DEEP PACKET INSPECTION AND ENCRYPTED TRAFFIC VISIBILITY FOR IP NETWORKS

Research Report

ROHDE&SCHWARZ

Make ideas real

CONTENT

1. INTRODUCTION

Encryption refers to the use of cipher suites and special keys to encode data. It ensures the privacy and confidentiality of data as it is transported within the network and between users.

The evolution in encryption methodologies has led to remarkable improvements in data security, pushing for its widespread use across networks and applications. However, as more and more traffic flows become encrypted, network administrators lose the required visibility to effectively and intelligently manage their networks.

About DPI

Deep packet inspection (DPI) is a key network functionality that network administrators rely on to deliver packet, flow and application level insights across IP networks. DPI supports a wide range of traffic processing tools, such as firewalls and IP probes, supplying real-time network analysis that helps in routing, filtering, securing and managing traffic flows. DPI's traditional traffic classification techniques can combine pattern matching with advanced statistical, heuristic and behavioral analysis and leverage extensive traffic signature libraries.

DPI vs. encrypted traffic

Over time, there has been an increasing debate about the efficacy of DPI in managing encrypted traffic flows. Encryption renders traditional DPI techniques partly ineffective, as payload information is secured by complex algorithms, obscuring the identity of the underlying applications. This debate has intensified in recent years, especially with the introduction of newer encryption protocols such as TLS 1.3 and ESNI, which severely limit the information that is available to DPI tools.

This research report is aimed at investigating the effect encryption has on network management and the evolution of DPI to address the visibility loss from newer encryption protocols. To do so, this document first assesses the extent to which visibility loss is a concern among networking vendors who rely on deep traffic analytics. The report focuses on five key functionalities, namely: security, analytics, network performance management, policy control and traffic management. It also looks at the impact of visibility loss on long-term network outcomes.

The research evaluates the most commonly used techniques for analyzing and understanding encrypted traffic, based on approaches adopted by the vendors. These techniques include SSL / TLS inspection, statistical / behavioral / heuristic analysis and machine learning (ML) / deep learning (DL).

Based on the strengths and limitations of each of the techniques above, this report identifies the requirements among vendors for a network intelligence tool that is capable of analyzing encrypted traffic. In particular, it assesses the demand for next-generation DPI, which combines conventional DPI techniques with cutting-edge ML / DL methodologies to enable encrypted traffic intelligence. The report also presents findings on vendor preferences in terms of types and deployment models for such DPI solutions.

The survey

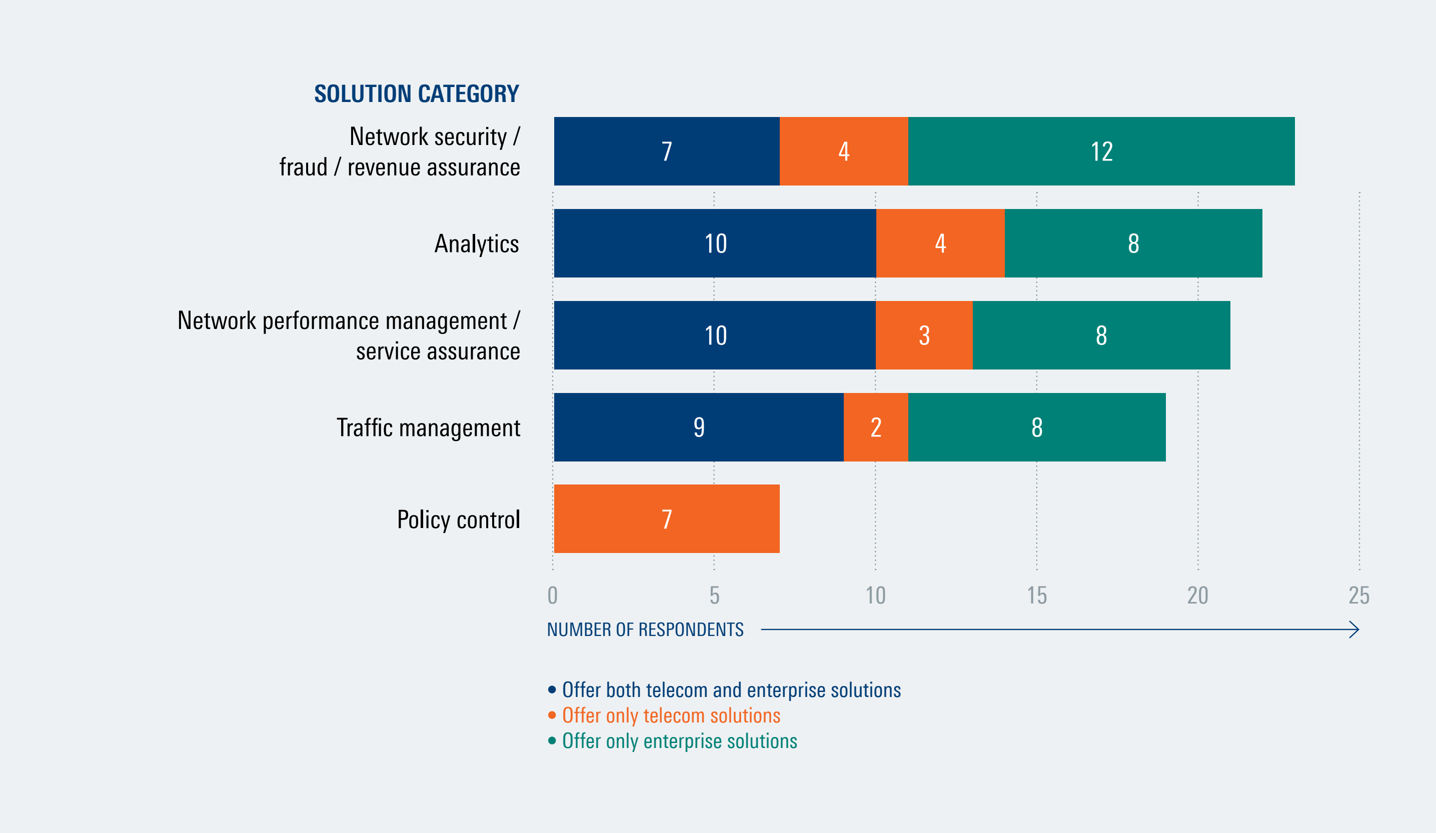
This research report is based on a joint industry survey, conducted by ipoque, a Rohde&Schwarz company and a market leader in next-gen DPI software as well as The Fast Mode, a leading telecoms / IT publication. The survey took place from October to December 2022 and 34 top-tier networking vendors participated.

Diagram 1 summarizes the profiles of the participating vendors in terms of their solution focus. Security / fraud / revenue assurance solutions were offered by 23 respondents, analytics solutions were offered by 22 respondents and network performance management / service assurance solutions were offered by 21 vendors. Traffic management solutions were offered by 19 of the vendors while policy control solutions were offered by seven of the vendors. The offers span three categories with enterprise-only and combination markets taking up a higher share compared to telecoms-only.

Survey: DPI and encrypted traffic visibility

Duration:	10/22-12/22
Participants:	34 networking vendors
Authors:	Rohde&Schwarz and The Fast Mode

DIAGRAM 1 Survey respondents' solution category



2. RISE OF NEW ENCRYPTION PROTOCOLS

Networking vendors highly aware of new encryption protocols

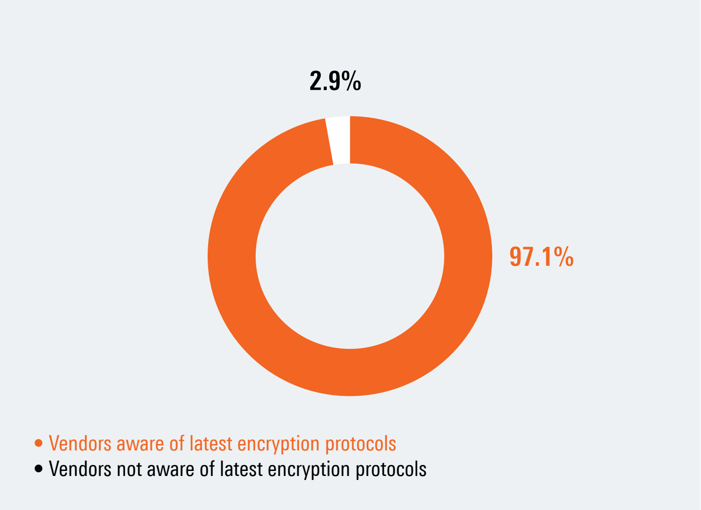
The widespread usage of encryption across networks has obliged vendors and service providers to know about the latest and most secure protocols. Public browsers, for example Google, report that 95.0% of the traffic is encrypted[1]. Leading technology research company, Gartner predicts that a heavier emphasis on cybersecurity philosophies, such as zero trust, has and will continue to make encryption a critical part of enterprises' security strategy[2].

The prevalent use of encryption across traffic flows and applications has led to the emergence of new and more complex protocols such as TLS 1.3, DNS-over-HTTPs, DNS-over-TLS and IPsec tunneling. They involve tighter, more advanced and rigorous techniques of concealing packet and traffic data.

Assessing the degree to which networking vendors are familiar with new forms of encryption, the survey found that a vast majority of respondents is aware of these protocols: 97.1% acknowledged them, and only 2.9% stated that they are unaware of these protocols and their usage in network security. These high awareness levels can be attributed to the rising security and privacy concerns as networks become increasingly distributed and remotely accessible. They also manage a growing number of third party SaaS and cloud applications and adopt complex architectures, such as microservices, which collectively increase the attack surfaces and security vulnerabilities of an enterprise.

Mitigation of these concerns with advanced security frameworks, such as NIST and ISO 27001, requires in-depth knowhow and expertise of the latest encryption protocols, among network vendors and operators alike.

DIAGRAM 2 Awareness of latest encryption protocols



[1] "Google Transparency Report." Google, Jan. 2023, transparencyreport.google.com/https/overview
[2] "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23." Gartner, June 2022, www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

Cloud security, remote working and traffic authentication to benefit the most

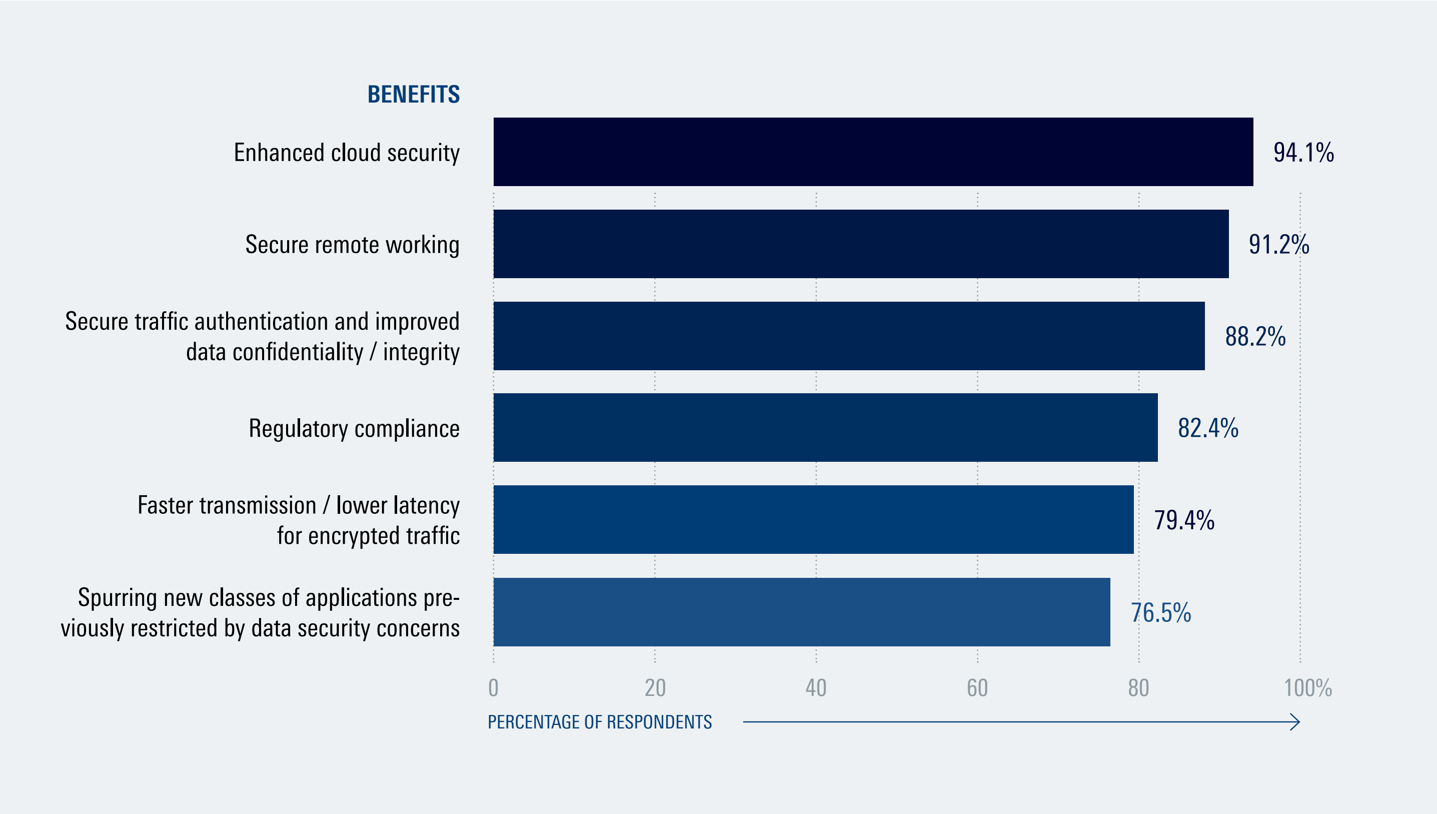
The benefits of new encryption protocols span a number of network use cases. Enhanced cloud security was selected by almost all networking vendors, with 94.1% of respondents identifying it as a key benefit of using the latest encryption protocols.

Enabling secure remote working is the second most identified benefit, with a total of 91.2% of respondents considering it a direct advantage.

Other perceived benefits of using the latest encryption protocols include securing traffic authentication and improving data confidentiality / integrity, as chosen by 88.2% of respondents; followed by aid in regulatory compliance (82.4%), faster transmission / lower latency for encrypted data (79.4%) and the ability to spur new classes of applications, previously restricted by data security concerns (76.5%).

These findings indicate the vulnerabilities and concerns that are rapidly pushing the evolution of new encryption protocols. For instance, cloud networking protection, as a whole, is a continuously growing priority for enterprises, with public cloud-based services spending expected to grow by 20.7% in 2023, according to Gartner[3]. Hybrid and public cloud networks can pose serious monitoring challenges due to their distributed nature. Also, their reliance on public channels for access leads to an increased attack surface. This makes them vulnerable to DDoS attacks and authentication fraud.

DIAGRAM 3 Use cases benefiting from latest encryption protocols



[3] "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023." Gartner, Oct. 2022, www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

Remote working, which skyrocketed during and after the pandemic, has also made enterprises more vulnerable to security attacks. Related risks include the use of third-party unsecured connectivity such as public and private WiFi channels for access, compromised personal devices and undetected account takeovers. Encrypted virtual tunnels in VPNs, for example, enable enterprises to obscure data-in-transit from outsiders and control access to enterprise, cloud and SaaS applications. Encryption also protects data-at-rest in the event of an intrusion.

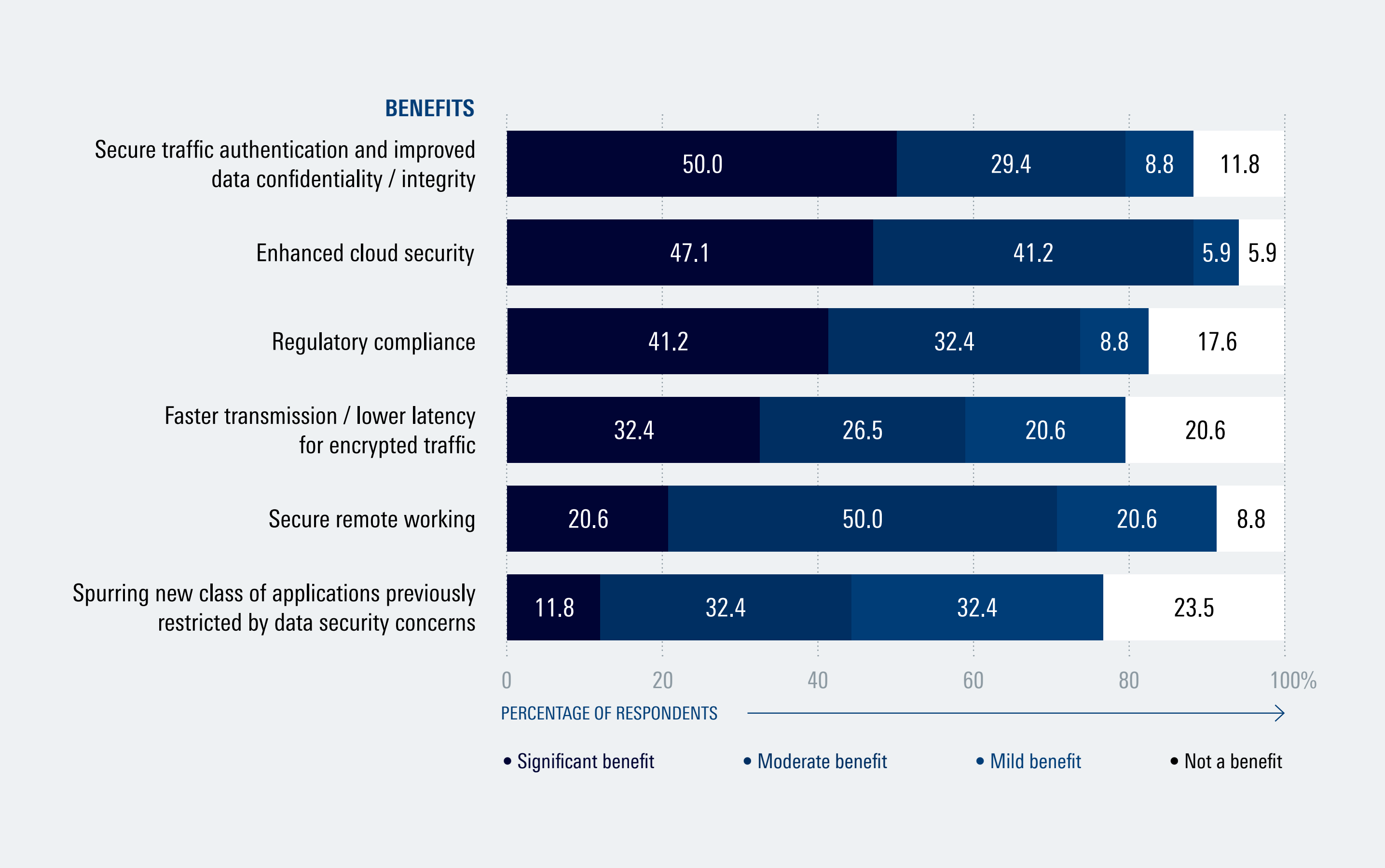
Where do the most significant benefits lie?

In terms of degree of the benefits, the highest ranked areas are secure traffic authentication and improved data confidentiality / integrity, enhanced cloud security and regulatory compliance, with 50.0%, 47.1% and 41.2% of respondents, respectively, rating these as areas to 'significantly benefit' from encryption.

Using encryption for traffic authentication and data integrity / confidentiality helps enterprises conceal sensitive data such as patient health records, banking credentials and authentication factors like passwords. Applying the latest protocols ensures that enterprise applications transport such data securely within and beyond the perimeters of the enterprise WAN, allowing secure communications between different offices, branches and end users. TLS 1.3, for example, uses Authenticated Encryption with Associated Data (AEAD), which authenticates both the encrypted payload and the unencrypted header of a packet.

In terms of ensuring regulatory compliance, data protection laws such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) require enterprises to demonstrate adequate protection measures. These include the encryption of data-in-transit and data-at-rest. As consumer and data protection laws expand, more robust encryption protocols will become necessary.

DIAGRAM 4 Use cases significantly benefiting from new encryption protocols



3. CHALLENGES OF NEW ENCRYPTION PROTOCOLS

Majority of networking vendors plagued by loss of traffic visibility

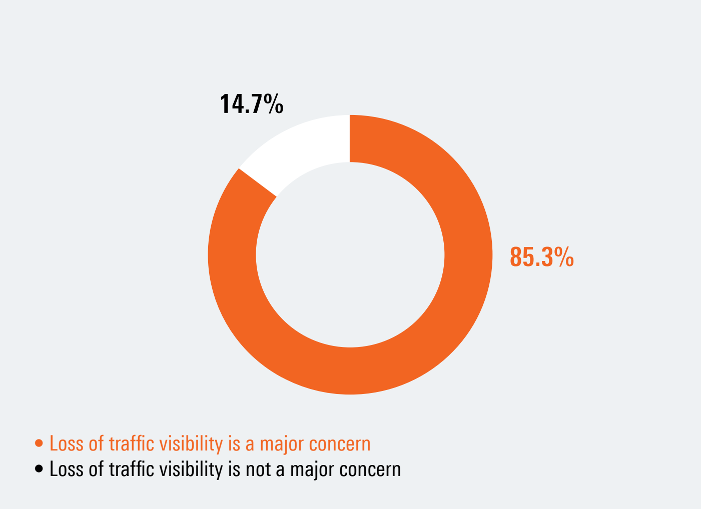
Traffic visibility refers to the cognizance of data as it traverses the network. Visibility enables network administrators to discern a wide range of traffic attributes such as origin and destination addresses, technical specifications such as packet size and number of packets per flow, performance attributes such as speed and latency, behavioral information such as packet intervals and packet duplication, and payload information such as applications and services.

Encryption interferes with traffic visibility to a great extent. Newer encryption protocols progressively conceal more information, spanning packet payloads as well as information that was previously readable from packet headers. Without decrypting the packets, traditional monitoring tools are no longer able to identify applications / services and their performance attributes. For example, administrators are no longer able to identify the jitter or packet loss associated with a video streaming application or behavioral anomalies associated with an email application.

A vast majority of vendors (85.3%) agree that loss of traffic visibility from new encryption protocols is a major concern for today's networks.

DIAGRAM 5

Vendors concerned by loss of traffic visibility from new encryption protocols



Malware and threat information most affected by encryption

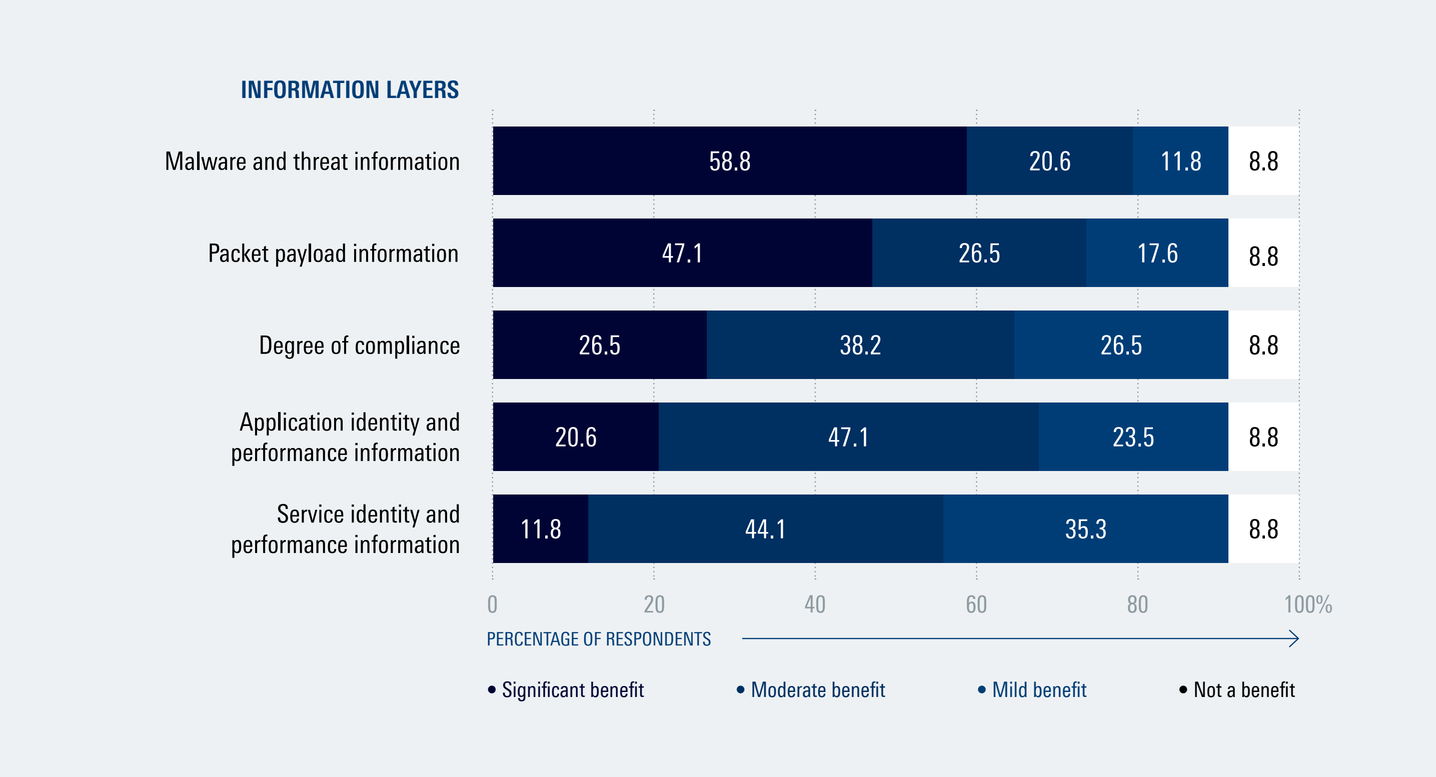
While encryption impairs traffic visibility, it affects different information layers differently.

According to the survey, the data layer that is most impacted is malware and threat information, with 58.8% of respondents agreeing that encryption significantly limits their insights into malicious and suspicious activities. Encryption protocol TLS, which encrypts web applications, conceals suspicious packet movements, for example. As a consequence, associated packets can no longer be identified and collectively analyzed to reveal traffic irregularities associated with incidences, such as DDoS attacks or fraudulent logins.

The next information layers most significantly impacted by encryption are packet payload information and degree of compliance, as selected by 47.1% and 26.5% of survey respondents, respectively. Packet payload information is necessary for security tools in detecting data breaches involving account credentials and unauthorized content. In terms of compliance, a loss of traffic visibility makes it impossible for network administrators to determine if they are adequately supervising and regulating the access and movement of sensitive data, such as health records, within and outside of the network perimeter.

Information on applications / their performance and information on services / their performance are the two other areas, mentionde by 20.6% and 11.8% of respondents, respectively. By not being able to identify applications and services navigating the network, administrators are no longer able to differentiate, for example, Facebook video traffic from virtual assistant messaging on a banking application. This significantly affects the control and management of traffic flows in the network.

DIAGRAM 6 Impact of encryption on different information layers



TLS 1.3 and TLS 1.3 0-RTT the toughest protocols

Encryption protocols have been evolving in tandem with enterprises' security and privacy needs.

TLS, for example, has gone through several iterations over the years. Each version of TLS, from TLS 1.0 to TLS 1.3, introduced new cipher suites that were tougher for malicious actors to break or replicate. Additionally, TLS 1.3 marked a new, faster handshake system that simplified the connection process while maintaining security. It also introduced mandatory perfect secrecy, enabling unique keys for each separate session for more holistic security.

It is important to note that different use cases require different protocols so that information are being safeguarded. TLS 1.3, for example, is commonly used to encrypt and authenticate traffic over the web. Its applications include video and audio communication, email, general web applications and server communication. The protocol is commonly deployed over IP and TCP transport protocols.

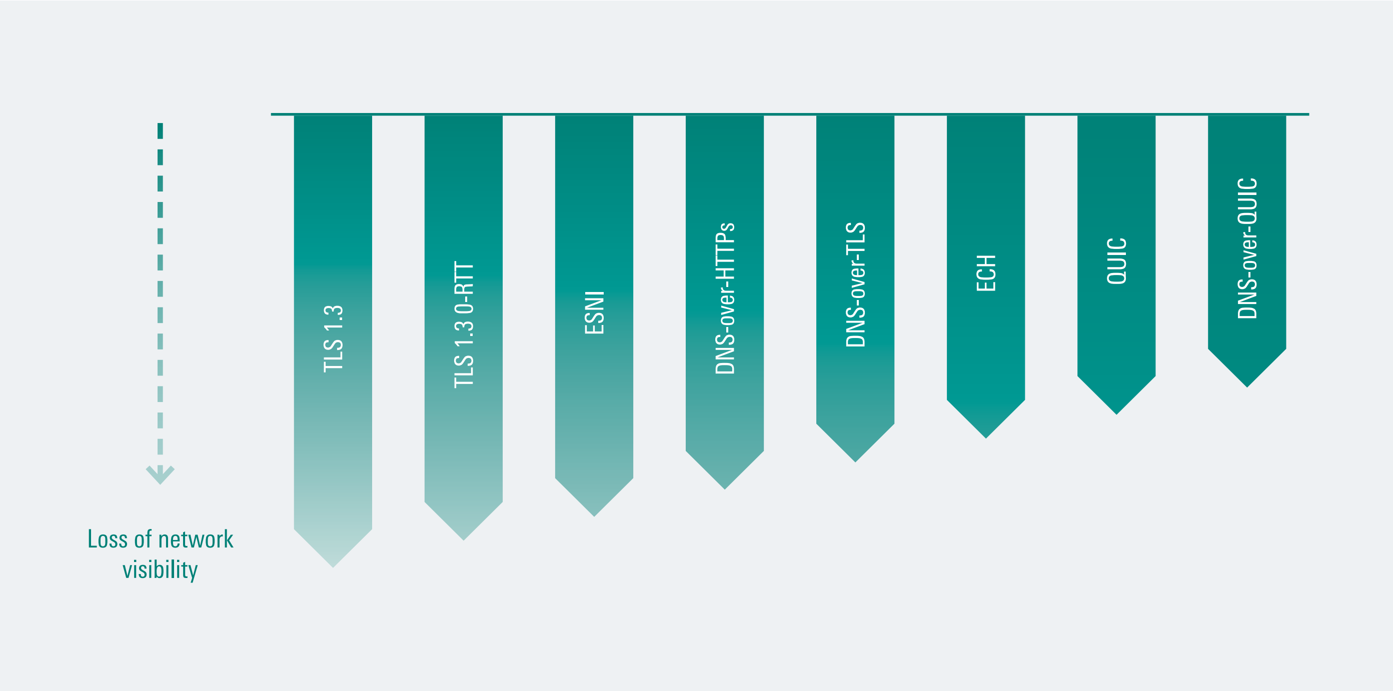
QUIC, on the other hand, is used for applications that require lower latency and mitigated packet loss. The handshake process is faster due to the encapsulation of the TCP layer, and the protocol has more agility in network / device switching. Google currently uses QUIC for YouTube, Hangouts, Chrome as well as other applications and services in its suite.

Based on the survey, the protocol that affects network visibility the most is TLS 1.3, followed by TLS 1.3 0-RTT and ESNI. The DNS-over-HTTPS, DNS-over-TLS and ECH protocols are ranked fourth, fifth and sixth respectively, while QUIC and DNS-over-QUIC are perceived to have the least impact on network visibility by respondents.

As with their methodologies and applications, each encryption protocol conceals network data differently and to differing degrees. TLS ESNI, for example, encrypts the server name indication in the TLS handshake, preventing network administrators from identifying the visited sites.

ECH, in comparsion, encrypts metadata from the TLS handshake in ClientHello, preventing administrators from seeing information such as the names of endpoints users are attempting to access.

DIAGRAM 7 Ranking of encryption protocols by their effect on network visibility



4. HOW LOSS OF VISIBILITY IMPACTS NETWORK MANAGEMENT

Security, network performance management and analytics among key networking functions to bear the brunt of encryption

A total of 87.6% of networking vendors find that encryption adversely impacts the networking solutions they offer.

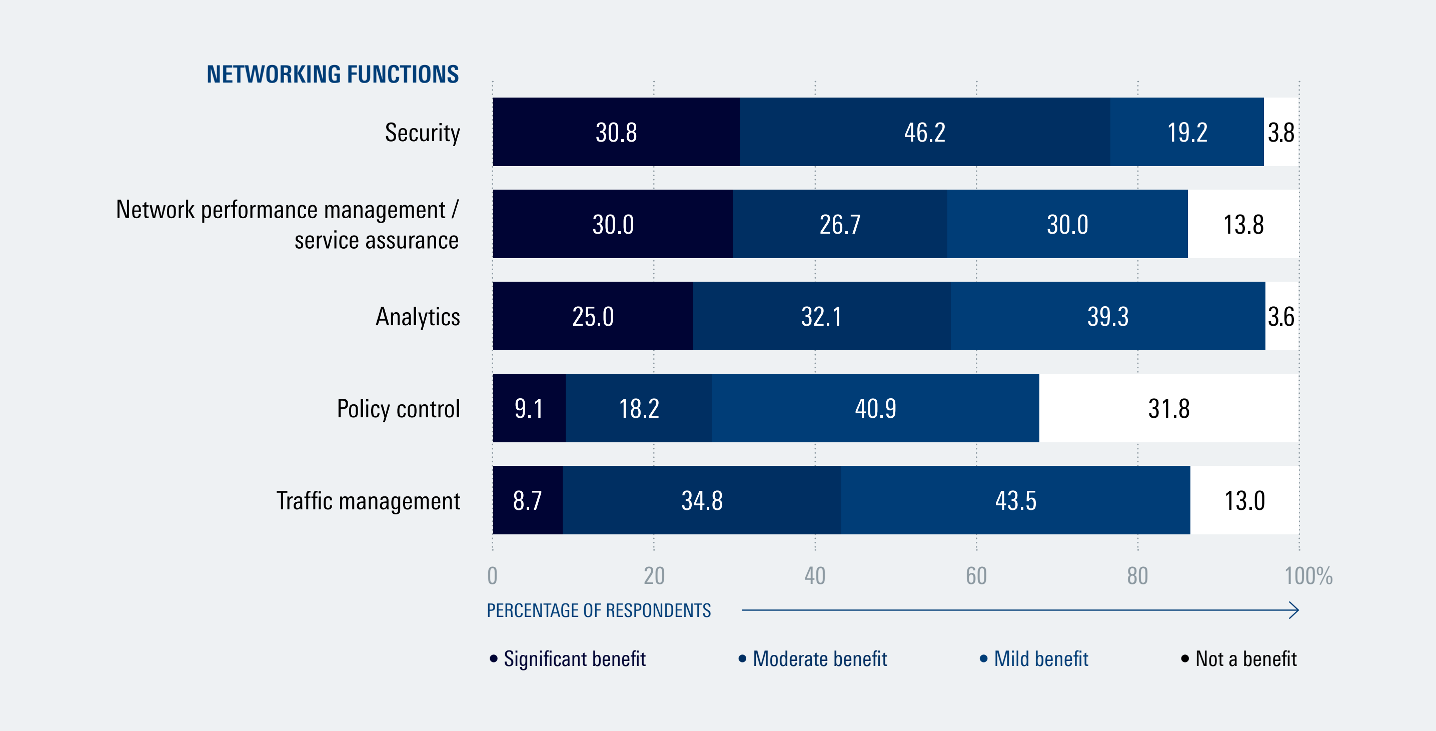
According to the respondents, security is the most affected function, followed by network performance management / service assurance and analytics with 30.8%, 30.0% and 25.0% of respondents, respectively. Up next are policy control and traffic management at 9.1% and 8.7%, respectively.

Encryption impedes threat detection capabilities and efficiency. Encrypted malware, when it originates from internal traffic sources or is hidden in authorized traffic flows from external users using the enterprise VPN or SASE gateways, remains invisible to network administrators.

Dynamic policies for managing network performance become unexecutable as packet payloads and headers are concealed. This is due to the non-traceability of application-based action triggers. This affects policies such as traffic prioritization, for example, the routing of critical applications over premium links.

A lack of insight into application and services limits administrators in their understanding of traffic flows and user behavior. Input provided by tools such as IP probes to other networking functions is also constricted. Bottlenecks and congestion remain unremedied due to incomplete diagnoses and delays in identifying the offending applications.

DIAGRAM 8 Networking functions adversely impacted by loss of visibility due to encryption



Encryption hampers detection of threats, abuse and fraud; major cost implications expected

Loss of traffic visibility as a result of encryption can greatly impair various key functionalities and impact network outcomes.

Based on the survey, 70.6% of participants cite the inability to identify and curtail threats / abuse / fraud as the biggest contributing factor towards this. Threats hidden in encrypted traffic flows, unchecked, can become highly disruptive and damaging to networks. Automated threat responses become muted when crucial analytics are removed from threat monitoring dashboards.

According to 52.9% of respondents, encryption also impacts network outcomes through increased network costs. Lack of visibility leads to suboptimal allocation of resources, resulting in network inefficiencies, and overconsumption of bandwidth and computing resources.

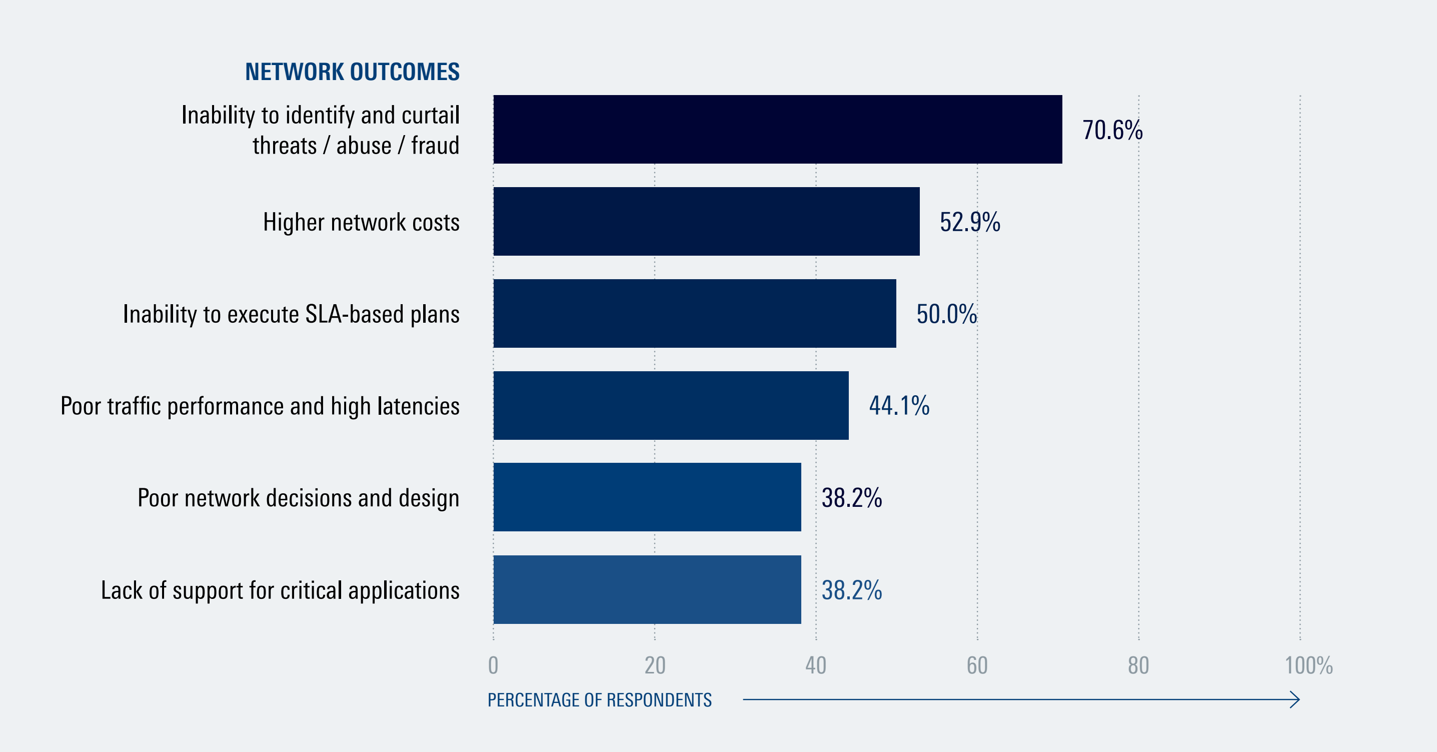
Half of all respondents surveyed state that a loss of visibility results in the inability to execute SLA-based plans. Without granular information on the performance of specific applications, network administrators are not able to adjust network parameters to maintain the required SLAs.

Loss of visibility also impacts traffic performance, say 44.1% of networking vendors. Blanket policies for all applications and traffic types will undermine the performance of, for instance, latency-sensitive applications, such as factory automation, autonomous vehicles and smart electricity grids, leading to poor service reliability.

Without visibility, network architectures remain unaligned to the needs of the enterprise — which is a concern for 38.2% of respondents. Provisioning of additional network services, such as intelligent load balancing and NGFWs in the case of WAN and SDWAN, requires comprehensive traffic analytics before the right mix of tools and capacity can be determined. These constraints also impact an enterprise's decision to adopt cloud-native or virtualized architectures.

A similar share of respondents (38.2%) also see a lack of support for critical applications. Without adequate performance data, broken links, compromised servers and breached databases remain undetected, and unremedied.

DIAGRAM 9 The impact on network outcomes from loss of visibility due to encryption



Encrypted threats make up more than a third of all security incidents

Evaluating the extent to which encryption compounds security risks, the survey finds that, on average, 37.6% of security incidents originate from encrypted threats.

Almost all of their security incidents are attributable to encrypted threats, say 5.9% of respondents. Another 2.9% of respondents attribute 80% of their security threats using encryption. A further 29.4% of respondents state that 60% of their security incidents are encrypted by nature. The share of respondents who attribute 40% and 20% of attacks to encrypted threats are 14.7% and 29.4%, respectively. Only 17.6% of vendors in the survey state that none of the threats they encounter are encrypted.

Cyber threats such as ransomware, malware, zero-day, DDoS and spear phishing are increasingly using encryption to avoid being detected by tools such as data loss prevention, IPS/IDS and NGFW. The malware TrickBot, for example, uses HTTPS to fetch injections from its command-and-control server, as it runs spear phishing campaigns and executes ransomware attacks on target devices. In 2020, TrickBot was responsable for an attack on several hospitals in the United States, resulting in large amounts of data being lost and many lives put at stake due to the downtime experienced by critical medical infrastructure[4].

Encrypted malware can compromise servers, critical applications, links, data, and end user devices, leading to performance disruption, data loss and reputational risks.

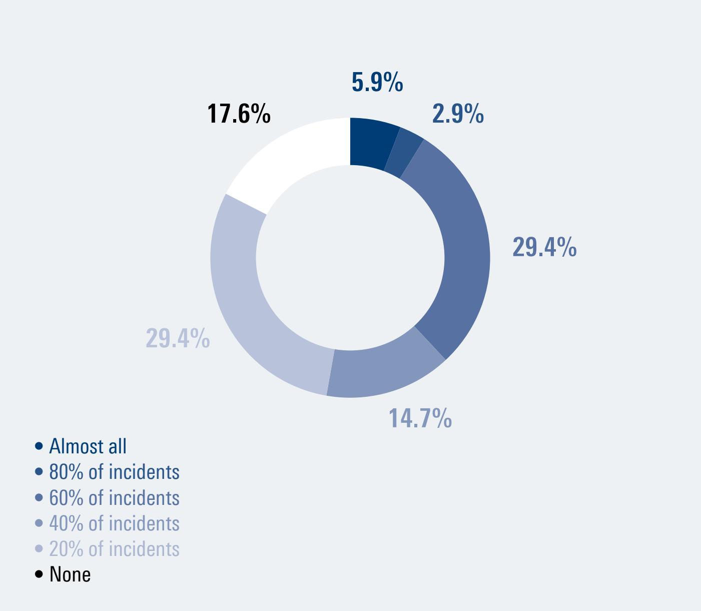
The majority of encrypted attacks use TLS/SSL, according to ZScaler's State of Encrypted Attacks 2022 report[5]. The vendor cites the heavy consumption of resources required to inspect TLS/SSL traffic as a driving factor, leaving the protocol as a preferred means to hiding malicious traffic.

37.6%

of security incidents originate from encrypted threats

DIAGRAM 10

Share of security incidents attributable to encrypted threats based on vendor experience



[4] "Ransomware Hits Dozens of Hospitals in an Unprecedented Wave." WIRED, Oct. 2020, www.wired.com/story/ransomware-hospitals-ryuk-trickbot

[5] "Over 85% of Attacks Are Encrypted: ThreatLabz Report." Zscaler, Dec. 2022, www.zscaler.com/blogs/security-research/2022-encrypted-attacks-report

5. ADDRESSING ENCRYPTION WITH THE RIGHT VISIBILITY TOOLS

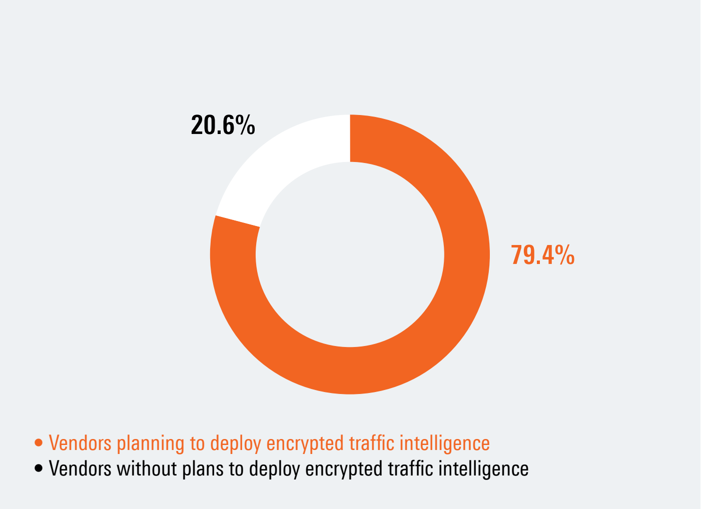
Four in five networking vendors plan to integrate encrypted traffic intelligence

A vast majority of networking vendors is aware of the need to address visibility gaps caused by newer encryption protocols. According to the survey, 79.4% of network vendors plan to integrate encrypted traffic intelligence into their solutions, while only 20.6% of vendors plan not to.

Encrypted traffic intelligence refers to the deep analysis of encrypted packets and flows, focusing on the identification of protocols, applications and services, and their behavior, performance and security attributes. Encrypted traffic intelligence enables network tools such as compression engines, intrusion prevention systems and charging engines to mete out policies selectively, based on the needs of the underlying applications and services and their performance metrics.

DIAGRAM 11

Plans for integrating encrypted traffic intelligence in networking solutions



Higher approval of analytical tools without decryption; Behavioral, statistical and heuristic analysis most popular

The introduction and widespread use of encryption necessitates novel approaches for analyzing and monitoring traffic flows. Networking vendors, whose solutions greatly depend on real-time traffic visibility, have adopted several approaches / tools to address this. The survey assesses three types of tools that are prevalently used in the market.

The most popular of these tools are based on behavioral and statistical / heuristic analysis, which are used by 70.6% of the surveyed vendors. This toolset includes metadata analysis; analysis of packet level data such as packet sizes, packet rates and interpacket delay; flow data such as traffic direction initiated by the protocol and / or app and number of flows; flow entropy; and statistical information such as mean, median and variation.

The second most used tool, selected by 55.9% of respondents, is ML and DL. This involves algorithms such as k-nearest neighbors (k-NN), LSTM, decision tree learning, CNN and RNN.

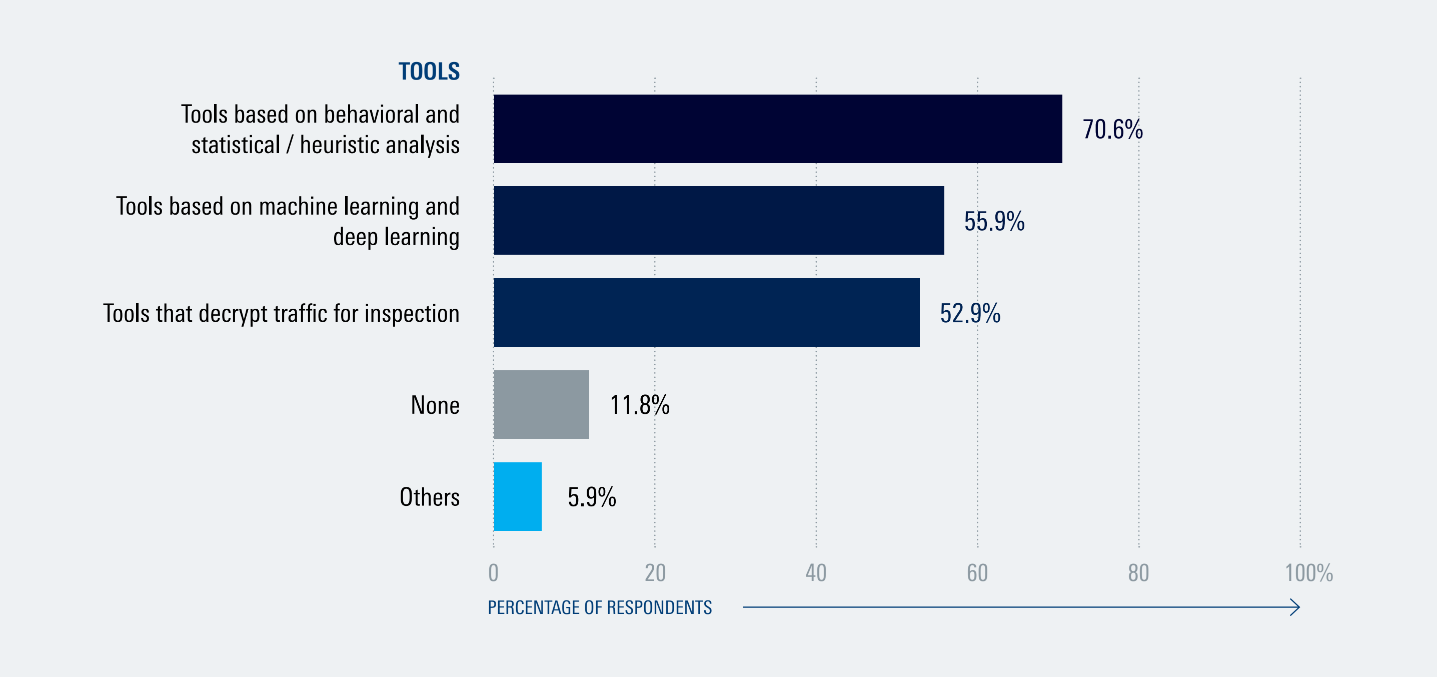
Both techniques - behavioral / statistical / heuristical analysis and ML / DL - are non-intrusive, inference-based packet examination methods. The payload remains locked in both techniques, and no decryption takes place. Advanced algorithms and high-intensity computing capabilities are key pre-requisites for both. Most networking vendors tap into proprietary or third-party advanced analytical engines built-in with these capabilities to help them acquire real-time insights into encrypted traffic flows.

Both above-mentioned methods involve a high-degree of expertise and continuous updates to a repository of parameters / metrics used to identify the underlying applications and services. Decryption, the third most used method for analyzing encrypted traffic flows, circumvents this by opening each packet and inspecting the payload directly. Decryption involves the use of SSL / TLS inspection (also known as middleboxes, MiTM, SSL / TLS proxy servers and HTTPS interception) to decrypt, read and re-encrypt packets. More than half (52.9%) of the respondents claim to use decryption for handling encrypted traffic.

Other tools not mentioned in the list, such as traffic emulation, are used by 5.9% of respondents.

A total of 11.8% of the vendors surveyed admit to not using any monitoring tools for encrypted traffic.

DIAGRAM 12 Usage of tools currently deployed for analyzing encrypted traffic



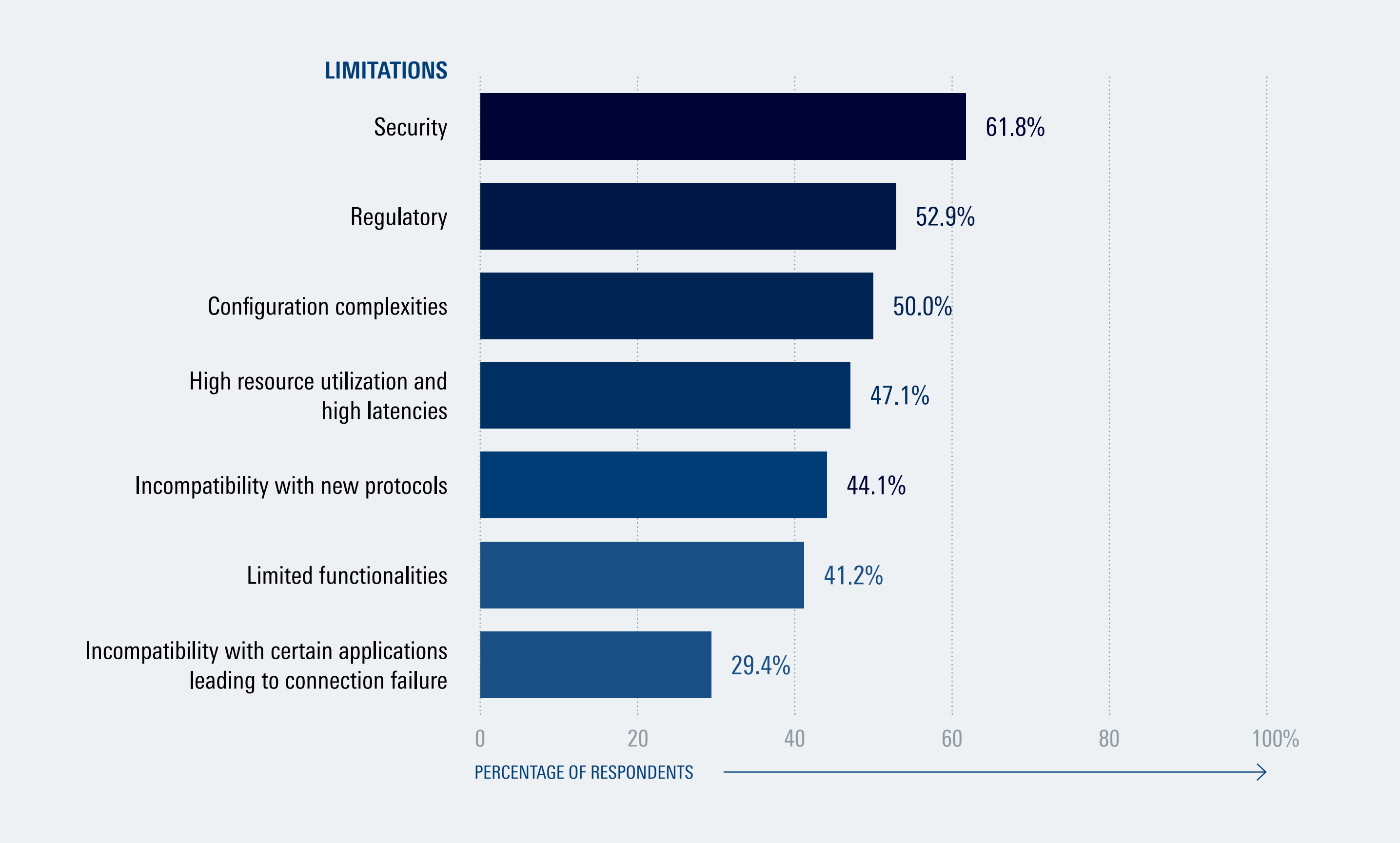
Security and regulatory issues loom large on SSL / TLS inspection

Despite its ease of deployment, the use of decryption for examining encrypted traffic is often challenged by various regulatory, security and technical concerns. The survey evaluated views of networking vendors on a number of concerns that are restricting the use SSL / TLS inspection for inspecting encrypted traffic flows.

Networking vendors rate security as their biggest concern when it comes to using SSL / TLS inspection tools (e.g. MiTM). Security is an issue for 61.8% of the vendors, followed by regulatory compliance, which is cited by 52.9% of respondents. Security risks include the routing of traffic through a forward proxy to create a TLS chain, which leads to plaintext data being exposed within the network. Regulatory concerns arise from inspecting sensitive data, such as healthcare, banking and personally identifiable information (PII), which is illegal in several states and countries.

Configuration issues are cited by half of the respondents as a challenge in using SSL / TLS inspection, where setting up a forward proxy and certificate authority and negotiating cipher suites can be difficult and complicated.

DIAGRAM 13 Limitations of SSL / TLS inspection for analysis of encrypted traffic



Resource utilization and high latencies are a concern for 47.1% of respondents when using SSL / TLS inspection. Decrypting, analyzing and re-encrypting each packet is memory-intensive and takes a huge toll on server resources.

According to 44.1% of respondents, another key issue associated with SSL / TLS inspection is the lack of support for new encryption protocols. For example, RSA key exchanges used by passive mode devices are depreciated in TLS 1.3, leading to partial inspection.

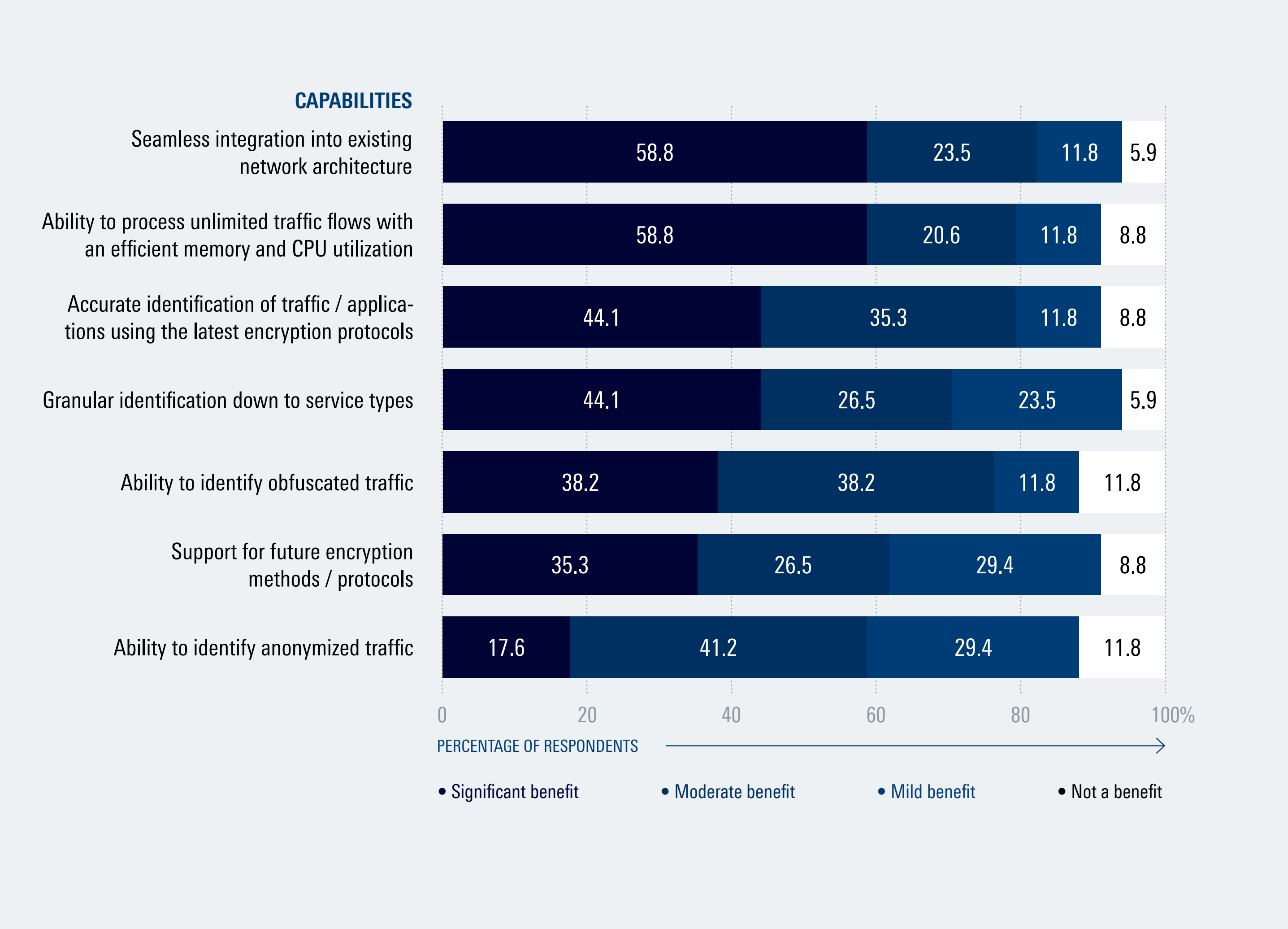
Limited functionalities offered by SSL / TSL inspection tools is a concern for 41.2% of the respondents. For example, the option to bypass traffic based on destination addresses by MiTM devices is no longer possible upon the introduction of protocols that encrypt SNI and certificate SAN which contains this data.

Finally, 29.4% of respondents are concerned with network failures. Certain applications, such as the Apple OS, are programmed to fail any connection whenever packets are identified to have gone through SSL / TLS inspection.

The ideal tool for analyzing encrypted traffic: Networking vendors demand seamless integration and efficiency

The quest for an ideal tool that can analyze and monitor encrypted traffic flows does not end with any single approach or methodology. It entails a comprehensive solution that is able to address current and future encryption protocols while ensuring adherence to various operational, privacy, regulatory and security requirements. It must also be a scalable and an easily deployable solution. The survey assessed a number of capabilities that are deemed important for a tool that is

DIAGRAM 14 Capabilities expected from an ideal tool for inspecting encrypted traffic



entasked with examining, analyzing and reporting encrypted traffic flows. According to the survey, a tool's ability to integrate seamlessly into existing network architecture and devices ranks topmost in terms of being highly significant. This feature is highly important for 58.8% of respondents. The same share of respondents also choose a tool's ability to process unlimited traffic flows while maintaining an efficient memory and CPU utilization, as a highly important pre-requisite.

The ability to accurately identify traffic / applications which use the latest encryption protocols such as TLS 1.3, TLS 1.3 0-RTT, ESNI, DNS-over-HTTPs and DNS-over-TLS is rated by 44.1% of respondents as highly important. The ability to deliver granular identification of packets and flows, down to application and service types ranks next, and is also chosen by 44.1% of respondents as a highly important capability.

The ability to identify obfuscated traffic that uses methods such as randomization, tunneling, domain fronting and mimicry is highly important, according to 38.2% of respondents. The ability to cater to newer and more complex encryption protocols and methods is judged by 35.3% of the respondents as a highly important capability.

Finally, the ability to identify anonymized traffic, transported via VPNs and proxies, is cited by 17.6% of the respondents as another highly important feature of an ideal tool for inspecting encrypted traffic.

6. DPI FOR ENCRYPTED TRAFFIC VISIBILITY

Four fifths of vendors use or plan to use DPI

One of the key technologies deployed for monitoring and reporting traffic intelligence is DPI. Conventional DPI tools combine both shallow and deep packet inspection to deliver real-time analytics on traffic flows.

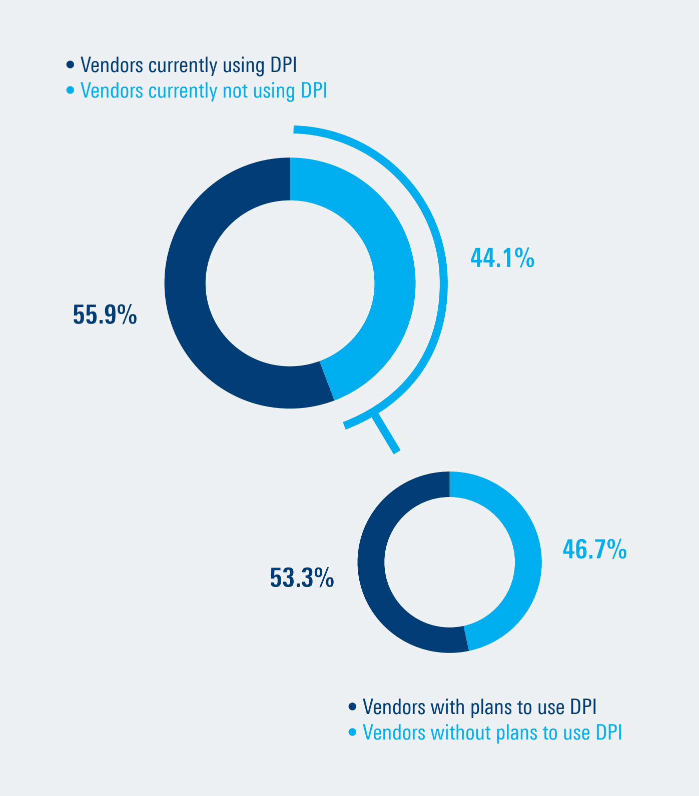
Shallow packet inspection involves the use of information available in packet headers to identify protocols (protocol matching) and basic packet information such as packet size, destination and source addresses. Deep packet inspection entails the examination of packet payloads for matching patterns, leveraging signature libraries containing strings of known applications and services.

A key attribute of DPI is that it depends entirely on payload readability to accurately detect the underlying applications and services. Before the advent of encryption, DPI was highly effective in delivering network intelligence for any use case, in any part of an IP network that requires granular, real-time traffic analysis.

The introduction of encryption, which encodes plaintext into ciphertext using algorithms and secure key exchanges, has resulted in DPI losing access to packet payload information, creating blind spots in its traffic analysis. This challenge is compounded by the introduction of newer and more complex encryption protocols that progressively conceal more information, rapidly narrowing the data points that are available to DPI tools.

In assessing the relationship between DPI and encrypted traffic, the survey first aimed to determine the existing use of DPI among networking vendors. Despite being challenged by encryption, it finds 55.9% of vendors using the technology. The survey, further, attempted to determine the future demand for DPI by assessing the intent of vendors without DPI to deploy it over the coming years. It reveals that more than half of the vendors currently not using DPI plan to do so in the future. This brings the total share of vendors using or planning to use DPI to 79.4%, indicating the importance of DPI in the eyes of networking vendors.

DIAGRAM 15 Current and future use of DPI



Future deployments of DPI may see a huge shift in procurement choices

Networking vendors deploying DPI or planning to do so have a wide range of solution options to choose from. While some vendors develop their own DPI in-house, others procure the capability, either in the form of a turnkey solution that can be readily deployed in the network; or a commercial solution that is licensed from a DPI expert and embedded into their own offerings. Open source DPI is another option that is available today. This option does not involve a licensing fee or up-front product investment, but it requires extensive customization and developer support before it can be integrated into any vendor solution.

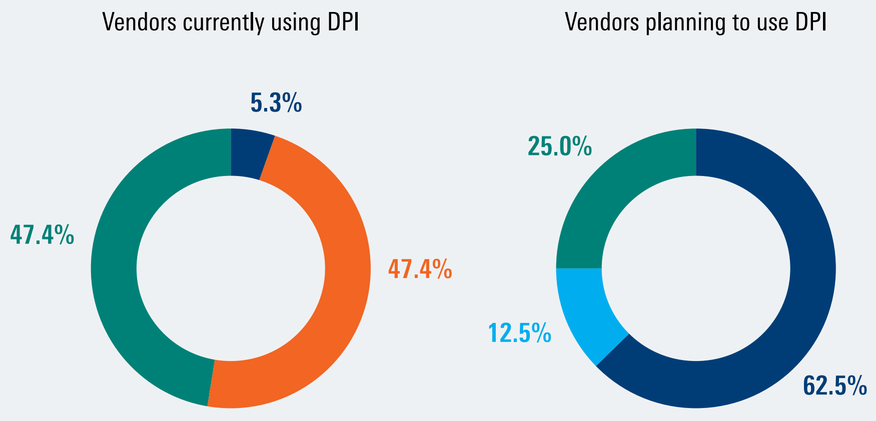
The survey also presents findings on vendors' DPI solution preferences. While turnkey DPI makes up 62.5% of all planned deployments, it only comprises 5.3% of actual deployments. Similarly, open source DPI makes up 12.5% of planned deployments, but none of the existing deployments.

On the other hand, in-house DPI makes up nearly half of the existing deployments but does not occur in the planned deployments. Likewise, 25.0% of vendors planning to use DPI, prefer commercial DPI, but when it comes to existing deployments, commercial DPI almost amounts to double that figure at 47.4%.

These results indicate a clear demarcation between the preferences of existing and future users of DPI. An obvious shift is in the surge in demand for turnkey solutions among potential adopters and a lack of demand for in-house solutions.

The complexities brought about by encryption and other traffic masking methodologies, such as obfuscation and anonymization, alongside the rapid growth in traffic volumes, necessitate advanced DPI techniques. They need to be capable of tackling new and emerging protocols and applications while ensuring superfast processing and a high level of detection accuracy. It is unlikely that vendors, exploring the use of DPI for their solutions, have the resources and time to develop such advanced DPI capabilities. This explains the high demand for turnkey and commercial solutions among future adopters.

DIAGRAM 16 DPI deployment preferences



- **Turnkey DPI** - a complete DPI solution that is sold as an end product and can be readily and immediately deployed into a network or larger networking solution
- **In-house DPI** - DPI developed by internal experts to suit vendors' specific solution
- **Open-source DPI** - DPI source code that is publicly available for use and modification, and is collaboratively maintained, such as nDPI
- **Commercial DPI** - a DPI solution licensed from a third party. Commercial DPI is often more comprehensive, frequently updated and tailored to vendors' specific use cases

A large chunk of DPI tools feature some form of encrypted traffic visibility

Given the widespread use of encryption, the ability to analyze encrypted traffic flows is expected to feature prominently as a key capability across today's DPI solutions. Based on the survey, 73.7% of vendors, currently using DPI, already have some form of visibility into encrypted traffic.

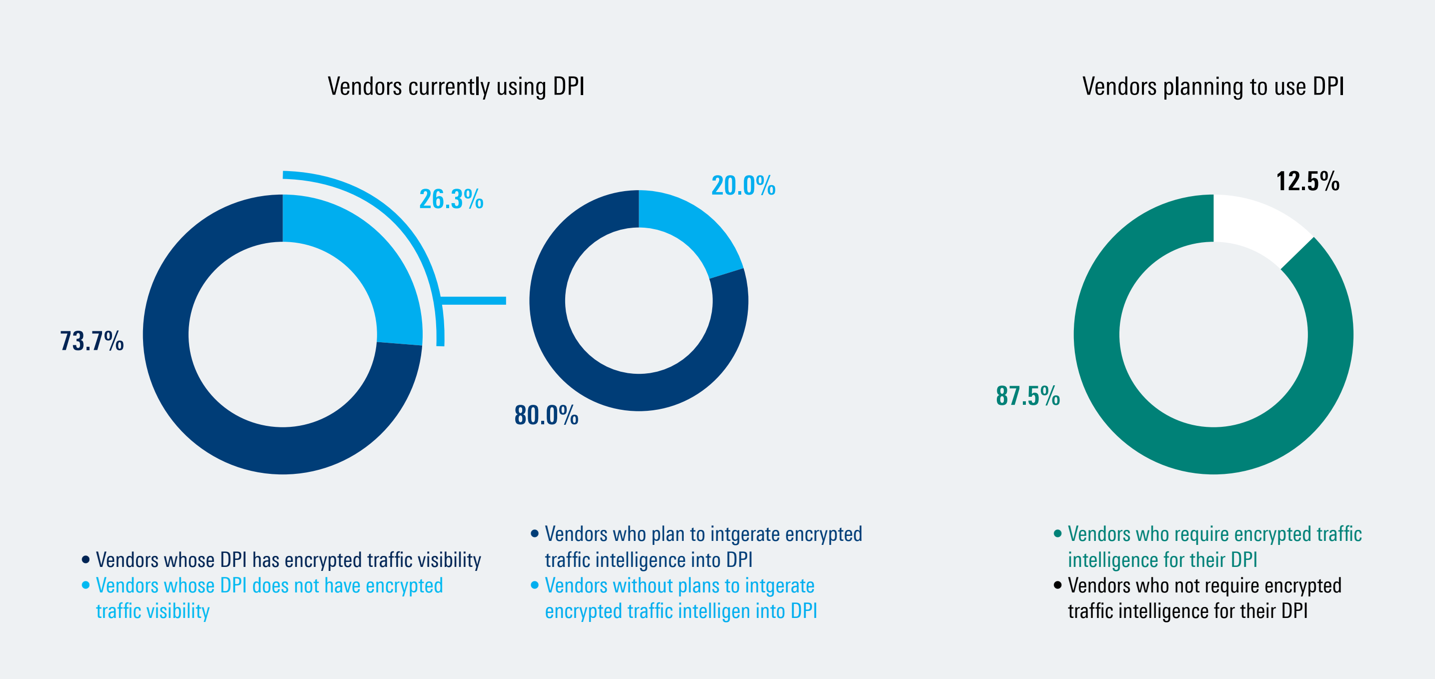
Of the 26.3% of respondents that do not have such visibility, 80.0% plan to integrate it into their DPI. As for the vendors intending to deploy DPI in the future, 87.5% say they would require encrypted traffic intelligence.

In total, the survey finds 92.6% of respondents to already have encrypted traffic intelligence or plan to have it in their existing or future DPI solutions.

92.6%

of DPI tools will have encrypted traffic intelligence in the future

DIAGRAM 17 Integration of encrypted traffic visibility into DPI



7. R&S®PACE 2 AND R&S®vPACE FOR ENCRYPTED TRAFFIC INTELLIGENCE

As a leading player in the DPI space, DPI technology by ipoque, a Rohde & Schwarz company, has to-date supported hundreds of networking vendors in delivering real-time traffic analysis.

The ipoque DPI product series, R&S®PACE 2 and R&S®vPACE, are market-leading OEM DPI engines that use advanced traffic classification methods to deliver detailed traffic insights in real-time. Both engines combine pattern matching with classification techniques such as statistical / behavioral / heuristic analysis to identify thousands of protocols, applications and service types. R&S®PACE 2 and R&S®vPACE are widely deployed by networking vendors across analytical, security and traffic management solutions.

In the wake of encryption, Rohde & Schwarz has steadily improvised its DPI suite of solutions to address the growing number of encrypted applications and services. Despite successfully mitigating major loss of visibility via advanced statistical / behavioral / heuristic analysis, the introduction of newer encryption protocols such as TLS 1.3 and ESNI has pushed Rohde & Schwarz to integrate new approaches to analyzing encrypted flows.

This has led to Rohde & Schwarz introducing encrypted traffic intelligence (ETI), a cutting-edge methodology that is capable of accurately and reliably detecting encrypted applications and services. ETI combines a mix of ML and DL algorithms with high-dimensional data analysis. These include k-nearest neighbors (k-NN), decision tree learning models, convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory (LSTM) networks. A highly optimized combination of these algorithms is used to achieve maximum accuracy on traffic detection and classification results. These algorithms employ thousands of features, including statistical, time series and packet-level features. Additional features are automatically identified by DL algorithms.

Capabilities supported by ETI

ETI enables R&S®PACE 2 and R&S®vPACE to support:

- **Application protocol classification**
  - Network / flow level analytics
  - Detection of anomalies and malicious activity involving specific protocols
- **Application type classification**
  - Usage control by application categories
  - Timely execution of application-based network policies
  - Security filtering based on different application risk tiers
- **Application classification**
  - Application performance monitoring
  - Identification of application-specific threats
  - Granular policies for user access, traffic management and resource triage
- **Application usage classification**
  - Application access and usage patterns
  - Impact of applications on network performance
  - Network resource optimization
- **OS, browser and application classification**
  - Patterns in user behavior and device types / usage
  - Identification of security vulnerabilities
- **Website fingerprinting**
  - User activity monitoring including navigation and transaction patterns of specific websites
- **Device identification**
  - Network entry identification and threat detection
- **DNS tunnelling detection**
  - Identification and mitigation of tunnelling threats

R&S®PACE 2 and R&S®vPACE complement their ML and DL capabilities with DNS and service caching to instantly and reliably detect encrypted applications and services, with zero false positives and nearly no false negatives. Combining traffic classification with metadata extraction, the ipoque DPI engines are able to deliver comprehensive and highly granular traffic performance and security metrics. These include attributes such as speed, latency, packet loss, time-to-first-byte, jitter, throughput and bandwidth.

The introduction of ETI also expands R&S®PACE 2 and R&S®vPACE's coverage of threats and security incidents. While pattern matching only identifies known attack vectors, the introduction of ETI, namely the incorporation of ML and DL, enables networking vendors to detect the behavior of malware, spyware, phishing attacks or ransomware that are yet to be discovered.

R&S®PACE 2 and R&S®vPACE engines can be deployed in any architecture, including virtualized and cloud-native networks, and across frameworks such as DPDK and VPP. Both engines boast high performance, linear scalability and low memory consumption.

Licensing DPI technology by Rohde&Schwarz equips vendors with a future-proof DPI solution with weekly signature updates, constant performance and reliability testing, as well as continuous research and development into the latest encrypted traffic classification methods by the Rohde&Schwarz team of in-house data scientists.

Additionally, vendors enjoy 24/7 service and support and the option to tailor their DPI solution to their specific use case, leveraging the long-standing expertise of Rohde&Schwarz and the suite of additional features and plug-ins.

8. SUMMARY

Loss of visibility due to encryption poses a significant challenge for networking vendors. It increases the exposure of networks to security threats and leads to suboptimal traffic management, inferior analytics, ineffective subscriber control and poor application performance.

This research report is aimed at identifying the impact of encryption on traffic visibility. It further investigates the relevance and potency of DPI in examining and analyzing encryption traffic in the wake of newer encryption protocols, such as TLS 1.3 and ESNI.

Results of this survey confirm that:

- Emerging encryption techniques greatly impact networking functions, namely security and analytics
- Left unaddressed, encryption can have serious destabilizing effects on the network
- Decryption using SSL / TLS inspection, despite being a straightforward method to analyzing encrypted traffic, is becoming highly impractical due to security, regulatory, configuration and performance concerns
- Non-decryption methods such as behavioral / statistical / heuristic analysis and ML / DL are growing in importance as preferred means to addressing encrypted traffic flows
- Despite being challenged by the loss of visibility from encryption, there is continuous dependency on DPI to deliver real-time traffic intelligence across IP networks
- There is an overwhelmingly strong demand for turnkey and commercial DPI solutions across new DPI deployments
- The incorporation of cutting-edge AI-based techniques such as ML and DL have given rise to next-gen DPI tools capable of accurately and reliably classifying the underlying traffic flows, by protocols, applications and services
- Encrypted traffic intelligence is seen as a critical feature for DPI, with widespread adoption expected in the near future

Next-gen DPI solutions, powered by encrypted traffic intelligence, can greatly augment the traffic filtering and analytical capabilities of today's networking tools. As a market-leading DPI specialist, Rohde&Schwarz is continuously tapping into breakthrough technologies such as ML / DL to deliver a powerful visibility solution that promises scalability and reliability. Next-gen DPI by Rohde&Schwarz not only preserves the privacy and confidentiality of information crossing today's networks, but also ensures a future-proof technology that keeps networks performing and secure at all times.

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.

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

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
Trade names are trademarks of the owners
Version 01.00 | March 2023
Deep packet inspection and encrypted traffic visibility for IP networks
Data without tolerance limits is not binding | Subject to change