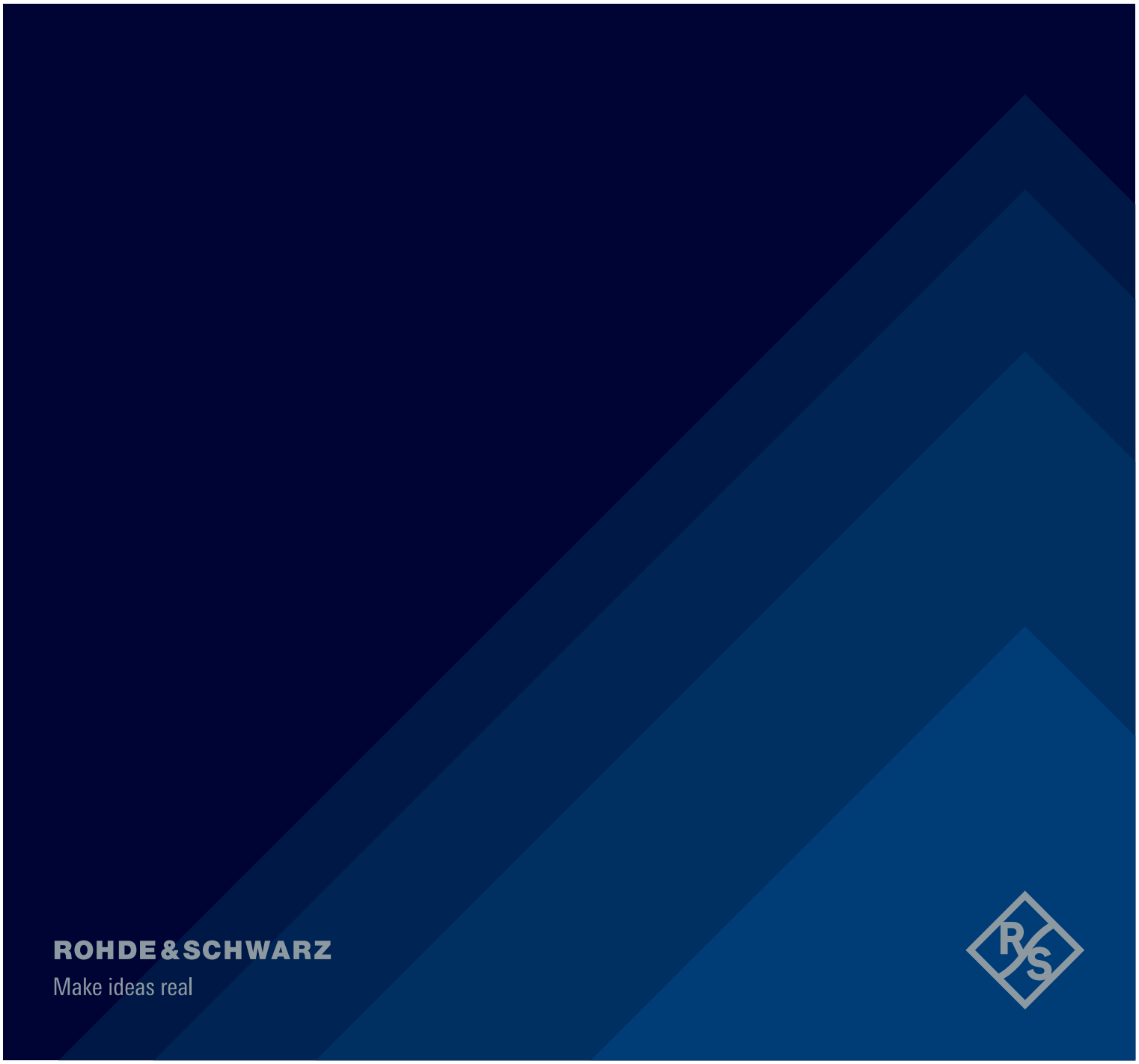
ANALYTICS AND AI IN OPEN RAN: THE ROLE OF DEEP PACKET INSPECTION

Research Report



ROHDE&SCHWARZ
Make ideas real

CONTENT

1. INTRODUCTION

The capacity and capability leaps enabled by next-gen wireless technologies, such as 5G, 5.5G and 6G, in combination with new, powerful data applications such as AR/VR gaming and V2X communications, are pushing mobile network operators (MNOs) to rethink their network architectures and operational models. This has given rise to Open RAN, a revolutionary approach that aims to improve network agility by replacing rigid architectures characterized by monolithic, single-vendor solutions with new, flexible structures that enable MNOs to respond rapidly to fast-growing traffic and application demands.

Open RAN, at its core, promotes openness. It's key tenets – virtualization, disaggregation, cloudification, multi-vendor and interoperability – are designed to enable different RAN hardware, control platforms and network functions to coexist. Open RAN brings mobile network adaptability to the next level, while improving efficiencies and performance. It also expands market opportunities for newcomers and specialist players, and fosters greater innovation.

Advanced analytics, specifically real-time traffic intelligence, are crucial to the changes introduced by Open RAN. In this regard, cutting-edge traffic detection technologies such as deep packet inspection (DPI) are indispensable in Open RAN implementations. DPI brings granular visibility into the network and propagates intelligent decision-making, thus supporting a highly-adaptive RAN architecture, comprising virtualized, cloud-hosted functions and extensive AI-driven automation. DPI data also provides transparency into new software stacks and open, standardized interfaces, while delivering insights into traffic, user and application patterns that enable MNOs to introduce innovative, custom-built features that correspond to their customer needs and experiences.

Survey: Deep packet inspection for Open RAN

Duration: 10/24-11/24

Participants: 60 networking vendors

Authors: Rohde&Schwarz and The Fast Mode

This report

This report dives deep into the topic of Open RAN and aims to assess the analytics requirements that underpin the new level of intelligence and automation it envisages. In particular, it looks at the significance of DPI-driven real-time traffic analytics in powering Open RAN's enhanced functionalities. The findings of this report are based on a survey of 60 leading Open RAN vendors that took place between October and November 2024.

To understand the role of DPI-driven real-time traffic analytics in Open RAN, the report uncovers complexities that arise from numerous independent RAN components, each built, programmed, and orchestrated individually to perform multiple tasks with different KPIs. The impact of these and other characteristics of Open RAN – including modularization, virtualization and cloud adoption – on traffic visibility needs in RAN are studied and analyzed.

Exploring Open RAN's enhanced AI and intelligence layer, the report assesses the workings of the Service and Management Orchestrator (SMO), the RAN Intelligent Controller (RIC) and emerging RAN applications, known as RAN applications (rApps) and extended applications (xApps). The functional areas supported by each of these elements are evaluated to illustrate how real-time traffic analytics enable instantaneous responses to network events and enhance AI-based automation. The role of real-time traffic analytics in fostering Open RAN use case innovations is also examined.

The report addresses the need for a traffic filtering technology that is highly scalable, fast and reliable, while also evaluating the use of next-gen deep packet inspection (DPI) in Open RAN, specifically in enriching data repositories and improving AI-driven predictive analytics. Additionally, it assesses DPI's state of adoption in Open RAN.

2. THE OPEN RAN ARCHITECTURE

The Open RAN architecture comprises various disaggregated RAN components that are connected via open interfaces. Radio antennas connect to user devices and transmit radio frequency (RF) signals while open radio units (O-RUs) filter, amplify and convert these signals into data signals.

In Open RAN, baseband functions, which involve the aggregation and processing of traffic from cell sites, are allocated between open distributed units (O-DUs) and open centralized units (O-CU) which connect to each other via a midhaul link. O-DUs process the lower layers of a RAN protocol stack, while O-CUs handle the higher layers. For example, O-DUs manage radio protocol handling, scheduling and radio signal processing while O-CUs handle session and mobility management, load balancing and QoS assurance. The Near Real-time Intelligent Controller (Near-RT RIC) controls and manages various nearreal-time processes that are executed by O-DUs and O-CUs, and is located close to these nodes.

The Near-RT RIC is controlled through the Non Real-time RAN Intelligent Controller (Non-RT RIC). The Non-RT RIC is part of the SMO platform, a software-based component that manages RAN planning, policies, operations, intelligence, optimization and conflict management. The SMO platform connects to all RAN components.

Open RAN specifications and definitions are provided by industry bodies, such as 3GPP, the O-RAN Alliance and the Small Cell Forum. These enable the standardization of various components and architectures used in Open RAN, ensuring interoperability between different vendors.

The complexities of RAN management are attributed largely to the presence of multiple vendors

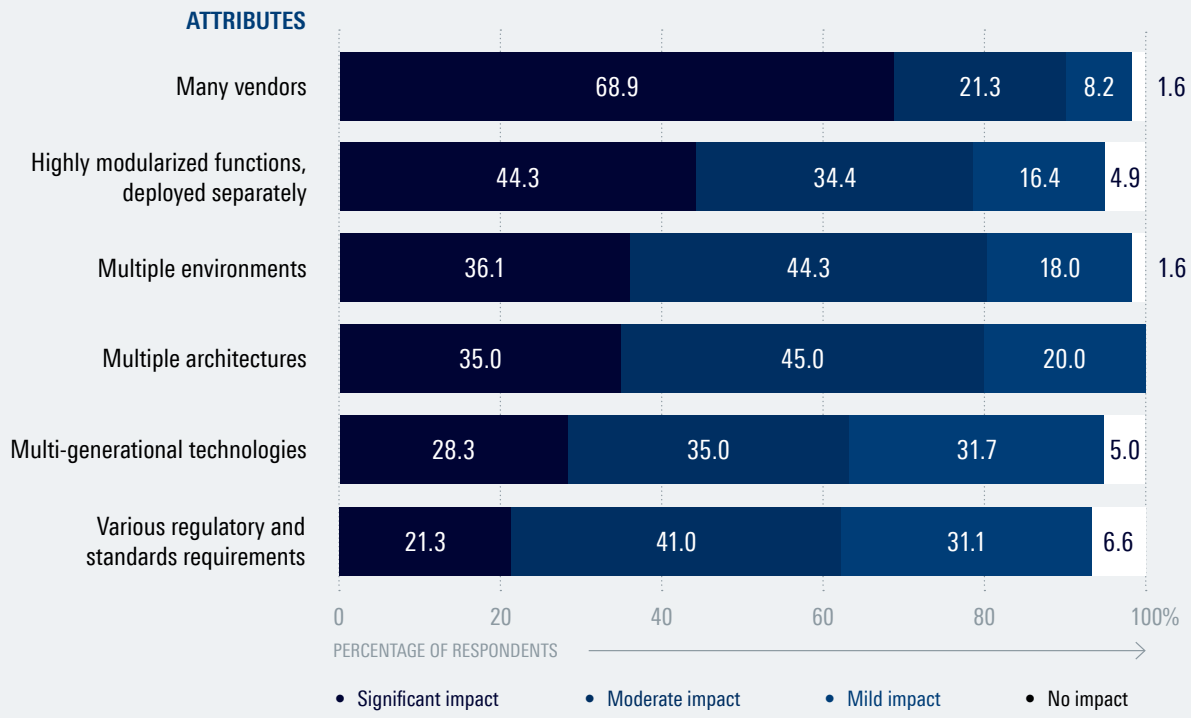
The mix of different components, vendors and processing sites introduces new complexities in managing the Open RAN network. It expands the network perimeter, and multiplies existing provisioning and management cycles and vendor interactions. It adds new compliance requirements and necessitates new domain knowledge. More importantly, it requires MNOs to consistently synchronize and monitor the interworking of hundreds of elements that run independently.

To assess the degree to which Open RAN increases RAN management complexities, vendors participating in the survey were asked to rate a number of Open RAN attributes. The presence of **many vendors** is seen as the biggest factor, with 68.9% of vendors agreeing that it has a significant impact on RAN management complexities. This is followed by **highly-modularized functions** which are deployed separately, with 44.3% of vendors expecting a significant impact.

68.9%

of vendors say that the presence of multiple vendors has a significant impact on RAN management complexities

DIAGRAM 1 Open RAN attributes and their impact on the complexities of managing RAN



Other factors are Open RAN's **multiple environments** and **multiple architectures**, with 36.1% and 35.0% of vendors respectively agreeing that these have a significant impact on RAN management complexities. These factors refer to the mix of on-site/on-premises, private cloud and public cloud/hyperscaler deployments and the co-existence of hardware-centric, virtualized and cloud-native architectures.

When it comes to **multi-generational technologies** or heterogeneous networks that include 2G, 3G, 4G and 5G, a share of 28.3% of vendors agree that they have a significant impact. **Various regulatory and standards requirements** impact RAN management complexities to a lesser extent, with only 21.3% of respondents saying that they have a significant impact.

3. TRAFFIC VISIBILITY IN OPEN RAN

To address RAN management complexities in the age of openness, MNOs need more visibility into their networks. Open RAN recognizes this fact, and incorporates a network intelligence and automation layer into its architecture. With adequate insights into the state and behaviour of the network – analytics on subscribers, devices, traffic flows, network topology and protocols – an MNO is able to autonomously and intelligently streamline its traffic flows and network components based on the network's performance, efficiency, QoS and security goals. According to the Dell Oro Group, the mobile industry's shift towards Open RAN will drive intelligence and automation, both of which heavily leverage network data.

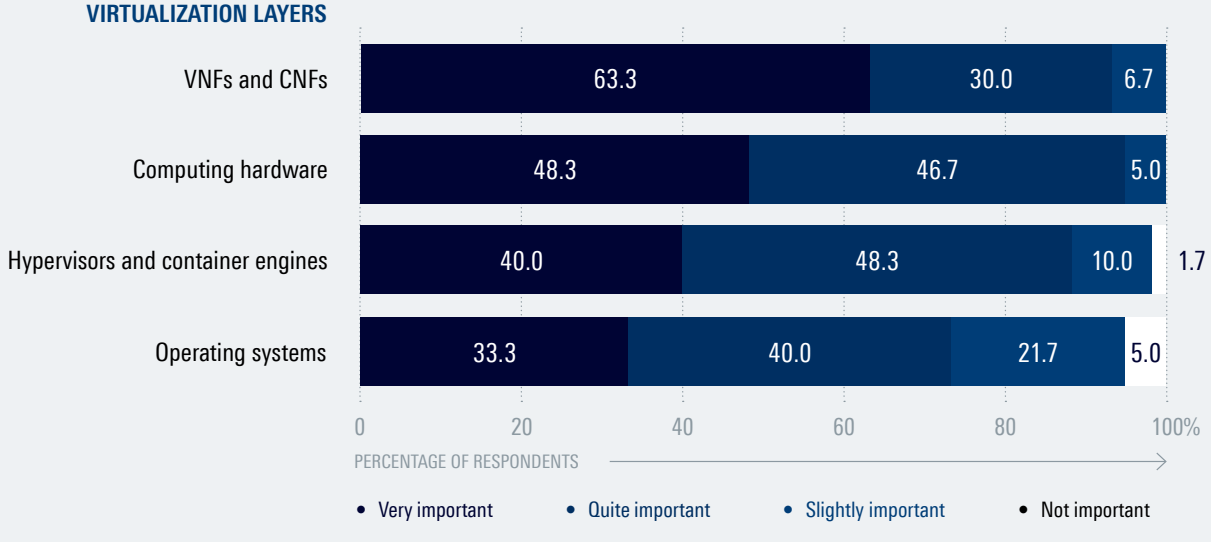
Traffic analytics

Network data comes from many sources, including network management systems where information on subscribers, network inventories and policies is stored. However, the most critical network data comes from traffic analytics, covering metrics on packets, flows, sessions, protocols, user applications, network devices, network functions and many others. This includes health and performance parameters, such as downtime, power consumption, jitter and packet loss, as well as information on traffic anomalies. Example network metrics are uplink/downlink throughputs and average admittance ratios in an O-DU, and error rates in interfaces, such as FH1, F1, E2 and A1. These metrics also include cloud-related parameters such as the CPU, memory and bandwidth used by cloud-native network functions (CNFs).

Real-time traffic analytics crucial in keeping tabs on virtualized RAN functions, according to 63.3% of vendors

Virtualization is one of the primary characteristics of Open RAN. It enables general-purpose computing hardware to host multiple RAN processes as virtualized functions which can be upgraded, added or replaced independently, based on traffic needs. Many DU and CU functions such as beam management, spectrum sensing, real-time scheduling, packet seg-

DIAGRAM 2 Importance of real-time traffic analytics in various network virtualization layers in Open RAN



mentation, and traffic analysis and classification can be completely virtualized and hosted as virtualized network functions (VNFs) or CNFs on commercial off-the-shelf servers.

Virtualization offers the flexibility and granularity needed to adapt an Open RAN network to different use cases, such as urban connectivity or private 5G. Due to a shared infrastructure, however, virtualization issues such as CPU contention, virtual machine (VM) sprawl and congestion can often occur, pushing MNOs to closely monitor the health and performance of their virtualized stacks.

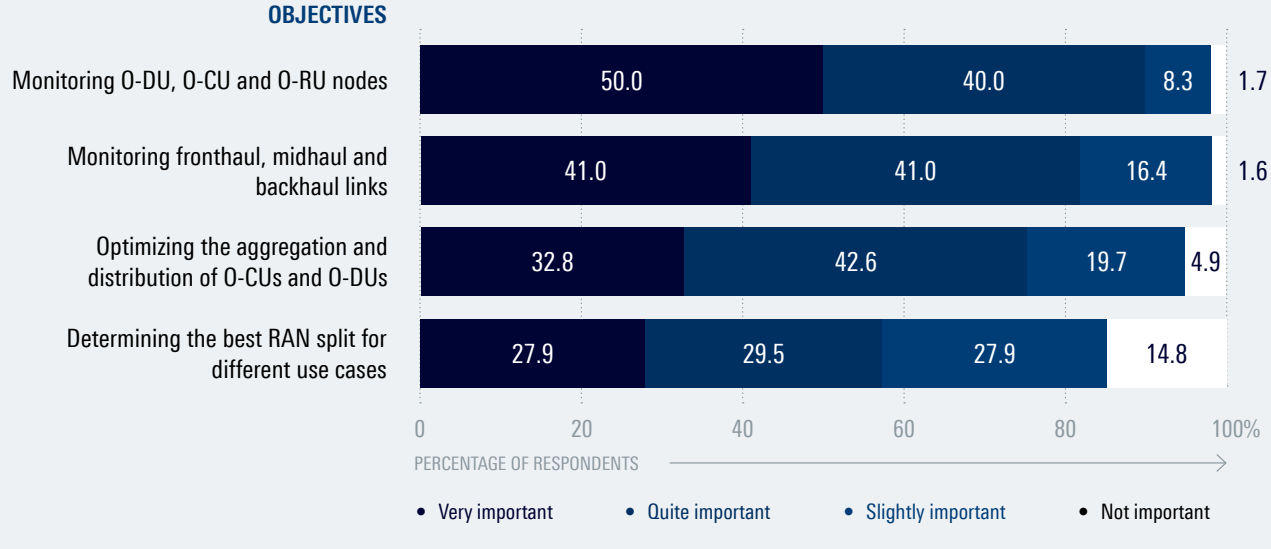
According to the survey, a majority of vendors think that real-time traffic analytics are most critical for visibility at the VNF/CNF layer, where RF and baseband processes are deployed in VMs or containers and orchestrated on their respective platforms. Computing hardware ranks second, with 48.3% of Open RAN vendors saying that traffic analytics are very important for visibility at this layer. This is followed by hypervisors and container engines whose corresponding percentage of vendors is 40.0%. For the OS layer, only a third of vendors (33.3%) feel that real-time traffic analytics play a very important role for visibility.

Monitoring requirements drive the use of real-time traffic analytics across disaggregated DU, CU and RU nodes

The RAN protocol stack comprises the following: Physical Layer (PHY), Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), Service Data Adaptation Protocol (SDAP), and Radio Resource Control (RRC).

The processing of these layers is distributed between O-RUs, O-DUs and O-CUs using RAN split options defined by industry bodies such as 3GPP and the O-RAN Alliance. Considerations such as fronthaul capacity and computing capabilities determine the optimal split. For example, in an urban use case, a low RAN split is complemented by a powerful fronthaul and high-capacity processing in O-DUs and O-CUs.

DIAGRAM 3 Importance of real-time traffic analytics in a disaggregated Open RAN architecture



Similarly, ultra low-latency (URLLC) use cases such as industrial automation and smart grids use a high RAN split so that traffic is processed closer to the user.

The survey explores the role of real-time traffic analytics in O-RUs, O-CUs and O-DUs. Half of the survey respondents (50.0%) say that real-time traffic analytics are very important for monitoring these nodes. According to 41% of respondents, real-time traffic analytics are also very important for monitoring fronthaul, midhaul and backhaul links. Continuous monitoring at both levels enables MNOs to establish the state and performance of each node and link, and mitigate issues promptly so that all radio and baseband elements remain performant, efficient and secure.

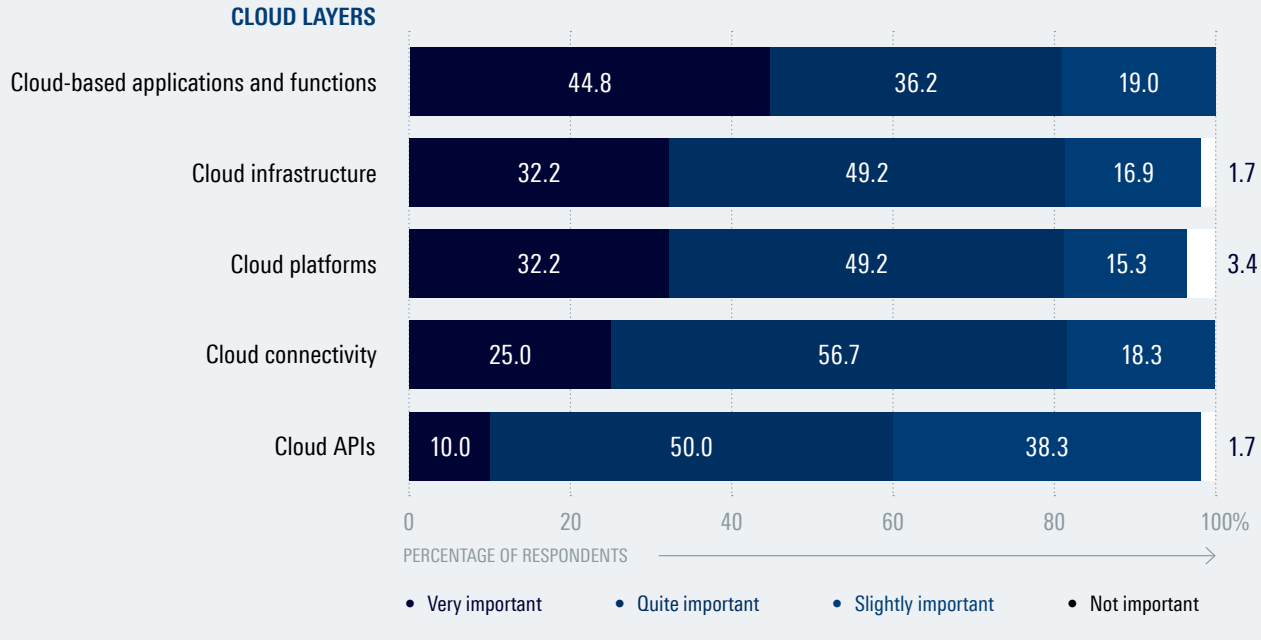
Close to a third of vendors (32.8%) agree that real-time traffic analytics are very important for optimizing the distribution of O-CUs and O-DUs, which can be located at either the cell site, the network edge or main data centers. This requires, among others, metrics on fronthaul and midhaul latencies, and computing and memory requirements.

The share of respondents who agree that real-time traffic analytics are very important for determining the best RAN split for a given use case is 27.9%. At this layer, traffic metrics such as QoS on a data voice call or latency of a remote surgery application enable an MNO to ascertain how the allocation of RAN protocol stack layers between O-RUs, O-CUs and O-DUs impact the KPIs of these use cases.

Four out of ten vendors think real-time traffic analytics play a crucial role in CNF visibility

Moving O-DUs and O-CUs to the cloud – at the network edge, in a regional data center or the main data center – enables O-DUs and O-CUs to scale up their processing capacity. It also improves RAN agility, leveraging a microservices architecture that allows new functionalities and applications to be instantiated quickly. Migration to the cloud also improves processing efficiencies as resources are abstracted on an as-needed basis, and any excess capacity can be reassigned to other functions such as AI processing.

DIAGRAM 4 Importance of real-time traffic analytics in various cloud layers in Open RAN



The move to the cloud, however, creates new challenges for MNOs. Cloud performance issues, costs, competition for shared resources, dependency on third-party infrastructure, lateral movement of threats and connectivity issues can impact RAN processes.

Real-time traffic analytics play a crucial role in managing RAN workloads in the cloud as they enable MNOs to identify capacity, performance and security issues at various layers. A total of 44.8% of Open RAN vendors find real-time traffic analytics to be very important for visibility at the cloud application or CNF layer.

At both the cloud platform and infrastructure layers, 32.2% of respondents agree that real-time traffic analytics are very important for understanding their underlying statuses. Examples of platform parameters are provisioning time and resource scaling efficiency, while examples of infrastructure metrics are computing and storage usage.

One fourth of Open RAN vendors (25.0%) see real-time traffic analytics being very important for insights into cloud connectivity. This includes metrics on WAN or direct connect links, as well as data center interconnects.

However, when it comes to observing cloud APIs, only 10.0% of vendors believe real-time traffic insights are very important.

rApps and xApps handling traffic management and security rely heavily on real-time traffic analytics

In Open RAN, the SMO-RIC combination creates an ecosystem of specialized and modularized control functions that can be deployed as a use case, or combined to create new use cases. Leveraging the SMO platform's analytics, AI capabilities and rApps, the Non-RT RIC provides insights, policies and recommendations to the Near-RT RIC. Examples of rApps are anomaly detectors, traffic predictors and energy saving applications. Insights, policies and recommendations from the Non-RT RIC are utilized by xApps which are hosted in the Near-RT RIC. xApps are used to control, optimize and automate the RAN. Examples of xApps are slice managers, RAN probes, massive MIMO optimizers and interference management applications. These applications enable MNOs to rapidly introduce innovative use cases such as automated slicing, prioritization of latency-sensitive applications and QoE monitoring for video-based services.

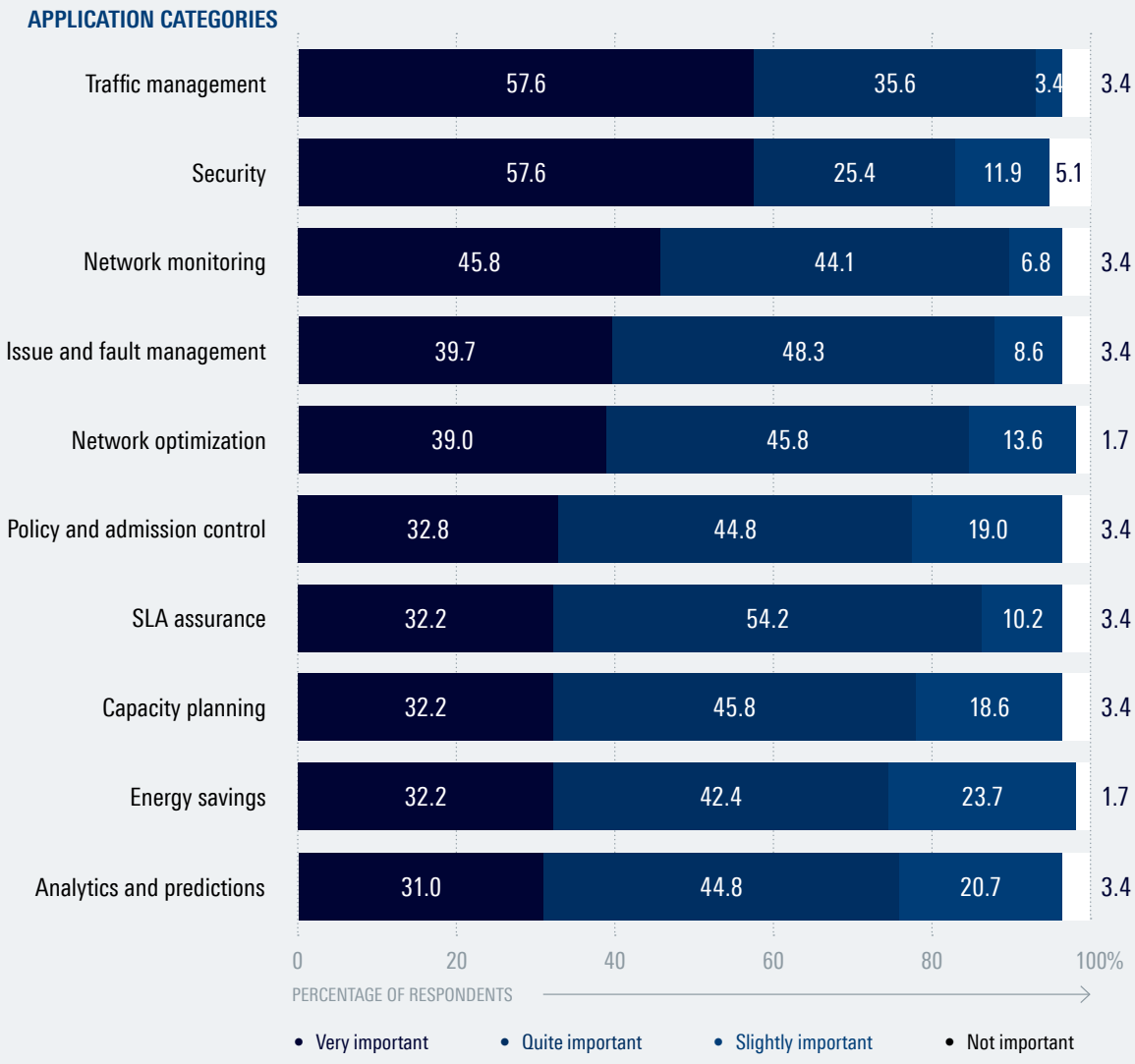
While the bulk of rApps and xApps are still being developed, the survey created a broad categorization of these apps based on common RAN management goals and assessed how real-time traffic analytics impact each category. **Traffic management** and **security** emerged as the highest-ranked categories, with 57.6% of vendors rating real-time traffic analytics as very important.

This is followed by **network monitoring**, with 45.8% agreeing that real-time traffic analytics are very important. The corresponding percentage for rApps and xApps that handle **issue and fault management** is 39.7%. For **network optimization**, 39.0% of vendors think that real-time traffic analytics are very important. The corresponding figure for **policy and admission control** is 32.8%.

57.6%

of vendors say that real-time traffic analytics are very important for traffic management rApps and xApps

DIAGRAM 5 Importance of real-time traffic analytics across different categories of xApps and rApps



For rApps and xApps that manage **SLA assurance**, **capacity planning** and **energy savings**, 32.2% of Open RAN vendors find that real-time traffic analytics play a very important role. Less than a third (31.0%) of respondents agree that real-time traffic analytics are very important for rApps and xApps that manage **analytics and predictions**. These results indicate that applications that do not handle real-time responses are less likely to rely on real-time analytics.

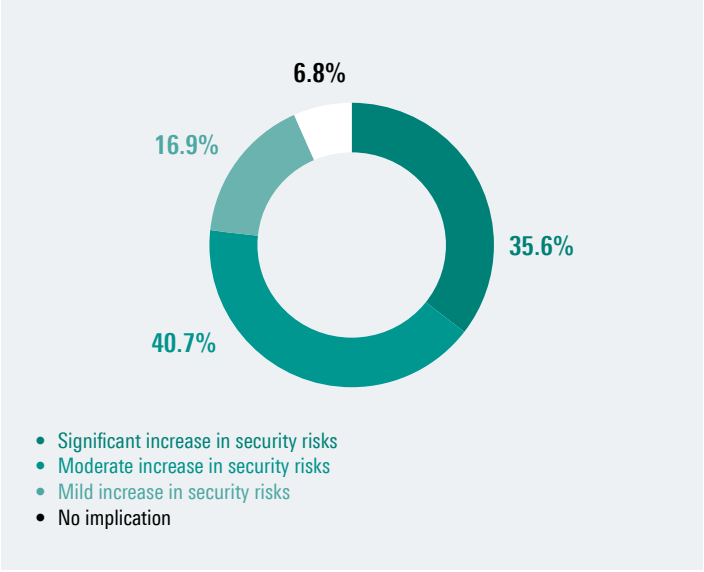
4. UNCOVERING SECURITY THREATS AND NETWORK ANOMALIES

A significant majority of Open RAN vendors agree that a multi-vendor, cloud-based disaggregated architecture increases RAN security risks

Security vulnerabilities in Open RAN are associated with a larger attack surface, arising from disaggregation of RAN workloads. Open RAN also features granular components and multi-vendor solutions, where security loopholes in any one component can affect the entire stack due to a domino effect or the lateral movement of threats, especially in the absence of micro-segmentation and zero-trust controls. The use of cloud, additionally, enables threats originating from a single cell site to affect other cell sites sharing a common traffic processing infrastructure. These factors, combined, increase an Open RAN network's susceptibility to attacks and service disruptions.

According to the survey, 35.6% of vendors believe that Open RAN's multi-vendor, cloud-based disaggregated architecture increases RAN security risks significantly, while 40.7% say that it increases RAN security risks moderately. Meanwhile, 16.9% of respondents say that the new architecture increases security risks only mildly and the remaining 6.8% of vendors think that the new architecture does not have any implication on RAN security.

DIAGRAM 6 Implications of Open RAN's multi-vendor, cloud-based disaggregated architecture on RAN security

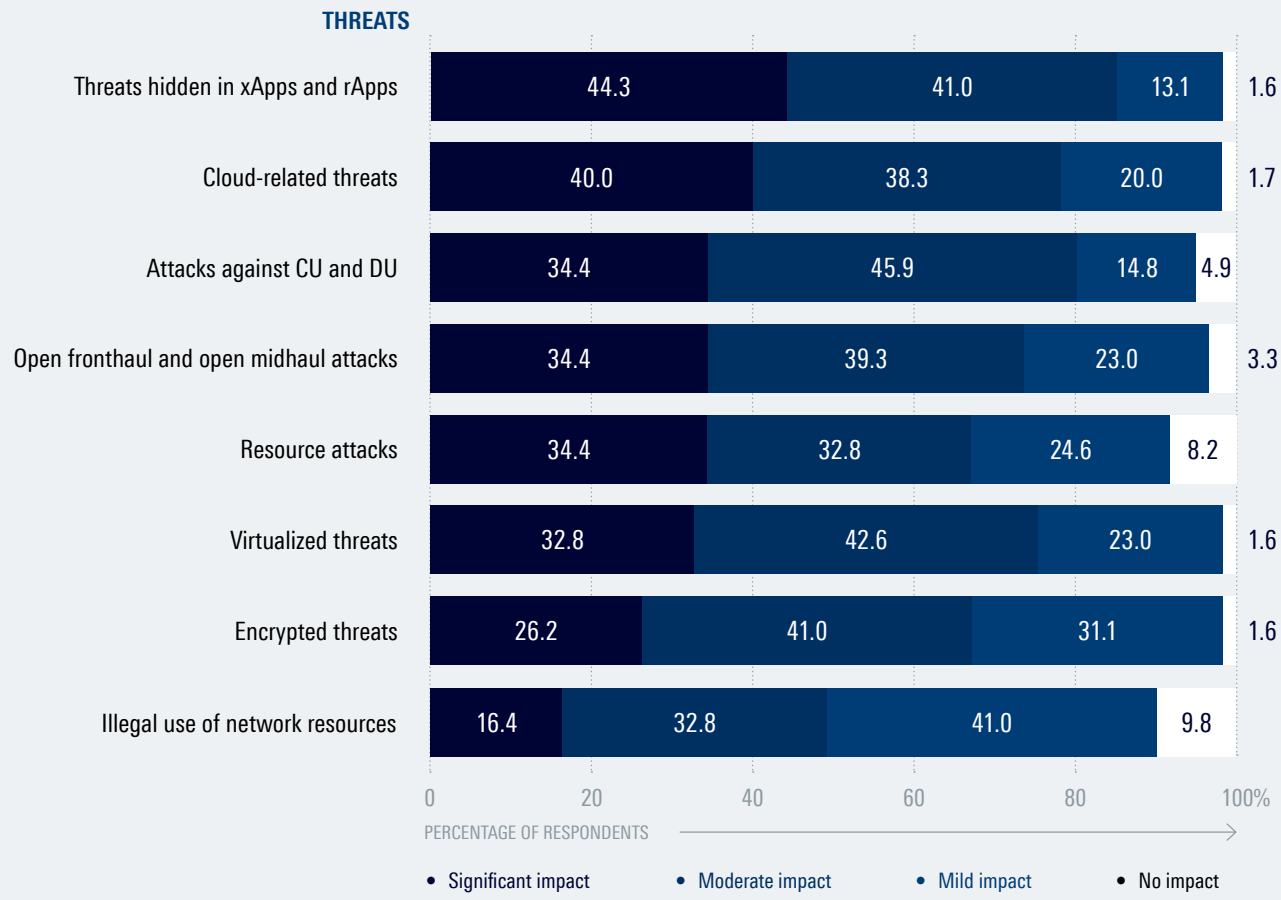


Threats hidden in xApps and rApps and cloud-related attacks pose the biggest security risks for Open RAN

The survey identified a number of attacks that are often associated with Open RAN. According to the respondents, the most serious threats are those hidden in xApps and rApps (e.g. malicious applications, code injections, misconfigurations and RMR spoofing/hijacking). About 44.3% of respondents say that the impact of these attacks on Open RAN is significant.

A similarly severe impact is expected from cloud-related threats (e.g. data breach, unauthorized access, DDoS and shared tenant attacks). The percentage of respondents who expect a significant impact from these threats is 40.0%.

DIAGRAM 7 Impact of network threats on Open RAN



When it comes to attacks against O-CUs and O-DUs (e.g. firmware attacks and unauthorized access) the percentage of vendors who see a significant impact is 34.4%. A similar share (34.4%) of respondents see a significant impact from attacks originating from an open fronthaul or an open midhaul (e.g. interception due to weak encryption schemes, poorly-defined protocols or insufficient authentication), and resource attacks (e.g. signal jamming, spectrum interference, DoS and IoT botnet).

Close to one third (32.8%) of Open RAN vendors agree that virtualized threats (e.g. container escape / cross container intrusion, virtual machine hopping, resource contention and orchestration attacks) pose a significant impact while another 26.2% say that they see a similar level of severity from encrypted threats (e.g. encrypted malware, encrypted ransomware and botnets disguised as regular traffic). For illegal use of network resources (e.g. illegal tethering and network abuse), the share of vendors who expect a significant impact is 16.4%.

Virtualized, multi-vendor xApps need the highest level of threat and anomaly monitoring

Threat and anomaly monitoring is critical in ensuring that MNOs are able to detect malicious activities in their Open RAN networks. Real-time traffic analytics and AI-based predictive analyses can equip MNOs with the insights necessary to uncover ongoing attacks and impending threats, as well as hidden vulnerabilities. Fine-grained insights can also unearth subtle irregularities that are indicative of persistent, low-key attempts to infiltrate and manipulate the network.

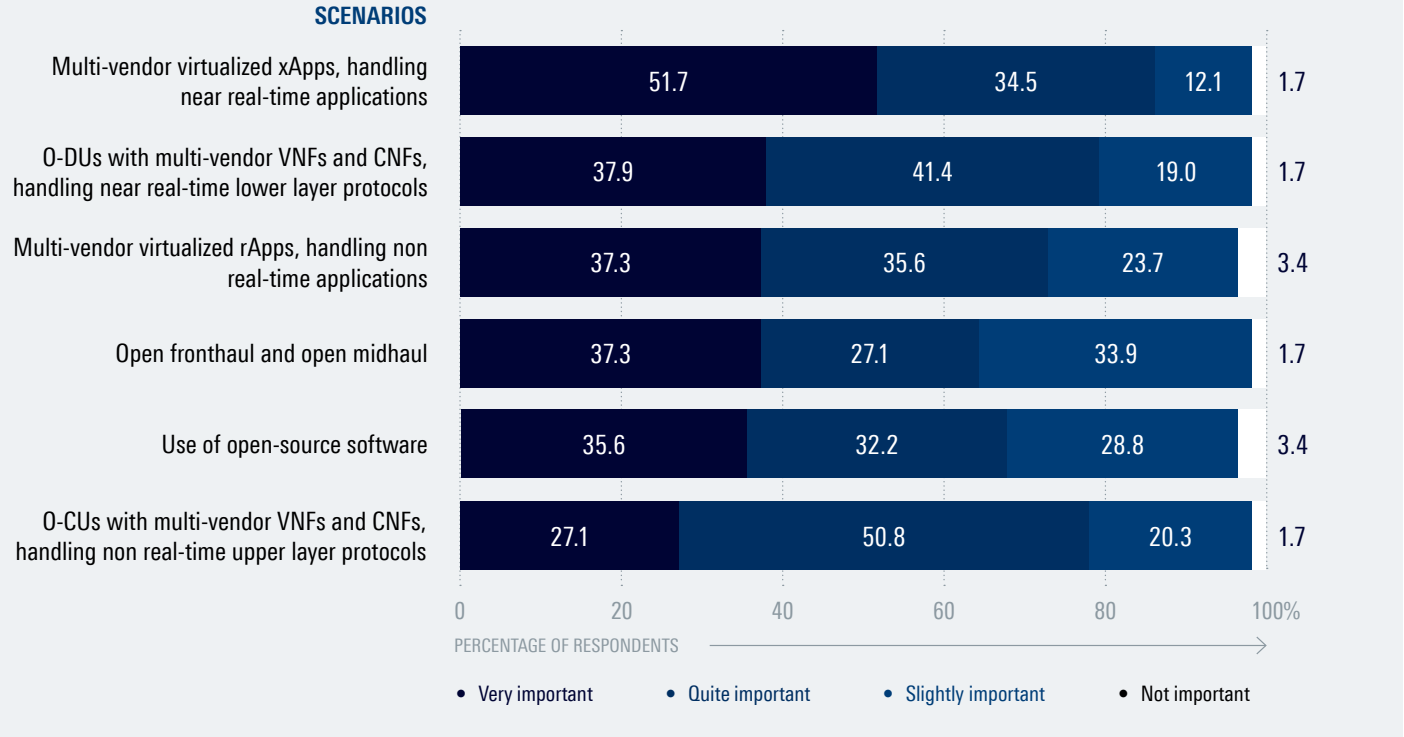
The survey respondents were asked to evaluate the importance of real-time threat and anomaly monitoring across a number of Open RAN scenarios that are regarded as high risk. **Virtualized xApps** from different vendors, handling near real-time applications (e.g. RAN slicing) are rated the highest. More than half of respondents (51.7%) agree that this is a very important scenario for real-time threat and anomaly monitoring.

The second-most critical scenario involves **O-DUs** handling near real-time processing of lower layer protocols (e.g. MAC/RLC) using VNFs and CNFs from different vendors. More than a third of respondents (37.9%) say that real-time threat and anomaly monitoring is very important in this case.

This is followed by **virtualized rApps** from different vendors handling non real-time applications (e.g. analytics and policies). The share of respondents who find real-time threat and anomaly monitoring very important in this area is 37.3%. Another scenario with the same results are **open fronthaul and midhaul links** that connect O-RUs, O-DUs and O-CUs.

Real-time threat and anomaly monitoring is also very important for **open-source software**, according to 35.6% of vendors. For **O-CUs** featuring VNFs / CNFs from different vendors and handling non-real time processing of upper layer protocols (e.g. RRC, SDAP), the share of respondents who think real-time threat and anomaly monitoring is very important is only 27.1%.

DIAGRAM 8 Importance of real-time threat and anomaly monitoring across various Open RAN scenarios



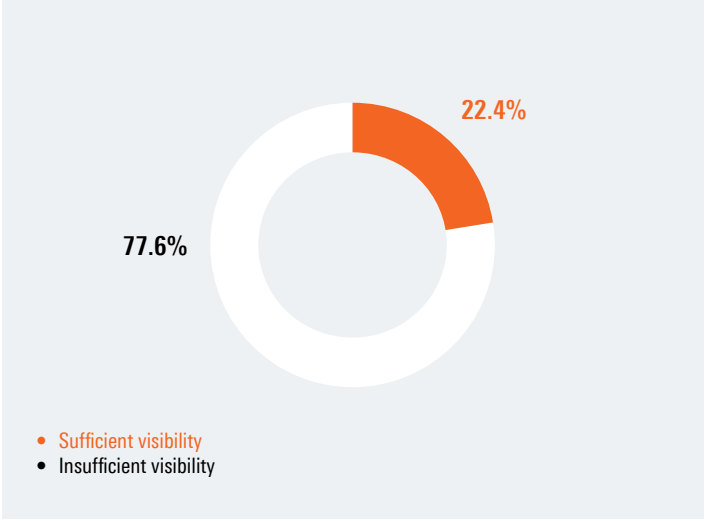
5. GAPS AND CHALLENGES

Close to 80% of MNOs lack sufficient visibility to implement ZTNA

Zero-trust network access (ZTNA) is a cloud-based framework that uses context and identity awareness for managing access control and security of network resources. ZTNA uses the concept of continuous adaptive trust to authenticate new users and ongoing sessions by verifying their unique identities and analyzing, in real time, user and traffic characteristics and behavioural attributes for a matching 'context'. ZTNA is crucial in Open RAN as it provides a robust framework for managing highly dispersed workloads that reside outside traditional network borders, for example, in the public cloud.

To establish identity and context awareness in real time, MNOs need sufficient visibility at the user, device and application layer. However, only 22.4% of survey respondents believe that MNOs have sufficient visibility at these layers, indicating a huge gap in the analytics needed in Open RAN for the adoption of ZTNA.

DIAGRAM 9 MNO readiness for ZTNA in Open RAN, in terms of user, device and application visibility

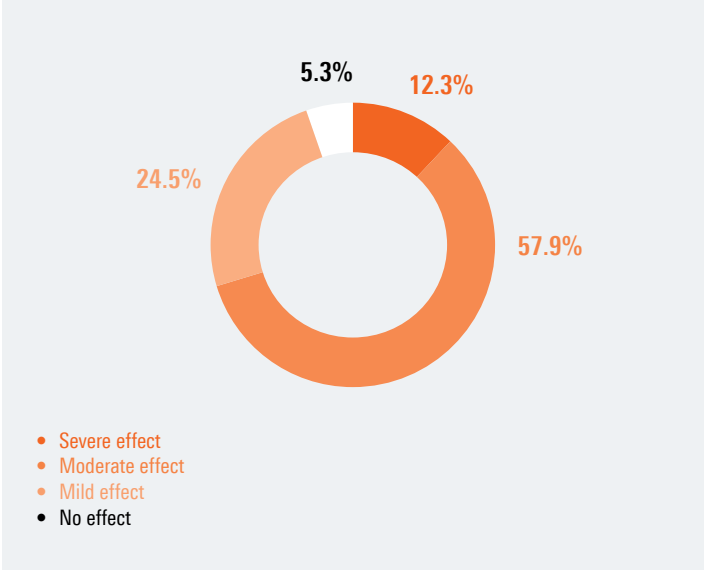


More than 70% of vendors think encryption has a severe or moderate effect on traffic monitoring and analysis

The introduction of new and stricter encryption protocols, such as TLS 1.3, ESNI, DoX and QUIC, and the widespread use of traffic obfuscation (e.g. mimicry and DNS tunneling) and anonymization (e.g. CDN and proxies) techniques remove large parts of traffic data that were previously available to RAN monitoring tools. For example, the TLS extension ECH encrypts the handshake's ClientHello, which conceals the SNI field and other metadata. Protocols like QUIC go a step further and encrypt the entire handshake, effectively hiding most connection details.

Encryption, obfuscation and anonymization techniques have a severe effect on the monitoring and analysis of traffic in Open RAN, according to 12.3% of Open RAN vendors. More than half (57.9%) of vendors agree that they have a moderate effect, while 24.5% say that the effect is mild. A small share (5.3%) of vendors say that these techniques have no effect.

DIAGRAM 10 Impact of encryption, obfuscation and anonymization on traffic monitoring and analysis in Open RAN

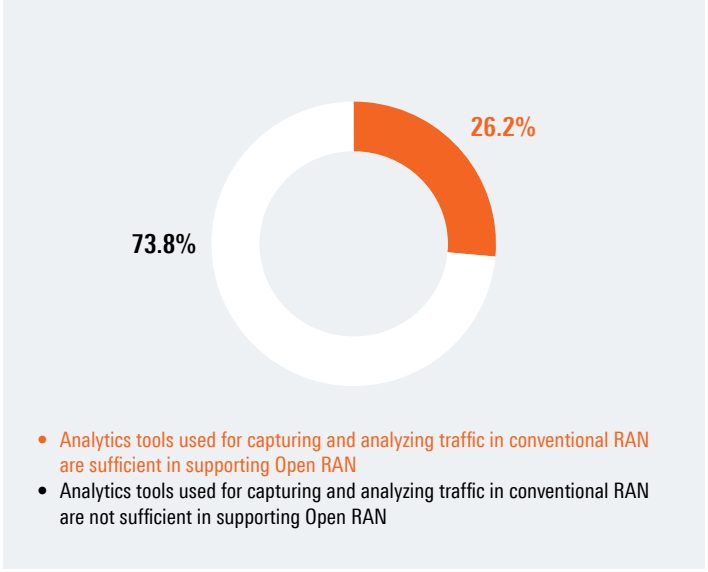


Close to 75% of vendors agree analytics tools used in conventional RAN are insufficient to support Open RAN

Open RAN necessitates broader and deeper insights into the network, compared to conventional RAN. Analytics tools must now incorporate data points from additional data centers, new edge nodes, extended network functions, multiple orchestration platforms, and novel RAN applications. These analytics must dig deeper into each session, flow, user and application so that sufficient data is available to power analytics and AI-based functionalities in the SMO platform. For xApps and time-sensitive functions in O-DUs and O-CUs, these updates must be available instantaneously to support near real-time processes.

73.8% of vendors surveyed agree that analytics tools used to capture and analyze traffic in conventional RAN are not sufficient to support Open RAN.

DIAGRAM 11 Adequacy of analytics tools used in conventional RAN in meeting Open RAN requirements



57.9%

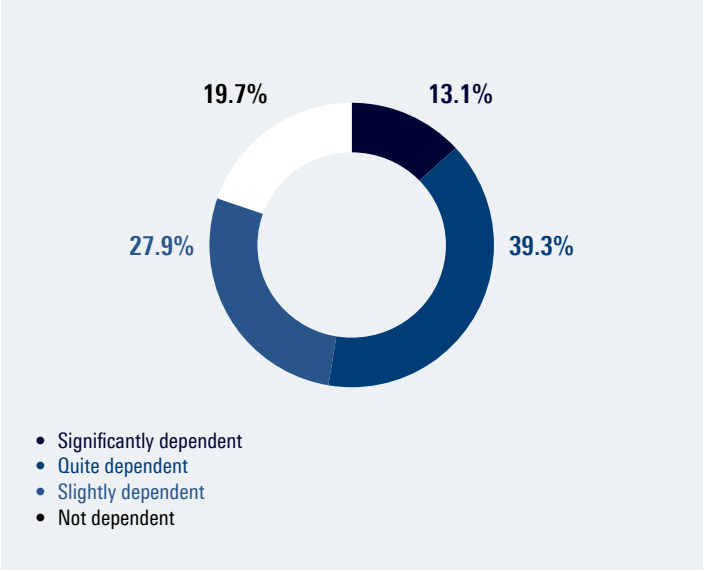
of vendors say that encryption, obfuscation and anonymization techniques have a severe effect on the monitoring and analysis of traffic in Open RAN

6. DEMAND FOR VISIBILITY AND GRANULAR INSIGHTS

More than 50% of Open RAN solutions are significantly or quite dependent on real-time traffic analytics

To assess the current use of real-time traffic intelligence in Open RAN, vendors surveyed were asked to identify the level of dependency their RAN solutions have on these analytics. Close to 13.1% of Open RAN vendors admit that their RAN solutions are depend significantly on real-time traffic analytics while another 39.3% say that their solutions are quite dependent. About 27.9% of vendors agree that there is slight dependency on real-time traffic analytics while 19.7% of vendors claim that their RAN solutions do not depend on real-time traffic analytics.

DIAGRAM 12 Dependency of vendors' RAN solutions on real-time traffic analytics



Performance metrics the most critical parameter for intelligent policies and decisions in Open RAN

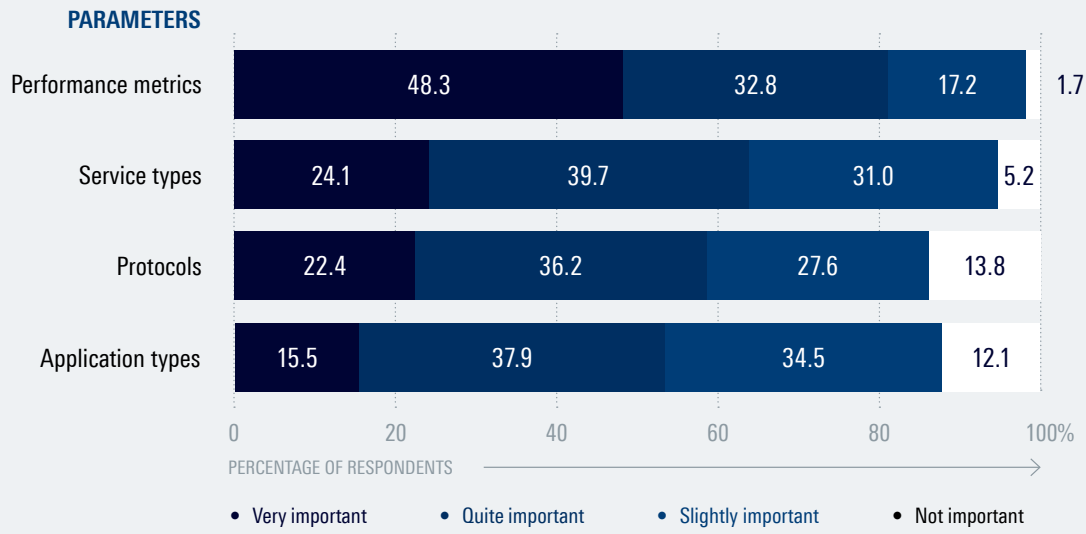
Granular traffic insights enable MNOs to implement targeted and highly contextual responses to network events where traffic-aware policies are used to manage both control and user traffic. For example, to support remote surgery applications, MNOs can introduce an xApp that automatically routes traffic to the network edge upon detecting IoT traffic carrying live video content. Likewise, at the control plane, granular insights on connection requests from a single IoT node can be used to throttle these requests once they exceed a specified threshold.

To understand the importance of granular traffic insights in Open RAN, vendors were asked to evaluate different levels of traffic awareness in enabling intelligent policies and decisions. Table 1 lists the examples of granular traffic parameters at the control and user plane.

	Control plane	User plane
Performance metrics	Speed, time-to-first-byte, packet loss, latency, jitter	
Service types	Network slicing, QoS assurance	Video streaming, email, chat
Application types	Handover signalling, connection setup	Skype, Google Cloud
Protocols	E2 application protocol, F1 application protocol	RTP, HTTPS

Table 1: Granular visibility by various traffic parameters

DIAGRAM 13 Real-time parameters required by RAN solutions to support intelligent policies and decisions



According to Open RAN vendors, real-time detection of **performance metrics** is the most critical, with close to half (48.3%) of vendors rating it as very important. This is followed by detection and classification of **service types** which is cited by 24.1% of vendors as very important. The corresponding share of vendors who rate detection and classification of traffic **protocols** as very important is 22.4%. According to 15.5% of vendors, real-time detection and classification of **application types** is very important.

48.3%

of vendors say that real-time performance metrics are critical for intelligent policies and decisions in Open RAN

7. DEEP PACKET INSPECTION FOR OPEN RAN

Recognizing the importance of traffic analytics in supporting Open RAN components and functionalities, the survey evaluates DPI's role in delivering real-time traffic detection and analysis. Deployed widely in mobile networks, DPI is an advanced technology that is able to scale rapidly to meet the visibility needs of today's Open RAN environments.

R&S®PACE 2 and R&S®vPACE

ipoque, a Rohde&Schwarz company and a leading network intelligence provider, offers advanced DPI software engines, R&S®PACE 2 and R&S®vPACE, which are highly suited for Open RAN. R&S®PACE 2 is hardware- and software-agnostic and can be deployed in virtually any networking equipment, while R&S®vPACE caters for VPP-based frameworks such as FD.io and DPDK Graph and supports VNFs / CNFs and 5G User Plane Functions (UPFs).

ipoque's DPI suite of solutions combine statistical, behavioural and heuristic analyses to classify traffic flows. This enables R&S®PACE 2 and R&S®vPACE to identify protocols (e.g. SMTP, FTP and HTTPS), applications (e.g. Microsoft Teams, YouTube and Skype) and services (e.g. chat, video call, voice call, file transfer and video streaming) in real time. Both engines also deliver analysis of malicious, suspicious and anomalous traffic.

Deployed in Open RAN, ipoque's DPI solutions bring:

- **Highly efficient, unlimited traffic analysis**
  R&S®PACE 2 and R&S®vPACE boast superfast, infinite filtering capacity that is able to support the analytical needs of even the most demanding RAN environments, including computing-intensive cloud deployments. Traffic analysis outputs from R&S®PACE 2 and R&S®vPACE enrich the SMO-RIC intelligence layer, enabling O-RUs, O-DUs and O-CUs to execute intelligent traffic-aware processes. They also enable prompt detection of performance and health issues across virtualized functions (CNFs / VNFs) and related platforms.

- **Small memory footprint**
  ipoque's DPI engines feature a small memory footprint, enabling MNOs to filter traffic flows across any node even when there is limited computing capacity, especially across O-DUs and O-CUs that are hosted at the cell site or at the network edge.

- **Granular traffic classification**
  ipoque delivers protocol-, application- and service-level classification of traffic, leveraging a weekly updated signature library that contains thousands of signatures. This equips Open RAN networks with fine-grained traffic inputs that enable MNOs to execute application-aware policies and functionalities, including custom xApps and rApps, and spur innovative use cases.

- **Real-time intelligence**
  Real-time traffic inputs from R&S®PACE 2 and R&S®vPACE support instantaneous actions, including AI-driven automated responses. This minimizes lags between trigger events and network responses, and benefits O-DUs, xApps and Near-RT RIC whose task execution times are of less than 1 second.

- **Highly accurate classification**
  Focusing on zero false positives, ipoque delivers a highly accurate analysis of the underlying traffic flows, significantly enhancing the reliability, consistency and effectiveness of data-driven decisions and AI-based predictions in Open RAN.

- **Encrypted traffic intelligence**
  ipoque's DPI suite comes with encrypted traffic intelligence (ETI). ETI combines machine learning (e.g. kNN and Decision Tree Learning) and deep learning techniques (e.g. CNN, RNN and LSTM), high-dimensional data analysis and advanced caching to classify traffic that is encrypted, obfuscated and anonymized. This enables Open RAN to address encryption techniques such as TLS 1.3 and QUIC and the growing use of CDNs and VPNs.

- **Threat awareness**
  Traffic analysis from R&S®PACE 2 and R&S®vPACE enables security tools to detect suspicious, malicious and anomalous traffic flows, even when these flows are encrypted, obfuscated or anonymized. Real-time threat awareness along with DPI's user, device and application insights enable MNOs to establish context awareness for zero-trust controls in Open RAN.

- **Automated global app coverage**
  ipoque boasts a stringent and robust quality assurance process. Its self-developed, globally deployed automation system, generates real-world traffic from hundreds of applications. These tests not only ensure its signature libraries are continuously updated – thus guaranteeing lasting insights into applications – but also produce large volumes of relevant data for AI/ML modeling.

- **Custom signatures**
  RAN vendors using R&S®PACE 2 and R&S®vPACE can easily add custom signatures based on their unique requirements. This enables MNOs to fine-tune their analytics to support granular policies, for example, policies aimed at improving latencies across V2X applications.

- **First packet classification**
  For applications that require ultra-low latencies, ipoque's first packet classification cuts traffic classification delays and significantly speeds up RAN processes that depend on classification data.

- **R&S flow data exporter plug-in**
  The R&S flow data exporter plug-in translates flow information collected by R&S®PACE 2 into IPFIX records, ensuring interoperability between multi-vendor components in Open RAN.

- **Superior service and support**
  ipoque offers 24/7 technical service and support, both online and on-site. Customers benefit from dedicated and highly specialized teams that provide integration support, hands-on trainings, system performance optimization, and remote consulting and assistance.

DPI's role in Open RAN

DPI's comprehensive, granular, real-time traffic intelligence plays a critical role in supporting Open RAN's goals such as:

1

Disaggregation of baseband functions

- Given its small footprint, DPI can be deployed in multiple points, providing end-to-end comprehensive visibility across a disaggregated architecture.
- The performance metrics on O-RUs, O-DUs and O-CUs, and the fronthaul and midhaul links can help MNOs determine the optimal RAN split.
- DPI data on control layer links (e.g. E2 and A1) can help MNOs ascertain if there are any latency issues.

2

Modularity

- DPI's granular traffic analytics can be used to identify performance and health metrics of any element – an entire node, hardware, software or an instance – without the need for multiple analytics engines. As DPI analysis is highly customizable to the needs of any network function, it addresses the fragmentation of traffic monitoring and reporting in Open RAN's highly modularized architecture.
- DPI is important in conflict resolution where its analyses of network parameters and traffic anomalies can be used to resolve conflicts between components, for example between two xApps with different KPIs.

3

Programmability

- DPI's real-time performance and security insights enable MNOs to handle software-layer complexities arising from Open RAN, particularly issues relating to VNFs and CNFs. Data on response times of each new xApp and rApp, and the impact of a new VM or container on traffic latency, for example, help MNOs fine-tune these components.
- As highly optimized software, DPI can be integrated seamlessly into software-driven RAN environments.

4

Cloudification

- High-performance DPI engines can be scaled rapidly to meet traffic filtering requirements in cloud-hosted O-DUs and O-CUs, and come with native VPP support to perform even better.
- DPI's insights enrich the SMO-RIC layer with extended analytics on cloud components such as the performance of containers and CNFs.

5

AI-based automation and predictive analytics

- ipoque's DPI technology enriches AI models with high-quality training and test data, leading to superior model/relationship parameters. This enhances an SMO platform's predictive analytics, which improves its recommendations and instructions.

6

A multi-vendor environment

- A multi-vendor environment can benefit from DPI's shared intelligence. DPI analysis can be exported into IPFIX records, ensuring interoperability between multi-vendor components in Open RAN. This reduces redundancies, and ensures policy consistency across RAN components from different vendors.
- DPI analytics on performance and resource usage enable MNOs to trim network functions, especially duplicated features across vendors.

7

Interoperability

- Standardized and Open APIs are critical to Open RAN. However, issues at the API layer can disrupt the entire network and impair the interoperability between components. By analyzing API communications, DPI can detect these issues in real time. For example, issues with xApps can be identified by monitoring its API communications with the RIC message router.

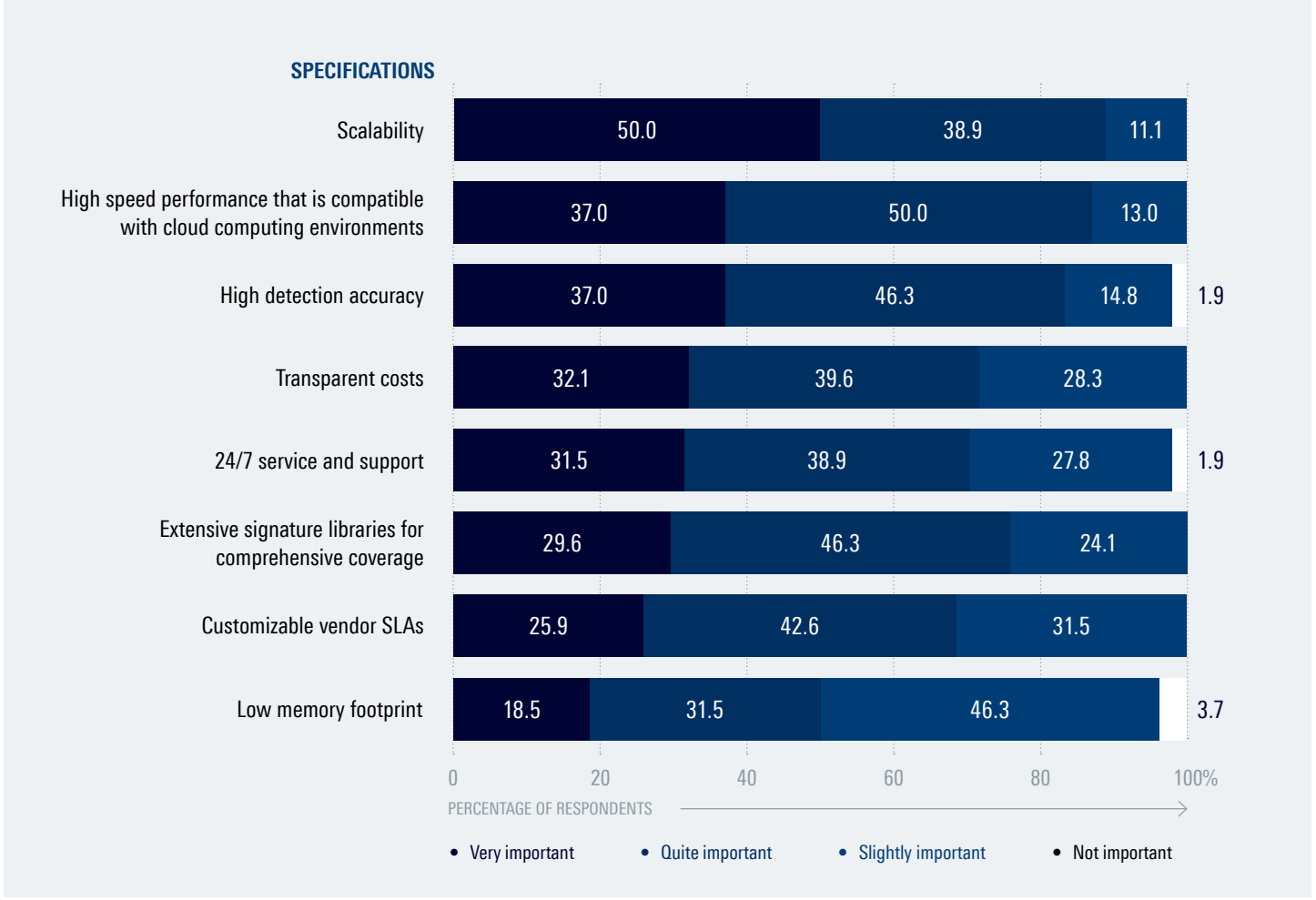
Scalability and cloud-grade performance most important specifications for DPI solutions deployed in Open RAN

To cater to Open RAN requirements and to support RAN workloads effectively, while ensuring that its own processes do not increase latencies or overheads in RAN, a DPI tool must fulfil a number of criteria. Open RAN vendors participating in the survey were asked to rate a number of DPI specifications that are deemed important for its use in Open RAN. Based on the results, **scalability** emerged as the most important criterion. Half (50.0%) of respondents say that this characteristic is very important. The next two highest rated criteria are **high speed performance** that is compatible with cloud computing environments, and **high detection accuracy** with virtually zero false positives, with 37% of respondents rating both aspects as very important.

These are followed by **transparent costs**, and **24/7 service and support** from a DPI vendor, which register with 32.1% and 31.5% respectively. **Extensive signature libraries** that provide comprehensive coverage are another consideration. Close to one third (29.6%) of respondents agree that this is a very important specification for DPI that is used for Open RAN.

More than a quarter (25.9%) of vendors feel that **customizable vendor SLAs** are very important. However, the corresponding figure for a **low memory footprint** is only 18.5%.

DIAGRAM 14 Specifications required for a DPI solution in Open RAN



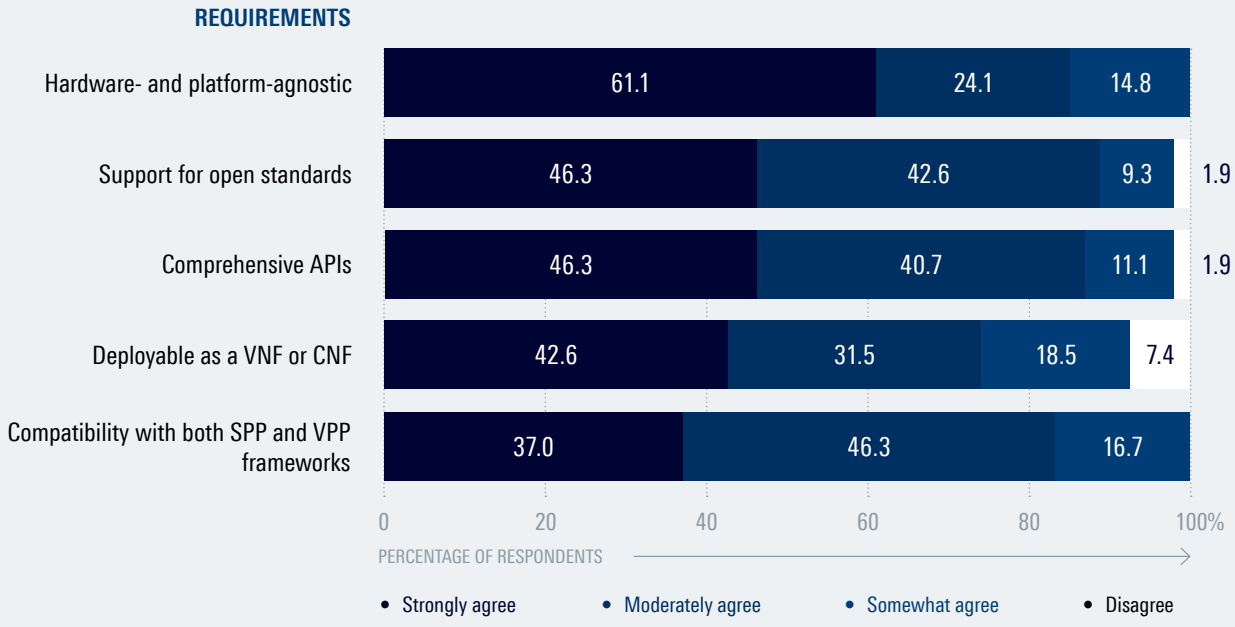
To be interoperable, DPI must be hardware- and platform-agnostic

The survey assessed a number of attributes that determine DPI's interoperability. The highest ranked attribute was a DPI tool being **hardware- and platform-agnostic** with 61.1% of vendors strongly agreeing that it is a crucial feature.

Support for open standards (e.g. IPFIX, JSON) is also deemed very important, with 46.3% of vendors saying that they strongly agree that this criteria is a must for DPI's interoperability. An equal percentage (46.3%) of vendors admit the same for **comprehensive APIs**.

A total of 42.6% of Open RAN vendors strongly agree that DPI should be **deployable as a VNF or CNF**. In the meantime, 37.0% of vendors strongly agree that DPI should be **compatible with both SPP and vector packet processing (VPP)** frameworks (e.g. FD.io, DPDK Graph and RF_Ping) to be deemed interoperable.

DIAGRAM 15 Interoperability requirements for a DPI solution in Open RAN



More than 42% of Open RAN vendors will be using DPI by 2027.

The survey results show that 13.0% of Open RAN vendors are already using DPI, while 11.1% are planning to use it within the next year. Another 18.5% of vendors are planning to use it in the next 3 years. In the meantime, 35.2% of vendors say that they might use it sometime in the future, while the remaining 22.2% say that they do not foresee using DPI.

Most Open RAN vendors prefer commercial DPI

In terms of deployment models, Open RAN vendors show a strong preference for commercial DPI solutions, with 42.8% of vendors opting for this model. Commercial DPI solutions typically provide rich features and superior support. An equally compelling model is open-source DPI, which was selected by 40.5% of vendors. Open-source DPI involves no upfront costs. However, extensive customization and a lack of support can be a drawback. A share of 16.7% of vendors say that they prefer in-house DPI. In-house DPI is suited for vendors with internal expertise in DPI. However it requires continuous maintenance and often has limited features.

DIAGRAM 16 Current state of DPI deployment in RAN solutions

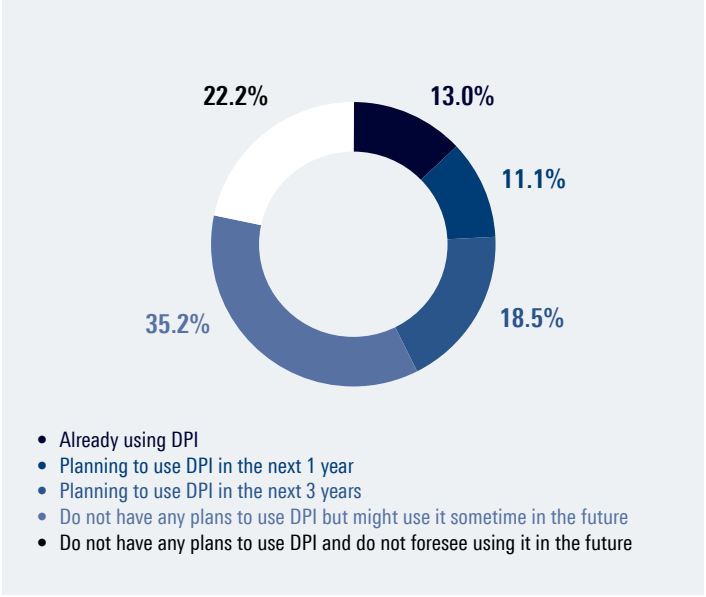
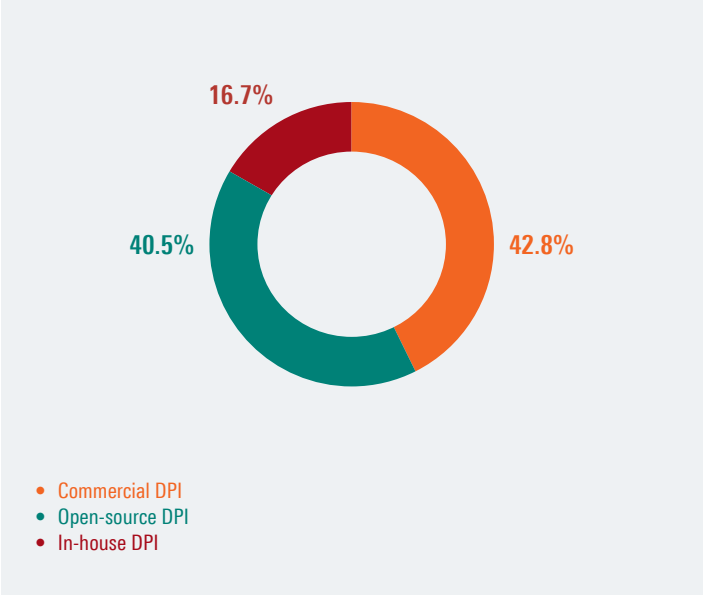


DIAGRAM 17 Preferred DPI deployment models in Open RAN



8. CONCLUSION

The shift to openness has many implications on RAN's analytics needs. Functionalities that were previously integrated in a 'black box' are now separated and exposed, making them visible, measurable and accessible. The expanse of the network has grown substantially, along with its attack surface. All these changes happen at a time when the adoption of more complex architectures, such as cloud-native architectures, is becoming more prevalent, and when traffic volumes continue to record new peaks.

These rapid developments translate to exponential growth in network data, from information on user applications and services, to health and performance metrics of networking devices, network functions and computing instances. It has also pushed data to the forefront of network management, where analytics and AI capabilities now power a majority of network processes.

The results of the survey illustrate how various architectural attributes of Open RAN drive the need for real-time traffic visibility, and how advanced traffic visibility tools such as DPI close these gaps. Findings from the report show that:

- RAN management complexities arise largely from the presence of multiple vendors and use of highly modularized components.
- Vendors believe that visibility into VNF/CNF and hardware layers is critical in managing virtualized Open RAN workloads.
- Monitoring requirements drive the use of real-time traffic analytics across disaggregated RAN components and links.
- Application or CNF/VNF layer metrics and platform layer information are critical for overseeing RAN processes in the cloud.
- Some functional classes of rApps and xApps, namely traffic management and security, rely on real-time traffic analytics considerably more than others.
- A large majority of vendors agree that a multi-vendor, cloud-based, disaggregated architecture increases RAN security risks. The most severe among these are threats hidden in xApps and rApps, and cloud-related threats.
- Threat and anomaly monitoring becomes critical when various Open RAN attributes are combined. The most critical scenario involves virtualized xApps from multiple vendors handling real-time applications.
- MNOs do not have adequate visibility at the user, device and application layer to deliver the 'identity and device context' needed for zero-trust implementations.
- Loss of visibility from new encryption techniques continue to affect the monitoring and analysis of traffic.
- Analytics tools used in conventional RAN remain inadequate in Open RAN.
- Open RAN solutions have a high dependency on real-time traffic intelligence.
- Fine-grained performance-related traffic metrics emerge as the most critical inputs for powering intelligent policies and decisions.
- A DPI tool deployed for Open RAN must be scalable, high-performant, cloud-compatible and accurate.
- To be interoperable, DPI must be hardware-agnostic and platform-agnostic, support open standards and provide comprehensive APIs.
- Rapid growth in DPI adoption in Open RAN is expected in the next 3 years. While commercial DPI solutions are still the most preferred among Open RAN vendors, there is strong traction for open-source DPI.

The reliance on real-time advanced traffic insights will become pivotal as openness continues to shape mobile ecosystems. In an Open RAN network, real-time traffic insights will deliver the transparency needed to evaluate, control and streamline hundreds of elements, while proactively addressing traffic and user needs. Traffic analytics will become even more crucial as AI-based autonomous networks decide how resources are allocated, traffic is managed and threats are handled. These insights will also underpin the adoption of GenAI-based network management, as GenAI outputs can only be as accurate as the data it learns from.

At the same time, analytics tools such as next-gen DPI are making huge leaps in the mobile traffic detection space, ensuring Open RAN — particularly its intelligence layer — has continuous access to every data point in the network. This allows MNOs to improve their real-time responses and predictive capabilities. It also ensures that a multi-vendor, multi-technology and multi-environment RAN operates harmoniously and delivers unparalleled performance and experience.

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 is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test&measurement, technology systems and networks&cybersecurity. Founded 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

The Fast Mode
The Fast Mode is a leading independent research and media brand, delivering breaking news, analysis and insights for the global IT/telecommunications sector. With a global reach spanning millions of readers annually, The Fast Mode partners with global technology companies to publish breakthrough ideas, critical analysis and latest updates on initiatives in the IT and telecoms space, focusing on IP/optical connectivity, network intelligence, security, cloud, internet of everything, CX and digital services.

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

The Fast Mode
Info: +60 12 2016 186
Email: admin@thefastmode.com
www.thefastmode.com

Version 01.00 | February 2025
Analytics and AI in Open RAN: The role of deep packet inspection