

The AI era is prompting organizations to rethink their IT strategies to keep pace with expanding AI use cases — and accelerating threats. IDC survey data indicates that AI for network management, particularly in security, is a key use case.

## *AI and Networking: Opportunities to Improve Network Security*

January 2025

**Questions posed by:** HPE Aruba Networking

**Answers by:** Brandon Butler, Senior Research Manager, Enterprise Networks, and Mark Leary, Research Director, Network Analytics and Automation

### **Q. According to IDC survey data, what impact has AI had on networking?**

**A.** AI impacts networking in two distinct ways: First, AI workloads drive significant new demands in network connectivity, performance, and security. Second, AI-powered networking solutions bolster engineering and operations across IT domains, especially in security. The use of AI to enhance network security comes at a critical time: Securing the enterprise has never been more important, but it's also never been more challenging. The intelligence, insights, and automated actions that AI capabilities enable allow for more precise and proactive network management and protection.

IDC's 2024 *Worldwide AI in Networking Special Report Survey* highlights the challenges and expectations around AI in supporting AI workloads across the network and applying AI to managing and securing the network. Global respondents — all from large organizations and most already leveraging AI for both business and IT advancements — consistently identify network service integrity, security improvements, and staff productivity as top priorities for their AI-related innovation and investment. For example, when identifying the top impediments to their GenAI rollouts, security concerns, data quality, and network performance rank highest among technical issues. In addition, when outlining road map priorities for AI-powered networking solutions, security and automation come out on top.

### **Q. What factors are contributing to the high priority of security in AI-powered networking?**

**A.** Modern digital businesses face an attack landscape that is vast and complex, with the volume and variety of users, devices, applications, and "things" on the network complicating security considerations. IDC survey data shows an increased realization among organizations about the power of AI in supporting network security protections and defenses.

The hyperconnected nature of today's digital business creates challenges and opportunities for network security. As Internet of Things (IoT) adoption continues, edge workloads proliferate, and a growing number of business groups each need connectivity, the challenge of securing the enterprise is significant. Network-based telemetry, enhanced by AI-powered analytics, creates an opportunity to enable continuous monitoring of users, devices, and applications for suspicious behavior. Given the amount of data to be mined, AI has become essential for effectively supporting network security.

A successful AI-powered network security strategy includes leveraging network telemetry data — user, application, device identities, and behavioral metrics, for example — and using AI and machine learning on large data lakes to continuously monitor and learn what is normal and expected behavior, and what is abnormal or harmful. AI-powered systems like network detection and response (NDR) speed the identification and response to security incidents and help prevent such incidents.

## Q. Where are organizations prioritizing the use of AI-powered networking for security?

**A.** Data from IDC's *AI in Networking Special Report Survey* shows that network security is a top focus for AI-powered networking, ranking in the top 3 use cases alongside operations and management. For example, the survey asked participants to identify the network management functions they consider most important when evaluating and adopting AI-powered network management tools and practices. The importance of network security — cited by 42.5% of respondents — surpassed network optimization (29.4%) and network automation (25.1%).

Leveraging AI models' analytical power is a key use case for AI-powered network security. The survey also inquired about the most valuable campus and branch AI-powered capabilities. AI-powered user/device profiling for network security was the top rated response, while AI-powered root cause analysis and guided remediation of network problems ranked next.

Respondents were also asked which network engineering and operations functions their organizations prioritize for AI investments. The top response was network automation, with NDR as the second-highest rated response. System configuration and deployment was the third. The survey data highlights how survey respondents prioritize security use cases for AI-powered networking.

## Q. What specific groups of organizations (e.g., by industry, by AI maturity level) stand out among survey respondents focused on the security aspects of AI networking?

**A.** Notable findings from IDC's *AI in Networking Special Report Survey* include:

- » Of respondents who report "substantial use" of AI within their organization, 29% prioritize threat detection and response as a top networking function for AI-powered networking versus only 24% that are in "early stage" of AI use in their organization. Among respondents at large enterprises (more than 20,000 employees), 32% selected

threat detection and response as a top network function for AI-powered networking, while only 23% of respondents at smaller enterprises (5,000–9,000 employees) chose it. This data shows that organizations more mature in their AI journey recognize the value of network-based threat detection and response as a top function for AI-powered networking. Moreover, large organizations, which are more likely to face challenges stemming from the complexity of network security, similarly prioritize threat detection over smaller organizations.

- » Industries in which respondents were more likely to select threat detection and response as a top AI-powered networking function compared with worldwide results include manufacturing, which leads at 35%, while healthcare and retail each account for 30% and government accounts for 29%. Vertical industries such as manufacturing, healthcare, and retail face unique challenges that contribute to their prioritization of threat detection and response as a top AI-powered networking function. For example, regulatory pressures in healthcare and retail raise the stakes for prioritizing security. Attacks can be detrimental to any organization, but attacks can risk patient outcomes in healthcare, lead to lost revenue in retail, or decreased manufacturing productivity.

## Q. What advice do you have for organizations considering AI-powered network management for security?

A. According to IDC's research and consulting on enterprise network security efforts, several management movements are proving successful. Particularly effective movements include:

- » **Streamline management.** A single source of truth, shared network data and tools, cross-IT collaboration, and AI-driven automation reduce vulnerabilities, speed threat mitigation, and protect resources. In addition, a unified AI-powered solution can support streamlined network and security management by recommending and automating actions to aid threat investigation and to support a rapid response to identified connectivity and security problems, along with proactive prediction and prevention.
- » **Unify hybrid environments.** AI-driven intelligence, insights, and automated actions must provide comprehensive visibility, control, and protection for cloud-based and on-premises elements. This unified approach raises the bar for network service and security management while also promising improvements in end-to-end performance and protection, staff productivity, and cost savings.
- » **Leverage a platform approach.** The digital infrastructure, particularly the network, is growing in criticality, complexity, vulnerability, and costs. Platforms — whether delivering vertically integrated solutions (e.g., GenAI) or specialized technology domains (e.g., datacenter networks) — boost simplicity and resiliency while reducing burdens associated with integration, remediation, and innovation. Built-in security capabilities can enable the AI-powered network to enhance protection without the added complexity that comes from multiple disparate tools.
- » **Heighten supplier responsibilities.** Prioritize system suppliers and service providers that emphasize security and trust in AI solution development and delivery. Strong commitments to supporting complete and secure data sets and models, establishing proven best practices, providing a highly secure supply chain, developing an extensive ecosystem, and driving customer success through training, installation, operations, and innovation are hallmarks of a strategic AI partner in networking and security.

- » **Assess the robustness and security of AI data.** The scale of the data lake that fuels AI-powered network security use cases is important to consider, along with the diversity of data, and how data is used and protected. AI is only as strong as the data behind it. Using telemetry from large data lakes can feed predictive analytics and recommendations, providing more in-depth and actionable insights, and bolstering protection and defense against threats.
- » **Shift to a proactive approach.** The intelligence, insights, and automation benefits of AI-powered networking are well suited to empowering teams to make critical security decisions earlier in the threat cycle, with better control of outcomes. For example, AI-powered NDR solutions can automatically identify anomalies, gather information, and recommend updates based on predicted impact. This can help security teams investigate issues, decide how to proceed, and apply changes that can help speed time to response, prevent compromising network components and resources (e.g., data sources, user transactions, and connected devices), and avoid unnecessary disruption to network operations.

## About the Analysts



### ***Brandon Butler, Senior Research Manager, Enterprise Networks***

Brandon's research focuses on market and technology trends, forecasts, and competitive analysis in enterprise campus and branch networks. His coverage includes technologies used in local and wide area networking, such as Ethernet switching, routing/SD-WAN, wireless LAN, and enterprise network management platforms.



### ***Mark Leary, Research Director, Network Analytics and Automation***

Mark's core worldwide research coverage focuses on the advancement and adoption of network observability solutions; the development of network automation capabilities by both technology suppliers and enterprise organizations; and the innovation and impact associated with AI workloads and AI-powered capabilities on network solutions, engineering, and operations.

## MESSAGE FROM THE SPONSOR

**About Hewlett Packard Enterprise**

HPE is the edge-to-cloud company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open, and intelligent technology solutions, with a consistent experience across all clouds and edges, to help customers develop new business models, engage in new ways, and increase operational performance.

Security-first, AI-powered networking from HPE Aruba Networking provides a common foundation that security and networking teams can use to power IoT- and AI-driven business initiatives without sacrificing cybersecurity protection. By combining network telemetry and AI-powered insights built on the industry's leading data lake, HPE Aruba Networking can protect data, infrastructure, and applications at scale — giving teams an AI edge in combating evolving threats.

For more information, visit [www.hpe.com/ww/network-security](http://www.hpe.com/ww/network-security).

 **IDC Custom Solutions**

**IDC Research, Inc.**  
140 Kendrick Street  
Building B  
Needham, MA 02494  
T 508.872.8200  
F 508.935.4015  
Twitter @IDC  
idc-insights-community.com  
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2025 IDC. Reproduction without written permission is completely forbidden.