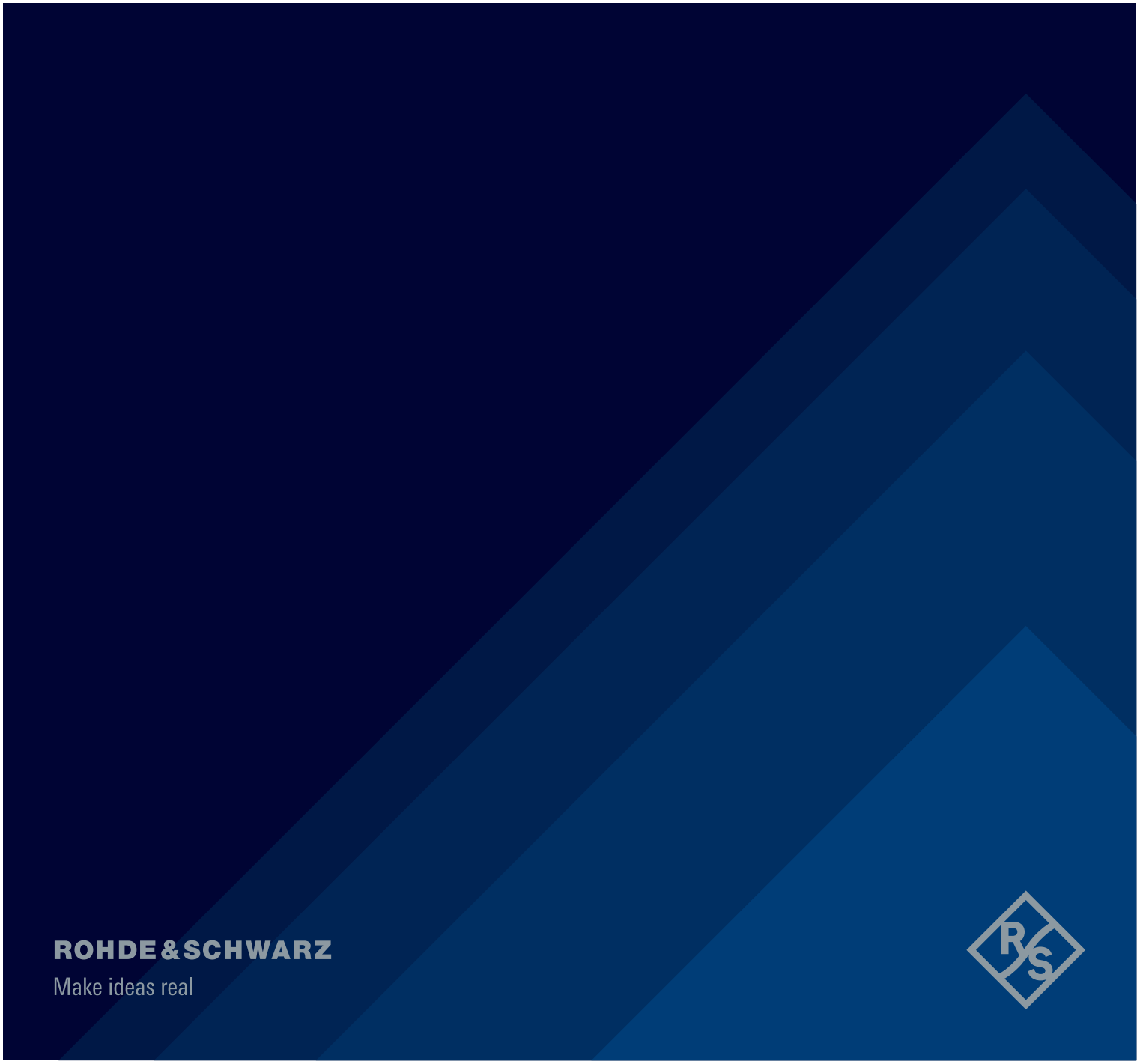
NEXT-GEN DPI FOR ZTNA: ADVANCED TRAFFIC DETECTION FOR REAL-TIME IDENTITY AND CONTEXT AWARENESS

Research Report



ROHDE&SCHWARZ
Make ideas real

CONTENT

1. INTRODUCTION

Zero-trust network access (ZTNA) refers to a category of network access and security solutions that are built on the idea of zero-trust. The concept of zero-trust assumes that no user should be implicitly trusted, and permissions to enterprise resources should be granted only to the extent that they are needed. ZTNA creates a comprehensive access control and security framework for all enterprise resource types – on-premises, cloud and SaaS, across any user or device.

Why zero-trust

Enterprise networks have evolved from static architectures and well-defined perimeters to become borderless entities defined purely by the interactions that take place between resources, users and devices. This has led to the inversion of enterprise networks, where resources are hosted and delivered from the cloud and users work in hybrid models, accessing these resources from anywhere. Traditional access controls to enterprise resources, mostly built around location-based rules such as head or branches offices, can no longer be used to manage these user requests. Similarly, security tools hosted locally to filter traffic flows to on-premises applications cannot be used to scrutinize and control traffic flows to hybrid, cloud and SaaS applications hosted on third party infrastructure.

ZTNA brings a major paradigm shift to how enterprises tackle the complexities of managing fluid networks. It enables enterprises to consolidate access control and security for their resources in a single solution, hosted in the cloud or on-premises. All requests are processed using standardized rules that are applied consistently based on the identity and context of the user.

Deep packet inspection (DPI) is a cutting-edge technology for gathering traffic insights needed for real-time network traffic analysis. It empowers network and security vendors to identify applications, protocols, and service types and capture performance and security metrics in real-time. Next-gen DPI combines traditional classification techniques like pattern matching with advanced statistical, heuristical and behavioral analysis as well as machine learning (ML) and deep learning (DL) algorithms to establish identity and context awareness. These capabilities support ZTNA's granular access policies and enable ZTNA to establish continuous adaptive trust.

Survey: Next-gen DPI for ZTNA

Duration: 10/23-12/23

Participants: 55 networking vendors

Authors: Rohde&Schwarz and The Fast Mode

About the report

This report aims to identify traffic visibility needs among ZTNA vendors for establishing continuous adaptive trust. It looks at the visibility challenges concerning ZTNA vendors and the impact of diminishing network visibility on ZTNA's effectiveness and market adoption. It also focuses on DPI's role in overcoming these challenges and delivering the much-needed insights for ZTNA intelligence.

Firstly, it examines the different deployment models of ZTNA, the concept of continuous adaptive trust and its dependence on identity and context awareness. It then explores the information and parameters ZTNA vendors deem necessary for establishing both identity and context awareness and the challenges they face in gathering this data. It also discusses how encryption technologies exacerbate visibility gaps and how these gaps impact ZTNA solutions and their vendors. The report evaluates the need for deep traffic insights for ZTNA automation, a must-have in today's complex networks. This is followed by an overview of the growing popularity of DPI among ZTNA vendors and the different types of DPI solutions that are currently deployed.

The findings and analyses in the report are based on a survey of 55 leading ZTNA vendors with diverse ZTNA implementations and solution features. The survey jointly conducted by ipoque, a Rohde&Schwarz company, and The Fast Mode took place from October to December 2023.

2. THE EVOLUTION OF ZTNA

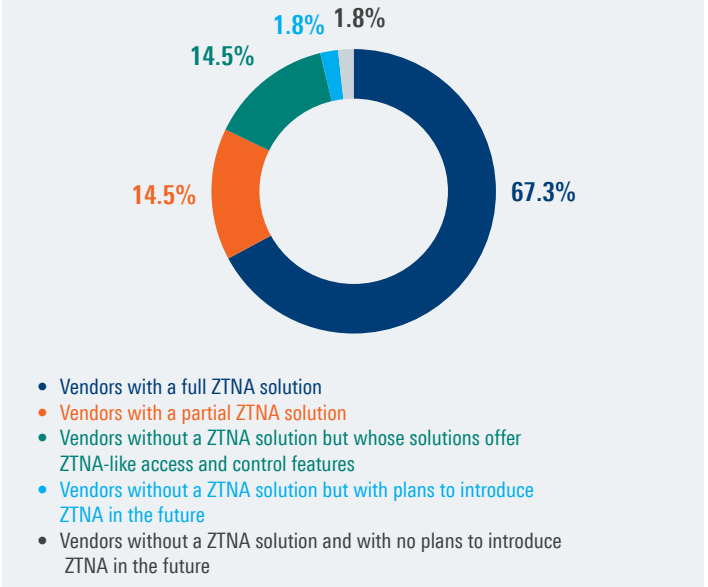
Two thirds of vendors offer comprehensive solution suites that fulfill all zero trust principles

As a relatively new market, ZTNA is continuously evolving. Players in this space are rapidly building out their solutions, innovating and adding new features to create offerings that are capable of addressing the inversion of enterprise networks as more and more resources and users are dispersed outside the traditional network perimeter.

Most ZTNA solutions take the form of a comprehensive toolkit that combines multiple mechanisms and methodologies. This survey saw that out of 55 respondents, 67.3% currently offer a ZTNA solution that encompasses all essential features of ZTNA while 14.5% of respondents offer a partial ZTNA solution, providing selected essential features. Essential features include least privilege access (LPA), microsegmentation, multi-factor authentication, single sign-on (SSO), encryption from endpoint to the application, continuous authentication, adaptive trust, coverage for all enterprise resources, support for both managed and unmanaged devices, cyber threat protection and a single data loss prevention (DLP) policy.

The extensive list of features required of ZTNA has created a market characterized by a diversity where no single offering is the same. Some solutions are born as ZTNA. Others morphed from existing security and access management solutions. There are also vendors who provide a mix of mechanisms that are associated with zero-trust, despite not labeling their solutions as such, creating an implicit presence in the ZTNA market. The survey found 14.5% of respondents offering ZTNA-like access and control features, despite not having a dedicated ZTNA portfolio. Of the remaining 3.6% of respondents who currently do not offer a ZTNA solution, half are planning to do so in the future.

DIAGRAM 1 Respondents' ZTNA offerings

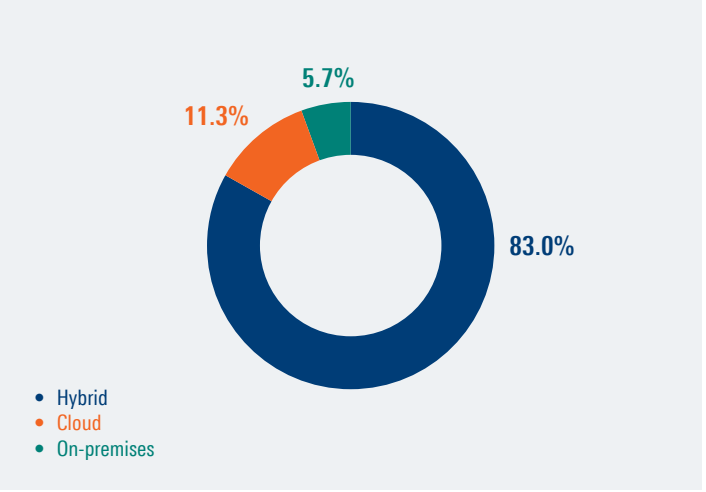


Majority of ZTNA vendors support a hybrid deployment model

The overwhelming majority (83.0%) of respondents who currently offer ZTNA or whose solutions carry ZTNA-like features provide a hybrid deployment model for their ZTNA solution. A hybrid deployment model offers cloud-based and on-premises components. This contrasts with the percentage of respondents who offer a cloud-only or on-premises-only deployment model, which is 11.3% and 5.7% respectively.

These results are in tandem with the shifts in the enterprise IT transformation space where the move to the cloud is now being balanced by cloud repatriation, where workloads are brought back on-premises for performance, cost and strategic reasons. The share of Work from Anywhere (WFA) employees continues to grow while Cloud and SaaS are adopted, which necessitates a cloud-hosted ZTNA. Critical resources will continue to be delivered on-premises, either from the edge or the main data center, with ZTNA hosted locally.

DIAGRAM 2 Respondents' ZTNA solution deployment models



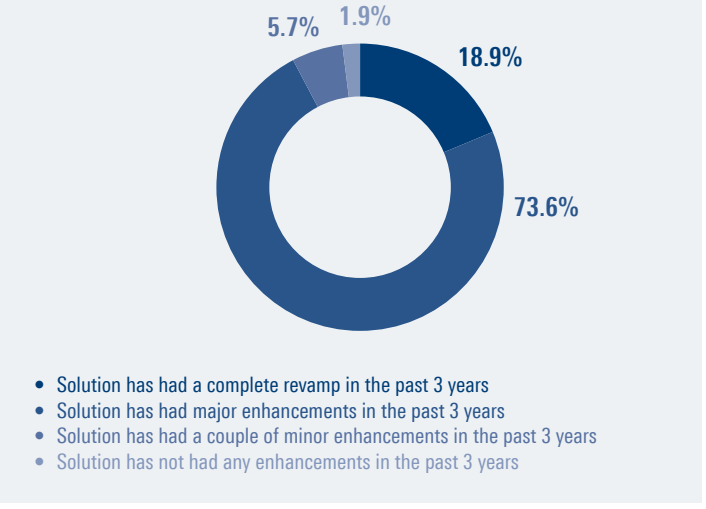
ZTNA solutions continue to evolve rapidly

When asked about the evolution of their ZTNA solutions, 18.9% of respondents stated that they had completely revamped their ZTNA solution in the past 3 years. Likewise, nearly three quarters of respondents (73.6%) made major enhancements within that time frame.

This continuous development in the ZTNA space underscores a dynamic and evolving enterprise IT landscape. Rapidly changing trends and technological advancements compel ZTNA vendors to continually enhance and refine their ZTNA offerings through cutting-edge technologies and mechanisms in order to stay resilient, relevant and marketable.

A small share of respondents (5.7%) made a couple of minor enhancements to their ZTNA solution while only 1.9% did not make any enhancements.

DIAGRAM 3 Evolution of respondents' ZTNA solutions

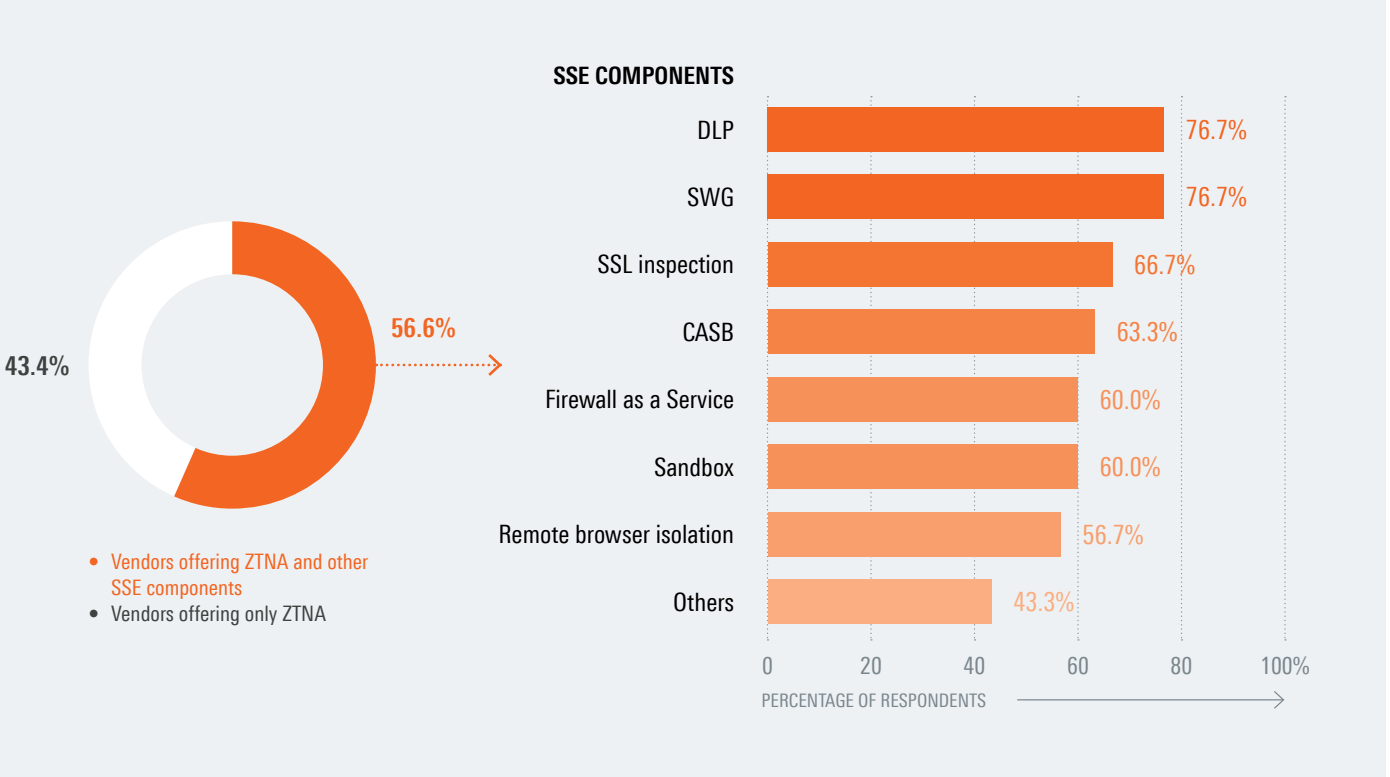


Growth in SSE is driving ZTNA

ZTNA is one of the many components of Secure Service Edge (SSE). More than half of the respondents (56.6%) offering ZTNA offer other SSE components. Of these, 76.7% offer DLP and Secure Web Gateway (SWG). Two thirds (66.7%) offer SSL inspection and 63.3% offer a Cloud Access Security Broker (CASB). Firewall-as-a-Service (FWaaS), sandbox and remote browser isolation are also offered by more than half of the respondents at 60.0%, 60.0% and 56.7% respectively. Other tools, offered by 43.3% of respondents, include Intrusion Prevention Systems (IPS), Digital Experience Monitoring (DEM), device and SaaS security posture management, Managed Detection and Response (MDR), DNS security and filtering, forward and reverse proxies, Virtual Private Network (VPN) and more.

SSE integrates robust security capabilities, including ZTNA, SWG, FWaaS and CASB, into a unified cloud-based service spanning all enterprise users and resources, regardless of their location. This consolidation simplifies security management and makes SSE a convenient and popular choice for enterprises navigating the complexities of managing multiple standalone security tools. By integrating ZTNA within the SSE framework, organizations can fortify their security posture, ensuring more effective access control and protection against a wider range of threats. The growing popularity of SSE is expected to drive ZTNA's adoption in a major way. Yet, 43.4% of respondents only offer ZTNA and no other SSE components.

DIAGRAM 4 Respondents' SSE offerings



3. POWERING IDENTITY AND CONTEXT AWARENESS

Continuous adaptive trust and the need for traffic visibility

ZTNA is based on trust and this trust is derived from the identity and context of each resource, user and device. Identity relates to IDs and credentials while context profiles a resource, user or device by assessing the underlying current circumstances. This involves application types, data sensitivity and criticality for resources. For users this can be the location, time, and history. For devices it involves ownership, hardware and software health as well as security posture. Leveraging identity and context, ZTNA goes beyond traditional static trust models and adopts continuous adaptive trust, where, in addition to identity verification, trust levels are continuously assessed and adapted based on changing conditions, behaviors and other contextual factors.

Establishing continuous adaptive trust requires live transaction data to be continuously analyzed against static attributes (e.g. IDs, privileges and risk profiles) from user, resource and device databases. For instance, real-time device location and security posture must be matched against user credentials and device ID, before initial access is granted. This enables virtual network perimeters to be established, ensuring the users access to authorized resources. Each live connection is continually evaluated against contextual information, such as the number of active sessions, resources accessed, bytes-per-minute and latency. This enables ZTNA to identify anomalies and safeguard resources against intrusion and abuse.

Resource, user and device databases, and live transaction data forms the intelligence requirements for ZTNA. Such intelligence can reside on the enterprise end via internal mechanisms that monitor, analyze and report traffic flows, or it can be introduced by ZTNA vendors via traffic inspection and reporting technologies that are integrated into their solutions. In most scenarios, intelligence from both parties are combined to create comprehensive inputs for ZTNA.

Incomplete asset inventory and poor traffic visibility pose significant challenges

To invoke and execute the right controls and policies, ZTNA requires not just intelligence, but also wider mechanisms and systems that ensure its comprehensiveness, accuracy and usability. This survey takes a look at various challenges faced by ZTNA vendors in delivering the intelligence needed to support ZTNA's identity and context awareness.

An incomplete inventory of resources, devices and users was ranked the most challenging, with 35.2% of respondents strongly agreeing that it poses a challenge for their clients deploying ZTNA. This can be attributed to increasingly complex networks with resources distributed across various platforms, and remote users connecting through diverse devices. Application and device inventories are typically fragmented by departments and locations.

Poor traffic visibility comes a close second, with 29.6% of respondents admitting that it is a significant challenge. The ability to monitor and analyze data packets traversing client networks is crucial for ZTNA. With newer protocols and multi-service applications, visibility tools often struggle to classify traffic by application and service type. Conversely, new monitoring tools can be incompatible with legacy, non-HTTP/HTTPS protocols. The increasing use of sophisticated obfuscation techniques and encryption protocols, like TLS 1.3, ESNI and TLS 1.3 0-RTT further exacerbate the visibility dilemma. In addition to all these, traffic visibility must be real-time so that ZTNA policies can be invoked instantaneously.

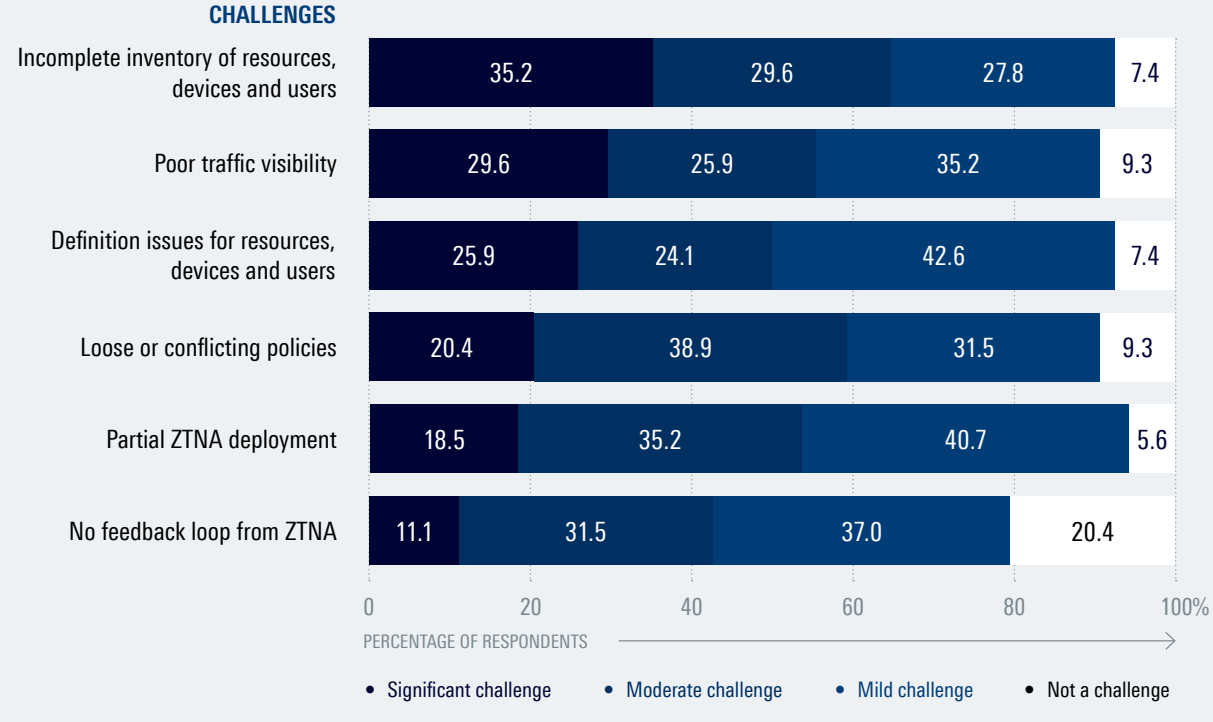
Definition issues for resources, devices and users and loose or conflicting policies also complicate ZTNA deployments, with 25.9% and 20.4% of respondents strongly agreeing that they are a challenge. Poor definitions or a lack of proper definitions across different resources, users and device types results in gaps, inaccuracies and conflicts in policy implementation, and may result in some sessions not being processed altogether.

Partial ZTNA deployments are also a major challenge, according to 18.5% of respondents. Partial coverage, for instance, covering only certain networks, devices, users and resources (e.g. remote workers or Cloud apps only), forces enterprises to fall back on basic access control for the remaining scenarios, which undermines ZTNA's overall effectiveness.

A lack of feedback loops from ZTNA is strongly agreed by 11.1% of respondents as a challenge. This often results in findings made by ZTNA not being incorporated into its future policies. For example, not utilizing ZTNA logs on blocked applications, rogue devices and DDoS attacks in establishing subsequent contexts perpetuates legacy context, resulting in outdated security measures and access controls.

Of all these challenges, real-time traffic visibility can be particularly complex to address. Other shortcomings, such as inventories and definitions can be addressed in just weeks via development and consolidation exercises. Partial ZTNA deployments can be eventually expanded using cloud or on-premise add-ons. Feedback loops can be coded. Delivering real-time traffic visibility demands advanced traffic monitoring and inspection technologies, and deep knowhow of latest traffic trends. Extracting traffic insights in real-time also introduces another layer of computing that can lead to additional latency across user sessions.

DIAGRAM 5 Challenges in establishing identity and context awareness for ZTNA

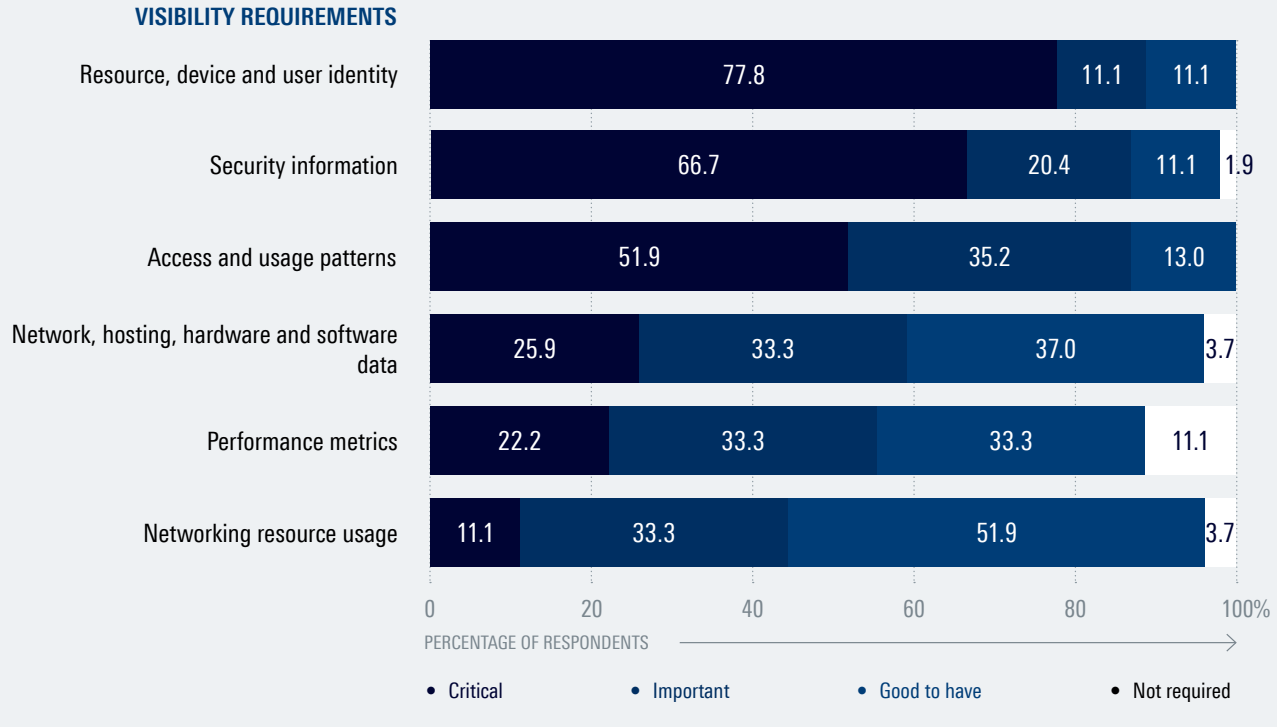


4. THE CRITICALITY OF TRAFFIC VISIBILITY

Traffic visibility most important in identifying resources, users, devices as well as threats and anomalies

In evaluating traffic visibility requirements, respondents were asked to rank the importance of different information categories in supporting ZTNA intelligence. Resource, device and user identity information emerges as the highest-rated category in terms of visibility needs, with 77.8% of respondents stating that it is absolutely critical for ZTNA. 11.1% of respondents agree that it is important and the remaining 11.1% say that it is good to have. Resources include clouds, multi-clouds, applications, databases, files, specific types of content, services, etc. Devices comprise user devices such as laptops, smartphones, IoT devices and servers. Users span on-premise and remote employees, third-party suppliers and customers. Users can also be non-human, as in the case of IoT modules and other applications and clouds that attempt to connect to an enterprise resource. Identifying specific resources, devices, and users enables granular and tiered ZTNA policies based on trust levels, privilege, sensitivity and any other attribute that has been assigned to each identity. It also enables ZTNA to associate real-time context and behaviors for dynamic access control.

DIAGRAM 6 Categories of real-time traffic visibility required for ZTNA across resources, devices and users



Security information, including information on anomalies and threats, is the second highest category, with 66.7% of respondents highlighting that it is an essential requirement for ZTNA. The ability to identify threats such as malware, ransomware and phishing, suspicious URLs such as known C&C IP addresses, and blacklisted applications enables ZTNA to detect potential attacks on the network before these impact enterprise resources. Security information is key to continuous validation of sessions especially in cases of device hijacking and credential thefts where legitimate accounts are manipulated for illegal access to critical data and for sabotage of resources.

More than half of the respondents (51.9%) state that information on user access and usage patterns, such as location, frequency, tenure and users are vital for ZTNA. This information helps ZTNA solutions establish acceptable behavioral baselines which can then be matched against real-time context and behaviors to identify anomalous or suspicious patterns.

This is followed by network, hosting, hardware and software data which is rated by 25.9% of respondents as a critical requirement for ZTNA. This information allows network administrators to identify authorized and unauthorized devices, including IoT devices before permissions are granted. It also enables ZTNA to identify risks associated with rooted or tempered devices and vulnerabilities associated with third-party networks such as public WiFi. This also covers requests from rogue servers or untrusted hosts.

Next are performance metrics such as speed, jitter, latency, packet loss and round trip time which are rated by 22.2% of ZTNA vendors as highly required information for visibility. These metrics are valuable in identifying changes in the state and performance of application stacks and in detecting user behavior that can impact application and network performance, for example large file downloads. It is also useful in identifying unauthorized user requests and DDoS attacks. It can also identify issues relating to ZTNA and other security gateways.

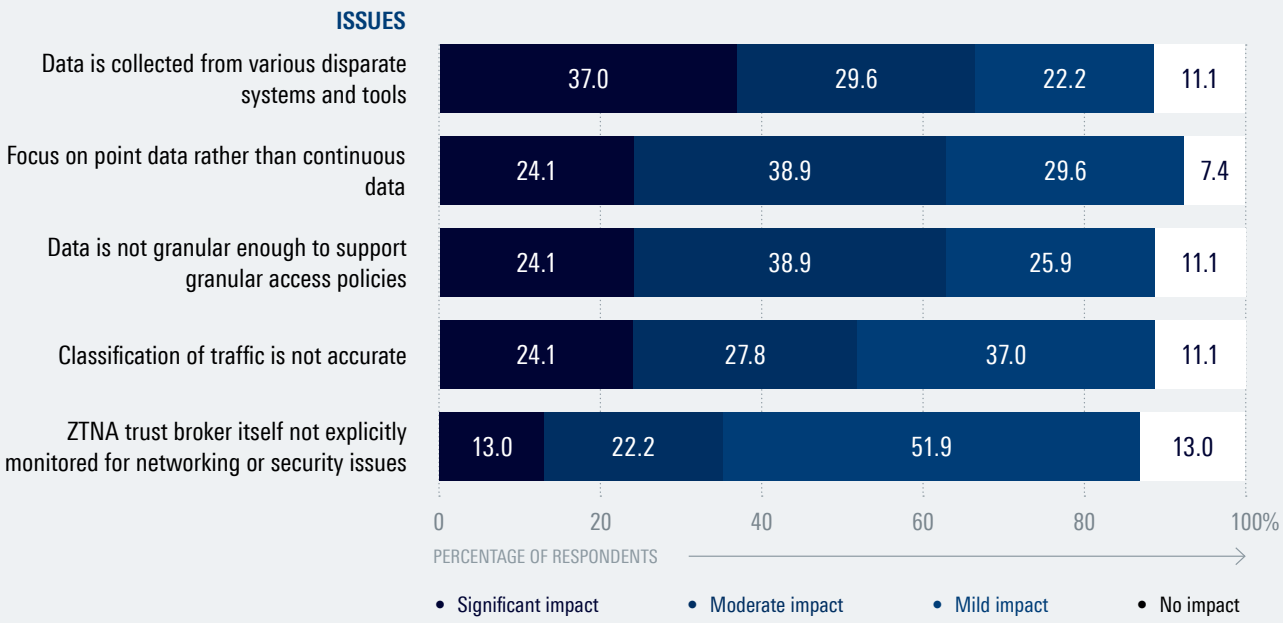
Only 11.1% of respondents state that visibility into networking resource usage, such as CPU, bandwidth and storage is critical. Information on the network is needed to identify and diagnose network congestion and performance degradation issues. It is also a key input in prioritizing critical users and applications.

In-silo traffic monitoring, lack of continuous data points, and generic insights are the biggest challenges in delivering real-time traffic visibility

Despite advancements in network and traffic reporting, there are many inherent gaps in today's monitoring architectures and systems that affect the quality of analytics that is available to ZTNA vendors and enterprises. Among these, disparate systems and tools rank the largest concern, with 37.0% of respondents strongly agreeing that it impacts the effectiveness of ZTNA. This is because data from diverse tools and systems creates inconsistencies and often leads to extensive reconciliation, which impacts network latency, application performance and user experience.

Focus on point data, rather than continuous data, is cited by 24.1% of ZTNA vendors as the second biggest challenge in delivering real-time traffic visibility. Where only point data is available, permission is granted using initial credentials with no further monitoring in terms of user behavior or transactions. Continuous data collection enables cumulative analysis such as session tenure and total bandwidth consumed, which allows deeper insights into the authenticity of each session, and enables access controls to be invoked at any point throughout a session.

DIAGRAM 7 Traffic visibility issues impacting the effectiveness of ZTNA



An equal percentage (24.1%) of ZTNA vendors admit that data not being fine-grained enough to support granular access policies is another significant challenge. Implementing microsegmentation for lateral traffic movement and privilege tiers for LPA is impossible without details at the application-, service-, transaction- and packet-level.

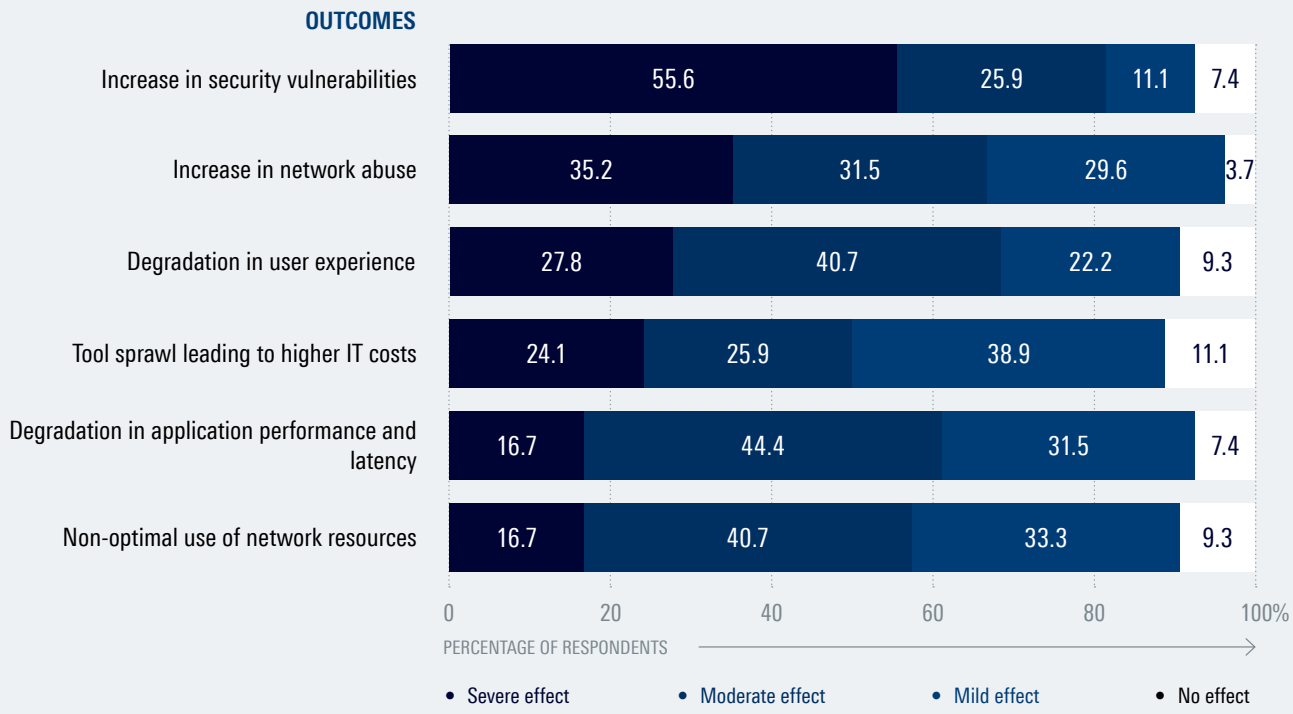
Inaccuracies in traffic classification is another challenge encountered by ZTNA vendors, with 24.1% of respondents strongly agreeing to this. Monitoring tools that lack advanced techniques capable of tackling large traffic volumes and various traffic types, and in some cases, outdated or incomplete references / libraries can lead to various identification errors. Another factor that contributes to this are new protocols, applications and novel attack vectors, which necessitate latest knowhow in application and security trends.

The final challenge is the ZTNA trust broker itself not being explicitly monitored for any networking or security issues, according to 13.0% of respondents who agreed that it has a strong impact. ZTNA gateways, connectors, and controllers form the first-line-of-defense and are vulnerable to cyberattacks like DDoS. Issues such as configuration errors, suboptimal routing and PoP disruption can also go unnoticed.

Deploying ZTNA without adequate traffic visibility may lead to abuse and serious problems with security and user experience

The survey also explored the potential consequences of implementing ZTNA without full visibility into traffic flows. The biggest outcome is expected in terms of an increase in security vulnerabilities, with over half (55.6%) of ZTNA vendors expecting the effects to be severe. Major consequences are also expected in network abuse, according to more than a third (35.2%) of ZTNA vendors, and in degradation in user experience, as anticipated by 27.8% of respondents. These gaps will lead to a serious tool sprawl and subsequently higher IT costs, based on the responses of 24.1% of ZTNA vendors. Application performance and latency is also expected to take a strong hit, according to 16.7% of respondents. Another major consequence, as cited by 16.7% of respondents, is the non-optimal use of network resources.

DIAGRAM 8 Impact of implementing ZTNA without adequate traffic visibility

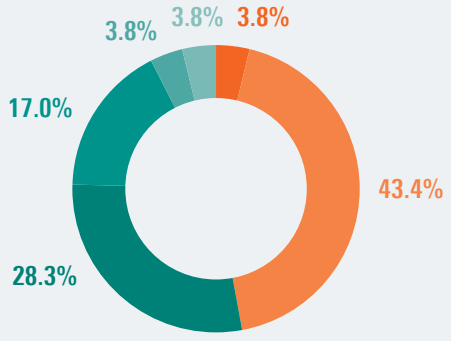


Shortfalls in real-time traffic visibility to undermine ZTNA adoption

The survey finds gaps in traffic visibility impacting not only the effectiveness of ZTNA, but also its adoption among enterprises. These gaps refer to poor monitoring and reporting mechanisms within a ZTNA solution, as well as a lack of monitoring on the enterprise end. According to 43.4% of respondents, the lack of adequate visibility has led to enterprises delaying ZTNA adoption. Another 3.8% of respondents admit to it resulting in enterprises not adopting ZTNA altogether.

Revenues in the ZTNA market are driven by ZTNA's effectiveness in addressing the inversion of traditional networks, where access control and security includes users and resources both inside and outside the network perimeter and where rules are meted out dynamically, based on changing trust levels. Limited analytics lead to generic and sub-optimal implementations, where users and traffic are over-scrutinized or under-scrutinized. Without significant benefits, enterprises are likely to put off their plans to deploy ZTNA or seek other alternatives.

DIAGRAM 9 Impact of gaps in traffic visibility on enterprise ZTNA adoption



While visibility is a serious challenge for ZTNA, 52.8% of respondents claim that this may not impact enterprises' decision to adopt ZTNA. According to 28.3% of respondents, enterprises believe that traffic visibility is something that can be enhanced over time, be it on the vendors' end or the enterprise end. Another 17.0% of the respondents claim that enterprises typically expect ZTNA solutions to come with built-in visibility tools capable of monitoring and filtering their resources, users and devices. These perspectives collectively underscore the indispensability of real-time traffic visibility for ZTNA deployments. Other respondents take a different stance on why a lack of adequate visibility may not impact enterprises' decision to deploy ZTNA. According to 3.8% of vendors, enterprises' access/usage policies are too broad-based and do not require advanced visibility. Similarly, 3.8% of respondents believe that ZTNA deployments are solely compliance-driven and implemented in adherence to best practices, hence, poor visibility has no impact on adoption.

According to

43.4%

of respondents, the lack of adequate visibility has led enterprises to delay adopting ZTNA.

5. A COMPREHENSIVE VISIBILITY TOOL

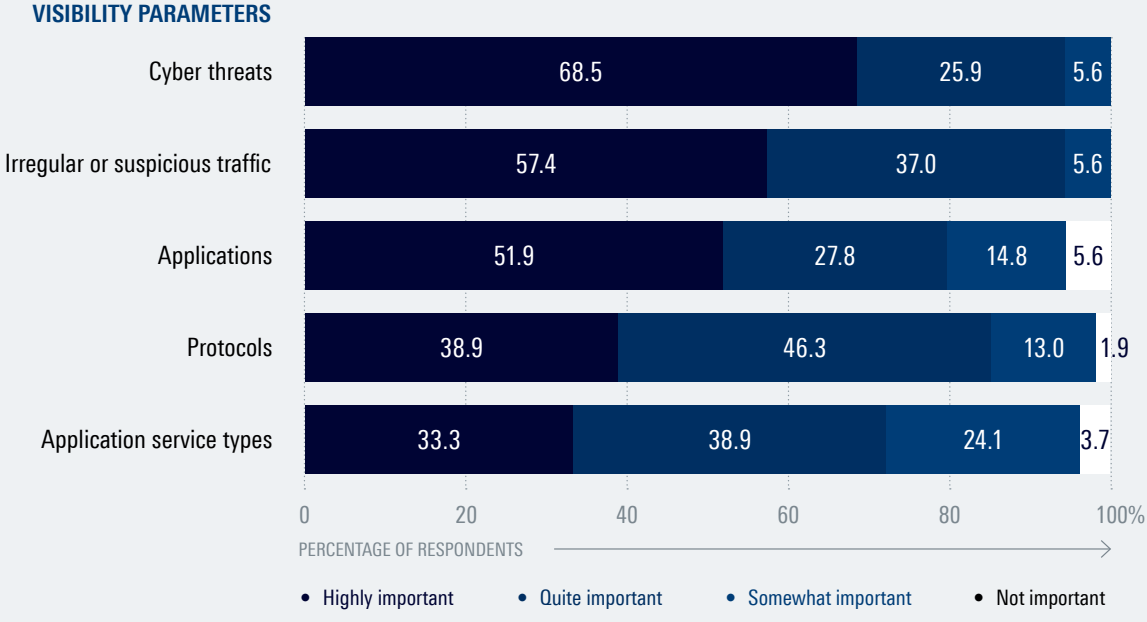
Threat identification, anomaly detection and application awareness among critical traffic parameters for ZTNA

Superior traffic visibility forms the very foundation of ZTNA's access control and security implementations, enabling dynamic, real-time policies that respond immediately to prevailing network conditions. The level of visibility that is required is determined by the mix of enterprise resources, users and devices, and the complexities of the enterprise's own access control and security requirements. Diverse resources, users and devices, and multiple layers of rules, thresholds and conditions often require deeper and more granular traffic information, covering various parameters, from user behavior to application usage, security and network performance.

The survey examined some of the most prevalent categories of traffic parameters in terms of their importance to ZTNA. Topping the list is the identification of cyber threats, with 68.5% of ZTNA vendors finding this highly important. These include threats such as malware, ransomware, denial-of-service (DDoS), phishing and man-in-the-middle (MITM) attacks. This information enables ZTNA solutions to establish continuous adaptive trust and decide whether to maintain or terminate sessions, which facilitates prompt mitigation of ongoing cyberattacks.

Ranking second on the list of parameters is the identification of irregular or suspicious traffic, with 57.4% of respondents stating that this is highly important to them. This category of parameters identifies unusual flows and transactions, for example large file downloads, concurrent log-ins and sudden traffic peaks. These parameters enable ZTNA to detect abnormal behaviors and trigger appropriate responses in real-time.

DIAGRAM 10 Traffic visibility parameters for ZTNA



For example, concurrent logins might prompt a connection freeze, while unexpected spikes in traffic volume may indicate a DDoS attack and lead to access denial.

Identification of applications emerged as the next most important traffic parameter, with 51.9% of respondents agreeing that accurate detection of the underlying applications is highly important. Application awareness enables ZTNA solutions to differentiate traffic flows and identify applications such as Microsoft Teams, Netflix, Skype, Salesforce, WhatsApp and SAP. Based on this information, ZTNA can enforce granular access policies and efficient resource allocation based on the type of application.

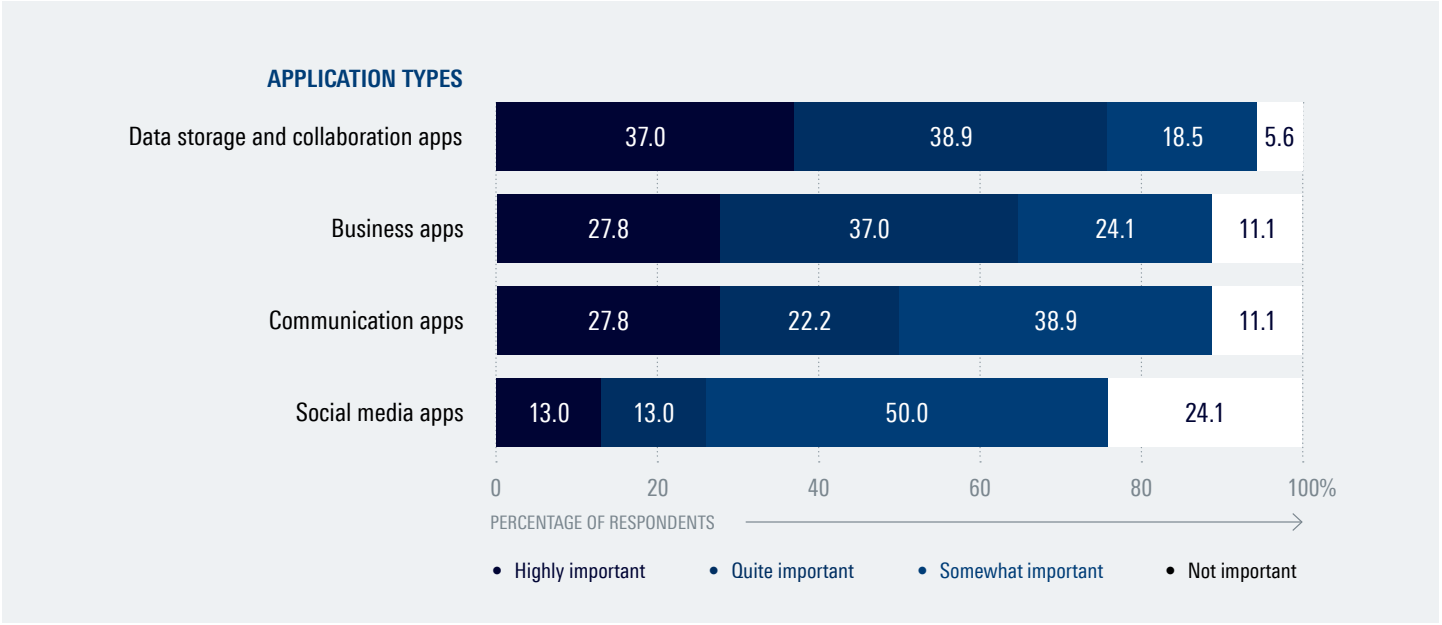
The detection of application protocols such as HTTPS, RTP, SMTP, SRT and WebRTC was ranked next, with 38.9% of respondents rating this as highly important. Each protocol carries different types of data and is associated with different applications. Accurate detection enables ZTNA to apply appropriate access control and allow prioritization of network resources accordingly.

Another one third (33.3%) of ZTNA vendors find that knowing the underlying application service types such as audio, video, mail, file transfer and chat is highly important. Again, this is crucial for fine-grained access controls as a single application may include diverse services with varying criticality. For instance, file transfers in communication platforms like Slack or Zoom may require stricter access controls compared to basic chat features.

Insights on data storage, collaboration and business apps most valuable to ZTNA vendors

ZTNA solutions must prioritize real-time traffic insights differently based on application, service, and traffic types. Critical applications demand intensive monitoring for resource protection and seamless user experience, while general Internet traffic requires lighter oversight. Achieving an optimal balance is crucial for efficient resource utilization without sacrificing security or performance. The survey saw data storage and collaboration apps such as OneNote, SharePoint and Dropbox being ranked the highest, with 37.0% of respondents agreeing that insights on this category of applications are highly important.

DIAGRAM 11 Importance of real-time granular traffic insights for applications



This is followed by business apps such as Salesforce or C4C, with more than a quarter of respondents (27.8%) rating real-time granular traffic insights into this group of applications as highly important. The same level of importance is accorded to communication apps such as Teams or Zoom.

Predictably, real-time granular traffic insights were found to be least necessary for social media apps such as Facebook, Instagram or TikTok with only 13.0% of respondents agreeing that it is highly important.

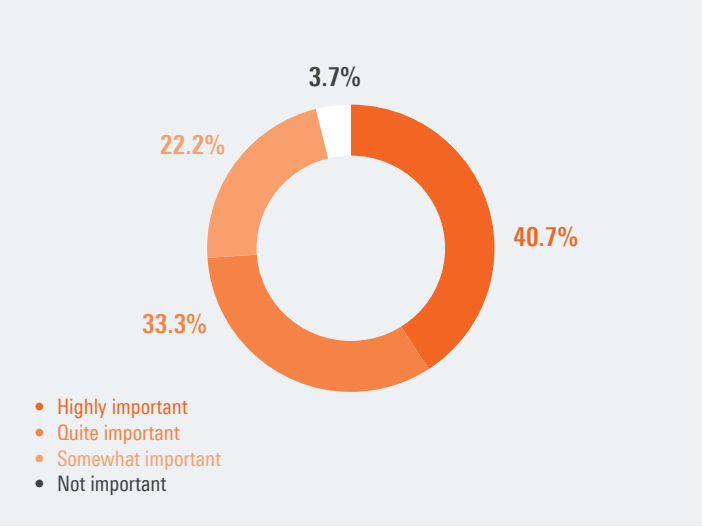
Real-time, granular insights deemed indispensable for ZTNA automation

Given the network complexity and the sheer volume of data traffic traversing enterprise networks, ZTNA solutions must leverage automation for enacting the best policy response without any human intervention. However, this automation requires a constant stream of accurate and fine-grained traffic data points to be collected and analyzed for authentication and dynamic control of user sessions. These data points are equally crucial for developing and validating the reliability of ML and DL models used for ZTNA automation as well.

When it comes to supporting ZTNA automation, 40.7% of respondents state that real-time granular traffic insights are highly important and another third (33.3%) say that these insights are quite important. Another 22.2% of respondents believe that these insights are somewhat important while a small minority of 3.7% of respondents find them to be unimportant.

Automation in ZTNA reduces operational costs by minimizing the need for manual intervention and human resources. It also enhances network performance by enabling more efficient processes and workflows that expedite access control and security decisions. As more ZTNA vendors adopt automation, the need for real-time granular traffic insights will continue to grow.

DIAGRAM 12 Importance of real-time granular traffic insights in supporting ZTNA automation



Regarding support for ZTNA automation,

40.7%

of respondents emphasize the high importance of real-time granular traffic insights.

Encryption tools and shadow IT worsen gaps in traffic visibility

Latest encryption protocols such as TLS 1.3, QUIC and ESNI alongside obfuscation techniques such as DNS tunneling, domain fronting and mimicry, and anonymization using methods such as VPNs progressively erode the traffic information available to monitoring tools. Despite improving data confidentiality and privacy, these methods have an implication on the implementation of zero-trust policies, specifically the effectiveness of ZTNA, as they introduce various gaps in traffic visibility.

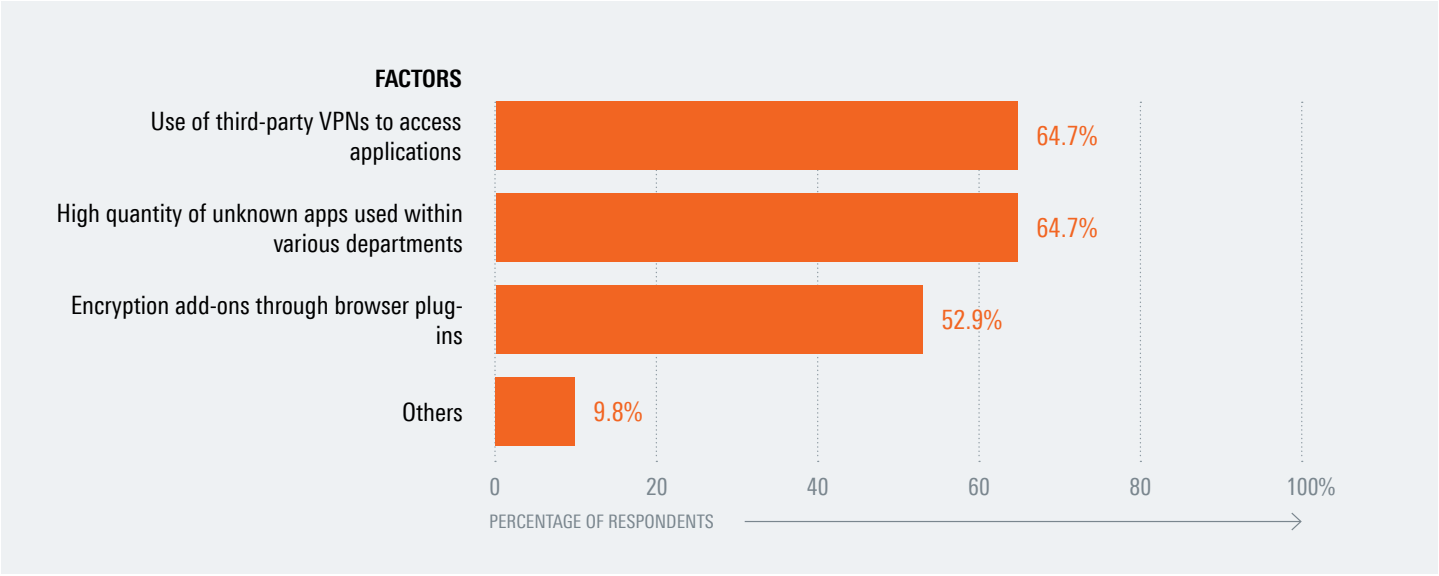
The survey listed a number of scenarios that make encryption, obfuscation and anonymization a huge challenge for ZTNA. The use of third-party VPNs to access applications, especially in the event of BYOD, arises as the top factor, according to 64.7% of respondents. In addition to BYOD and WFA initiatives, employees may use third-party VPNs to circumvent application or geographical restrictions. VPNs obscure critical traffic data points, such as user location, device specification, destination IP address and network usage patterns. This hampers ZTNA's ability to identify applications, classify services and detect behavioral anomalies associated with them, leading to ineffective access control and security vulnerabilities.

An equal percentage (64.7%) express that a high quantity of unknown apps used within various departments may be another factor. Otherwise known as shadow IT, this refers to the use of unknown or unauthorized applications by employees without the approval or oversight of the IT department. When encryption is then used by these applications, it exacerbates traffic visibility challenges, as the encrypted data becomes opaque to network monitoring tools. This hinders ZTNA's ability to identify the applications used, apply relevant access policies, detect potential security threats and monitor the flow of sensitive information effectively.

The enablement of encryption add-ons through browser plug-ins was pointed out by 52.9% of respondents. Users enable such add-ons for private browsing. However, third-party plug-ins can create opportunities for malicious actors to inject and intercept website content, compromising legitimate enterprise web applications. Traffic from these plug-ins can then evade ZTNA due to encryption-induced visibility gaps.

A few respondents (9.8%) also mentioned other causes. Regardless of the cause, advanced encryption and obfuscation mechanisms significantly hinder ZTNA's ability to build behavior models and baselines to detect anomalies and deviations.

DIAGRAM 13 Factors resulting in encrypted, obfuscated and anonymized traffic being a challenge for ZTNA



6. DEEP PACKET INSPECTION

DPI leverages packet and flow-level analysis to deliver cutting-edge application awareness, as well as behavioral and performance metrics, empowering ZTNA's identity and context awareness with real-time traffic visibility. Next-gen DPI takes this a step further by expanding visibility to encrypted traffic, ensuring in-depth and comprehensive insights across any flow.

ipoque, a Rohde&Schwarz company, is at the forefront of delivering next-gen DPI technology made available through its advanced OEM DPI engines — R&S®PACE 2 and R&S®vPACE. These highly adaptable software engines seamlessly integrate into any ZTNA solution, providing detailed IP traffic insights in real-time. Both engines provide:

- **Real-time IP traffic classification** through a combination of pattern matching and behavioral, statistical and heuristic analysis, for accurate and reliable identification of applications, protocols and service types.
- **Extensive weekly-updated signature library** with thousands of signatures that are kept up-to-date via continuous automated testing, monitoring of traffic captures for new application versions, and a robust global QA infrastructure.
- **Encrypted traffic intelligence (ETI)**, a built-in technology leveraging complex ML and DL techniques, high-dimensional data analysis and advanced caching for the reliable classification of encrypted, obfuscated, and anonymized traffic flows.
- **Metadata extraction** for high-quality, in-depth statistical and advanced metadata to determine KPIs and QoS / QoE metrics. These include source and destination addresses, packet size and timing, payload content, flow information, timestamps, session information and user identifiers.
- **Deployment support** for any physical or virtualized environment. R&S®vPACE, in particular, is VPP-based and tailored for virtualized and cloud-native functions (VNFs and CNFs) within cloud computing environments.
- **Unlimited, high-performance** packet filtering, especially with the VPP-based R&S®vPACE which delivers the fastest real-time processing in the market, suitable for highly demanding cloud computing environments.
- **Exceptionally low memory footprint**, ensuring fastest real-time processing with efficient resource utilization for a lean implementation.

Together, these capabilities enable R&S®PACE 2 and R&S®vPACE to offer unparalleled visibility and intelligence in today's complex network environments. Both engines empower ZTNA vendors to provide effective access control and comprehensive network security while maintaining impeccable performance.

Here's how R&S®PACE 2 and R&S®vPACE fulfil the entire spectrum of ZTNA intelligence needs:

- **Granularity:** The ability to classify applications down to the service type enables ZTNA solutions to process access requests for any type of traffic — audio, video, file transfer and more. It enables ZTNA solutions to enforce precise access control policies instead of implementing broad and binary decisions.
- **Comprehensiveness:** Continuous R&D by an in-house team of developers, and extensive partnerships with leading universities ensure ZTNA vendors can tap into state-of-the-art ML-based DPI capabilities and stay ahead of latest trends in the application and threat landscape.
- **Real-time filtering:** High-performance engines enable real-time decision-making with no additional latency. Latency is a critical factor for enterprises processing traffic at the edge, for instance in 5G URLLC services, such as autonomous driving, robotic surgeries, and industrial automation.
- **High throughput processing:** Unrivaled throughput and linear scalability ensure that enterprises of all sizes can rely on ipoque-powered ZTNA solutions.
- **Lightweight architecture:** Both engines are lightweight with incredibly efficient memory usage, ensuring little-to-no impact on ZTNA in terms of computing overheads.
- **First packet classification (FPC):** Classifies traffic from the very first packet of a flow. Compared to solutions that offer detection after a few packets have already traversed the network, FPC ensures that ZTNA solutions can make decisions that are instant and consistent for the entire flow.
- **Industry and vertical knowhow:** ipoque's support engineers can help ZTNA vendors tailor tracking and monitoring of traffic types and patterns that are specific to the industries they serve, such as IIoT / smart manufacturing and private 5G networks in education or mining.

- **Comprehensive threat awareness:** ipoque's threat awareness through pattern and signature matching, behavioral baseline comparison and advanced AI and ML algorithms ensures that malicious traffic can be detected straightaway.
- **Flexible SLAs:** Even the simplest ZTNA solution can leverage ipoque's traffic intelligence.
- **Custom DPI signatures:** Enables enterprises to define custom or lesser-known applications on the fly, for complete coverage.

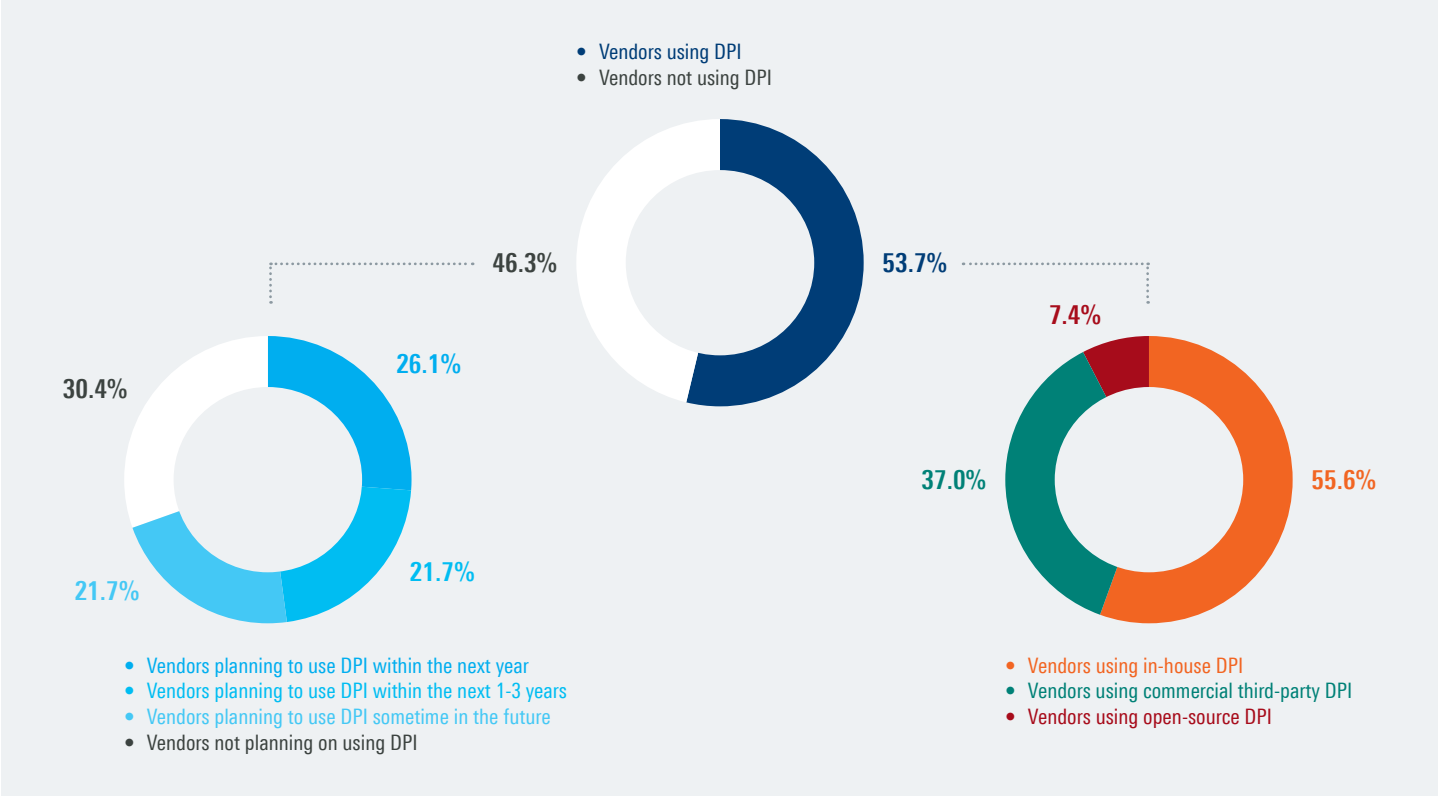
More than half of ZTNA vendors use DPI for real-time traffic visibility

The use of DPI for monitoring and analyzing traffic flows across IP networks has seen steady growth over the years. Deployed directly as a network component as in the case of mobile core networks, or embedded as part of today's expanding suite of networking and cybersecurity tools such as packet brokers and next-generation firewalls (NGFWs), DPI has a profound influence on how network owners and vendors monitor and manage their traffic flows.

It is therefore not surprising that DPI is deployed widely in the ZTNA space. Of the 55 vendors surveyed, more than half (53.7%) are currently using DPI for real-time traffic visibility. Next-gen DPI tools such as R&S®PACE 2 and R&S®vPACE deliver unparalleled capabilities in detecting and analyzing traffic flows in real-time, enabling ZTNA to establish continuous adaptive trust for any user. It drives the instantiation of virtual network perimeters for each validated request to ensure users have seamless access to as many resources as they need, while keeping these sessions secure from end-to-end.

The remaining 46.3% of respondents comprise of 3 different groups. The first are vendors who use DPI in addition to a number of other techniques such as heuristics. The second group has home-grown visibility tools such as home-grown parsers. The third group uses third-party visibility or filtering solutions, including probes and firewalls. These tools incorporate DPI in some way, while others comprise non-DPI techniques such as flow-based monitoring, endpoint monitoring and AI/ML.

DIAGRAM 14 Vendors' current and future use of DPI for ZTNA



ZTNA vendors predominantly favor in-house and commercial DPI solutions

The survey looked into the different models governing DPI deployments.

Among them, the first is in-house DPI, developed and managed internally by the ZTNA vendor. It helps ZTNA vendors avoid licensing fees and dependence on third-party providers. ZTNA vendors can have complete control over their DPI technology, allowing them to incorporate customizations, integrations, and security measures tailored to their ZTNA solution and customer needs. Among the ZTNA vendors using DPI, the majority (55.6%) use in-house DPI.

The second largest share of ZTNA vendors (37.0%) use commercial third-party DPI. This refers to DPI technology developed and maintained by a third-party DPI vendor. These vendors focus solely on DPI technology and staff DPI specialists expert at developing solutions leveraging the latest AI and ML techniques. They offer extensive libraries built through continuous research into global and local traffic flows, ensuring comprehensive coverage. Commercial DPI vendors also bring wide industry experience to the table as their technology is already deployed across industries. This allows ZTNA vendors to access DPI solutions tailored to cater to specific verticals, such as health, IT, finance or others based on their enterprise customer portfolio. ZTNA vendors using third-party commercial DPI also benefit from robust support and customer service, eliminating the need to engage additional third-party experts for consultation or issue resolution.

The last model is open-source DPI, which involves using freely available codebases. Its benefits lie in accessibility and lower initial costs, particularly for new ZTNA vendors. However, open-source DPI implementations can be highly susceptible to security risks due to their open nature — anyone can access the code. They may also lack advanced features, leading to high customization costs down the line. Long-term sustainability is also uncertain, as open-source providers may discontinue support at any time. The survey shows that only a small share (7.4%) of respondents rely on open-source DPI.

Close to half of ZTNA vendors without DPI plan to adopt the technology in the next 3 years

Among vendors who are currently not using DPI, 26.1% plan to use DPI for their ZTNA solutions in the next year while 21.7% plan to use it within the next 1-3 years. Another 21.7% plan to use it sometime in the future. These findings point to a steady demand from the ZTNA sector for DPI solutions that can align their capabilities and outputs to meet the needs of rapidly evolving zero-trust solutions. Additionally, with the growing popularity of SSE, demand for DPI is expected to be pushed further by other sister components within SSE, such as CASB and SWG.

The survey also finds that 30.4% of ZTNA vendors who are currently not using DPI do not have any plans to do so in the future. A common factor cited by these vendors is that their existing tools are adequate in delivering the insights they need.

Two vendors however, cited performance degradation concerns, especially in latency sensitive environments such as virtual desktop infrastructures (VDIs) and operational technology (OT) environments. This stance can be attributed to the fact that not all DPI solutions are built the same way and may have varying capacity and capabilities. Next-gen DPI suite of solutions, for example R&S®PACE 2 and R&S®vPACE, are designed to handle higher capacities and perform excellently in various domains, including ZTNA. R&S®vPACE specifically, which is VPP-based, caters for computing-intensive environments and is capable of supporting CNFs such as 5G UPFs. Cloud-based ZTNA solutions benefit tremendously from the speeds and throughput capabilities from DPI that is optimized specifically for the cloud.

Of ZTNA vendors not currently using DPI,

26.1%

plan to integrate it into their ZTNA solutions within the next year.

7. CONCLUSION

ZTNA has emerged as a pivotal security measure for enterprise networks characterized by flexible architectures and hybrid data, users, and communications. However, ZTNA requires comprehensive, granular and real-time traffic visibility across these intricate networks to effectively implement dynamic access controls based on continuous adaptive trust.

This report focused on identifying the traffic awareness needs and challenges encountered by ZTNA vendors and the role of DPI in addressing these challenges. Findings from the survey reveal that:

- ZTNA solutions are rapidly evolving, prompting vendors to consistently enhance their offerings to stay ahead of the market.
- Continuous adaptive trust in ZTNA relies on identity and context awareness, which requires live transaction data to be matched against information from ZTNA databases.
- Establishing identity and context awareness presents several challenges, with poor traffic visibility being one of the most significant. Poor traffic visibility leads to insufficient or inaccurate live transaction data, and prevents ZTNA databases from being dynamically updated with the latest analytics on resources, users and devices, effectively impairing ZTNA intelligence.
- Real-time traffic visibility on resource, device and user identity is the most critical for ZTNA, followed by visibility on security threats, as well as access and usage patterns.
- Visibility challenges, such as incomplete, inaccurate and coarse-grained data, can hinder ZTNA's ability to implement granular access policies and deliver continuous authentication based on adaptive trust.
- Without traffic visibility, ZTNA solutions fail to prevent security vulnerabilities, network abuse, and user experience and application performance degradation.
- Current visibility challenges are a major hindrance to enterprise ZTNA adoption and impede immediate revenue for ZTNA vendors, except in cases where enterprises expect to improve traffic visibility over time.
- Important traffic visibility parameters that need to be identified include threats, anomalies, applications, protocols and application service types.
- ZTNA automation is imperative for timely and precise decision-making and it largely depends on real-time, granular traffic insights.
- Latest encryption protocols and obfuscation techniques, such as third-party VPNs and encryption plug-in usage, progressively erode traffic visibility, complicating ZTNA implementations.
- DPI has become a critical network intelligence tool for ZTNA vendors struggling to deliver application awareness and critical behavioral and performance metrics.
- The demand for turnkey and commercial DPI solutions is likely to increase across ZTNA vendors serving enterprises from various industries.

Findings from the survey reiterate the importance of deep visibility in ZTNA solutions, underscoring the crucial role of DPI within ZTNA deployments. As a leading DPI provider, ipoque continuously leverages advanced ML and DL for delivering real-time, fine-grained traffic analysis via its next-gen DPI engines, R&S®PACE 2 and R&S®vPACE. Both engines offer high-speed, granular analytics, enriching ZTNA solutions with real-time identity and context awareness for continuous adaptive trust and dynamic policy enforcement. Empowered by next-gen DPI, ZTNA vendors can deliver an industry-tailored, scalable solution that covers all essential elements of zero-trust with top-notch QoS. As DPI-driven insights are equally indispensable for related SSE components like CASB and SWG, ZTNA vendors can diversify their services to ensure competitiveness and optimize revenue potential.

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

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG
Trade names are trademarks of the owners
Version 01.00 | March 2024
Next-gen DPI for ZTNA: Advanced traffic detection for real-time identity and context awarenesss
Data without tolerance limits is not binding | Subject to change
© 2024 Rohde&Schwarz GmbH&Co. KG | 81671 Munich, Germany
© 2024 ipoque GmbH | 04109 Leipzig, Germany