ADVANCING NETWORK MANAGEMENT WITH GENERATIVE AI: THE ROLE OF DPI-DRIVEN TRAFFIC INTELLIGENCE

Research Report

ROHDE&SCHWARZ
Make ideas real

CONTENT

1. INTRODUCTION

The age of AI is rapidly redefining how data influences today's economic and social facets. Leveraging advancements in computing, AI enables machines to acquire human-like intelligence, facilitating data-driven tasks that involve intensive analysis and complex decision-making.

AI's latest frontier, Generative AI (GenAI), introduces yet another major leap in this space, debuting machine-driven creative capabilities through generative deep learning (DL) models. It builds on earlier AI techniques, including machine learning (ML) and non-generative DL models, which introduced advanced identification and predictive capabilities that paved the way for intelligent and responsive networks.

With GenAI, networks are able to develop novel information using GenAI models. This involves large language models (LLMs), which train on text-based sources, and multimodal models such as generative adversarial networks (GANs), variational autoencoders (VAEs), diffusion models and recurrent neural networks (RNNs), which learn from non-text sources. Extensive training enables machines to acquire different forms of knowledge, such as knowledge of natural languages and knowledge of domains.

In network management, knowledge of languages augments human-machine interactions while domain-specific knowledge, for example, industry knowledge, enables machines to create realistic and contextually relevant outputs. Combined, this simplifies and speeds up complex and time-consuming network tasks such as the selection of optimal routing paths, creation of truck roll schedules and analysis of the impact of bandwidth-hungry applications on the network.

At the heart of GenAI and network management lies data—specifically, network data. Traffic analytics, a primary source of network data, enriches information sources used to train and fine-tune GenAI models, while providing deep context for user prompts and queries during inferencing. In this regard, next-gen deep packet inspection (DPI), an advanced technology for traffic analysis, holds significant potential for enhancing GenAI implementations. It offers reliable, fine-grained traffic insights at scale, making it a valuable source of network intelligence for GenAI-based network functions.

This report

This report aims to assess the role of traffic analytics in the adoption of GenAI for network management, specifically in enhancing network processes and functions, and in improving network outcomes. It also evaluates how traffic analytics facilitates the integration of GenAI workloads into existing network architectures. Addressing key concerns such as scalability, data quality, and security risks associated with gathering and analyzing extensive traffic data, this report seeks to uncover major data-related challenges faced by vendors implementing GenAI. It also examines traffic visibility issues arising from the latest encryption techniques.

The report further evaluates next-gen DPI as a potential source of network insights for GenAI-based network functions. It explores how DPI's core capabilities — such as real-time application insights, encrypted traffic intelligence, advanced threat awareness, and metadata extraction — enable vendors to improve their GenAI models and speed up deployments. The scalability, customizability and reliability offered by advanced DPI engines are also analyzed in the context of high-performance networks and modern application architectures.

Survey: Traffic visibility for GenAI-driven network management

Duration:	Q4 2024 - Q1 2025
Participants:	75 networking vendors
Authors:	Rohde & Schwarz and The Fast Mode

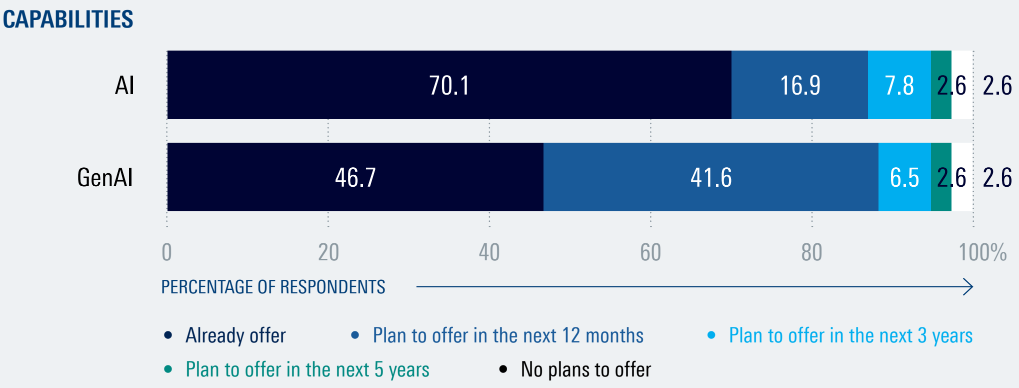
This report is based on a survey conducted by The Fast Mode during Q4 2024 and Q1 2025, involving 75 leading network management vendors. The findings from the report are summarized in the following chapters.

2. THE ROLE OF GENAI IN MODERN NETWORKS

More than 97% of vendors will be offering GenAI capabilities; close to half already do so

The results of this survey show that a whopping 97.4% of vendors plan to offer AI and GenAI capabilities in the next five years. However, there is a notable gap in the adoption of GenAI at present, compared to AI. While 70.1% of vendors already offer AI capabilities, only 46.7% say that their network functions incorporate GenAI capabilities. This gap, however, is expected to close in the next year, given that 41.6% of vendors are planning to introduce GenAI capabilities in their network functions during this period, compared to only 16.9% of vendors who plan to do the same for AI. Networking vendors who plan to offer AI and GenAI in their network functions within the next three years are 7.8% and 6.5%, respectively. Meanwhile, those who plan to incorporate AI and GenAI over a five year timeline make up 2.6% of the respondents, in both areas. Only 2.6% of vendors admit that they have no plans to offer either GenAI or AI capabilities in their network functions.

DIAGRAM 1 Networking vendors' plans to offer AI and GenAI



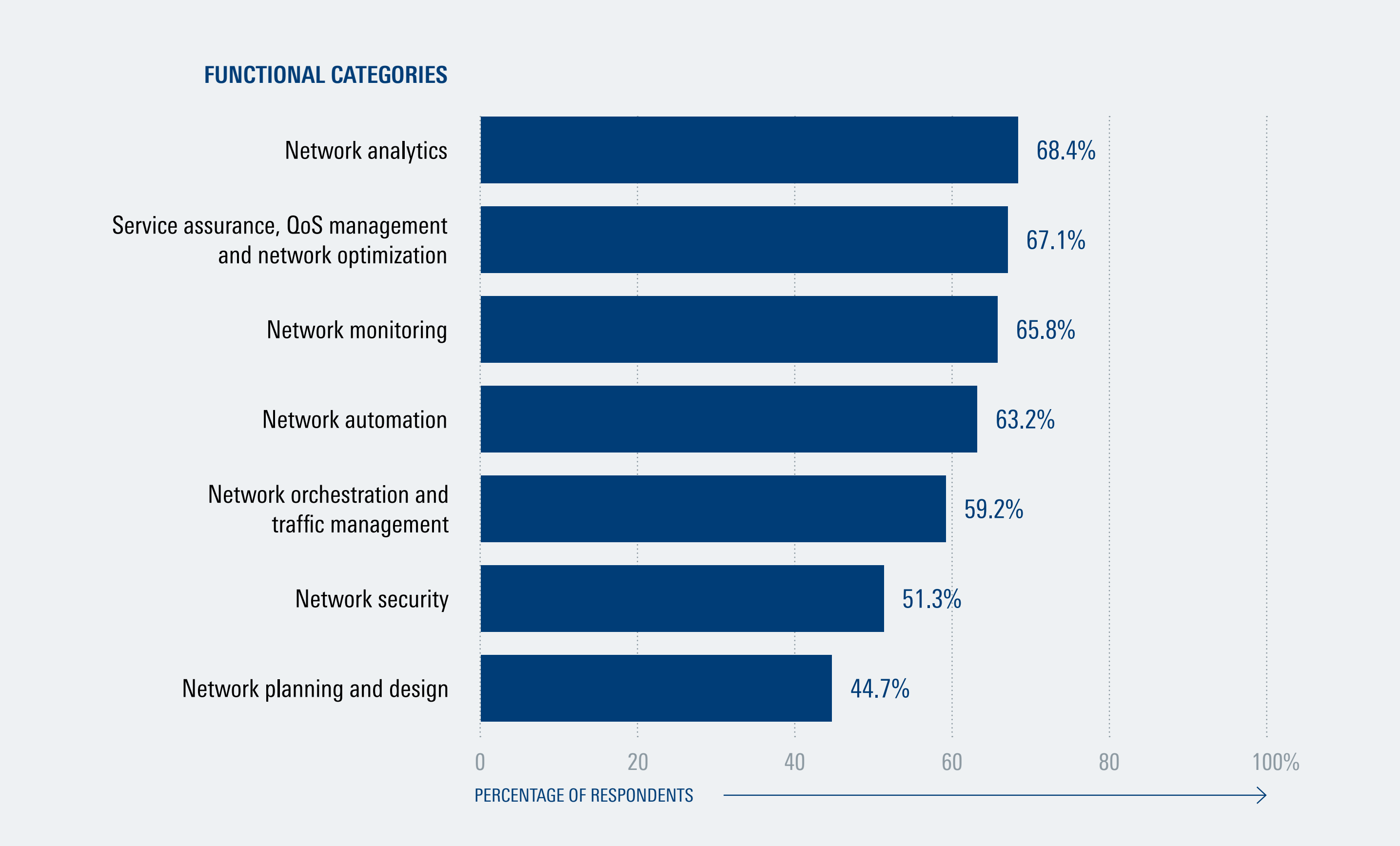
97.4%

of vendors plan to offer AI and GenAI capabilities in the next five years

Analytics, QoS and network optimization, monitoring and automation are four most popular functional areas for GenAI adoption

Findings from this report show that the adoption of GenAI is more prominent across some network functions than others. Analytics, QoS management and optimization, monitoring and automation emerged as the areas with the strongest GenAI adoption. More than two-thirds (68.4%) of vendors providing GenAI capabilities offer solutions in the network analytics segment, while 67.1% offer solutions related to service assurance, QoS management and network optimization. The share of vendors who offer solutions in network monitoring and network automation are 65.8% and 63.2% respectively. For the network orchestration and traffic management segment, the share of vendors is 59.2%. More than half (51.3%) of vendors surveyed offer network security solutions, while 44.7% of vendors are involved in network planning and design solutions. These results show that network management tasks that demand continuous and extensive measurement and analysis of network activity are driving the adoption of GenAI in network management.

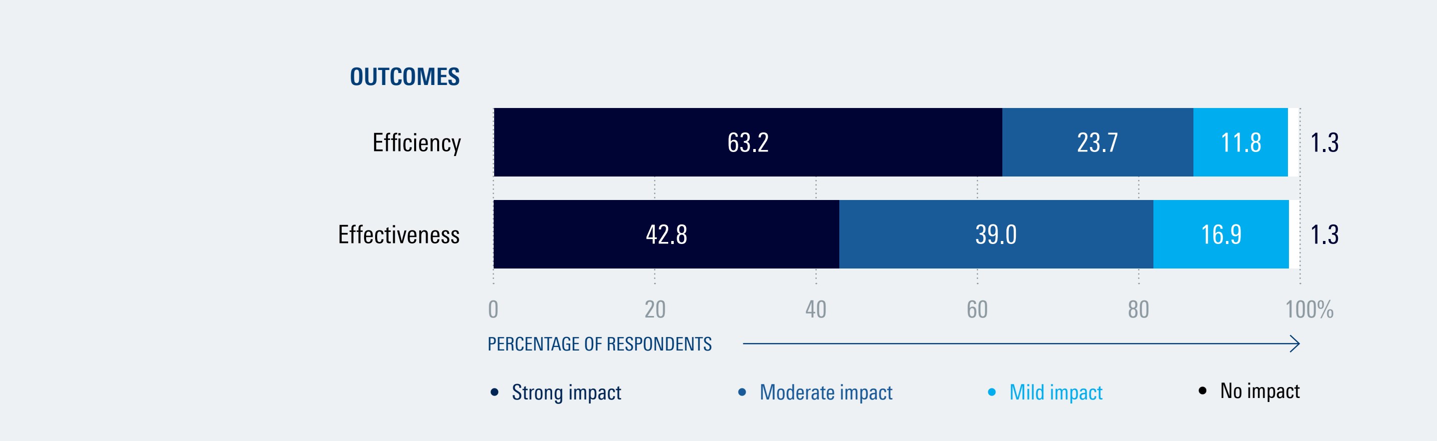
DIAGRAM 2 Solutions offered by networking vendors, by functional category



Networking vendors expect GenAI to significantly improve the effectiveness and efficiency of networking tools, processes and teams

To understand the role and impact of GenAI on network functions, the survey respondents were asked to rate GenAI's impact on networking tools, processes and teams. 'Tools' refers to the hardware and software solutions installed in networks to manage traffic flows. This includes various network devices such as routers, load balancers, web gateways, compression engines and probes. 'Network management processes' refers to actions involved in managing traffic, such as provisioning, monitoring, filtering, maintenance and fine-tuning, while 'teams' refers to technicians, engineers, managers and other personnel involved in areas such as planning and operations.

DIAGRAM 3 Impact of GenAI on the effectiveness and efficiency of networking tools, processes and teams



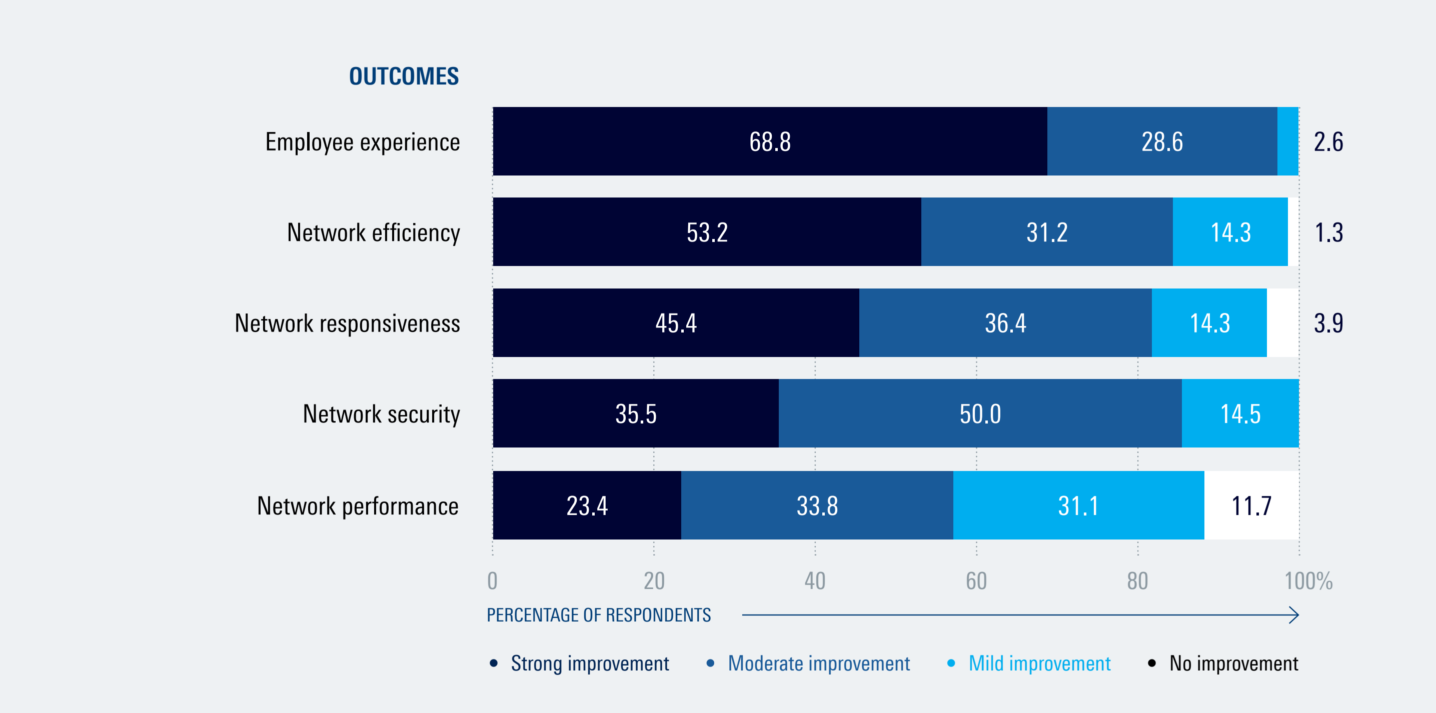
A share of 63.2% of respondents agree that GenAI has a strong impact on the efficiency of network management tools, processes and teams. The ability to access domain knowledge and generate vital analytics and analysis in a matter of seconds delivers substantial time and cost savings, and minimizes the need for human effort, especially across complex tasks. The survey also shows vendors expecting significant improvements in the effectiveness of these tools, processes and teams from the use of GenAI, with 42.8% of respondents expecting a strong impact. Highly contextual outputs based on deep domain knowledge enable network functions to invoke the right policies, rules and actions, and also minimize response lags.

98.7%
of vendors say that GenAI will improve the effectiveness and efficiency of networking tools, processes and teams

Improvement in employee experience expected to be one of the biggest network outcomes from the implementation of GenAI

Evaluating how network functions infused with GenAI capabilities impact network outcomes, the survey finds the biggest expected improvements to be in the area of employee experience. A share of 68.8% of vendors think that GenAI will lead to strong improvements in employee experience by taking over tedious and mundane tasks. Improvements in network efficiencies, specifically in terms of cost, time and resource savings, emerge second, with a share of 53.2% of vendors expecting strong improvements. This is followed closely by improvements in network responsiveness which creates agile networks capable of responding rapidly to network events. A share of 45.4% of vendors expect strong improvements in this area. Concurrently, more than one-third (35.5%) of the respondents project strong improvements in network security. GenAI-enhanced security tools are able to significantly improve tool testing, threat detection and threat mitigation, as knowledge of past attack vectors and remediation steps is available at users' fingertips. Interestingly, when it comes to network performance, measured in terms of parameters such as speed, latency and QoS, the share of vendors who expect significant benefits is somewhat lower, at 23.4%. This may be influenced by the fact that real performance gains are harder to achieve in rapidly changing network landscapes, which require novel and highly contextual approaches designed by humans rather than machines.

DIAGRAM 4 Impact of GenAI-powered network functions on network outcomes



68.8%

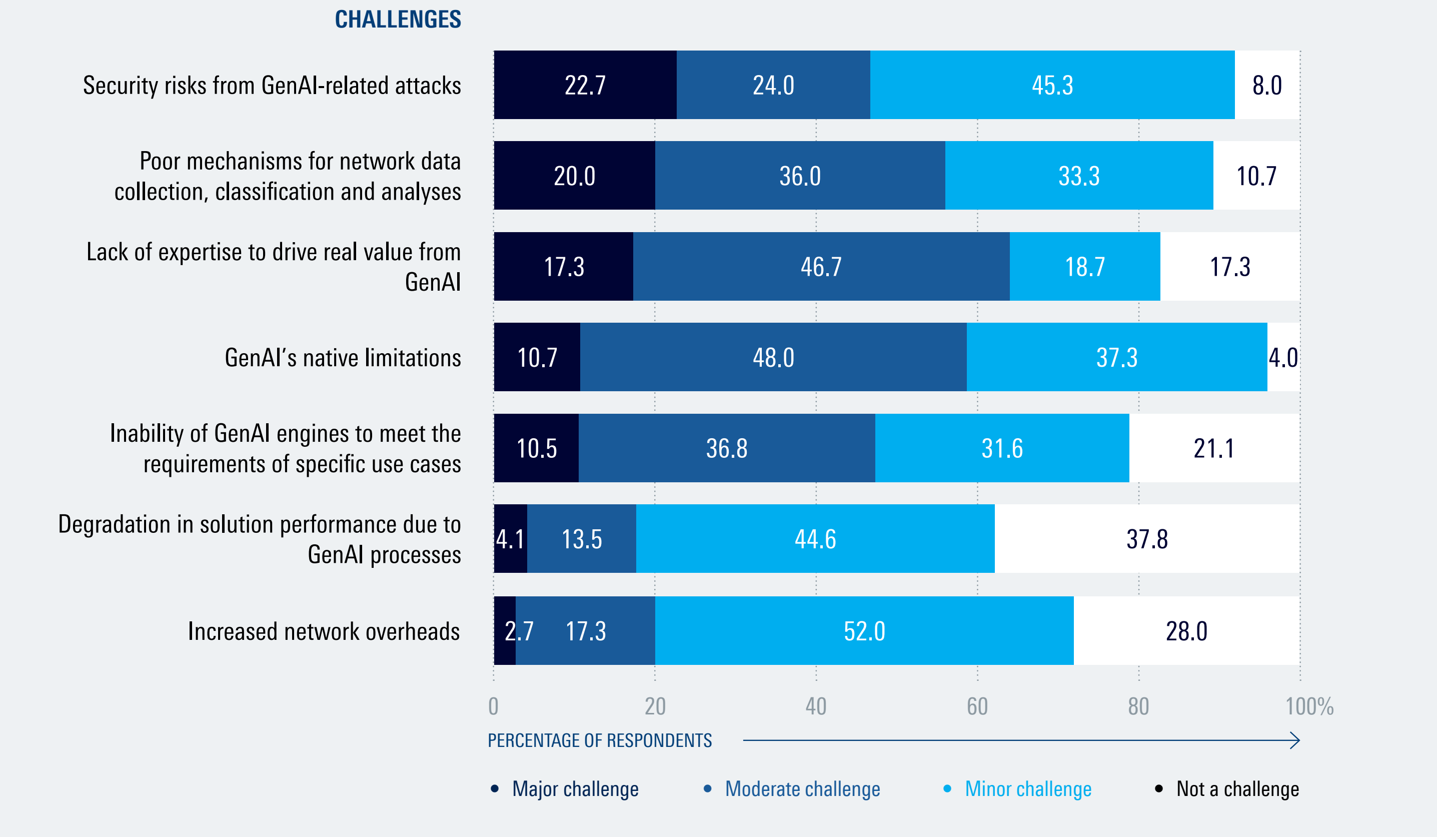
of vendors think that GenAI will lead to strong improvements in employee experience

Security and data collection are two major technical challenges faced by vendors in adopting GenAI

Introducing GenAI can be technically challenging. Close to a quarter (22.7%) of vendors surveyed believe that security risks such as poisoning of training data and data leakage via prompting and querying pose a major challenge to its adoption. These can stem from intentional or accidental acts, and can involve either external or internal parties. Overall, 92.0% of vendors agree that security risks impact them. Vendors acknowledge a similar level of concern over mechanisms used to collect, classify and analyze network information. Poor network information sources can lead to various gaps in data and analytics used in GenAI. A fifth of vendors agree that this can be a major challenge. The total share of vendors who are concerned about poor network data sources is 89.3%.

A lack of expertise to drive real value from GenAI can impact its use, with 17.3% of vendors admitting it poses a major challenge. Likewise, GenAI's native limitations, for example, the inability to cater to networking use cases requiring creative and original outputs, is seen as a major challenge by 10.7% of networking vendors.

DIAGRAM 5 Technical challenges faced by networking vendors in introducing GenAI capabilities



Another challenge often faced by vendors is the lack of a reliable, robust and customizable GenAI engine that suits specific network management use cases. This can be attributed to weak, or poorly trained GenAI models and non-customizability of these models to highly-specific use cases. A share of 10.5% of vendors admit that this is a major challenge.

Two other areas of concern in adopting GenAI for networking is the degradation in the performance of network functions, and the increase in network overheads. GenAI can slow down or complicate core network functionalities as it introduces new computational requirements within a solution. At the network level, computing-, bandwidth-, and power-intensive GenAI workloads can strain both vendor and customer networks as they crowd out existing resources. The share of vendors who consider the impairment of network functions and the degradation of the network to be major challenges is 4.1% and 2.7%, respectively.

92.0%

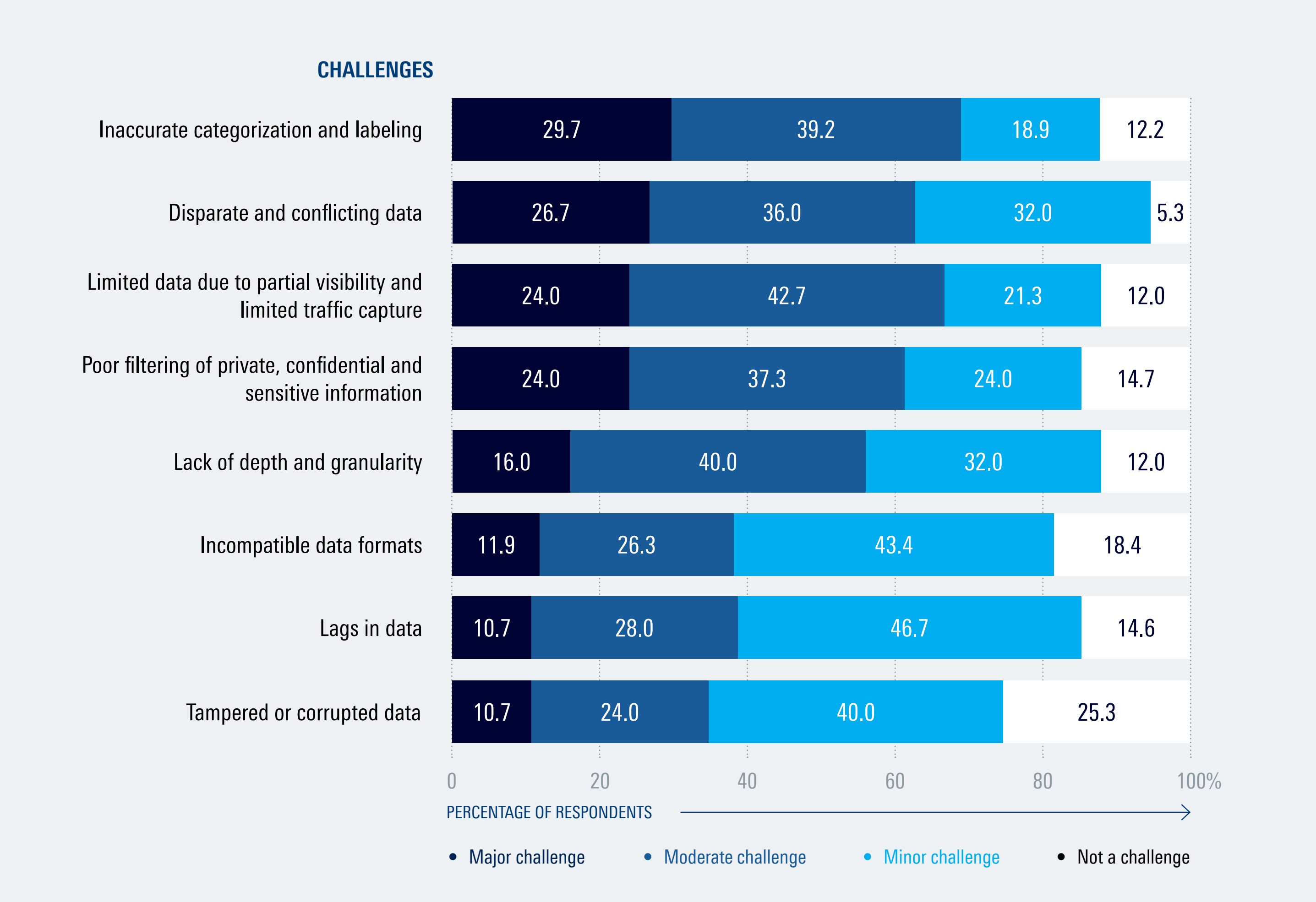
of vendors agree that security risks from GenAI-related attacks are a challenge when it comes to introducing GenAI capabilities

3. DELIVERING HIGH-QUALITY TRAFFIC ANALYTICS FOR GENAI

Quality of traffic analytics affects a large majority of vendors; inaccurate categorization and labeling, and disparate and conflicting records among top concerns

A major source of network information is traffic analytics. Traffic analytics enables network managers to ascertain the state of the network in terms of capacity, behavior, performance, security and others. Network information extracted from traffic analytics is foundational to the development, operation and management of GenAI-based network functions. Apart from providing training and fine-tuning data for pure generation models such as LLMs, GANs and VAEs, traffic analytics is important for delivering direct data references for RAG models. More importantly, traffic analytics forms the bulk of prompt and query inputs. Traffic insights are also crucial in managing GenAI processes such as measuring its impact on a function's responsiveness and its effect on the network.

DIAGRAM 6 Data-related challenges faced by networking vendors in introducing GenAI capabilities



The survey evaluated a number of challenges often encountered by vendors in ensuring the quality of traffic analytics used in GenAI-based network functions. According to the survey, the biggest challenge comes from inaccurate categorization and labeling, with 29.7% of vendors stating that this is a major challenge. Disparate and conflicting data is rated second, with 26.7% of vendors seeing such data as a major challenge. Limited data due to partial visibility and limited traffic capture, for example the omission of encrypted traffic records, is a major challenge, according to 24.0% of vendors. A similar share of vendors see poor filtering of private, confidential and sensitive information, which can lead to compliance risks, as a major challenge.

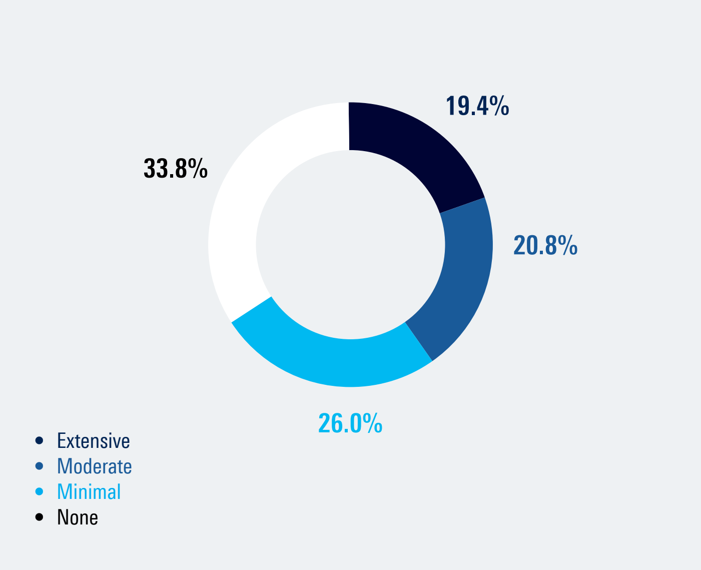
Data that lacks depth and granularity, which consequently impacts the application of GenAI outputs in highly specific use cases is also a major challenge, based on the views of 16.0% of the respondents. A share of 11.9% of vendors feel that incompatible data formats pose a major challenge. A share of 10.7% of vendors agree that lags in data, which impact the time-context of GenAI generated outputs, is a major concern. The share of vendors who think that tampered or corrupted data is a major challenge is also 10.7%.

Over half of vendors grapple with zero or limited visibility into encrypted, obfuscated and anonymized traffic flows

The survey examined in further depth, growing traffic visibility issues due to the prevalence of stricter encryption, obfuscation and anonymization methods. While these techniques enable data owners to safeguard their information, they impair the process of collecting traffic data, which results in poor analytics. A share of 33.8% of vendors admit that their current traffic inspection technologies are not able to deliver packet- and application-level insights on encrypted, obfuscated and anonymized traffic, especially for the purposes of supporting GenAI's network information needs. More than a quarter (26.0%) of vendors agree that their traffic inspection technologies have minimal capabilities to tackle these techniques, while another 20.8% rate their capabilities in this aspect as moderate. Only 19.4% of vendors believe that their existing technologies have extensive capabilities to deliver insights into encrypted, obfuscated and anonymized traffic flows. Unaddressed, complex traffic-concealing techniques including the latest encryption protocols such as TLS 1.3, QUIC, ESNI, and DoX are expected to worsen traffic visibility issues faced by networking vendors who provide GenAI capabilities in their solutions.

DIAGRAM 7

Ability of current traffic inspection tools to deliver packet- and application-level insights on encrypted, obfuscated and anonymized traffic

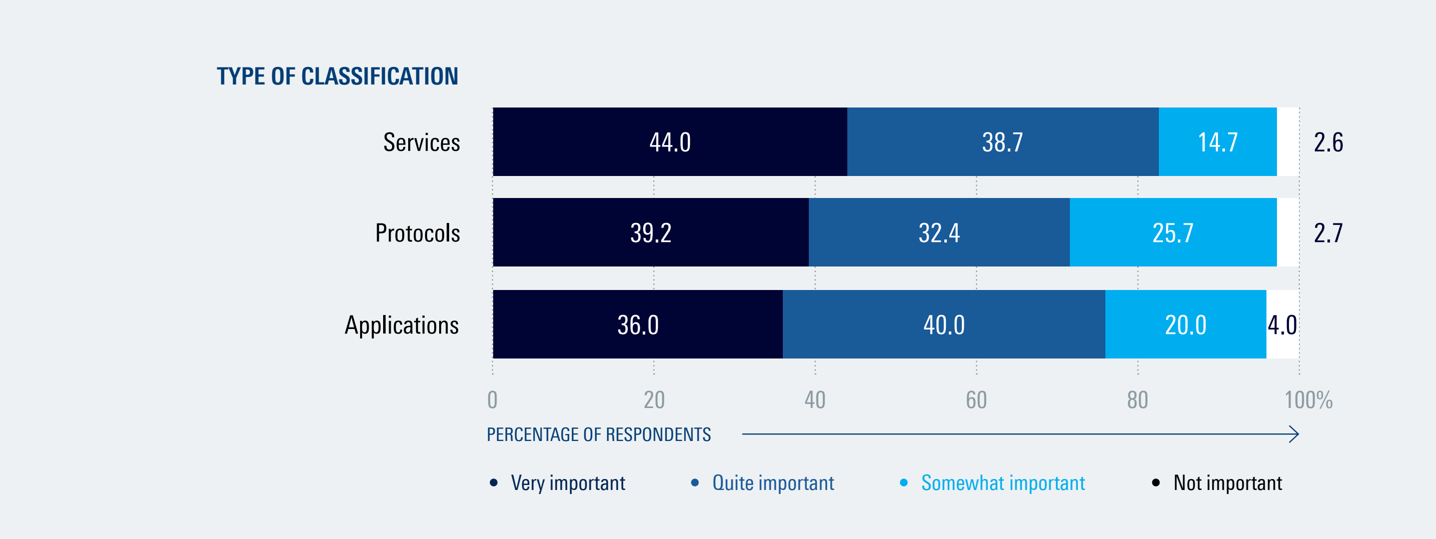


Granular traffic classification by services, protocols and applications deemed important by more than 96% of vendors

Application-aware policies and rules dictate most network management functions, ensuring SLAs are maintained while resources are optimized. The survey assessed the depth and breadth of traffic analytics that are needed to support network management tools offering GenAI capabilities. In particular, it looked at the timeliness and granularity of this analytics, particularly in supporting GenAI model training, fine-tuning and inferencing, and in monitoring and managing GenAI workloads.

The share of respondents who think that real-time classification of traffic by service and protocol is very important is 44% and 39.2%, respectively. Classification of traffic by services enables operators to discern traffic flows by the services being delivered, e.g., email, video streaming and web browsing. Similarly, classification by protocols enables network administrators to break traffic down by categories such as SMTP, HTTPS, FTP and others, for better understanding of data transmission types. The proportion of respondents who think that real-time classification of traffic by application is very important is 36.0%. This information enables networks to identify the exact application being used, e.g., Netflix, YouTube, Instagram or WhatsApp. The survey shows that for all three layers of awareness, a staggering 96.0% of vendors, or more, think that real-time classification is important.

DIAGRAM 8 Importance of real-time traffic classification for analytics used in GenAI-based network functions



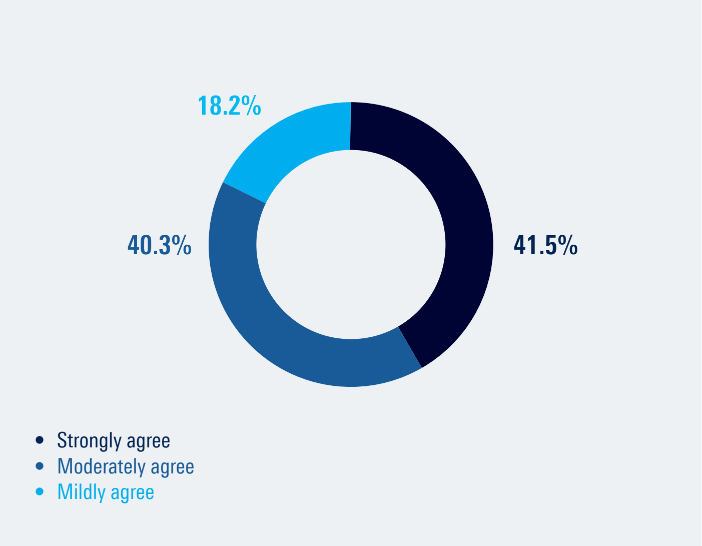
> "The survey shows that for all three layers of awareness — protocols, applications and services — a staggering 96.0% of vendors, or more, think that real-time classification is important"

Vendors unanimously agree on the need for automated traffic capture frameworks to generate highly customized, high-quality traffic analytics

Gathering traffic insights requires multiple methodologies and technologies. A common method deployed across today's networks is the monitoring and analysis of packets. Packets traversing a network leave valuable data footprints that can be harvested to form various insights into its traffic flows. Advanced traffic capture mechanisms can extract a broad range of attributes and parameters that can be reconstructed to form a deep understanding of the network and its behavior. These insights can be sufficiently powerful to fulfill the network information needs of GenAI-based networking tools, particularly in training and fine-tuning GenAI models. Capturing an infinite number of packets and flows however, requires a high-level of scalability that can only be achieved via automation. Automated traffic capture ensures every packet is accounted for rapidly and accurately, leading to comprehensive, high-quality analytics. Additionally, configurable settings are typically used to customize traffic capture to cater to different network environments.

All of the vendors surveyed agree that automated traffic capture frameworks for generating highly customized, high-quality traffic analytics, are essential for GenAI-based network functions. Of all the vendors surveyed, 41.5% strongly agree that automated traffic capture frameworks are essential, while another 40.3% of vendors moderately agree. The remaining 18.2% of vendors mildly agree.

DIAGRAM 9 Importance of automated traffic capture frameworks for highly customized, high-quality traffic analytics



100%

of vendors agree that automated traffic capture frameworks are essential to generate highly customized, high-quality traffic analytics

4. THE INTERRELATIONSHIP BETWEEN GENAI AND THE STATE OF THE NETWORK

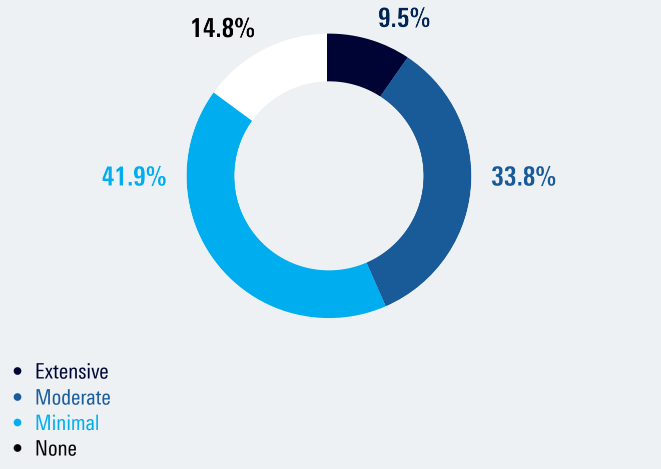
More than 90% of vendors are not able to fully ascertain how network conditions impact the performance of their GenAI-based network functions

As the adoption of GenAI accelerates, network tools, e.g., QoS controllers, web filtering engines and WAN optimizers, will incorporate some form of GenAI. These can be a simple add-on feature such as an LLM-based prompt and query box. It can also be an addition of a new GenAI-based module, for example, a module that generates different traffic scenarios for rule testing. In some cases, vendors can introduce an entirely new solution that is developed as a GenAI-native offering.

Consequently, this will lead to an increasing number of network tools that handle compute-heavy processes involving colossal datasets and resource-intensive architectures. An example of this is a load balancer that rapidly adjusts its distribution algorithms based on the recommendations of its GenAI engine, or a router that updates its routing tables based on inputs from a remote GenAI-enhanced controller. In such cases, it is critical for administrators to keep tabs on traffic bottlenecks, power outages, security threats and other network conditions that can affect the performance of GenAI computing stacks, database systems and connection pathways.

The survey respondents acknowledge that their current traffic analytics tools fall short of identifying, in real time, the impact of network conditions on the performance of their GenAI-based network functions. A share of 14.8% of vendors admit that their tools are not at all capable of doing this, while 41.9% believe that their tools have only minimal capabilities. Close to a third (33.8%) of vendors say that their tools are able to moderately identify the impact of network conditions on GenAI-based network functions, while only 9.5% agree that they have extensive capabilities in this area.

DIAGRAM 10 Ability of current traffic analytics tools to identify the effect of network conditions on the performance of GenAI-based network functions



56.7%

of vendors say that their current traffic analytics tools cannot adequately detect the impact of network conditions on GenAI-based network functions

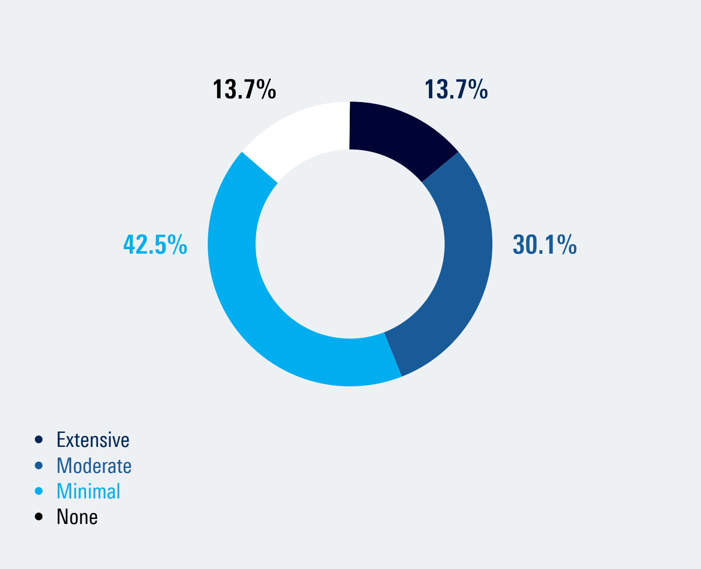
A majority of vendors remain in the dark on the effect of their GenAI workloads on the state of the network

On the contrary, the computing and networking demands introduced by GenAI processes can strain existing network resources, potentially degrading the performance and QoS across other parts of the network. Whether it is an LLM-based virtual assistant or a GAN-based map generation feature, the sheer amount of data that is transported in the network during an active session can erode substantial bandwidth. Furthermore, availability of simplified chat interfaces may result in behavioral modifications in users, leading to a rapid escalation in user engagements. As prompts and queries increase, so will the usage of network resources and capacity. Another potential challenge arises when the vulnerabilities of GenAI applications and databases create fresh impetus for threat actors to mount attacks on a network, resulting in further erosion of network capacity.

Recognizing the importance of monitoring the effects of GenAI on the network, respondents were asked if their current traffic analytics tools are able to identify, in real time, the impact of GenAI workloads on network performance and resource consumption. A share of 42.5% of respondents have minimal capabilities to do so, while 13.7% have none. Another 30.1% have moderate capabilities. Only 13.7% believe that their traffic analytics tools are able to extensively identify the impact of GenAI workloads on their networks.

DIAGRAM 11

Ability of current traffic analytics tools to identify the impact of GenAI workloads on network performance and resource consumption



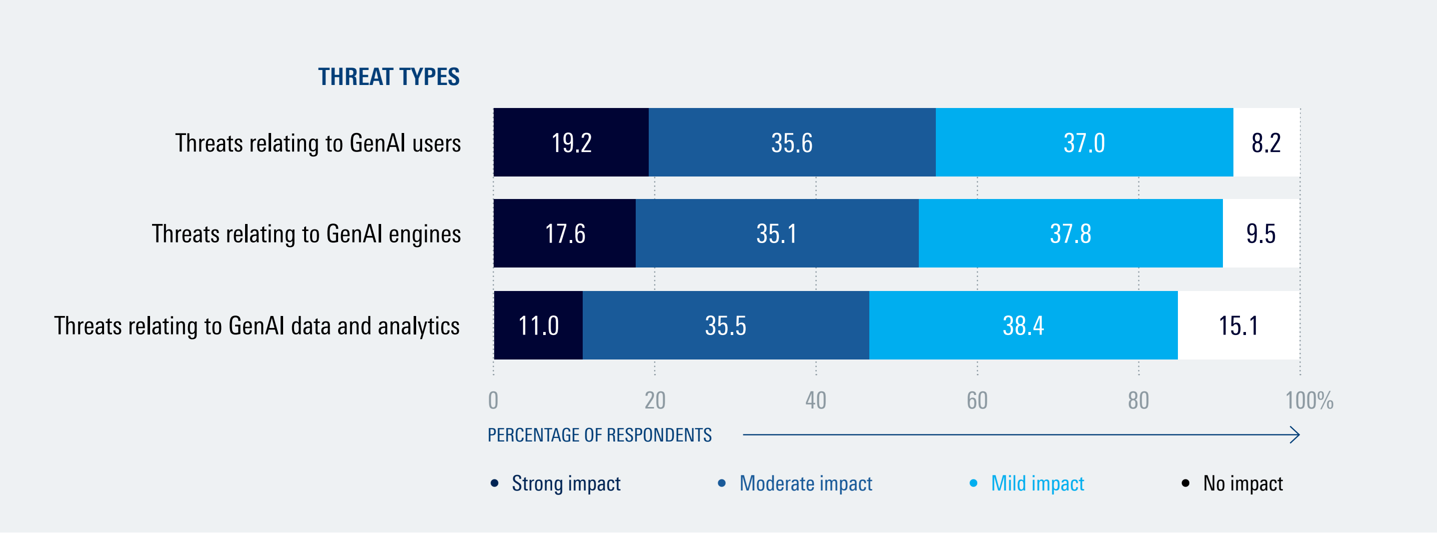
5. ADDRESSING SECURITY CONCERNS THROUGH COMPREHENSIVE VISIBILITY

Bulk of network functions are impacted by GenAI-related security threats

GenAI involves an entire array of computing and networking elements – TPUs, GPUs, data capture tools, databases, AI frameworks, libraries, APIs, applications and clouds. These are often distributed and are accessed and managed by multiple parties. As a consequence, the use of GenAI inadvertently increases the attack surface and multiplies the security vulnerabilities in the network.

The survey assessed the impact of different categories of threats precipitated by GenAI. Threats relating to GenAI users, for example DoS attacks launched via an infinite number of prompts and queries, and unauthorized access by users, emerged as the most critical. Close to one-fifth (19.2%) of vendors think that these threats have a strong impact on their GenAI-based network functions, with 91.8% in total, agreeing that these threats impact their networks to a certain degree. Threats relating to GenAI engines, for example, model-level attacks such as adversarial attacks on neural networks and system-level attacks such as code errors, zero-day exploits and malware also have a strong impact on these functions, according to 17.6% of vendors. A total of 90.5% of vendors believe that these attacks impact their network functions to some extent. Threats related to data and analytics used in GenAI affect 84.9% of vendors, with 11.0% admitting that their functions are strongly impacted. Typical attacks in this category are model inversion attacks, data exfiltration, data poisoning and data corruption.

DIAGRAM 12 Impact of GenAI-related threats on network functions



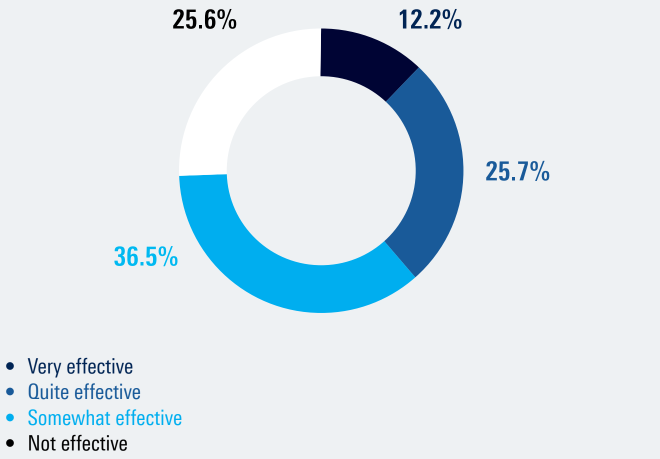
Close to a quarter of vendors admit their traffic analytics tools are not effective against threats introduced by GenAI; only one in ten vendors agree their tools are 'very effective'

Threats originating from GenAI-related processes and elements, e.g., infiltration of data lakes, query flooding and API abuse, require continuous security monitoring, detection and remediation. These security implementations however, rely on advanced traffic analytics tools that can, among others, single out flows that relate to GenAI activities, detect irregular and suspicious GenAI application behavior, uncover encrypted and hidden threats in GenAI traffic, detect rogue devices and illegitimate users in a GenAI ecosystem, and block malicious GenAI traffic.

The survey finds that only 12.2% of vendors are confident that their traffic analytics tools are very effective in identifying GenAI-related threats. Close to a quarter (25.6%) of the respondents admit that their traffic analytics tools are not effective while more than one-third (36.5%) of respondents agree that their tools are only somewhat effective. The remaining 25.7% say that their traffic analytics tools are quite effective in identifying these threats.

DIAGRAM 13

Effectiveness of current traffic analytics tools in identifying GenAI-related threats



62.1%

of vendors say that their tools have limited effectiveness when it comes to detecting GenAI-related threats

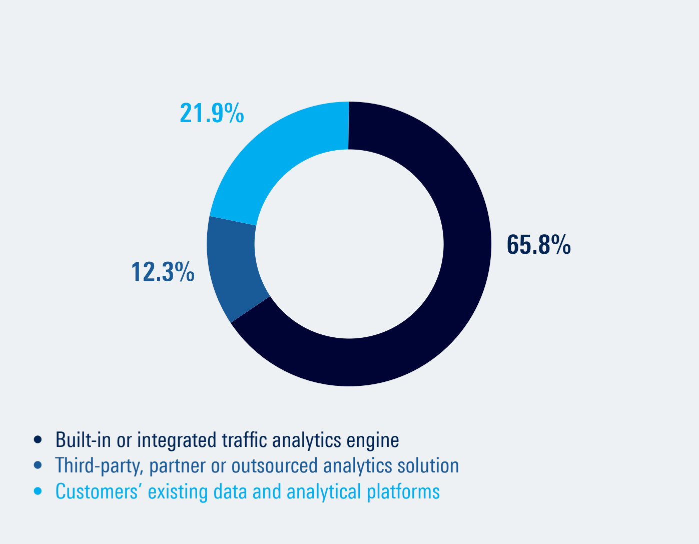
6. SCALABLE TRAFFIC CAPTURE

Vendors strongly prefer built-in traffic analytics engines for extracting network information needed for GenAI

The introduction of GenAI in networking is expected to result in a surge in traffic analytics needs. Traffic analytics will be necessary not only for GenAI processes such as model training, testing, fine-tuning and inferencing, but also for optimizing, securing and managing GenAI infrastructure and workloads. As networks expand, the demand for information will grow further to encompass new users, devices, links, computing nodes, network functions and various network events. Consequently, vendors and network administrators will be faced with the task of gathering infinite data streams that must be filtered and analyzed in real-time, from every part of the network.

This survey evaluated the most common models used by networking vendors to source traffic analytics in GenAI implementations. Close to two-thirds (65.8%) of vendors are integrating or planning to integrate traffic analytics as part of their solutions. This enables vendors to customize the level and rate of information capture and analysis based on the functionalities they support.

DIAGRAM 14 Networking vendors' preferred source of traffic analytics for GenAI-based network functions



For example, deep threat information, including analysis of anomalous traffic patterns, is more pertinent for solutions such as intrusion detection systems (IDS) and firewalls. In this model, vendors can use traffic analytics capabilities that have been developed in-house, or take advantage of third-party commercial engines or open-source technologies.

Meanwhile, 21.9% of vendors are tapping or plan to tap into customers' existing data and analytical platforms. This option is highly workable for customer-managed platforms that provide comprehensive and highly consolidated datasets as well as advanced analytical capabilities that meet the needs of various GenAI-based network functions.

Only a small fraction (12.3%) of vendors are using or plan to use an independent analytics solution provided or managed by a third-party provider or partner vendor. This allows networking vendors to leverage full-featured analytics solutions from specialized players.

7. MEETING GENAI ANALYTICS REQUIREMENTS WITH NEXT-GEN DPI

The need for advanced traffic analytics in GenAI deployments is expected to drive the demand for traffic detection technologies that are built to filter traffic flows at scale. In this regard, a well-known technology that is already being widely deployed to support various network functions is deep packet inspection (DPI). DPI is a cutting-edge traffic filtering technology that offers unlimited capacity for capturing and analyzing IP traffic flows. It can be deployed as a proprietary hardware solution or a software engine that is embedded in the host solution, to support real-time analysis of traffic flows.

ipoque, a global leader in DPI and network analytics, offers a market-leading next-gen DPI suite comprising the renowned DPI engine R&S®PACE 2, and its vector packet processing (VPP)-native counterpart, R&S®vPACE. R&S®PACE 2 supports high-speed filtering in scalar packet processing environments while R&S®vPACE, which caters for VPP frameworks such as FD.io or DPDK graph, delivers substantial speed and performance gains for computing-intensive VNFs and 5G UPFs.

R&S®PACE 2 and R&S®vPACE combine advanced statistical, heuristic and behavioral analyses to classify applications, protocols and services in real-time. The engines feature a weekly updated library with thousands of signatures. Apart from application awareness, the engines also execute metadata extraction, providing insights into parameters such as speeds, latency, jitter and time-to-first-byte. Additionally, R&S®PACE 2 and R&S®vPACE are able to detect malicious, suspicious and anomalous traffic, ensuring continuous vigilance against network threats.

Both DPI engines come with encrypted traffic intelligence (ETI), which delivers complete visibility into traffic flows even when these are encrypted, obfuscated or anonymized. ETI uses ML algorithms (e.g. k-nearest neighbors (k-NN) and decision tree learning), DL algorithms (e.g. convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory (LSTM) networks), high-dimensional data analysis and advanced caching to enable users to tackle the latest encryption protocols such as TLS 1.3, TLS 1.3 0-RTT, ESNI, ECH, DNS over HTTPs, and DNS over TLS.

R&S®PACE 2's and R&S®vPACE's specifications include:

High-performant engines with unparalleled speeds

Lightweight engines with the lowest memory requirements in the industry. Both R&S®PACE 2 and R&S®vPACE are optimized for minimal memory usage per flow. For lean deployment scenarios, R&S®PACE 2 allows further adjustments in the minimum build configuration.

Embeddable in traditional, virtualized and cloud environments

Option to easily define custom DPI signatures

First packet classification for instant detection of applications, allowing for consistent flow handling

Option to translate R&S®PACE 2 outputs into standardized formats such as IPFIX and sFlow

A robust quality assurance process, including automated traffic generation and testing, expert analysis and network emulation, which ensures exceptional accuracy and a near zero false negative rate. This utilizes automation nodes across the globe, enabling 24/7 monitoring and validation.

Over 20 years of experience serving networking vendors, ensuring top-of-the-class functional and vertical expertise

24/7 support and excellent service, ensuring customers are able to access assistance and information any time

Traffic insights provided by R&S®PACE 2 and R&S®vPACE can greatly augment the GenAI capabilities of network functions that rely heavily on network information. The following GenAI-related deployment processes highlight areas where DPI-driven traffic insights can deliver significant impact to:

1. **GenAI training data:** DPI data can enrich both text-based sources that are used to train LLMs and non-text sources that are used to train other types of generative models, such as GANs and VAEs. Examples of text-based sources that can benefit from DPI analysis are traffic monitoring reports and threat detection reports while examples of non-text sources are network performance charts, scatter plots illustrating congestion bottlenecks and heat maps of packet loss. By applying AI techniques such as ML and DL, real data provided by DPI can also enrich sources that relay predictive information, enabling network managers to generate outputs such as application trend forecasts or future time series. With granular and customizable traffic analysis, DPI outputs can support model training across various use cases, as outlined below:

   a) **Specific functions:** DPI can be used to produce datasets tailored to specific tasks handled by a networking solution. For example, when training GenAI models to support a QoS manager or an SD-WAN controller, DPI analysis can be customized and optimized to capture fine-grained metrics that track the performance of applications from end-to-end.

   b) **Niche applications:** When a networking solution is tasked with managing non-standard traffic flows, DPI enables vendors to define custom signatures to detect and extract insights from specific applications or domains. Examples include industrial applications accessed in a wireless IIoT network or critical enterprise applications accessed on a private 5G network.

   c) **Security functions:** Security-related functions such as NGFW, intrusion prevention systems, data loss prevention, zero-trust network access and secure web gateways can tap into DPI's advanced threat awareness to enhance their GenAI capabilities. Comprehensive and highly accurate data on malicious activities and network irregularities strengthens GenAI models used to develop responses to security events.

   d) **Protected or hidden traffic:** Next-gen DPI engines such as R&S®PACE 2 and R&S®vPACE are equipped with ETI, enabling vendors to tackle encryption, obfuscation, and anonymization. This eliminates blind spots in traffic monitoring and analysis, improving training data and contributing to superior GenAI models.

2. **GenAI test data:** DPI provides accurate real-world traffic data that can be used to assess the effectiveness of GenAI models in producing realistic outputs. DPI's customizability also enables vendors to optimize data collection and analysis, speeding up testing and improving efficiency.

3. **Fine-tuning data:** Pre-trained GenAI models must be fine-tuned to align with the environments, functions, and use cases they support. R&S®PACE 2 and R&S®vPACE are resource-light, allowing seamless integration into any customer network (e.g., mobile core, cloud SD-WAN and on-premises LAN) without affecting performance or resource usage. This provides customer-specific network insights, simplifying and accelerating the fine-tuning of GenAI models.

4. **Rich, real-time prompt data:** Real-time traffic inputs from DPI are important in populating and enriching user prompts. Whether these prompts are automated or crafted manually, real and predictive analytics constructed from DPI inputs enable extensive inferencing, driving GenAI-based network functions to their full potential.

5. **GenAI infrastructure and application optimization:** GenAI-based network functions involve a complex network of CPU, TPU, and GPU clusters, storage devices and routers/switches. They also involve various operating systems, orchestration platforms, AI frameworks, data lakes, data processing tools, application and web servers, and APIs. Traffic awareness from DPI helps administrators monitor each of these components, enabling better resource allocation, improved response times, and minimal downtime. These insights also allow them to optimize their GenAI architectures, for example, refine their GenAI computing stacks.

6. **Managing network externalities:** With continuous insights into traffic performance and security parameters, vendors are able to monitor how network conditions impact the performance of their GenAI applications. This information enables network owners to align their network strategies, architectures and processes to accommodate rapidly increasing GenAI workloads.

7. **Managing GenAI effects:** Using DPI data, vendors can determine if their GenAI-based network functions are impacting other parts of the network. Analyzing traffic flows that navigate their GenAI components—at various times, such as during peak traffic or during an adverse network event—helps vendors distinguish genuine downgrades in network performance from those caused by their GenAI workloads.

8. **Attacks on GenAI:** By leveraging DPI's ability to detect anomalous, suspicious, and malicious traffic flows, vendors can protect their assets and workloads from attacks aimed at exploiting vulnerabilities in GenAI applications and processes.

9. **Assessing functional effectiveness:** DPI data on network outcomes, such as performance and security KPIs, enables network vendors to isolate failures caused by poor strategies or policies from those originating from inaccurate or weak GenAI models.

10. **Harmonization of network actions:** Comprehensive analytics and compatibility with IPFIX reporting formats enable network owners to use R&S®PACE 2 or R&S®vPACE to create a unified source of shared traffic intelligence for various network functions. With multiple vendors utilizing the same data to train, fine-tune and test their GenAI models, networks can achieve greater harmonization of policies, rules, and decisions, ultimately improving GenAI-based implementations across the network.

11. **Monetization:** The availability of comprehensive traffic intelligence from DPI enables networking vendors to incorporate advanced analytics into their offerings. From prompt enrichment to providing real-time traffic data references for queries, vendors can package DPI-driven traffic intelligence as a value-added feature in their GenAI-based network functions.

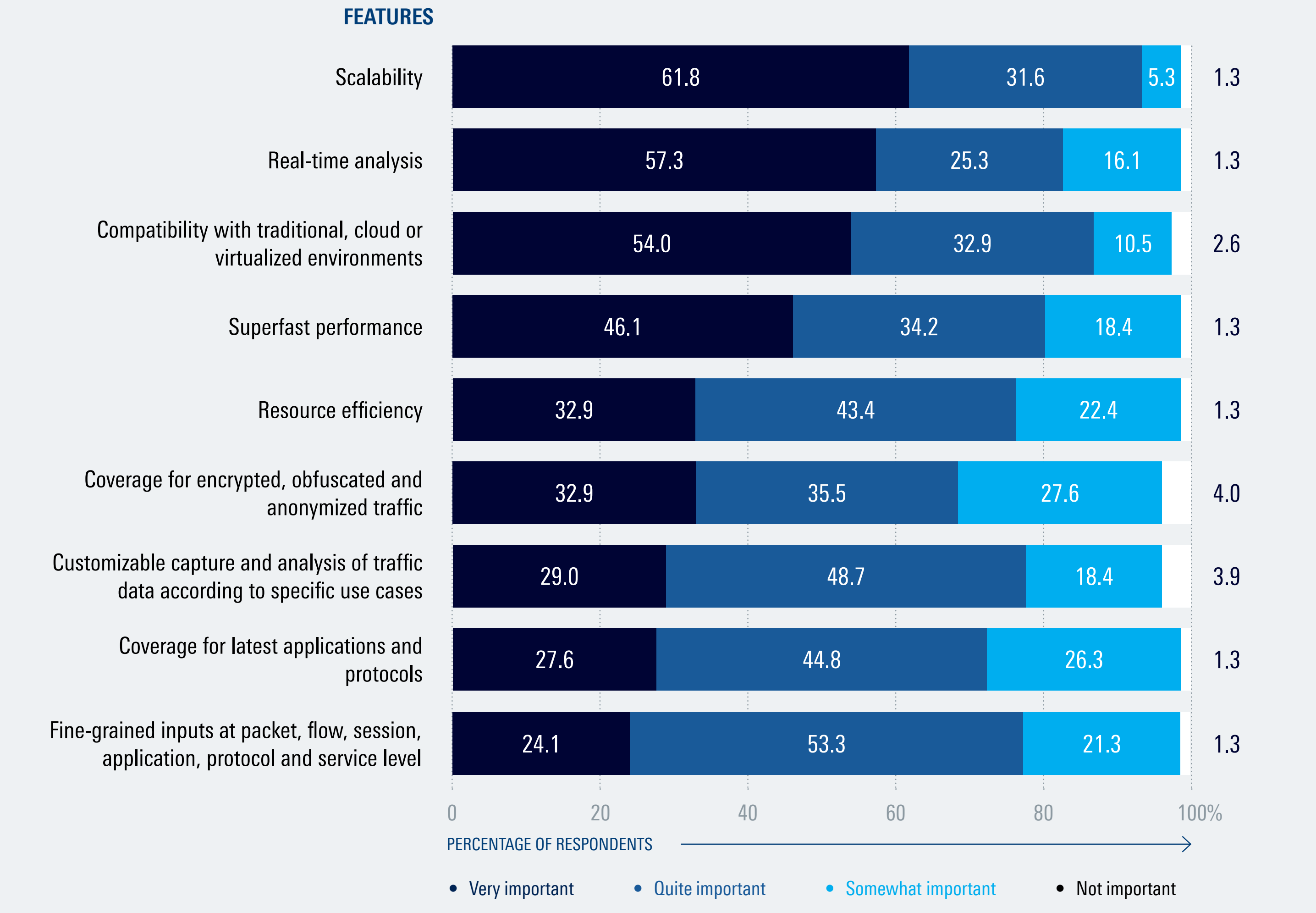
> "DPI data can enrich both text-based sources that are used to train LLMs and non-text sources that are used to train other types of generative models, such as GANs and VAEs"

8. DPI IMPLEMENTATION MODELS

Scalability and real-time analysis rank highest among vendors' criteria for a traffic analytics tool; compatibility with traditional, cloud and virtualized environments ranks third

The survey evaluated the requirements for a traffic analytics tool designed to deliver network intelligence in GenAI implementations. Scalability emerged as the top priority, with 61.8% of vendors rating it as very important. This was followed by the availability of real-time analysis, considered very important by 57.3% of vendors. Compatibility with all types of environments—such as traditional, cloud, and virtualized environments—ranked third, with 54.0% of vendors viewing it as a crucial feature for a traffic analytics tool supporting GenAI. Superfast performance is very important, according

DIAGRAM 15 Important features for a traffic analytics tool used for GenAI-based network functions



to 46.1% of vendors, while being efficient or resource-light, which supports extended deployments and reduces overheads, is deemed very important by 32.9% of vendors.

Similarly, 32.9% of vendors think transparency across encrypted, obfuscated, and anonymized traffic is very important. This covers traffic encrypted with the latest protocols such as ESNI, QUIC, and TLS 1.3, as well as traffic using CDNs, VPNs, or mimicry techniques. Additionally, 29.0% of vendors feel that customizable capture and analysis of traffic data for specific networking use cases is very important. When it comes to coverage for the latest applications and protocols through frequently updated signature libraries, 27.6% of vendors regard this as very important. Just under a quarter of respondents (24.1%) consider fine-grained inputs at the packet-, flow-, session-, application-, protocol-, and service-level to be very important.

These results illustrate the huge potential for DPI in GenAI, particularly in network management. DPI's ability to scale indefinitely provides sufficient data for GenAI training and fine-tuning, while its ability to analyze traffic flows in real-time provides highly contextual, deep reference data and predictive analytics that can be used in inferencing and the assessment of network outcomes.

DPI widely used to deliver real-time traffic analytics for GenAI-based network functions; two-thirds of vendors will have deployed DPI within the next five years

The survey shows that close to half (48.1%) of networking vendors are already using DPI. Among the vendors not currently using DPI, 5.1% plan to adopt it within the next year, while 28.2% and 2.6% plan to do so within the next three years and five years, respectively. This brings the total share of vendors expected to use DPI within the next five years to 66.7%, indicating the growing adoption of DPI across GenAI-based network functions.

DIAGRAM 16 Current adoption of DPI among networking vendors

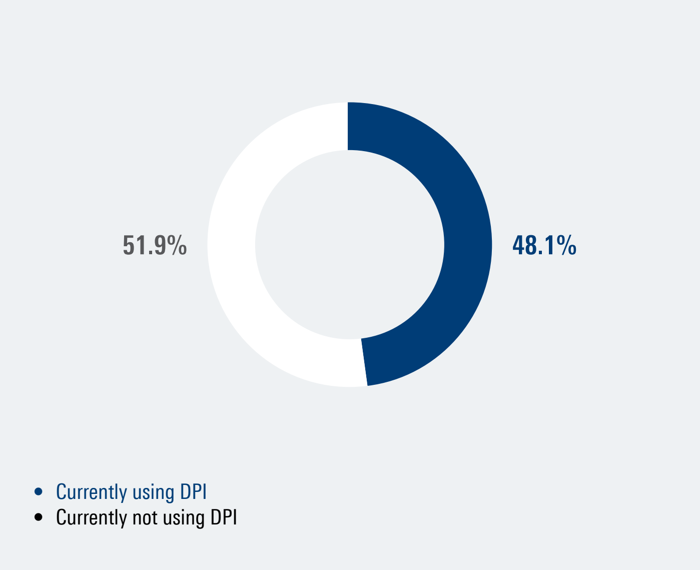
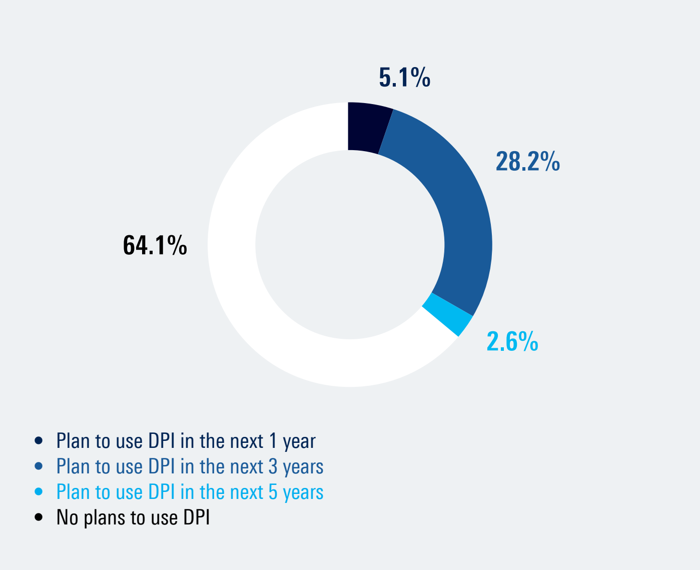


DIAGRAM 17 Adoption plans among networking vendors currently not using DPI



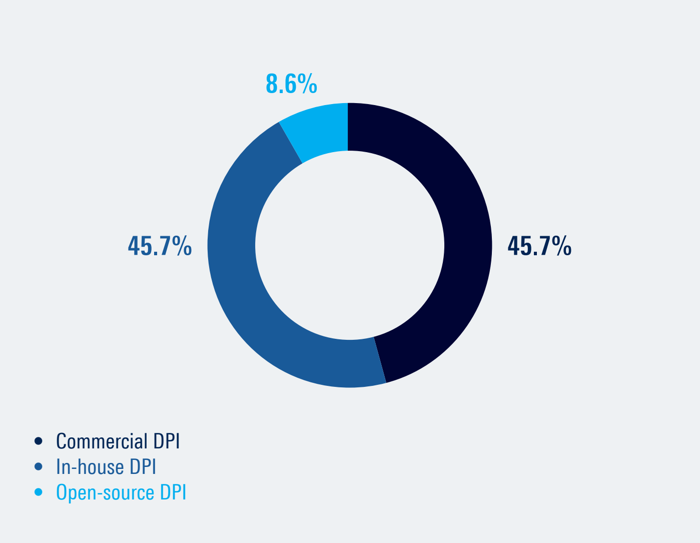
Commercial and in-house DPI two most popular deployment models in GenAI implementations

Among networking vendors already using DPI, the most popular deployment models are commercial DPI and in-house DPI, with each model accounting for 45.7% of vendors. Another deployment option is open-source DPI, but only 8.6% of vendors are currently using this model.

Commercial DPI engines are provided by DPI specialists who offer deep industry expertise and end-to-end support, from deployment to issue resolution and upgrades. These solutions allow networking vendors to focus on their core functionalities, as their analytics needs are fully addressed by a full-featured intelligence tool that has been tested and proven in many previous deployments. In contrast, in-house DPI enables network vendors to custom build and continuously adapt their DPI technology to meet evolving needs. In terms of costs, commercial DPI requires a licensing fee while in-house DPI entails development and operational costs.

Open-source DPI, despite being free of upfront costs, typically relies on the support of the maintaining organizations, user forums and third-party experts. Without adequate internal expertise, costs for customizing and maintaining an open-source-based DPI tool may be higher over the long run.

DIAGRAM 18 Networking vendors' preferred type of DPI deployment model



66.7%

of vendors expect to use DPI within the next five years

9. CONCLUSION

With traffic analytics driving the effectiveness, performance and security of GenAI-based network functions, there is an increasing focus on tools used to collect and analyze traffic flows. This is pushing the demand for next-gen traffic intelligence tools that are not only high-performant, but are capable of addressing various complexities associated with the detection and analysis of live traffic. This includes issues such as latencies, resource consumption, fragmentation, security vulnerabilities, protected data and a lack of customizability. Unaddressed, these issues can result in poor GenAI implementations and jeopardize network outcomes.

The findings of the report confirm the growing importance of advanced traffic detection tools such as DPI in fortifying traffic analytics used to support GenAI-based network functions. Key highlights from the report are summarized below:

- GenAI adoption is highest in network functions that rely heavily on real-time, continuous traffic analysis; network analytics, QoS and optimization, monitoring and automation are the most popular categories
- GenAI is expected to become an indispensable feature across network functions in the next five years; current adoption rate is close to 50%
- Network management tools, processes, and teams are expected to see notable improvements in efficiency and effectiveness with the adoption of GenAI
- GenAI's greatest expected outcomes are improvements in employee experience and enhancements in network efficiency and responsiveness
- The top three technical challenges vendors face in incorporating GenAI are security risks from GenAI-related attacks, data quality issues, and a lack of expertise to extract real value from GenAI
- The main issues impacting the quality of traffic analytics used in GenAI are inaccuracies in categorization and labeling, disparate and conflicting data, incomplete data, and privacy and confidentiality concerns
- More than half of vendors are inadequately equipped to analyze encrypted, obfuscated or anonymized traffic flows, resulting in poor packet- and application-level visibility
- Service-, protocol- and application-layer classification of traffic is critical for the majority of network functions that use GenAI
- There is strong demand for automated traffic capture tools that generate highly customized, high-quality traffic analytics for GenAI implementations
- Close to 55.0% of vendors have limited insights into how traffic conditions impact their GenAI processes
- The majority of vendors agree that they lack adequate information on how GenAI impacts network performance and resource consumption
- GenAI-related security threats affect a significant proportion of network vendors, with the most prevalent threats being those originating from users and GenAI engines
- The majority of traffic analytics tools are limited in their effectiveness in detecting GenAI-related threats
- Vendors strongly prefer built-in or integrated traffic analytics across their functions
- Scalability, timeliness and compatibility with different IT environments are among the most important requirements for a traffic analytics tool used in GenAI-based network functions
- Close to half of vendors are already using DPI and another 18.6% plan to use it in the future. The most preferred deployment models are commercial DPI and in-house DPI

These findings confirm the role of advanced traffic analytics in producing high-quality and comprehensive network information required for GenAI-based network functions. Real and predictive insights, delivered by technologies such as DPI, can significantly improve GenAI models and the accuracy of their outputs. Insights from DPI are also crucial in GenAI prompting and for assessing how GenAI workloads impact the network, and vice versa. Whether simulating a network's self-healing behavior, conducting packet loss analysis, or forecasting a WAN's traffic profile, GenAI-based network functions need every data point that can be harvested from the network.

The role of traffic analytics will become even more important as networks move towards higher levels of automation. Agentic AI, an extension of GenAI, relies on a continuous flow of real-time analytics to power virtual agents who will be running their own queries, tapping hundreds of information sources, and feeding instructions into execution pipelines. Agentic AI, along with other emerging GenAI applications, will push real-time traffic analytics to the forefront of the GenAI race. This will drive the need for tools such as next-gen DPI, which will serve as crucial building blocks for the intelligent and autonomous networks of tomorrow.

ipoque

ipoque, a Rohde & Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform data into intelligence. As a subsidiary of Rohde & Schwarz, we take advantage of potential synergies.

Rohde & Schwarz

The Rohde & Schwarz technology group develops, produces and markets innovative information and communications technology products for professional users. Rohde & Schwarz focuses on test and measurement, broadcast and media, cybersecurity, secure communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries.

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

ipoque GmbH
Augustusplatz 9 | 04109 Leipzig, Germany
Info: + 49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

Version 01.00 | August 2025
Advancing network management with Generative AI
Data without tolerance limits is not binding | Subject to change