visibility and management across network domains

**Unified, end-to-end visibility is essential for AI in networking because it provides a comprehensive view of the entire network infrastructure.**

Without it, each domain—campus, branch, data center, WAN, cloud, and edge—tends to be siloed and managed in isolation, making it difficult to detect cross-domain issues or coordinate troubleshooting efforts. **A unified platform approach** brings these pieces together, offering real-time insights into how network components interact so that IT teams can quickly pinpoint and resolve performance or connectivity problems.

Removing silos greatly improves operational efficiency. Instead of switching between tools and interfaces for each network segment, IT teams can monitor, configure, and troubleshoot from a single dashboard. This reduces complexity, accelerates decision making, and frees up valuable time and resources. And by integrating AI across every layer of the network, organizations can achieve significant reductions in networking-related trouble tickets, faster threat detection, and time to incident resolution. Improved performance and better end user and operator experiences are direct results.

This level of visibility also enables consistent policy enforcement across all domains. Security policies, access controls, and quality-of-service settings can be centrally defined and uniformly applied, reducing the chances of misconfiguration and ensuring that users have a consistent experience no matter where or how they connect. With centralized management, organizations can also better maintain compliance with internal policies and external regulations, while minimizing the risks introduced by fragmented operations.



In a recent survey from theCUBE Research and ZK Research, **42%** of respondents said **lacking a single AI engine** was their biggest challenge in deploying AIOps in the enterprise<sup>2</sup>.

## 03 Must-have #2

# Vast amounts of complete, accurate, timely, and context-rich data

**Quality data—and lots of it—is the foundation of effective AI in networking operations because AI systems rely on large volumes of accurate, timely, and relevant data to make informed decisions.**

This collected data includes traffic patterns, device performance metrics, network usage statistics, application insights, security logs, real-time wireless user states, and streaming telemetry from routers, switches, and firewalls. Understanding what data is important is also critical, something that takes time and expertise.



As they say, garbage in, garbage out. The wrong data—as well as inconsistent, incomplete, or delayed data—can cause AI models to draw incorrect conclusions, leading to false positives (that waste IT's time), false negatives (resulting in missed issues), and too many alerts (alarm fatigue). The right clean, structured data ensures that AI can recognize patterns, detect anomalies, and produce reliable insights.

Accurate data is especially critical for troubleshooting and root cause analysis. AI platforms are designed to correlate information from across the network stack to determine where a problem originated and root cause. If the underlying data is flawed or lacks necessary context, the system may misidentify symptoms as root causes or fail to detect issues altogether. High-quality data allows AI to zero in on problems faster and with greater confidence, significantly reducing mean time to resolution (MTTR) and improving service reliability.

Quality data also supports the safe and effective automation of network operations. AI-native automation depends on trusted inputs to trigger actions such as rerouting traffic, reconfiguring devices, or isolating unauthorized endpoints. If the data feeding the AI is noisy or inaccurate, automation can lead to unintended consequences, such as service disruptions or security gaps.

Lastly, quality data is essential for ongoing learning and model refinement. AI systems improve over time by continuously retraining on fresh data that reflects real-world conditions. Poor-quality data can slow or distort this learning process, limiting the system's effectiveness as the network evolves. With high-quality, well-labeled data, AI models stay current, adaptive, and better equipped to handle the growing demands of modern, multi-domain networks.

## Garbage in = garbage out

The effectiveness of any AI algorithm is directly proportional to the quality of the data it is fed.

## 04 Must-have #3

# Accurate, actionable insights delivered in real time

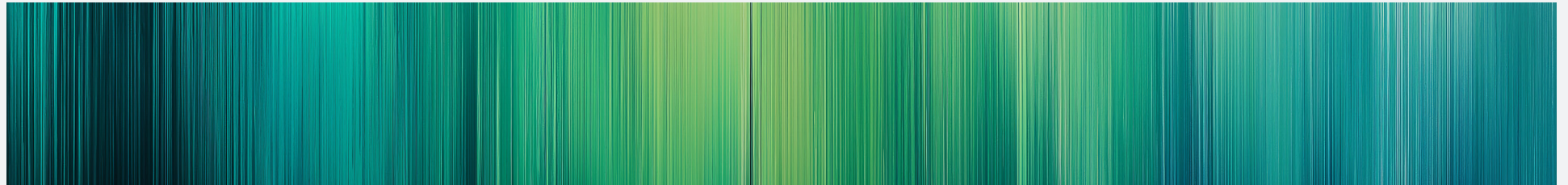
**Actionable insights are critical for AI in networking because they translate complex data analysis into clear, specific recommendations that drive tangible outcomes.**

AI systems in networking environments process enormous volumes of telemetry, logs, and behavioral data. This data only becomes valuable when it leads to a clear understanding of what's happening and what needs to be done about it. Actionable insights enable IT teams to move from passive monitoring to proactive operations, reducing guesswork and enabling faster, smarter decision making.

One of the primary benefits of actionable insights is their ability to drastically reduce MTTR. Instead of requiring engineers to sift through logs or dashboards to identify the root cause of a problem, AI can help pinpoint the issue and suggest the exact next step—whether that's adjusting an antenna, changing a faulty cable, repositioning an access point (AP), or checking DHCP servers that are not responding. In addition, AI assistants enable asking questions in natural language via a conversational interface. This process streamlines troubleshooting, minimizes downtime, and ensures a consistent user experience across applications and services.

Actionable insights are also essential for driving effective automation. AI-native recommendations can be programmed to trigger automated workflows that fix issues in real time without manual intervention, such as rebooting a malfunctioning device, reconfiguring a misconfigured port, or automate channel selection on an AP. This not only improves performance and reliability but also reduces the burden on IT staff, enabling them to focus on more strategic tasks rather than constant firefighting.

In addition, actionable insights contribute to long-term optimization and strategic planning. By analyzing trends in network usage, performance degradation, or security events, AI can recommend infrastructure enhancements (e.g. new cable) or architectural adjustments (e.g. add an AP to a coverage hole). These insights help organizations stay ahead of growing demands, evolving threats, and shifting user behaviors. In essence, actionable insights are the link between raw data and effective, intelligent network management.



# 48%

**Respondents who prefer AI-powered network management that both determines and executes automated actions for problem remediation and optimization<sup>3</sup>**

## 05 Must-have #4

# A scalable, cloud-based infrastructure

**Scalability is crucial for AI in networking because it ensures the AI systems can handle increasing data volumes, user demands, and network complexity without performance degradation.**

Modern networks generate massive amounts of telemetry and behavioral data. As these networks grow, AI systems must process more and more data in real time. The volume of data being processed, and the speed at which it needs to be processed, necessitates that AIOps systems have the power of a scalable and elastic cloud-based infrastructure. The cloud provides the infrastructure needed to ingest, store, and analyze this data efficiently, enabling timely and accurate insights.

Scalability also supports real-time decision-making, which is essential for tasks like anomaly detection, traffic optimization, and automated threat response. As more users and devices connect to the network, AI models must adapt quickly to changing traffic patterns and usage behaviors. A scalable, AI-native infrastructure—built with flexible compute, storage, and network resources—ensures that performance remains consistent even during peak demand or in large, distributed environments. This allows the AI to continue making fast, intelligent decisions that keep the network stable and responsive.



As enterprises adopt more complex, hybrid architectures, AI must work across all domains to provide unified visibility and coordination. A rigid or siloed architecture limits the AI's ability to correlate data and automate actions across these environments. Scalability enables centralized control while supporting the distributed nature of modern IT environments, ensuring that AI can operate effectively at any scale.

Finally, scalability ensures that AI systems can grow and evolve along with the organization's needs. As new services are added, user populations expand, or new threats emerge, AI systems must continuously learn and adapt. Scalable architectures support the ongoing training, deployment, and refinement of machine learning models, helping maintain accuracy and relevance over time. In this way, a scalable foundation not only supports current AI use cases but also future-proofs the network by enabling continuous innovation and operational agility.

**Having a cloud-based management solution ensures rapid innovation and scale, in addition to relieving operations teams of the burden of lifecycle management, security patches, and bug fixes<sup>4</sup>.**

## 06 Must-have #5

# Secure, trustworthy AI

**Security is critically important for AI in networking because AI systems have deep access to network data and often control sensitive operational functions.**

These systems monitor traffic patterns, user behavior, and application performance, and may have the authority to automatically adjust network settings or isolate devices. Ensuring that AI systems are secure protects the integrity and confidentiality of both the data they process and the actions they perform.

The reliability of AI-driven insights depends on data that is genuine, aligned, and unaltered. That means using only data that is required for an AI task, encrypting data in transit and at rest, validating data sources, applying stringent data privacy controls, adhering to security compliance standards, and following ethical governance policies. Proper AI encryption and isolation measures inherently support data integrity by preventing unauthorized access and manipulation. Secure, untampered data ensures the accuracy of AI insights, leading to more reliable network performance and fewer disruptions.

Finally, maintaining a secure AI infrastructure builds trust, accountability, and compliance. As organizations increasingly rely on AI to manage core networking functions, stakeholders must have confidence that the system is reliable and behaves predictably. Detailed auditing, explainability (XAI), and secure design principles help demonstrate that AI decisions are safe, lawful, and traceable. In this way, security not only protects the technology but also supports broader business goals and regulatory requirements.



**“Protecting data is not just about preventing unauthorized access. It also involves ensuring data integrity and availability.”**

Enamul Haque , AI Horizons: Shaping a Better Future Through Responsible Innovation and Human Collaboration

## 07 Conclusion

# AI for networking is only as valuable as the outcomes it delivers

**Mist™, Juniper's AI-native networking platform, was purpose-built from the ground up to deliver AI that transforms network operations.**

Powered by the Marvis® AI engine, Mist leverages the right data and the right infrastructure to deliver the right responses when and where they're needed, all protected by the right security. The 100% open API platform enables unified management of all hardware and software across all network domains, including purpose-built Juniper APs, routers, switches, and firewalls.

The platform offers unmatched visibility into network health, automated event correlation, root cause identification, and proactive anomaly detection, which significantly reduces troubleshooting time and frees IT teams for more strategic initiatives.

Using quality data collected over 10 years via rich, relevant, real-time telemetry, Mist analyzes and optimizes operations across the network in real time, providing actionable insights down to the level of individual users and sessions.

Mist provides smarter recommendations, faster issue identification, and automated resolutions through continuously improving AI models that are trained on anomaly detection, unique service levels, and event correlation. Leveraging the industry's only virtual network assistant, operators can more quickly determine and resolve root cause, whether it's wireless, WAN, an application, or a security breach.

Juniper helps customers stay ahead of the evolving threat landscape with easy-to-automate Zero Trust at scale via a unified management Mist dashboard, common Junos OS, and single policy framework. By consolidating security, networking, and AIOps under a single UI, routers, switches, firewalls, and full network access control (NAC) work together to coordinate effective threat protection and consistent policy enforcement across all domains—for all users—regardless of location.



# 97%

**Organizations who state that they are open to evaluating new network vendors if they have superior AIOps technology<sup>5</sup>**

# Next steps

As IT continues to become a growth enabler, the network's importance in enabling that growth is becoming more critical. That's why Juniper is making it easier than ever for you to transform your network operations with AI.



## Discover the Mist platform

Purpose built to deliver industry-leading AI for networking, Mist simplifies operations and empowers smarter decisions.

[See what's possible →](#)



## See a demo

Learn how the Mist platform elevates user and operator experiences from average to exceptional.

[Register now →](#)



## Begin your journey

Juniper's Blueprint for AI-Native Acceleration is designed to simplify and streamline your adoption of AI in networking.

[Start today →](#)



## Get a free AP

Try the Mist platform with a complimentary Juniper access point (AP) and 90-day Juniper Wi-Fi Assurance subscription trial.

[Get yours now →](#)

## Why Juniper

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Mist™, Juniper's AI-native networking platform, is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Additional information can be found at [juniper.net](https://juniper.net) or connect with Juniper on [X](#) (formerly Twitter), [LinkedIn](#), and [Facebook](#).

## More information

To learn more about Juniper AIOps, contact your Juniper representative or partner, or visit <https://www.juniper.net/us/en/solutions/artificial-intelligence-for-it-operations-aiops.html>

## Notes and references

- 01 Technology Spending Intentions Survey (TSIS), ETR, April 2024. <https://etr.ai/tsis>
- 02 Ibid.
- 03 Worldwide AI in Networking Special Report, IDC, 2024.
- 04 AI-Native Requirements for Modern Networks, Enterprise Strategy Group, January 2024.
- 05 Technology Spending Intentions Survey (TSIS), ETR, April 2024. <https://etr.ai/tsis>



[juniper.net](https://juniper.net)

© Copyright Juniper Networks Inc. 2025.  
All rights reserved.

Juniper Networks Inc.  
1133 Innovation Way  
Sunnyvale, CA 94089

7400209-002-EN June 2025

Juniper Networks Inc., the Juniper Networks logo, juniper.net, Marvis, and Mist AI are registered trademarks of Juniper Networks Incorporated, registered in the U.S. and many regions worldwide. Other product or service names may be trademarks of Juniper Networks or other companies. This document is current as of the initial date of publication and may be changed by Juniper Networks at any time. Not all offerings are available in every country in which Juniper Networks operates.