Omdia
by informa techtarget

JUNE 2026

Accelerating Action: The Need for Speed in Network Incident Response

Jim Frey, Principal Analyst, Enterprise Networking

Introduction: When tomorrow is not good enough

Enterprises understand their networks are critical infrastructure. Networks aren't just a skeletal framework for organizational operations but rather the lifeline carrying business-critical data and applications to employees, customers, and partners. Such heavy reliance on networks creates intense pressure to ensure their continuous performance and resilience and do everything possible to reduce the time needed to recognize and correct any degradation or loss of function. Not only does subpar network performance impair business activity, but it can also lead to outages and interruptions, which have direct, tangible financial impact. Several factors shape this challenge:

- **The complexity crisis.** Accelerated digital transformation, multicloud environments, and hybrid workforces have led to steady increases in network complexity. Omdia research indicates that 79% of organizations feel their networks have become significantly more complex over the past two years.[1] This makes finding and solving network performance issues more difficult.
- **Operational bottlenecks.** While 93% of enterprises agree that automating networks will be essential for keeping pace with future change,[2] organizations often remain more reactive than proactive. Continued reliance on manual maintenance of complex, legacy infrastructure is a sub-optimal use of engineering talent, time, and money.
- **Strategic growth.** Network teams are already stretched thin in most organizations and are left with little time to look ahead for planning and proactive, preventative maintenance. Most are just trying to keep the lights on, rather than playing to strategic roles needed to keep important projects, like AI, on track and on target. The transition toward applying automated workflows can free up internal engineering talent to refocus on those strategic roles.
- **Paradigm shift to automation.** To maintain business agility and market leadership, organizations need to swing from human-intensive incident response to automated solutions that support sophisticated diagnostics and self-healing in real time. But finding effective automation solutions is not simple; it requires careful technical study and judicious application of guardrails and fail-safes to ensure that changes don't create more problems than they solve.

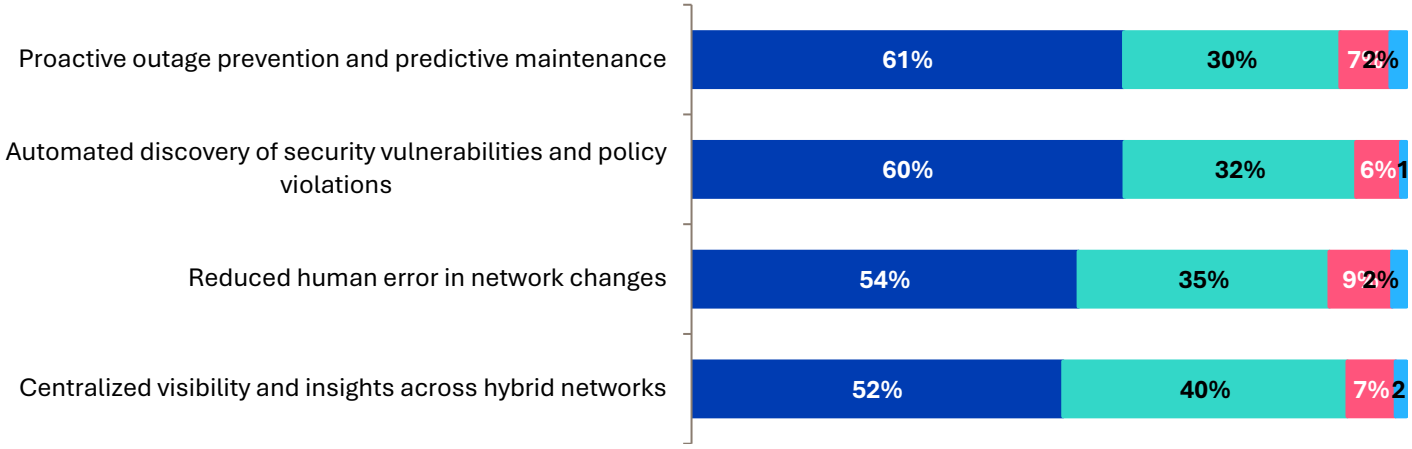
[1] Source: Omdia Research Report, *Network Observability in the Agentic AI Era*, April 2026.
[2] Source: Omdia Research Report, *The Return of NetDevOps: Inside the Convergence of AI, Networking, and Automation*, January 2026.

Network automation done right

Making the move to embracing network automation doesn't mean handing the network wholesale to scripted, expert, or agentic AI systems. There are many steps along that path that can deliver solid value and help organizations improve network performance and resilience along the way. For instance, network automation initiatives carry numerous operational benefits, ranging from security posture to outage prevention to better change accuracy (see **Figure 1**).[3]

Figure 1. Important capabilities of network automation projects

Please rate the following capabilities in terms of their importance to your organization's network automation projects. (Percent of respondents, n=400)



Source: Omdia

Those undertaking network automation projects most often start with basic scaling up of traditionally work-intensive tasks, such as software and firmware updates and patches and configuration backups and restores. But many automation task objectives are focused on improving operations. For instance, 86% of organizations reported having partially or fully automated analytics and reporting; 81% reported having partially or fully automated monitoring, visibility, and observability; and 72% reported having partially or fully automated corrective actions or remediations.[4]

Ideally, automation platforms bring to bear a combination of important capabilities, including workflow chaining, accelerated or automated troubleshooting, and integration with ticketing or change management systems. The optimal outcome uses network automation to replace time-consuming and potentially error-prone manual processes with faster, more accurate task flows.

One of the ways that organizations can capture the benefits of network automation is as part of services that come with a fully managed network. Providers of managed services have the expertise and incentive to build out automations that can accelerate a range of network tasks and processes. Organizations that want to fully offload complex network automation tasks can outsource capabilities to a service provider partner for a wide range of functions, including initial design, setup, automated troubleshooting, and real-time repairs. Co-

[3] Ibid.
[4] Ibid.

managed approaches are also available and are particularly well-suited for organizations with mid-level network maturity and strong in-house teams. Using a co-managed approach can bring advanced network automations to bear, while alleviating the staffing challenges of 24/7 oversight.

Verizon's approach: From insights to action

To position itself as a trusted business partner and provider of network connectivity, Verizon Managed Network Services (MNS) come with service-level agreements regarding network performance, resilience, service quality, and response times for changes and outages. Verizon owns the outcome, and to make sure it is doing everything possible to meet and exceed expectations, Verizon MNS has built an AI Insights platform that delivers and leverages network automation to accelerate tasks wherever possible.

The platform automates data collection, performance analytics and machine learning models to determine root cause analysis. Verizon does this through predictive insights that proactively recognize and assess actual and potential service-impacting incidents. Verizon then uses business rules to trigger corrective actions available in existing runbooks and, when appropriate, automates those runbooks to apply remediation. These automated workflows integrate predictive insights, event log management, business rules, ticketing, notification, and service management platforms.

Verizon MNS has a demonstrated track record in linking automation, analytics, and global service and support across clients' physical and virtual environments, resulting in reduced downtime and improved service resilience. Verizon's extensive operational experience, along with its integrated management tools and on-staff security and network infrastructure experts, helps organizations plan, deploy, and manage incident response and resolution, keeping networks up and supporting the business.

Conclusion

Networks have never been more critical, and no organization can afford to stick with historical, manual-centric processes for incident response and network change deployments. Now is the time to embrace network automation to improve organizational agility in detecting, preventing, and responding to network performance interruptions. However, automation must be trustworthy, transparent, secure, and manageable. Verizon Managed Services leverages AI Insights and automation to smooth network changes and minimize the time needed to detect and address incidents, even correcting them automatically, if possible, so organizations can keep their network—and their business—humming.

Get in touch: www.omdia.com askananalyst@omdia.com