SPOTLIGHT

Sponsored by: Forward Networks

In the hyper-connected digital business model, the network infrastructure must be both resilient and responsive. Service levels and capabilities must be maintained — or even strengthened — as the network adapts to continually shifting business and IT demands.

Navigating the Shift to Autonomous Networking

May 2026

Written by: Mark Leary, Research Director

I. Introduction

The digital business environment is fast-moving and far-reaching. It also must be failsafe. Business and end user requirements can change dramatically and rapidly. All the while, the network must deliver consistent high-quality services and service levels that meet both existing and imminent digital demands.

To meet these demands, the network must best balance often opposing forces. The network must be both stable and agile. It must be both accessible and secure. It must be both efficient and effective. Connectivity demands are many, and network failure is not an option — for the business, for the IT organization, and for connected workers, customers, and smart devices.

With demands rising and resources under pressure, traditional manual network management methods and tools are causing IT organizations to fall behind or fail altogether. Network automation has become a foundational element for an increasingly autonomous digital infrastructure.

AT A GLANCE

KEY TAKEAWAYS

Organizations are looking to do more with their networks, while also wanting to do less for their networks.

- **Networks must adapt.** To match the speed of digital business, change must come fast — without sacrificing service levels.
- **Networks must advance.** Heightened and hastened adaptation and innovation is required as demands shift and pressures rise.
- **Networks must automate.** Manual management practices increase delays and risks. Bolstered by detailed intelligence and deep insights, autonomous networks drive gains along

The Network in the Digital Age

Networks are growing in both criticality and complexity. In this hyper-connected digital era, the network forms the core of the IT infrastructure and functions as a vital utility serving the business. A recent IDC research study of large enterprises indicated that 86% of business executives believe an automated AI-powered network bolsters digital business initiatives. Other IDC research studies cite consistent alignment between business, IT, and networking executives when ranking top strategic business priorities — with all groups focused on operational efficiency, worker productivity, customer satisfaction, digital innovation, and risk reduction. It is easy to map the benefits of an intelligent and autonomous network to these critical business outcomes.

Challenges to Network Excellence

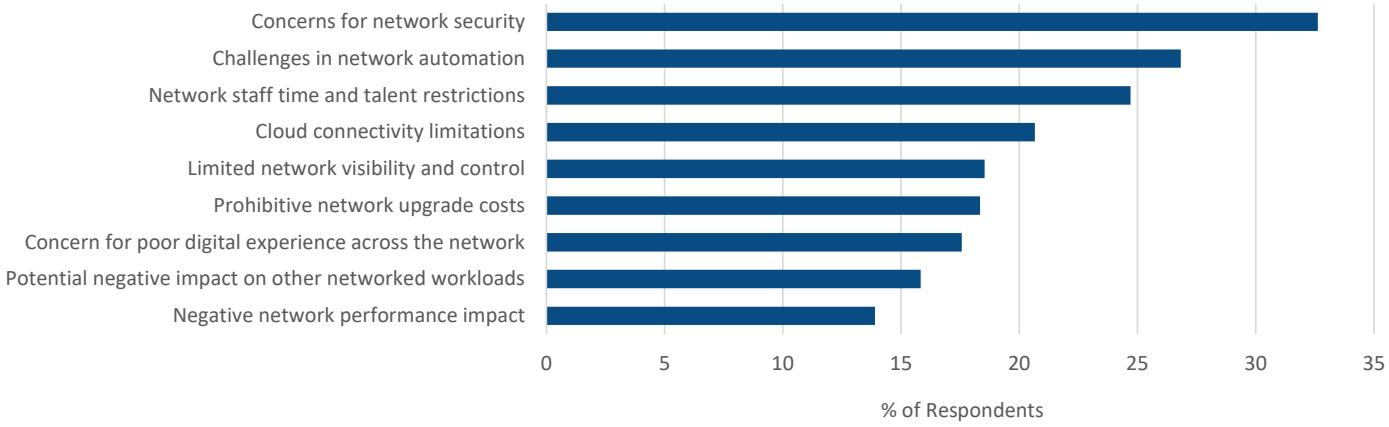
Unfortunately, network complexity all too often limits the network staff's ability to respond to the immediate and developing needs of the business in an agile manner. The network infrastructure is comprised of a vast assortment of technologies, components, configurations, policies, internal and external users, smart devices, management tools, and suppliers — all of which must be made to always work together by a highly pressured staff. This complexity serves to:

- Increase risk of system failures and security breaches
- Limit visibility or lead to blind spots
- Slow problem resolution and threat mitigation
- Increase testing cycles and change windows
- Heighten manual management efforts and human errors
- Delay network solution and service innovations

Furthermore, established methodical and manual network operations, paired to networks that are fixed in nature and slow to adapt, are a mismatch to the highly dynamic infrastructure (e.g., virtual computing, software containers and micro-services, SaaS applications, ever-expanding security mechanisms, and the accelerating agentic AI) and digital business model served.

Network complexity and inflexibility are on full display when examining the delayed production deployments of AI workloads for many organizations. A recent IDC study of AI maturity levels for large enterprises indicated that the movement from select to substantial use of AI has stagnated over the last two years. And the network has played a big part in this delayed AI adoption (see Figure 1).

Figure 1. Network-Related Drivers of AI Project Delays or Abandonment



Source: IDC, 2026

While AI projects have been delayed over the last couple of years, the advancement and even acceleration of AI workloads and components across the network is inevitable. Something must change if the network is to better serve AI workloads and successfully embrace secure autonomous networking into the future.

Critical Requirements and Responses

The network is being asked to move at the speed of digital developments on the business side and AI developments on the technology side. As a result, expectations for network automation are rising fast and furiously. IDC evaluations of network automation projects show that automating network tasks can accelerate critical network capabilities. For example, automation can reduce the time dedicated to configuration management by up to 80% and cut unplanned downtime by up to 89%. This drive towards network automation heightens requirements across the following four critical areas:

- **Detailed network intelligence:** Knowing all there is to know about your current network environment is crucial to successful operations, service assurance, budget management, problem solving, and optimization efforts. Intelligence related to network components, configurations, and conditions enables comprehensive visibility and control over secure and reliable connectivity. Network data pertaining to performance metrics, utilization rates, trending conditions, detailed inventories, experience measurements, and more drive the accurate analysis to follow. Of course, all this intelligence must extend across networks that include multiple vendors, a wide mix of technologies and hardware and software solutions, and public/private cloud environments.

- **Deep network insights:** Fueled by detailed intelligence and, increasingly, powered by AI, network analysis supports vital management functions such as change management, root cause analysis, anomaly detection, and predictive analytics. The resulting insights support both network engineering and operations. Problems can be pinpointed and corrected faster. Resources can be measured and allocated to ensure consistent service and usage levels. Changes that improve performance, security, or utilization can be identified readily. Trending conditions can drive adjustments that resolve developing problems and ensure consistent service levels. And as insights deepen with AI, the more trustworthy network automation becomes. IDC research shows that 78% of networking leaders believe their automation efforts must be fueled by AI. And over 80% believe AI will drive improvements in network service excellence, management simplicity, resource and cost savings, and their security posture.

- **Deterministic network outcomes:** Owing to the complex nature of networks, problem repairs, threat responses, and system/service adjustments are rarely straightforward. Network engineers can often disagree on proposed changes. Even AI-powered network management systems can often present a list of possible changes to execute in response to a problem, threat, or adjustment. Automation can make matters even worse by executing improper changes at speed. With networks, change is constant. Determining any one or any one set of changes to the network produces the desired outcomes — before actual execution in the production network — becomes a vital requirement when automating the network.

- **Directed management actions:** Detailed intelligence and deep insights serve to direct precise management actions. Increasingly, these actions are expected to be executed autonomously. Understanding the criticality and complexity of their networks and facing network budget and staff shortfalls, 46% of network executives surveyed by IDC for an AI-powered networking study favor networking solutions that both determine and execute management actions autonomously. Another 40%, while relying on the human operators to execute actions, trust networking solutions to determine the proper management action to take or to recommend alternative actions.

Advancements in agentic AI certainly represent the next wave of innovation aimed at network automation. Here, intelligent distributed agents can gather needed intelligence, develop in-depth insights, and even take necessary actions.

II. Autonomous Networking: Critical Barriers and Crucial Practices

While network automation is proving very valuable, the fully autonomous network is still years away. Confidence in network automation has been slow to develop, and, increasingly, organizations are looking at the variety and quality of data facilitating automation, the controls used to ensure precise and proper automated actions, and the impact of automation across the end-to-end network. When done right — applying the right set of data, capabilities, and practices — network automation can readily improve such key network management functions as change management, root cause analysis, anomaly detection, and predictive analytics. And success builds confidence!

Critical Barriers to Autonomous Networking

First, let us look at where most organizations are in their autonomous networking journey and identify barriers to forward progress for autonomous networking.

- **Limited or no coupling to network intelligence and insights.** Yes, one can automate discrete repetitive management tasks (e.g., device deployment, policy distribution) with standalone CLI scripts, Python programs, or Ansible runbooks, but gains will be limited, the network retains its static nature, and automation is targeted and executed blindly. Ready. Fire. Aim.
- **Limited or no governance over autonomous networking.** Network automation without proper guardrails, continual testing, or consistent tooling and practices is likely to do more harm than good over time. Networks are ever-changing, and automation is fast-acting. A supposed simple automated change that worked three weeks, three days or even three hours ago can blow up an entire network and cost hours or days of network downtime, IT service interruptions, and business losses. An executed change can sometimes produce unintended consequences in the future. The negative impact may not be immediate, but the danger to service levels is no less. Development of network automation is easy. Governance of network automation is extremely challenging but highly critical.
- **Limited or no unified network management.** Every network is comprised of multiple technologies, devices, domains, security systems, and vendors. In addition, IDC research indicates most enterprises have tens of specialized and singular management, observability, and automation tools in use across their networks. All these tools drive up network costs and complexity, while driving down staff productivity and still leaving gaps in network management. And yet, networking staff are expected to measure, monitor, and manage the network as an end-to-end entity. Autonomous networking a unified concert rather than an untethered collection. Integration, consolidation, and standardization should be key focal points for those seeking to achieve autonomous networking.

An IDC study focused on network automation efforts in large enterprises indicated that steps towards autonomous networking have mostly ignored network intelligence and insights, focused on simple repetitive maintenance tasks, supported no governance at all, and operated on one type of device, one vendor's solution, and one network domain. Autonomous networking can indeed be a lengthy journey for some.

Crucial Practices for Autonomous Networking

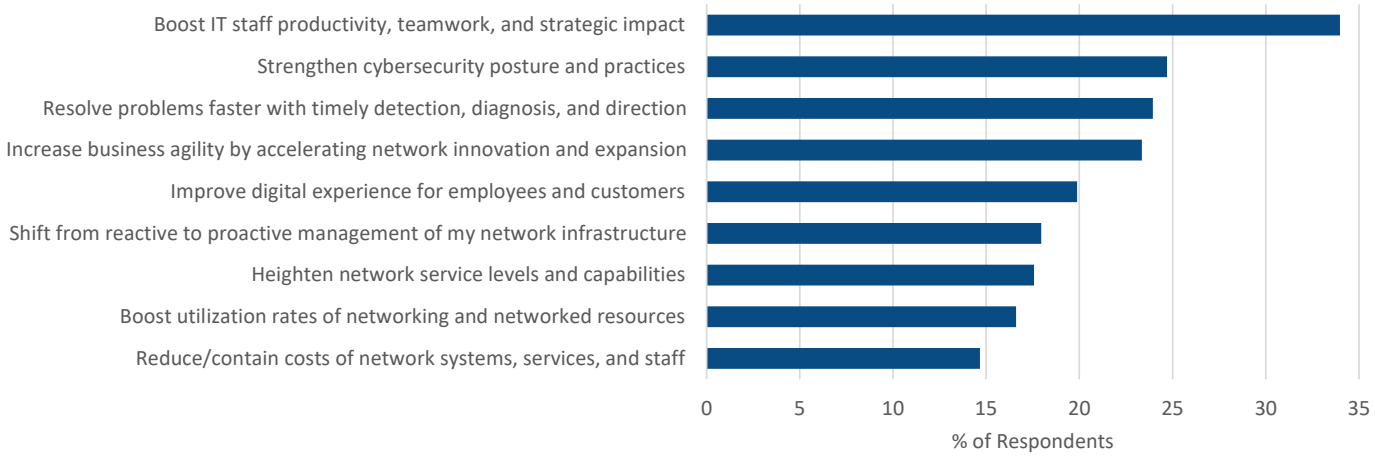
The complexity of the network heightens the complexity of autonomous networking. Just as success in networking is driven by sure and incremental movements forward, so too is the journey towards autonomous networking. The following focal points ensure this journey starts and continues advancing, while eliminating or minimizing delays, detours and, worst of all, dead ends:

- **Fully understand your network environment.** It is imperative that operations teams work from a complete behavioral model of the network; telemetry and inventory is not enough. Safe automation requires behavioral knowledge of the network. This foundational view should include on-premises systems and cloud-based resources, solutions from all vendors, and insights into both network performance and security. Going beyond a detailed inventory of hardware, software, and services, a truly comprehensive understanding of the network should include network behaviors and dependencies. This comprehensive view into the network infrastructure drives all subsequent analysis and actions.
- **Properly balance network advancement and assurance.** The digital business model demands pervasive, performant, and protected connectivity. As such, the network must constantly adapt to keep pace. However, any adaptation must be properly evaluated and validated — using trusted data and thorough analysis — to ensure success for the network and the business.
- **Target critical management tasks.** Full network autonomy is years away. But that should not temper expectations nor slow advancement towards autonomous networking. IT organizations should be focused on automating network management tasks that drive visible near-term gains and solidify core capabilities that will prove useful to future autonomous networking efforts. IDC's 2026 research into AI-powered networking indicates that the Top 5 network management tasks targeted for automation are:
    - Threat response execution
    - Configuration management and validation
    - Problem diagnosis
    - Traffic control and management
    - System deployments and service activations
- **Leverage AI for networking.** Armed with comprehensive network data and AI-driven insights, autonomous networking is growing more trustworthy and capable. While network-focused agentic AI solutions are still nascent, IDC research already indicates that networking leaders are prioritizing network optimization, security, visualization, and troubleshooting for agentic AI investment.
- **Emphasize proactive management.** Averting problems will always drive greater value than solving them. Forward-looking analysis and future-proofing actions provide for a continually resilient and responsive network infrastructure — regardless of demands or developments. Tools that enable AI-directed automation, early threat detection, change validation, and trend analysis serve proactive management. The aim is to predict, prescribe, prove, prepare, and prevent!

III. Benefits of Trustworthy Autonomous Networking

The benefits of a trusted autonomous network are wide-ranging (see Figure 2). As the network is enhanced by automation, both IT and business gains are significant. And the more autonomous the network, the more substantial the gains!

Figure 2. Business and IT Benefits of Autonomous Networking



Source: IDC, 2026

Tactical Impact

Here, the focus is on more immediate and, oftentimes, more visible gains. The following applies:

- **IT Tactical Benefits**: Serving as a foundation within the digital infrastructure, the production network is required to provide consistent service levels, rich service capabilities, and secure access. This is no place for limited visibility, unproven changes, or technology experiments. **In an IDC study focused on the advantages of comprehensive visibility and isolated and thorough testing of changes prior to production deployment, unplanned downtime incidents decreased 33%.** This same study revealed that comprehensive visibility and remedy validation reduced mean time to resolution (MTTR) by 44%. **And when adjustments were made to the network for improvements — versus repairs — device and service deployments were executed 71% faster**. And because the results of these improvements were verified before "going live," risks are minimized or even eliminated.

- **Business Tactical Benefits**: Complete and accurate visibility into network components configurations and conditions combined with automated management provide improved control and utilization of network and networked resources. Best guesses and sporadic reviews result in unnecessary network spending or compromised network service levels. This added visibility into the network also satisfies internal, supplier, and regulatory compliance needs by providing for timely, accurate, and automated reporting. And the combination of detailed visibility and validated change management reduces risks to financial results, operational processes, and information integrity — the result of a more resilient network infrastructure.

Strategic Impact

Often, the evaluation and selection of networking solutions focus too much on shorter-term tactical gains (e.g., cost savings, speeds and feeds, and supplier familiarity) and not enough on the longer-term impact and, potentially, higher value benefits. These more strategic gains are as follows:

- **IT Strategic Benefits:** IDC research consistently highlights improved staff productivity as the #1 benefit of autonomous networking. This is particularly valuable given that IT organizations are looking for senior-level network engineers and architects to focus on strategic business and technology initiatives and to heighten the role and responsibilities for early- and mid-career staff. Also, by relieving staff of mundane manual tasks (e.g., problem diagnosis, resource monitoring), staff satisfaction, retention, and value rises. Looking at the greater IT organization, a more resilient and responsive autonomous network bolsters IT confidence and credibility. The network moves from being a roadblock to IT and business initiatives to being ready and able to satisfy oncoming IT and business demands whenever and wherever. Turning to network technology, autonomous networking enables more timely adoption of innovative networking solutions — whether those innovations involve new connections, new devices, new software or new services**. In an IDC study focused on advanced network observability and change management, network planning, design and testing efforts were executed 36% faster.**

- **Business Strategic Benefits:** As stated previously, worker productivity and customer satisfaction are consistently top-ranked business priorities for business, IT, and network executives. While the network is not the sole determinant of a positive user experience for workers and customers, network downtime and slowdowns severely undercut worker productivity and customer satisfaction. Given the volume and value of networked interactions for workers and customers, IDC research indicates that even the slightest network service disruptions for these users can have grave consequences for any enterprise. Beyond the impact on individual users, autonomous networking reduces the financial and operational risks tied to shortfalls in network resiliency and vulnerabilities to cybersecurity incidents. The digital business model demands secure connectivity and reliable exchanges to all resources at all times. Simply put, without connectivity, there is no digital business, which negatively impacts revenue and profitability. Looking even further out into the future, digital business acceleration and innovation is constrained by a network that cannot readily respond to new business demands. Autonomous networking keeps the network ready for anything through improved resource efficiency and service effectiveness.

IV. Forward: Enabling Change, Enforcing Resiliency, Enhancing Responsiveness.

Forward provides network digital twin and automation capabilities that assure the delivery of consistent network service levels, defense for security vulnerabilities and exposures, and assured success of network changes and intentions. Forward has over a decade of experience supporting enterprises worldwide across every major industry and offers integration with an extensive list of technology suppliers offering networking and security solutions and cloud services.

Key Capabilities and Components

- **Forward Enterprise**: Forward's platform builds a complete behavioral model of the network as a digital twin using configuration and state data to map all possible traffic paths and deliver actionable insights into network forwarding behaviors. Forward's digital twin is a complete behavioral model that establishes the network state and security posture with mathematical precision. This is the structural foundation that makes safe autonomous

networking possible. Owing to the diverse nature of enterprise networks, Forward Enterprise applies this digital twin to both multivendor networks and multicloud services.

- **Forward Predict**: Introduced in May 2026, Forward Predict enables networking staff to define and validate intended network changes to their production network. Changes to the network are first applied to Forward's digital twin, a virtual equivalent of the targeted enterprise network environment, enabling engineers and operators to verify intended outcomes and expose any network or security vulnerabilities. This protects the production network from disruptive changes, streamlines and solidifies the network change process, and boosts staff productivity, value, and satisfaction. This ability to validate the proper functioning of the network in reaction to changes is necessary for autonomous networking to be trustworthy rather than threatening.
- **Forward AI :** Introduced in February 2026, Forward AI is the natural-language interface to Forward's digital twin, enabling engineers, operators, and autonomous agents to investigate the network in plain language and receive evidence-backed answers in seconds. Every Forward AI response is grounded in the digital twin and cited to the exact path, policy, or configuration line that proves it, so the operator, the auditor, and the next agent can all inspect the reasoning behind the answer. Through the Forward MCP Server, this same intelligence extends to custom agents and orchestrates closed-loop workflows across ServiceNow, Slack, and Infoblox, turning answers into verified action across the systems teams already use.

Sample Use Cases

Combining Forward's digital twin capabilities and the Forward Predict application enables organizations to thoroughly test the results of proposed network change before deploying that change in the production network and putting at risk network integrity. In addition, the visibility provided into the network environment and the validation provided for intended changes catches errors before they are put in production preventing outages and security incidents. The positive impact of applying Forward's digital twin technology and Forward Predict is evident across many critical fronts.

- **Assure Network Resiliency and Responsiveness**
  - **Routing validation**. Routing configuration updates, such as those involving border gateway protocol (BGP) and open shortest path first (OSPF), can be verified against the full production-equivalent network model before execution. Given that complicated routing changes are responsible for many network outages and slowdowns, this validation step is critical.
  - **Firewall and access control list (ACL) verification**. New security rules can be tested for intended access — without creating unintended exposure to the production network. Additionally, access is evaluated end to end, not just for a single firewall level.
  - **Segmentation and compliance verification**. Policy changes verified against compliance requirements across all vendors and zones. Compliance is enforced at design time.
- **Accelerate Network Design and Service Delivery**
  - **End-to-end path analysis.** Every change is analyzed for its impact on end-to-end connectivity and physical paths across the entire network, providing complete insight into how traffic will flow before any change is made. This level of service assurance protects against negative digital experiences for end users and smart devices.

- **Automated regression testing**. The equivalent of regression testing for software development applied to the network digital twin. Test every proposed change against your comprehensive list of allowed and required network behavior prior to live deployment in the production network.

Challenges

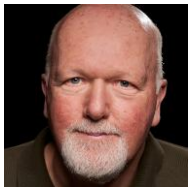
Organizations of all sizes, across industries and locations are challenged by complex network infrastructure (and associated tool portfolio), demanding digital business needs, shifting IT security and connectivity requirements, and shortages of budget and staff. Fighting — and often failing — along these many fronts has these organizations looking for help and raising the bar for networking suppliers such as Forward. Here, the challenge for all suppliers is to balance simplicity and sophistication with their automation efforts, enabling IT organizations to do more *with* the network while doing less *for* the network. For Forward, combining detailed intelligence and deep analysis to deliver autonomy to high-priority network management tasks such as configuration and security management require continual technology advancement, promotion of best practices, high-touch support services, and expansive ecosystem partnerships.

V. Conclusion

Within the network infrastructure, shifting and highly interdependent technologies, configurations, policies, applications, connections, endpoints, and threats raise the risk of failures, slowdowns, cost overruns, staff overload, and, worst of all, digital deceleration. And help is not coming in the form of significantly increased networking budgets or staff numbers. The answer for all organizations is autonomous networking — powered by AI and powering a more resilient and responsive digital infrastructure. Although the fully self-driving, self-healing network is still years away, advanced network management capabilities such as Forward's digital twin technology and predictive change verification represent a significant step forward for network automation. Platforms that provide detailed network intelligence, deep network insights, deterministic network outcomes, and directed automated actions are to be foundational elements of the autonomous networking future.

Platforms that provide detailed network intelligence, deep network insights, deterministic network outcomes, and directed automated actions are to be foundational elements of the autonomous networking future.

About the Analyst



Mark Leary, *Research Director*

Mark Leary is Research Director within IDC's enterprise infrastructure global research domain. He covers Network Observability, Automation, and Artificial Intelligence as part of the Network Infrastructure and Services subdomain. Mark's research covers the advancement and adoption of network observability, the development of network automation capabilities, and AI-powered network solutions, engineering, and operations. It includes end-to-end visibility, service assurance, tool consolidation, predictive analytics, and Agentic AI. Mark also examines the advancement and adoption of enterprise and cloud network infrastructure and services technologies, networking-related professional and managed services, network management best practices, IT staff roles, and skills in this demanding hyperconnected digital era.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA