APPLICATION AWARENESS

REAL-TIME TRAFFIC VISIBILITY FOR ZTNA WITH NEXT-GEN DPI

Enhancing ZTNA's adaptive trust with advanced DPI for continuous application and threat awareness

ROHDE&SCHWARZ

Make ideas real

CONTENT

1. INTRODUCTION

Emerging solutions in the networking and cybersecurity space demand deeper traffic visibility. Zero-trust network access (ZTNA), sometimes referred to as a software-defined perimeter, is a prime example of this. ZTNA is designed to utilize every bit of network information to establish 'trust', to control user access to resources and to continuously monitor user behavior.

This whitepaper explores the principles of zero-trust in ZTNA and how methodologies such as least privilege access (LPA) and microsegmentation create virtual network perimeters that keep resources hidden and secure from unauthorized usage and threat actors.

It examines in depth the concept of continuous adaptive trust and how the identity and context of users, devices and resources can be established in near real time using a wide range of network and traffic variables mined from the network. This however, is easier said than done due to the growing visibility gaps introduced by newer, more complex traffic delivery techniques aimed at securing, concealing and disguising the underlying applications and services.

The above analysis is followed by an introduction to next-gen deep packet inspection (DPI) as a cutting-edge technology for extracting network and traffic analytics in real time. This looks at how DPI's comprehensive and accurate traffic intelligence strengthens ZTNA's mechanisms for continuous adaptive trust and supports ZTNA's dynamic context-aware policies. DPI's capabilities in supporting the detection of cyberthreats and network abuse are also analyzed.

Also discussed are a number of popular ZTNA use cases that illustrate DPI's flexible reporting and adaptability to different network environments. This paper also provides guidance on DPI build-or-buy decisions for vendors in the zero-trust space.

2. ERA OF ZERO-TRUST

2.1. LPA and microsegmentation

ZTNA originates from the idea of zero-trust, where no user is trusted by default, but only until and unless they are verified.

Why zero trust?

Today, enterprises manage distributed applications and multi-cloud architectures. Users and devices connecting to these resources are also becoming increasingly dispersed – across branches, campuses, mobile networks, home offices, IoT sites and public venues. This has two implications. Firstly, granting access to resources becomes complex as requests originate from untrusted networks and unmanaged devices. Secondly, more and more resources are accessed via the Internet, exposing IP addresses and increasing the network's attack surface. ZTNA addresses these concerns by putting in place the concept of LPA, where access to any part of the network is denied unless explicitly granted. It enforces granular access policies with microsegmentation and privilege tiers, where every additional application, folder and file requires re-authentication and every user is continuously validated based on the latest profile inputs. ZTNA simplifies access control with a verification framework that works for users inside and outside the network perimeter, and enhances network security by keeping the network topology hidden at all times.

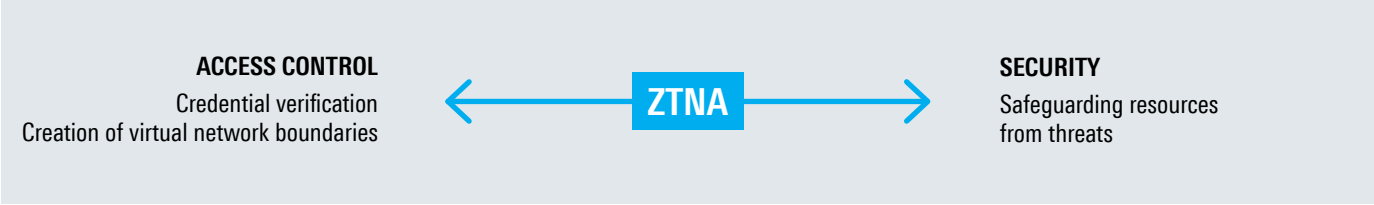

Figure 1: ZTNA key functions

2.2. ZTNA key functions

The main functions of ZTNA are access control and security. Access control uses credential verification to create virtual network boundaries, ensuring seamless access to enterprise resources. Security aims to keep resources safe from intended and unintended security threats. ZTNA combines both point verification and continuous validation to secure a session end-to-end.

A ZTNA solution comprises controllers, which handle control plane communications, as well as gateways and connectors, which handle user traffic. Instead of MPLS links, ZTNA uses encrypted tunnels over the public Internet to connect to private resources, while reverse proxies are used for Cloud and SaaS resources. ZTNA can be deployed in the cloud or on-premises. It uses on-device agents for managed devices, while unmanaged devices use a browser portal. With a per-user licensing method, ZTNA ensures consistent features and policies for every given identity and context.

Agent-based	Agent-less
On-device client	Browser plug-in + ZTNA portal
Authentication of user by ZTNA controller	Authentication of user by ZTNA controller
Traffic is filtered through a firewall and tunneled directly to the resource	Traffic is filtered through a ZTNA connector which acts as a reverse proxy for the resource
Any resource	Resources using web-based protocols (HTTP/HTTPS) only
Supports device health and security checks	Does not support device health and security checks
Managed devices only	Managed and unmanaged devices (work-from-home (WFH), external users)

Table 1: Agent-less and agent-based ZTNA

Figure 2 depicts the architecture for Cloud ZTNA for both agent-less and agent-based models.

The details for each model are summarized in Table 1.

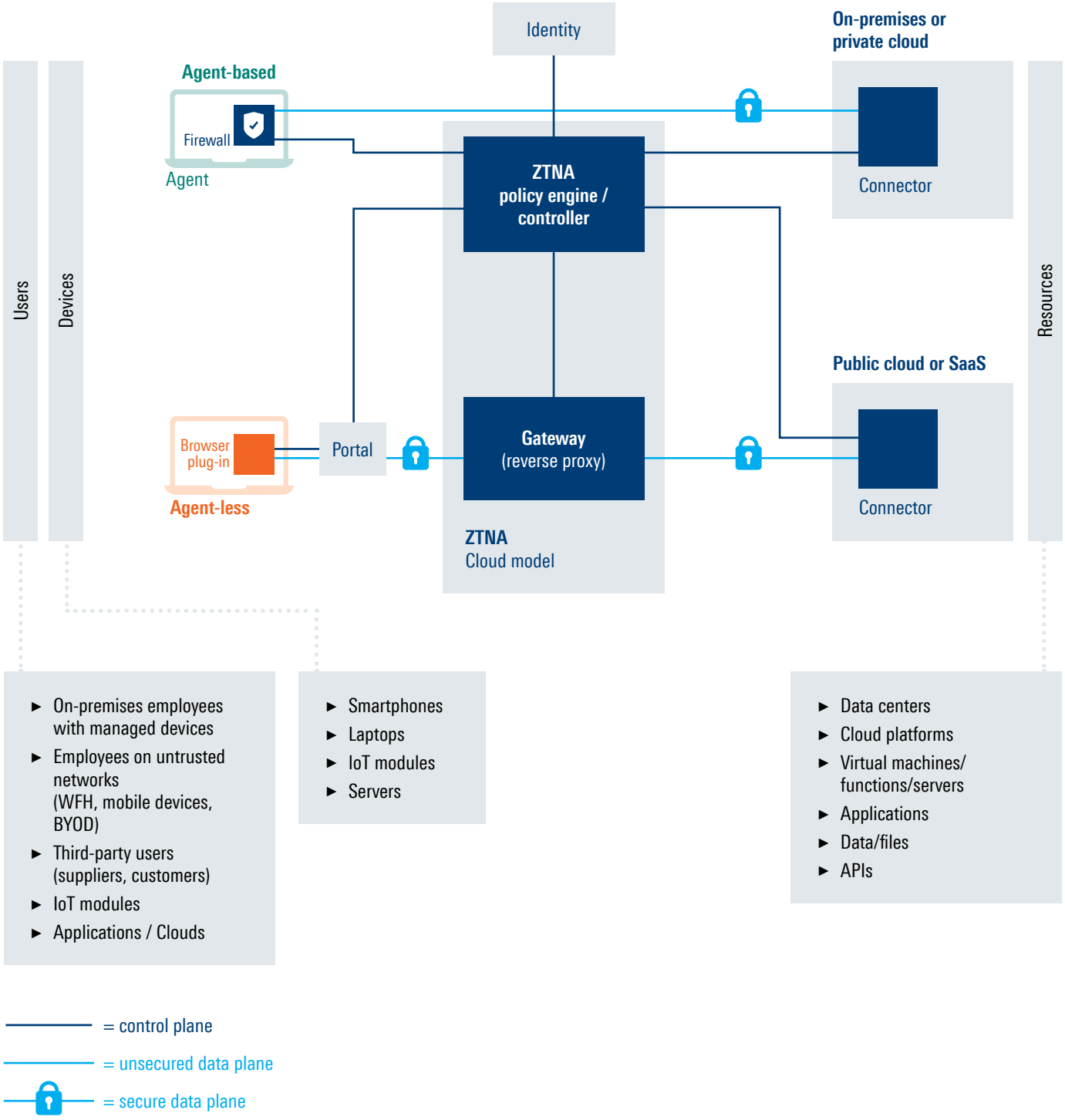

Figure 2: Architecture of Cloud ZTNA

2.3. Factors driving ZTNA

There are a few key factors driving the deployment of ZTNA.

The rapid growth of work-from-anywhere users and the increase in IoT deployments has led to an inverted network. ZTNA enables access control and security to be moved to the service edge, close to where distributed users are concentrated and where IoT modules are clustered. This ensures better application performance and enhanced QoS.

The growing number of hybrid users necessitates network access rules which are consistent and uniform regardless of user location. By providing on-premises / standalone deployment options in addition to cloud-based deployment, ZTNA ensures a universal framework for managing access, especially for BYOD use cases and for users at the branch or campus.

IoT endpoints and API-based communications have led to a steady rise in machine-initiated connections to enterprise resources. ZTNA is designed to authenticate these requests, for example IoT modules transmitting telemetry data and third-party servers making API requests.

Apart from on-premises and private cloud-hosted applications, distributed users need access to SaaS and cloud resources. ZTNA utilizes reverse proxies to hide cloud and SaaS applications from discovery, while delivering the same level of protection for all resources.

A distributed application architecture requires traffic to move between multiple Clouds or between the Cloud and an enterprise's data center, resulting in security vulnerabilities from lateral movement of traffic. ZTNA circumvents this by using microsegmentation.

Using VPN for remote connectivity, especially for work-from-anywhere and small branches, can be prohibitive due to hardware costs and additional backhauling. ZTNA uses encryption over the public Internet to link up as many remote users as necessary, making remote access cost-effective.

Increasingly complex cyberthreats make enterprises require a stronger security framework for managing users. By combining a few strategies – hiding resource discovery, minimizing the attack surface and keeping each session monitored – ZTNA significantly reduces the risks of network attacks and abuse.

Laws and regulations governing data privacy and data protection have become increasingly stringent. ZTNA simplifies compliance by leveraging context-aware authentication using the LPA principle and microsegmentation.

Thanks to ZTNA, access control and security can be moved to the service edge, close to where distributed users are concentrated and where IoT modules are clustered, ensuring better application performance and enhanced QoS.

3. BUILDING CONTINUOUS ADAPTIVE TRUST

3.1. Defining continuous adaptive trust

Trust is at the core of ZTNA. Two key components used to establish trust are identity and context – applicable to resources, devices and users. Identity (ID) is determined via unique identification records. Context is pinpointed by profiling a user, device or resource, for example by timing, location, health of hardware / software, behavior and security posture. The combination of identity and context paves the way for continuous adaptive trust in ZTNA, where decisions are no longer based on identity records alone, but dynamically evolving parameters.

3.2. Visibility issues in establishing continuous adaptive trust

Continuous adaptive trust requires data from resource, device and user databases to be matched against live transaction data. Databases include user directories, resource lists and device inventories. Live transaction data, in contrast, comprises traffic analytics captured via in-built network systems, such as SNMP or Netflow, and/or specialized tools, such as network performance monitoring (NPM) software and IP probes.

Visibility challenges

With emerging traffic trends, acquiring adequate data points on live transaction data can become complex and challenging. One such data point is classification of traffic by applications (e.g. Salesforce or Microsoft Teams) and by services (e.g. video gaming or audio streaming). New protocols, for example dTLS, and latest applications are not readily detected by most visibility tools. However, some tools have issues in supporting legacy (non-HTTP/HTTPs) protocols and applications. These visibility issues are exacerbated by the prevalence of stricter encryption, obfuscation and anonymization methodologies, which add to the number of blind spots on monitoring radars. Latest encryption techniques such as TLS 1.3, ESNI, DNS over HTTPS/DNS-over-TLS and TLS 1.3 0-RTT progressively erode readable data from packet communications, making it impossible to determine the underlying application.

A lack of application awareness can be debilitating for ZTNA. Access rules can only be based on static parameters such as ID and location, with risks associated with a specific application or service not imputed during authentication. As a result, enterprises are forced to fall back on default ZTNA policy settings that may not be aligned to the enterprise's vulnerabilities. Additionally, losing visibility of certain app groups, be it private applications running on legacy protocols or newly launched SaaS and Cloud applications, hinders the adoption of universal ZTNA that is expected to work on all application classes.

Insufficient processing capacity to filter today's traffic volumes can pose additional visibility challenges. ZTNA's continuous adaptive trust requires uninterrupted packet capture, so that user behavior is monitored throughout the entire session. At the same time, some user sessions have to be processed in edge computing nodes which are built on super-fast packet processing techniques such as vector packet processing (VPP), aimed at supporting low-latency applications. As an edge application, ZTNA thus needs a traffic filtering capability that can handle huge traffic loads and match up to the latency requirements that are typical in cloud and edge environments.

ZTNA also requires a traffic filtering tool that can deliver asset metrics. This would include hardware attributes such as a device's OS version and its recent software updates, which are important in detecting misuse of user credentials. Similarly, metrics relating to resources, for example, server addresses and application responsiveness, are important in detecting threats such as IP spoofing and man-in-the-middle attacks.

For a successful implementation, ZTNA also needs insights on its own performance and security. ZTNA gateways, connectors and controllers form the first line of defense and are highly susceptible to threats from compromised devices and DDoS attacks. ZTNA solutions can also be impaired by configuration and API errors, hardware/software issues, sub-optimal routing, PoP disruption and ineffective redundancy/failover mechanisms. Identifying traffic irregularities can be challenging for conventional tools that are not programmed to detect elusive anomalies.

4. NEXT-GEN DPI FOR ZTNA

4.1. Introducing DPI

DPI is a traffic detection technology that uses packet-level and flow-level analysis to deliver application and threat awareness as well as a wide range of metrics relating to traffic behavior and performance.

A leading provider of cutting-edge DPI technology, ipoque, a Rohde&Schwarz company, offers next-gen DPI that merges:

- **Traffic classification methodologies** encompassing pattern matching and advanced behavioral, statistical and heuristic analysis to accurately and reliably identify protocols, applications and services. It boasts a comprehensive signature library, comprising thousands of signatures which are updated weekly.
- **Encrypted traffic intelligence (ETI)**, a cutting-edge technique which combines machine learning (ML), deep learning (DL) and high dimensional data analysis as well as advanced caching methods to identify encrypted, obfuscated and anonymized traffic.
- **Metadata extraction** which provides high-quality metrics and fine-grained communication details. These include basic, statistical and advanced metadata, such as speeds, packet loss and QoS.
- **Additional features and plug-ins**, including tethering detection, output interface for standardized formats such as IPFIX, first packet classification and the ability to define custom application signatures.

ipoque's DPI technology is available through its renowned DPI engines, R&S®PACE 2 and its VPP-based counterpart, R&S®vPACE. R&S®PACE 2 boasts high-performance packet filtering with a throughput per core of 14 Gbps on average, while R&S®vPACE delivers up to three times speedup to support more demanding environments such as cloud computing.

4.2. DPI: A great fit for ZTNA

DPI enables unlimited packet filtering and is both highly adaptable and easily scalable, making it suitable for ZTNA. For example, R&S®PACE 2 and R&S®vPACE are available as software engines that can be embedded directly into a ZTNA solution. As most current ZTNA solutions are cloud-only, R&S®PACE 2 and R&S®vPACE can be deployed in a ZTNA broker or controller as either a traditional or as a virtualized/containerized function. This flexibility is important, given that different ZTNA solutions are built on different architectures based on the environment and functionalities they cater for.

DPI's form factor also contributes to ZTNA's performance efficiencies and is important in optimizing its overheads. In this regard, R&S®PACE 2 and R&S®vPACE both boast exceptionally low memory footprints which ensure resource efficiency and enable a lean implementation.

4.3. Establishing context-aware trust with R&S®PACE 2 and R&S®vPACE

DPI enhances ZTNA primarily via in-depth, fine-grained traffic insights that power ZTNA's mechanisms for continuous adaptive trust and support its granular access policies. For example, credentials of a remote user and the device ID are matched against the information extracted from DPI analysis, for example data on user location, services being accessed (e.g. uploads of files), applications used (e.g. Salesforce), device posture and the ZTNA agent version. This enables initial authentication and sets up a connection.

To establish continuous adaptive trust and keep the connection alive, a ZTNA broker can tap into analytics streams provided by DPI throughout a session, which enables it to establish subsequent 'contexts'. This includes data such as bytes used per minute, cumulative usage, duration of usage, real-time device updates, total number of applications accessed, type of transactions and session performance. This brings errant behavior and anomalies that would otherwise be hidden to the surface.

For example, ten unrelated application sessions accessed under an employee ID may indicate device hijacking. Similarly, a legitimate transaction performed repeatedly over hours, despite a matching device ID and correct user credentials, may require a connection freeze until the usage is verified further. High latency on a CRM app will require ZTNA to restrict low-priority users temporarily. Likewise, a sudden slowdown of a sensitive application may require ZTNA to terminate an existing session and re-establish connection.

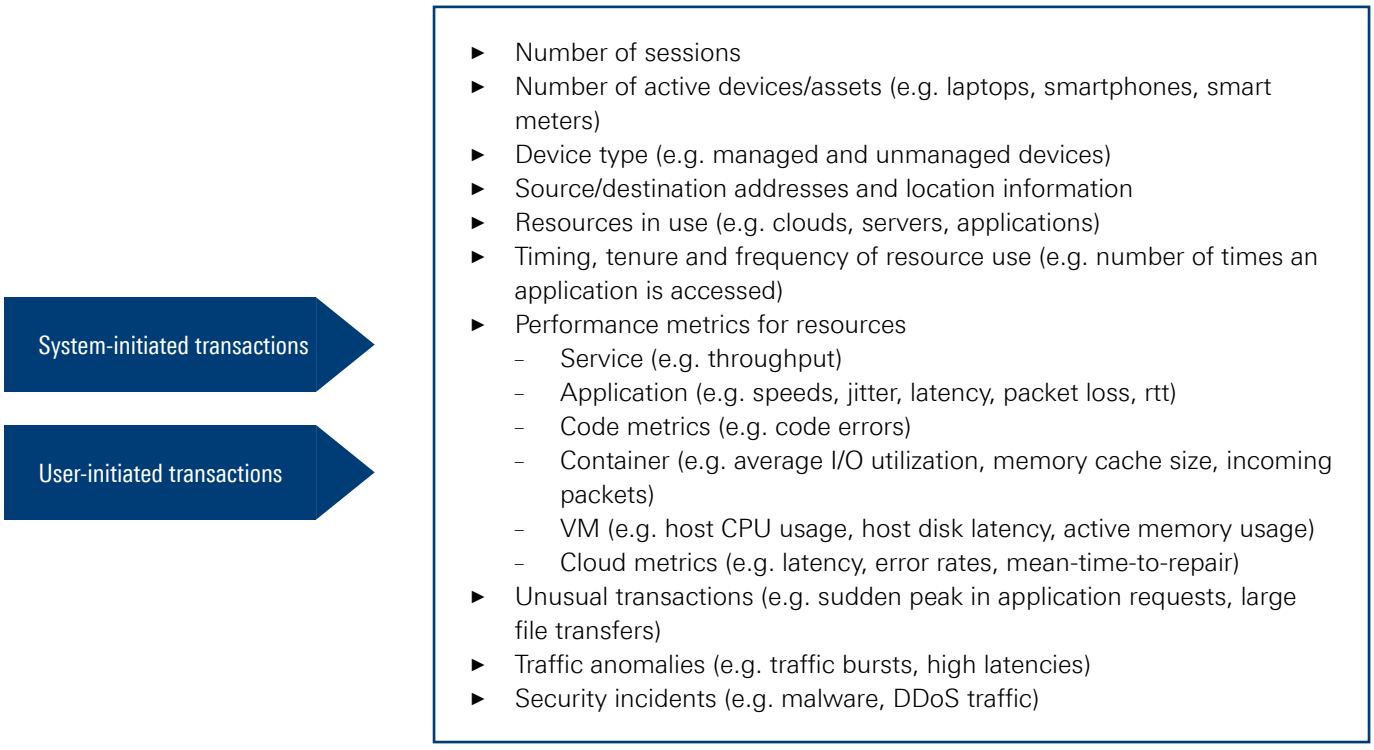

Figure 3: Live transaction data supported by DPI

Figure 3 lists live transaction data that can be established using real-time traffic analytics provided by next-gen DPI engines such as R&S®PACE 2 and R&S®vPACE. Live transactions can be system-initiated or user-initiated. System-initiated transactions refer to automated communications by servers and devices that arise from activities such as OS upgrades, database updates, database backups, auto caching, system notifications and API requests. User-initiated transactions cover activities by a human user, such as file creation, browsing and downloading of content.

Apart from live transaction data, ZTNA uses a dynamic database that provides referential information for executing access control policies and actions for each enterprise. Analytics from DPI plays an important role in validating, updating and enriching these databases. Figure 4 illustrates how DPI analytics feeds into such a database.

DPI enhances ZTNA primarily via in-depth, fine-grained traffic insights that power ZTNA's mechanisms for continuous adaptive trust and support its granular access policies.

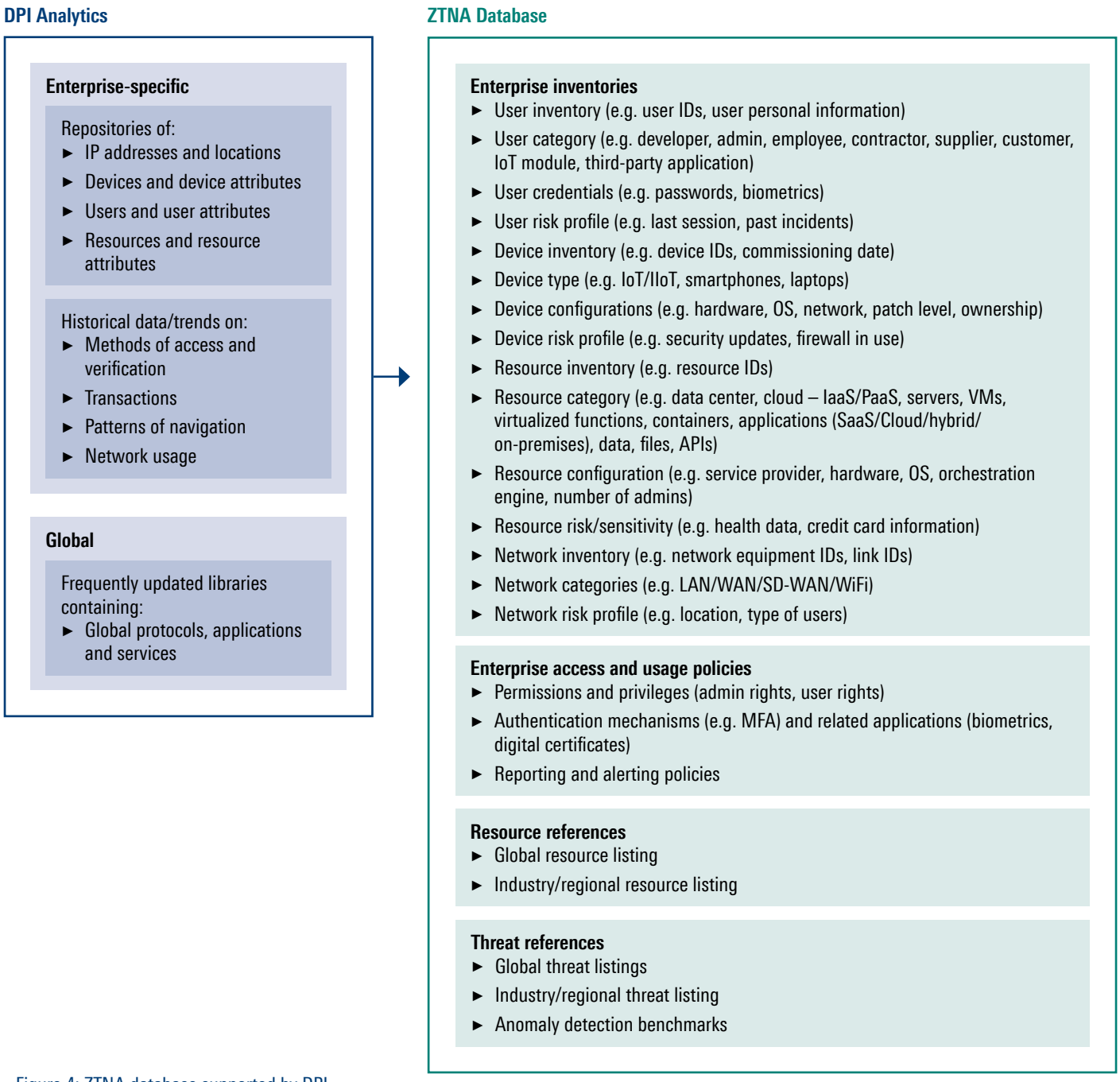

Figure 4: ZTNA database supported by DPI

4.4 How application awareness supports granular ZTNA policies

Apart from supporting ZTNA's mechanisms for continuous adaptive trust, DPI also plays a significant role in shaping ZTNA's granular policies, leveraging real-time application awareness. This is illustrated in the following example of a proprietary video conferencing application that manages live demonstrations for customers:

- At the highest level, network administrators are granted access to the entire cloud, allowing them to manage the computing, storage and networking needs of all co-hosted applications. For example, it enables them to optimize cache storage and assign additional CPU based on current workloads.

- At the next level, application managers are provided access to the main application folder comprising only the sub-applications and components related to the video conferencing application. This will include databases, files, programs, templates and media folders. This allows application managers to perform backups, execute code upgrades, compress files for extra space, troubleshoot application performance issues such as high latency and resolve network bugs.

- At the subsequent level, content managers are provided access to only the content hosting sub-application within the main folder where they can upload, download, transfer, modify and delete media files.

- At the lowest level, session hosts and registered attendees are provided access to only the front-end interface which allows live hosting, streaming and messaging. Users at this level have their specific rights configured in their respective user accounts.

Next-gen DPI libraries deliver highly reliable, accurate classification for any application, protocol or service, leveraging thousands of signatures accumulated over time. Table 2 shows how ipoque's DPI technology classifies traffic from two popular video conferencing applications.

DPI tools such as R&S®PACE 2 and R&S®vPACE additionally provide enterprises the flexibility to add their own custom signatures. This expands the universe of identifiable resources to include private applications and private clouds, in line with an enterprise's resource ecosystem.

Layer 4	Layer 7		
Protocol	Protocol	Application	Services
UDP	SRTP	Microsoft Teams	File transfer Audio Video Controlflow
TCP	HTTPS	Zoom	Audio Video Controlflow
UDP	SRTP	Cisco WebEx	Audio Video Controlflow

Table 2: DPI classification for sample video conferencing applications

4.5 Enhancing security with DPI-driven threat intelligence

Enterprise resources are susceptible to various forms of cyberattacks such as malware, zero-day attacks, code injection and ransomware. These resources are also vulnerable to user negligence, which can lead to accidental data exposure and data loss.

ZTNA endeavors to detect every unauthorized transaction, regardless of whether these involve outright damage to the resource as in the case of data infiltration, exfiltration and theft, or are aimed at slowing down application performance or breaking into private data records without the necessary permissions. DPI-powered threat intelligence can greatly fortify ZTNA's defense against any form of prohibited access and unauthorized transaction by:

- **Detecting flows that are anomalous, suspicious or malicious.** DPI information can be used to identify traffic irregularities at various levels as listed below:

  - User-level
    - New user
    - Failed request
    - Unusual timing
    - Unusual transaction (e.g. file sharing)
    - Frequent access
    - Concurrent access attempts
    - Concurrent sessions

  - Device-level
    - New/unknown device
    - Unusual device location/IP address
    - Unknown ISP

- New software version
- Automatic device update
- New removable media device
- Reappearance of a lost/stolen device
- Poor security posture

– Resource-level
  - New resource
  - Unusual request to sensitive/restricted resources
  - Modification or deletion of resources
  - Large data transfer/export/import
  - New administrator account
  - Changes in user privileges
  - Changes in security policies/controls
  - Deletion of access/error logs
  - Deletion of security records
  - Brute force authentication
  - System configuration changes

– Performance
  - High latency
  - Sudden high throughput
  - Significant drops in network activity

► **Identifying known threats using threat signatures**
By matching anomalous, suspicious and malicious traffic flows against updated threat intelligence, R&S®PACE 2 and R&S®vPACE can help detect threats on the network in real time. For example, unusual IP addresses, URLs and file hashes can be part of a phishing campaign. A DV SSL certificate can indicate a possibly malicious website being used to send unauthorized requests.

► **Uncovering issues with a ZTNA solution**
R&S®PACE 2 and R&S®vPACE traffic analysis can identify issues with the ZTNA solution itself. Examples of these are:

– A sudden spike in control traffic can indicate a brute-force attack on the ZTNA broker
– Changes in ZTNA user traffic throughput/performance can mean software and hardware issues in one or more ZTNA gateways and connectors
– Requests from or to new/unknown applications and IP addresses can point to malware or rogue servers
– Verification failures can be caused by API issues instead of a credential mismatch

ZTNA endeavors to detect every unauthorized transaction, regardless of whether these involve outright damage to the resource as in the case of data infiltration, exfiltration and theft, or whether they are aimed at slowing down application performance or breaking into private data records. DPI-powered threat intelligence can greatly fortify ZTNA's defense against any form of prohibited access and unauthorized transaction.

5. REAL ZERO-TRUST

5.1 Comprehensive zero-trust execution via DPI

Continuous adaptive trust, granular policies and embedded threat detection are not the only zero-trust tenets powered by DPI. With many ZTNA vendors steering their ZTNA solutions towards full compliance, DPI can be capitalized on further to support comprehensive zero-trust execution which involves the fulfilment of the following principles:

LPA – Using DPI analysis, access can be restricted as narrowly as possible to a single application (e.g. Slack), single service (e.g. messaging) or single transaction (e.g. read/write), ensuring access is given only to what is required.

Microsegmentation – DPI also helps in enforcing microsegmentation as lateral movement of traffic across files, applications and cloud is detected automatically via traffic metadata and application classification information.

SSO – DPI mitigates risks associated with ZTNA's single sign-on (SSO) implementation. For example, more than five device locations in a single day can point to compromised passwords. A prolonged SSO application session can indicate an ongoing brute-force attack. DPI analysis of user behavior can also reveal eavesdropping and token thefts, among others.

MFA – Apart from providing system-level information on locations and devices used to impute passwords, thumbprints, voice signatures or OTPs, DPI can also provide the analytics needed to identify techniques commonly used to circumvent MFA, for example replay attacks, MiTM and SIM swapping.

Latest encryption protocols – Next-gen DPI solutions such as R&S®PACE 2 and R&S®vPACE come with encrypted traffic intelligence, which enables full visibility into encrypted, obfuscated and anonymized traffic flows, even across latest protocols such as TLS 1.3. This equips ZTNA with the visibility needed to identify and monitor all traffic flows traversing enterprise resources as well as packets channeled via its own TLS encrypted tunnels. This mitigates the risk of data infiltration and data loss.

Universal coverage – Through weekly updated signature libraries, continuous R&D and custom signatures, DPI identifies any application hosted in any environment – on-premises, Cloud or SaaS, enabling coverage across all enterprise application types.

Support for unmanaged and BYOD devices – DPI analytics on a device, including its OS, browser, software updates, IP addresses, ISPs and security information such as its patch level, endpoint security solution and recent security updates, is useful in establishing device profile and security posture. This information is also used in hybrid ZTNA deployments to keep tabs on BYOD devices used on-premises.

Single data loss prevention – To ensure a single data loss prevention (DLP) policy, all traffic that is relevant to the enterprise, including shadow IT applications, SaaS and web applications must be identified and filtered in real-time. Advanced DPI libraries are continuously updated with the signatures of these applications, including new version releases, allowing real-time detection across any protocol, application or service.

5.2 Next-gen ZTNA

Next-gen ZTNA solutions, which will be superseding first-gen offerings in the near future, are expected to pack many new features and bring ZTNA performance and coverage to the next level. Advanced DPI solutions will fast track vendors' efforts in this space, by supporting:

- **Next-level performance**
  High-performance DPI engines, built on the VPP framework, can support next-gen ZTNA solutions to achieve the following performance benchmarks:
  - 99.999% uptime
  - Scalability for any number of users and resources
  - Extremely low-latency for security processing (10ms)
  - Performance SLA for SaaS applications

- **Digital experience monitoring**
  Digital experience monitoring (DEM) allows ZTNA to couple access control and security with experience monitoring. As enterprise application stacks expand to include Internet pathways, third-party CDNs and edge computing, DPI's analytics enable next-gen ZTNA to deliver DEM metrics such as webpage load times, the processing speed for an e-commerce payment and traffic latency between a connected windmill cluster and the server. This enables ZTNA to detect even the smallest degradation or anomaly in user experience.

- **AI/ML based automation**
  The level of data granularity delivered by DPI enhances ZTNA's ML/DL algorithms used in automating the authentication and control of user sessions. This is crucial as accurate data points collected over extended periods, such as those provided by DPI, are required in developing, testing and validating the reliability of ML/DL models. Additionally, next-gen DPI tools such as R&S®PACE 2 and R&S®vPACE ensure zero gaps in traffic visibility and coverage by using advancements such as ETI and first packet classification (FPC).

- **Many-to-many and multi-tier access requests**
  DPI's real-time classification of existing and new protocols, applications and services, covering both private and SaaS applications, combined with rich traffic metadata, allows next-gen ZTNA to expand its scope to cover:
  - Resource-to-device communications, for example an enterprise learning portal updating course literature via a device client installed on a managed laptop
  - Inter-resource communications, for example, a web server hosted on-premises drawing updates from an archived database hosted in the cloud
  - Intra-network communications, for example a data center firewall sending automated updates to the firewall at a branch LAN

- **Assigning identities to API originators**
  DPI analytics helps ZTNA solutions to identify API originator details such as the IP address, the location and tokens, alongside the applications and services that are involved. This information enables ZTNA to assign identities and control third-party access to its APIs and network resources, ensuring better API security.

- **Automatic network segmentation**
  DPI's application awareness can be used to identify the most optimal sub-net architecture, based on patterns of user access and navigation. By using DPI's data points on variables such as IP address ranges or server clusters, and application performance and user experience metrics, the rules for automated segmentation can be optimized according to application performance and user experience.

Next-gen DPI tools such as R&S®PACE 2 and R&S®vPACE ensure zero gaps in traffic visibility and coverage by using advancements such as encrypted traffic intelligence and first packet classification.

One of DPI's core propositions is its ability to stay ahead of the latest advancements in the IP traffic space, which leaves virtually zero blind spots in traffic detection and classification. This quality sets DPI apart from other visibility tools in delivering the reliability and accuracy that is much needed by ZTNA.

6. USE CASES

DPI benefits virtually every ZTNA solution, across any use case. The following use case examples illustrate how ZTNA solutions are enhanced with real-time traffic awareness from DPI.

6.1. DPI for ZTNA in secure service edge

Secure service edge (SSE) comprises a set of cloud-based access control and security services, namely ZTNA, SWG, CASB, NAC, Sandbox, SSL Inspection and FWaaS. Each of these services caters for specific user types (e.g. ZTNA caters for remote users and unmanaged devices), and specific resource types (e.g. CASB caters for cloud and SaaS applications). The popularity of SSE is driven primarily by the widespread adoption of work-from-anywhere (WFA) and the increasing dependence on Cloud and SaaS applications.

DPI supports WFA policies with real-time traffic intelligence, which allows 24/7 monitoring of employee activities and resource usage. By combining information on applications, IP addresses and behavioral anomalies, DPI can detect security vulnerabilities associated with WFA, which include device hijacking, theft of credentials, illegal hotspots and malware.

An SSE solution can deploy R&S®PACE 2 or R&S®vPACE as a shared source of cloud-delivered traffic intelligence, leveraging DPI's software form-factor, lean implementation and super-fast performance. This would allow uniformity across SSE's entire toolset, specifically across access control and security rules, monitoring and reporting formats, and threat responses. It allows application signature updates to be accessible in real time, across the entire network. Enterprises with hybrid applications and hybrid IT architectures, in particular, benefit significantly from having an SSE solution that is enriched with a shared DPI capability.

SSE can also benefit from DPI that is deployed exclusively in ZTNA, by tapping into ZTNA's security alerts. An unknown device or a behavioral trigger, such as a WFA employee's attempt to access a non-authorized application, can preempt sister components such as CASB (for Cloud- and SaaS-related transactions), NAC (for transactions relating to on-premises resources) and SWG (for web-related transactions).

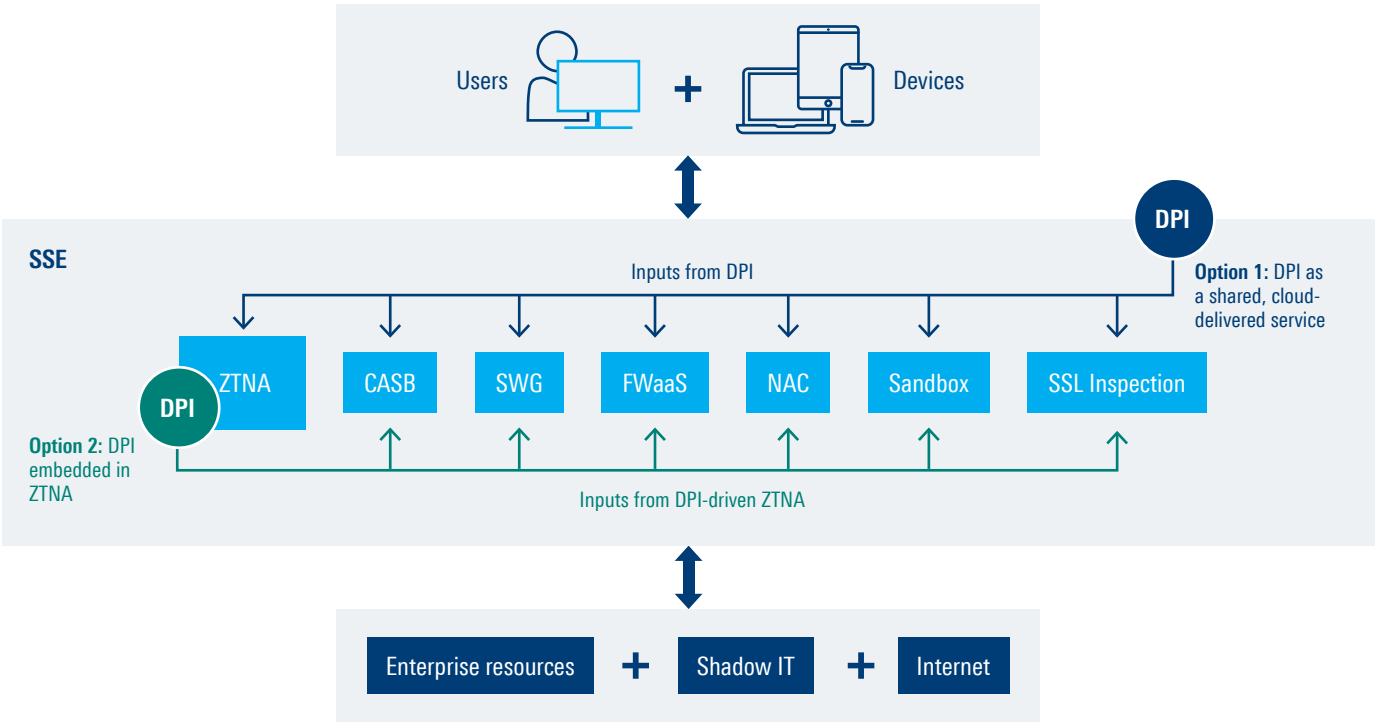

Figure 5: DPI-enhanced ZTNA for SSE

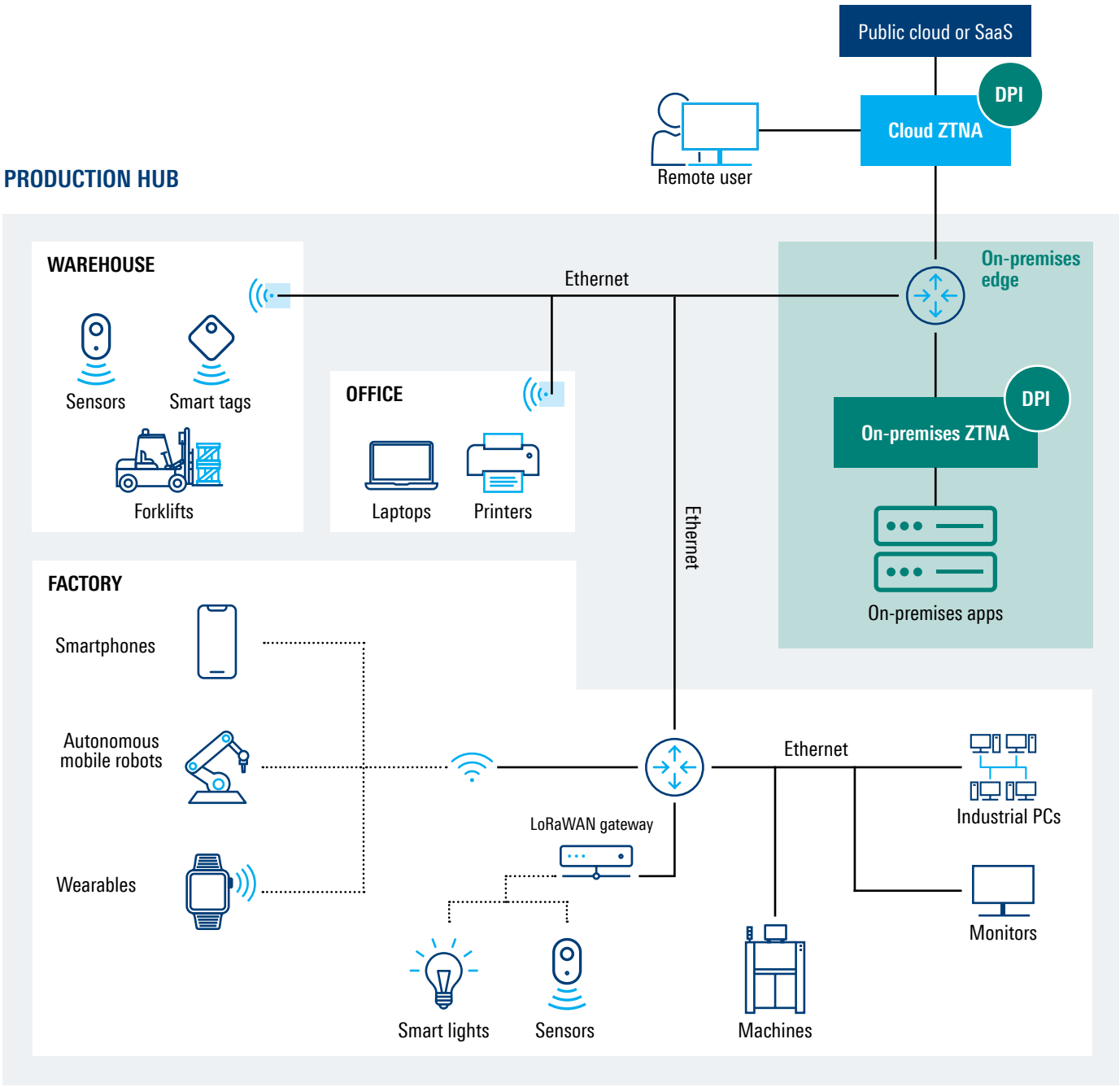

Figure 6: DPI-driven ZTNA for IIoT in smart manufacturing

6.2. DPI for ZTNA in IIoT-based smart manufacturing

Precedence Research[1] expects the global Industrial IoT (IIoT) market to reach USD 1.56 trillion by 2032, increasing at a CAGR of 17.2% from 2023 to 2032. A key concern that overshadows this rapid growth is security, with enterprises already investing millions to reduce vulnerabilities and mitigate potential threats. In its recent report, Straits Research[2] estimates the IoT security market to grow at a CAGR of 29.8% between 2023 and 2031, reaching USD 122.3 billion. One of the key industry verticals within IIoT is smart manufacturing, where high-speed, low-latency applications control and manage a wide range of IT/OT assets and infrastructure. Smart manufacturing benefits from ZTNA as it enables IIoT assets such as computers, robots, machines, wearable devices, sensors, vehicles, monitors, smart tags, meters and cameras to securely access various applications hosted on-premises and in the Cloud. Figure 6 illustrates a typical network architecture for smart manufacturing. In this use case, DPI equips ZTNA with fine-grained traffic analytics that supports access control and security. A sample of these analytics is listed below:

1) Industrial IoT Market Report, Precedence Research
2) IoT Security Market Report, Straits Research

Resources

- IIoT application type (e.g. on-premises, cloud and SaaS applications)
- IIoT applications (e.g. Azure IoT, SAP Predictive Asset Insight)
- Protocols (e.g. Profibus, Modbus TCP, Profinet, AMQP, MQTT, CoAP)
- Data centers, Clouds and servers

Devices

- IT/OT device IDs (via digital certificates)
- IT/OT device public /private IP addresses and location
- IT/OT device health status (e.g. downtime, hibernation)
- IT/OT device security posture

IIoT Networks

- IIoT network topology (e.g. LAN, WLAN, 5G, data center)
- Network devices (e.g. CPEs, routers, wireless transmitters, wireless receivers, probes, firewalls, Internet gateways)
- Performance of network devices (e.g. speeds, latency)
- End-to-end network performance and bandwidth utilization (e.g. packet loss)
- M2M communications between sensors and machines
- Application-to-machine communications (e.g. automated system updates for OT assets)
- Suspicious, malicious and anomalous traffic flows (e.g. new protocols, changes in network throughput)

In a smart manufacturing setting, access requests take place continuously as devices (analog and digital), wired and wireless, operate around the clock in active and hibernation modes. These devices draw instructions and send messages to remotely hosted engineering, control and automation applications. In this environment, DPI analytics are used to ensure that all active sessions on the network are authorized. This mitigates security risks that arise from malicious activity by external parties, employee negligence and internal sabotage. By deploying DPI, a ZTNA solution used in an IIoT setting is able to:

- Identify unauthorized IT devices (e.g. laptops) and OT assets (e.g. remote terminal units, programmable logic controllers)
- Identify IT/OT asset failures or disruptions (e.g. machine breakdown, power issues)
- Identify device-related cyberthreats (e.g. corrupted software, denial-of-sleep attack, device hijacking)
- Identify user-related cyberattacks (e.g. credential stuffing, employee sabotage)
- Identify unauthorized users in the facility (e.g. facility intruders, unauthorized staff)
- Monitor movement of workers on-site (e.g. navigation outside designated zones and outside shift hours)
- Identify unauthorized resources (e.g. malicious sites, banned URLs)
- Implement additional access controls for critical resources (e.g. intellectual property, patent information, formulae, financial records, customer records) both on-premises and in the Cloud
- Identify resource-related cyberattacks such as ransomware, spyware, phishing attacks, data theft and malware
- Identify security issues related to the network (e.g. MQTT hijacking, Modbus hijacking, eavesdropping, sinkhole attacks)
- Identify unauthorized network usage (e.g. for personal use)

DPI-enhanced ZTNA is specifically important in smart manufacturing use cases which involve:

- A large number of connected OT assets
- Interconnected production plants, managed centrally
- Connected OT assets which are dispersed over extended distances within a production facility
- Multiple wireless networks (both IP and non-IP networks such as WiFi, LTE/5G, LTE-m, NB-IoT, Zigbee, LoRa, Sigfox)
- Operations which are controlled remotely by hybrid employees
- Presence of connected devices (such as smartphones, USB devices and delivery vehicles) which are owned and managed by third-parties.

6.3. DPI for ZTNA in private 5G campus networks

As of February 2023, around 200 private 5G deployments were registered globally, according to GSMA Intelligence[3]. Private 5G networks are expected to become a critical infrastructure across many key economic sectors, powering shipyards, energy plants, airports, university campuses and stadiums, to name a few. A private 5G network can be an open network that grants mobile connection to any user within a gated physical area, or a closed network that grants mobile connection exclusively to the organization's devices and users. Taking the example of a private 5G network deployed in a university campus, the following illustrates sample analytics provided by DPI:

Devices

- Device type (e.g. managed laptops, unmanaged smartphones, IoT modules)
- Device IP address, location and mobility pattern
- Device health status
- Device security posture

Users

- Active users
- User session data such as timing, tenure and bandwidth consumed
- Behavioral pattern (e.g. frequency of access)

Resources

- Application type (e.g. on-premises, SaaS, web apps including shadow IT apps)
- Applications (e.g. Splunk, proprietary smart campus apps)
- Protocols (e.g. FTP, HTTPS, SMTP, dTLS webRTC)
- Services used (e.g. video conferencing, email, messaging)
- Public and private cloud
- VMs/Containers

Campus networks

- Active connections to private 5G
- Active connections to local 5G small cell nodes
- Managed device connections to public 5G
- Network devices (e.g. CPEs, small cells, Wi-Fi routers, gateways, RAN equipment)
- Performance of network devices
- Network performance metrics at each of the following layers:
  - Entire private 5G network
  - 5G Slice (eMBB, URLLC and mMTC)
  - Small cell nodes
  - WiFi nodes
  - FWA nodes
- Network congestion, QoS degradation and network failure
- Anomalous traffic flows such as sudden surge in traffic or unusual data/file transfers

This information powers granular ZTNA rules for network access, which enables the university to:

- Identify unauthorized devices (e.g. guest laptops, third-party drones)
- Monitor unmanaged devices (e.g. private wearables)
- Detect device-related cyberthreats such as device hijacking and credential abuse
- Identify unauthorized users and their physical location (e.g. library, dormitory, auditorium)
- Identify user-related cyberthreats (e.g. abuse of admin credentials)
- Identify users with cloned SIMs
- Identify illegal resources (e.g. malicious or piracy sites)
- Implement additional verification steps for sensitive data (e.g. student health records, student exam records, staff personal information)
- Block resource-related cyberattacks (DDoS, data infiltration, malware)
- Identify performance and security issues related to network devices such as RAN nodes, small cells, CPEs, WiFi routers, FWA nodes
- Ensure traffic flows are channeled via the right 5G slice (e.g. URLLC for autonomous on-campus buses)
- Optimize mobile network resources by prioritizing bandwidth for managed devices and critical applications (e.g. campus security application)
- Ensure network resources are not abused by internal users and guests (e.g. cloud gaming, file torrenting, video downloading)
- Detect 5G network-related threats (e.g. interception, MNmap, packet reflection, DNS spoofing, uplink/downlink impersonation)
- Maintain ZTNA performance for fast access to emergency services applications
- Ensure the university private network is not abused as a base to perpetrate cybercrimes

3) Exploring 5G private network opportunities in Asia Pacific, GSMA Intelligence

Figure 7 illustrates how static and mobile endpoints connecting to a university's private 5G network are managed through ZTNA. DPI, embedded in a ZTNA controller, augments traffic awareness to enable identification and continuous authentication of each session while ensuring the security of local and cloud-hosted applications.

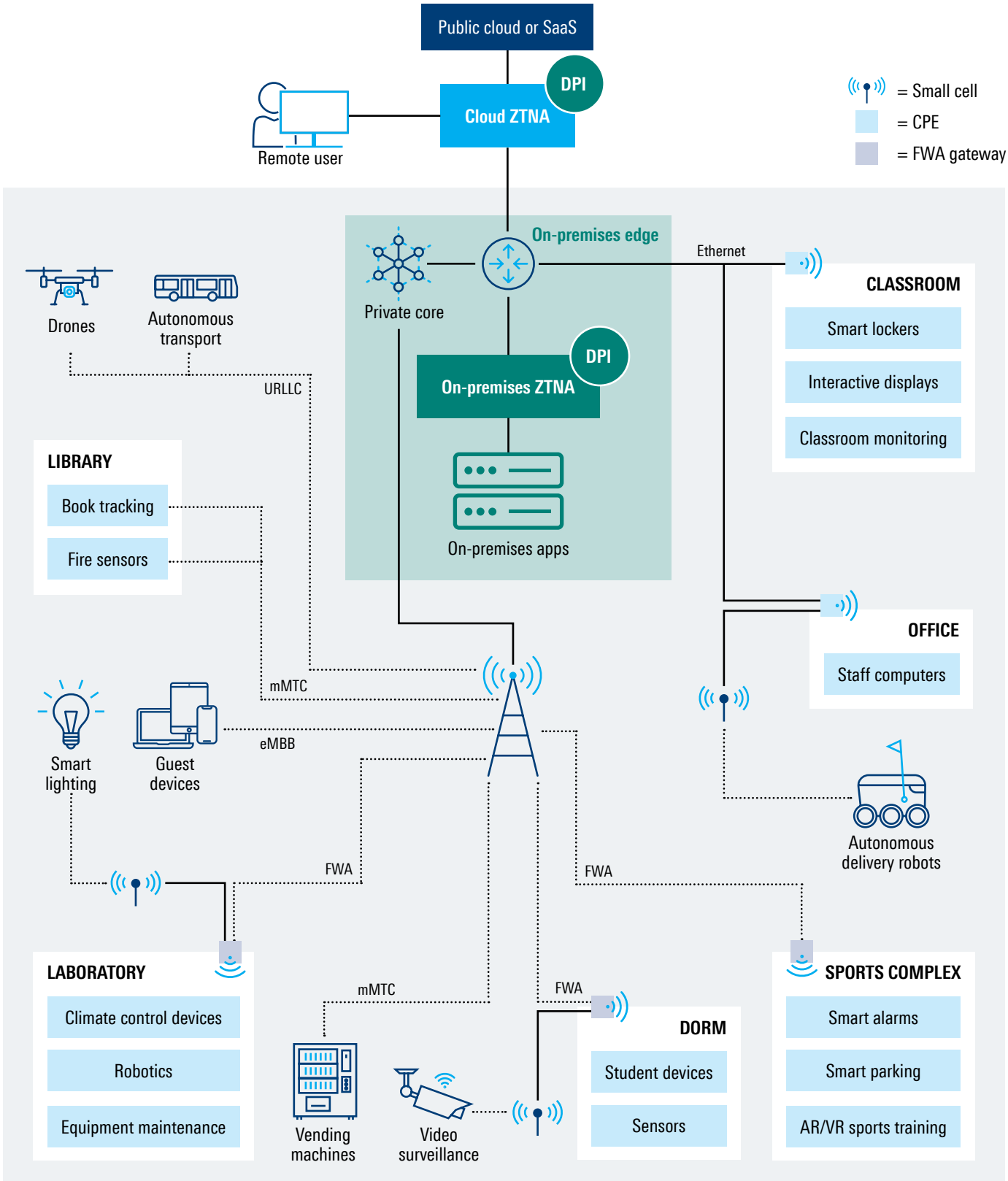

Figure 7: DPI-driven ZTNA for a private 5G network deployed in a university

7. DPI: BUILD OR BUY?

ZTNA vendors can choose to develop their own DPI capabilities or source external DPI solutions. External DPI options include open-source DPI and commercial DPI. To decide on the best option, ZTNA vendors must weigh the long-term benefits and costs associated with each.

In-house DPI requires ZTNA vendors to embark on continuous R&D and testing to ensure their detection methodologies and reference libraries are updated with the latest protocols and applications. In-house developer teams must also possess deep know-how on emerging computing frameworks, such as DPDK and network architectures based on virtualized and cloud-native technologies, to ensure their traffic inspection capacity aligns to the traffic loads of modern enterprise networks.

Embedding a DPI engine in a ZTNA solution also requires experience in integrating DPI capabilities and functionalities for cloud-based implementations. Industry knowledge and vertical experience is also a must. Without adequate experience, vendors may grapple with complex integration processes, long deployment cycles and performance issues. These concerns are also found in open-source DPI deployments where a lack of active support can lead to high training and learning costs and constant reliance on third-party experts for customization and performance optimization. Open-source DPI additionally comes with the security vulnerabilities typically associated with open-source software. There is also the risk of discontinuation that often leaves vendors in a fix.

7.1. Choosing ipoque

With years of expertise and leadership in the DPI space, ipoque's technology has powered hundreds of networking and cybersecurity solutions in managing and securing IP networks globally. Partnering with ipoque gives ZTNA vendors immediate access to its repository of traffic signatures that undergo stringent scrutiny using comprehensive QA methodologies, including its mobile automation framework where thousands of traces are collected and analyzed every week. By collaborating with ipoque, ZTNA vendors also benefit from regional and global insights, its team of analytics experts and exceptional customer support.

Key solution features of ipoque's DPI engines, R&S®PACE 2 and R&S®vPACE, are summarized here:

Advanced classification and inspection techniques

- Statistical, behavioral and heuristic analysis
- Encrypted traffic intelligence, which combines ML (e.g. k-NN and decision tree learning), DL (e.g. CNN, RNN and LSTM), high-dimensional data analysis as well as advanced caching to address the following:
  - Latest encryption protocols such as TLS 1.3, QUIC, ESNI, ECH and DNS-over-TLS
  - Obfuscation methods such as traffic type obfuscation, randomization, tunneling and mimicry
  - Anonymization methods such VPN, data masking, data swapping and generalization
- Automatic identification of applications without manual work
- A signature library, updated weekly, featuring thousands of the latest applications, protocols and service types
- Seamless and flexible creation of own DPI signatures
- Metadata extraction for comprehensive traffic performance information

Performance

- Most efficient memory usage in the industry
- Highly optimized performance with unrivaled throughput and linear scalability
- VPP-based R&S®vPACE's improved clocks-per-packet ratio with a significant speedup compared to SPP DPI
- First packet classification, which enables ZTNA to shorten policy enforcement timelines

Integration with other network intelligence tools

- Flow data exporter plug-in which allows integration with Netflow
- Well-defined APIs

Service and support

- Flexible and adaptable SLAs
- Quick integration, enabling rapid time to market
- 24/7 support from DPI experts before, during and after deployment
- On-site system performance optimization, hands-on training and application engineering
- Opportunity to share feedback and influence the product road map
- Global presence

8. CONCLUSION: NEXT-GEN ZTNA NEEDS NEXT-GEN DPI

ZTNA will play an increasingly critical role as enterprise networks continue to adopt an open and fluid framework to host, run, manage and deliver their data and IT workloads. With traditional borders replaced by virtual perimeters built around heterogeneous networks, ZTNA must be able to address:

- Hybrid resources and hybrid users
- Server- and machine-initiated access requests
- Encrypted and obfuscated traffic
- Complex and highly evasive cyberthreats
- Data protection regulations

To manage and secure access to enterprise resources, ZTNA needs DPI to deliver real-time, fine-grained traffic analysis. This enables ZTNA vendors to address network visibility challenges they often face, namely:

- A lack of real-time application awareness
- Use of complex encryption and obfuscation techniques
- Use of legacy and novel protocols
- Limitations in traffic filtering speed and capacity, leading to added latencies
- A lack of mechanisms for continuous session monitoring
- Limited insights on health, performance and security posture of devices and resources
- A lack of insights on ZTNA solution/components in terms of performance and security

Leveraging DPI's latest application and threat awareness, ZTNA vendors can fortify their solutions against access and transactions that are unauthorized. DPI analysis is particularly useful for the following ZTNA functionalities:

- Establishing continuous adaptive trust
- Enforcing granular policies
- Detecting anomalies and threats
- Facilitating LPA and microsegmentation
- Mitigating risks associated with MFA and SSO
- Managing latest encryption, obfuscation and anonymization techniques
- Delivering universal coverage, spanning on-premises, cloud and SaaS applications
- Managing unmanaged and BYOD devices
- Creating a single DLP policy

Next-gen DPI engines such as R&S®PACE 2 and R&S®vPACE combine cutting-edge techniques, such as ML and DL, and advanced caching techniques, to deliver insights into latest protocols and applications. The speeds and performance as well as the analytical granularity delivered by R&S®PACE 2 and R&S®vPACE enable ZTNA vendors to scale their processing capabilities and enrich their services to deliver:

- A comprehensive solution that espouses all key aspects of zero-trust
- Next-gen ZTNA that brings new levels of performance and includes advanced features such as DEM, AI/ML-based automation, rich connectivity, API access management and automatic network segmentation

Additionally, DPI's traffic analysis can be easily adapted to any ZTNA use case, including emerging verticals such as SSE, IIoT and private 5G. This flexibility is enabled by DPI's speeds, efficiency and breadth of analysis, as well as its ability to stay abreast of global traffic trends.

Armed with next-gen DPI, vendors can augment their hybrid, cloud and on-premises ZTNA solutions with near real-time context awareness to deliver thousands of virtual network instances that support seamless and secure access to enterprise resources, while maintaining superior QoS and user experience.

Leveraging ML and DL, next-gen DPI delivers a future-proof technology that aligns perfectly with the growth seen in the ZTNA space. It brings scalability, automation, flexibility and efficiency to every zero-trust implementation, even across the most complex and demanding networks.

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.

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

PD 3672.9550.52 | Version 01.00 | March 2024
White paper | Next-gen DPI for real-time traffic visibility for ZTNA

3672955052
3672.9550.52 01.00 PDP 1 en