DEEP PACKET INSPECTION

WHY NETWORK SECURITY REQUIRES DEEP PACKET INSPECTION

ROHDE&SCHWARZ

Make ideas real

CONTENT

1. **Introduction: Modern security needs modern technology** 3

2. **Network traffic complexity meets network security** 4
   2.1 How an all-IP world is bringing new challenges 5
   2.2 The perimeter is dead 5
   2.3 Why focusing on the Cyber Kill Chain is not enough 6

3. **Building the right cybersecurity solution** 7
   3.1 In-depth security requires a layered model 7
   3.2 Understanding new responsibilities and processes 7
   3.3 Avoid breaches: Design networks with a zero-day approach 7
   3.4 Include automated remediation and mitigation 8

4. **Why DPI is necessary for modern network design** 9

5. **How DPI empowers network security** 10
   5.1 Building a better next-generation firewall 10
   5.2 Advanced malware protection using DPI 11
   5.3 DPI and advanced threat protection 11
   5.4 How DPI enables deception-based security 11

6. **Conclusion and outlook** 12

7. **DPI engine by Rohde&Schwarz** 14

1. INTRODUCTION: MODERN SECURITY NEEDS MODERN TECHNOLOGY

In our modern IT world, the number of paths available to cyberattackers continues to grow. Cloud deployment, SaaS applications, remote locations and mobile workers all make today's IT infrastructure complicated and very hard to protect. Applications have become inviting targets for cybercriminals, but securing them, protecting and controlling the networks that connect them is a huge challenge for network security providers. As these providers try to secure networks to protect users and businesses, new types of malicious technologies keep emerging. It is impossible for network security vendors to constantly rewrite their entire solution and include all new technologies and features needed to fend off attackers.

Today's network security devices must not only understand the network, but also be fluent in the language of applications. And the application layer, also known as layer 7 of the OSI (Open System Interconnection) model, is the hardest to defend. It is the most accessible layer and most exposed to the outside world. When exploited, an entire application can be manipulated, user data can be stolen and the network can be shut down completely. Attackers use many different paths through applications to harm businesses and organizations. Each path represents both a serious risk and an area for focusing protective efforts.

The big picture of security does not look any better. A recent threat report[1] presents chilling results: hackers have gotten more sophisticated and bold, with state-sponsored hacking joining rogue actors to carry out larger attacks. The people attacking computer systems, whether corporate, government or consumer, are using both standard and newer technologies for maximum effect. The impact is felt by both companies and consumers in a loss of trust and money. One researcher found that nearly 5 million data records are lost or stolen every day, and that the global average cost of a data breach is USD 3.6 million.

Some of the common network-based attacks include browser attacks, SSL/TLS man-in-the-middle (MITM), denial of service, brute force, DNS amplification attacks and more. Most network security providers and enterprises have probably seen an increase in the number of networks coming in and out of their infrastructure with the rise of SaaS applications, cloud and remote users. All of these increase the area vulnerable to attacks.

For enterprises, these security threats are an overwhelming trend, and one that IT security teams need to tackle. They are relying on network security vendors to stay ahead of threats with cutting-edge technology and to ensure that all network paths are safe. New standards like the GDPR will force vendors to update their security measures or face large fines, which further adds to the cost of any data breach. In addition, network security vendors need to consider how AI, machine learning and IoT deployments will affect their solutions' security postures and they also need to think about how to incorporate these technologies to create better products.

Additionally, today's networks are more complex and distributed than ever. Together with the adoption of cloud and SaaS applications, this has fundamentally changed the way applications are built, deployed and used. Providers of traditional perimeter security are now struggling with a major problem: the lack of application visibility and control. SaaS and cloud applications are hosted off-premises, and when network security vendors cannot see what users are seeing or look inside networks and applications, they are flying blind. To serve customers, it is imperative that there is a plan to address these new challenges and threats.

What is needed to identify, investigate and block attacks in this ever-changing threat landscape? The answer is deep visibility into network traffic, up to the application layer and beyond. For network security vendors to help customers effectively block and mitigate threats, this visibility is a critical prerequisite for the stability and reliability of modern cybersecurity solutions.

In this paper, we will look at the security challenges that are surfacing and how network traffic visibility can help address these, as well as why embedded deep packet inspection (DPI) is essential for cybersecurity. We will also discuss what else DPI has to offer beyond application layer visibility.

> "Today's network security devices must not only understand the network, but also be fluent in the language of applications."

[1] 2017 Internet Security Threat Report, Symantec.

2. NETWORK TRAFFIC COMPLEXITY MEETS NETWORK SECURITY

While IT teams are adding new applications and users and building modern network infrastructures, they are opening up new vulnerabilities and avenues of attack. Businesses today are distributed and many continue to acquire new lines of business and expand branch and remote locations. This means the network perimeter keeps extending, making it more difficult for network security providers to defend. More users are connecting to these networks with more devices, from more places than ever before.

Network security vendors need to provide modern technologies to their customers, because the security models and technologies that used to be deployed at every branch office have become prohibitive in cost and complexity. Traditional security tools are ill-equipped to handle emerging technologies and quickly changing IT infrastructures.

When it comes to network security, understanding potential weak spots comes from visibility—and visibility disappears as the network perimeter expands. A lack of visibility limits a business's ability to deliver network diagnostics and prove compliance. It also complicates the ability to protect the interior of the network from threats both inside and outside the network.

There are a few key challenges faced by network security vendors today:

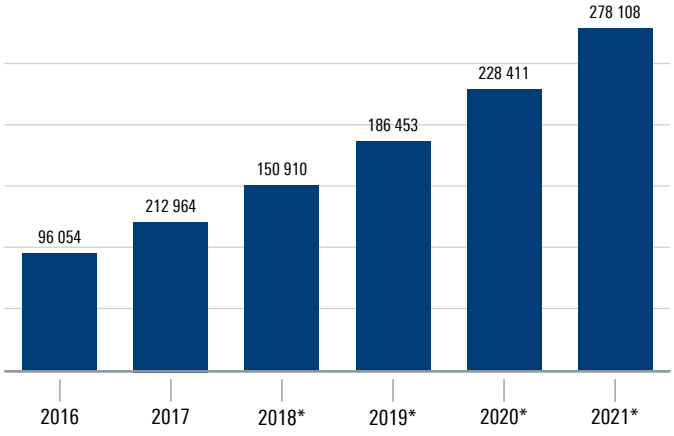
1. Data growth
2. Application growth
3. Protocol complexity
4. Encryption and obfuscation

1. Data growth

Global data growth is staggering: IP data traffic is expected to rise from a little under 100,000 petabytes per month to more than 270,000 petabytes per month. This means that traffic in 2021 will be equivalent to 127 times the volume of the entire global Internet in 2005. The increasing use of mobile devices, the emergence of the Internet of Things (IoT), cloud computing—all of these phenomena increase network traffic, demand greater bandwidths and require close attention and powerful tools to ensure secure operations on enterprise networks.

But the cybersecurity devices in use are often overwhelmed by the increasing network traffic. It's an issue of volume: There are simply more sessions, packets, flows, applications and protocols to keep track of. The inability to process all network traffic and insufficient IT resources for analyzing the collected data create security risks.

GLOBAL IP DATA TRAFFIC FROM 2016 TO 2021 (IN PETABYTES PER MONTH)



* Forecast
Source: https://www.statista.com/statistics/499431/global-ip-data-traffic-forecast

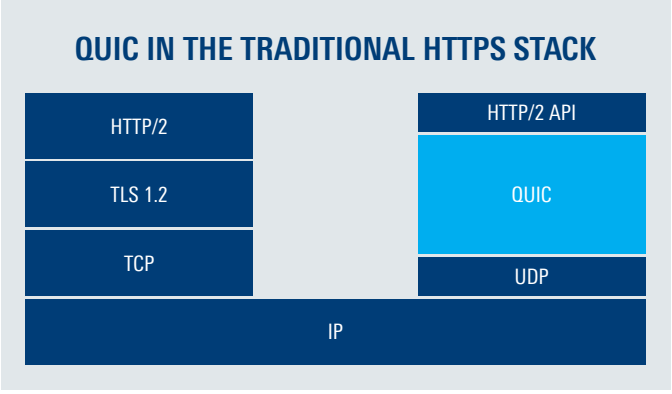
2. Application growth

Another security challenge stems from the evolution of applications. In the last few years, there has been an immense growth in web-based applications. The web browser is now the most commonly used application user interface and this has changed the dynamics of security.

In the past, specific applications were associated with specific protocols and ports. Setting and enforcing policies at the host level was relatively straightforward. Now, network security solutions operating solely on basic Internet Protocol (IP) layer information are unable to distinguish between permitted and malicious activity. Attacks at the application layer thus have become a challenge, because malicious code can masquerade as valid client requests and normal application data.

More users are connecting to the networks with more devices, from more places than ever before. When it comes to network security, understanding potential weak spots comes from visibility—and visibility disappears as the network perimeter expands.

3. Protocol complexity
In parallel to application growth, the emergence of new and complex protocols used by modern web browsers present a significant challenge. These protocols may be either proprietary or non-proprietary, such as HTTP/2, QUIC, ZERO or TLS 1.3. All of these protocols introduce new features, such as binary header compression and 0-RTT handshakes, which create critical vulnerabilities and have a negative impact on network-based security solutions. These new protocols have introduced a new blind spot for IT teams and legacy security solutions. For example, the QUIC web protocol is standard for popular sites like YouTube, but typical firewalls do not understand QUIC.



4. Encryption and obfuscation
In addition to the growing number of mobile users, devices, applications and complex protocols, network security vendors face another challenge: encryption. More and more network traffic is encrypted as people and businesses try to keep their data private and secure. According to Gartner, more than 80 percent of enterprise web traffic will be encrypted by 2019. Although that gives business users and consumers greater privacy and security, network security teams now have to address a massive influx of traffic that they cannot look inside without proper decryption technologies.

Today's hackers have quickly learned to use data encryption to their own benefit, concealing delivery, command and control activity, as well as data exfiltration. They easily bypass standard security measures, such as input filters, output encoding mechanisms used in web-based intrusion detection systems (IDS) and firewalls.

In addition to encryption challenges, network security vendors are also up against obfuscation. For example, SQL obfuscation can help attackers to bypass web and database application firewalls or an application's input validation controls.

2.1 How an all-IP world is bringing new challenges

New technologies are also bringing challenges for network security vendors to solve. The Internet of Things (IoT) is becoming more of a real possibility for many businesses, especially in healthcare, manufacturing and retail. It offers great opportunities but also entails great risks.

Essentially, the IoT represents enormous numbers of unsecured devices and a new weak spot for businesses. The devices used in IoT networks often lack proper configuration and security, which leads to botnets emerging and may cause attacks and data theft. IoT devices are usually produced with very low security standards and no way to update security flaws. Moreover, these devices are often used in DDoS attacks. Without any built-in device security or IoT security standards, IT teams are hard-pressed to protect their infrastructure from all these possible attack avenues. This provides an excellent opportunity for network security vendors to fill in visibility gaps.

IP traffic is increasing because more and more devices are going online. This makes it difficult for Internet providers to provide detailed web traffic information. Adding DPI to network security products can capture the details needed.

2.2 The perimeter is dead

Before this era of cloud-driven, distributed IT, enterprise networks had a clear boundary to the outside world. Network engineers could see what was connected to their networks and keep devices under control with various security measures. Network security vendors had a fairly straightforward view of what they needed to protect. Now, there is no clear boundary. IT network and security teams are trying to protect dispersed networks that are using lots of cloud and SaaS applications. On top of that trend, the teams often lack the IT resources on site. Remote and branch offices are connected to the main office, adding a lot of complexity and risk. In addition, the users who access corporate networks often use their own devices to work. This bring-your-own-device (BYOD) trend, combined with remote work, adds a lot of potential security holes to any enterprise network. It is essential that network security vendors keep up with this ever-expanding network perimeter.

2.3 Why focusing on the Cyber Kill Chain is not enough

Traditionally, security equipment such as firewalls and intrusion detection systems (IDS) has relied on signatures to stop known threats. But traditional equipment is not keeping up with modern threats. Recent events such as massive data breaches and hacking attacks have shown that unknown threats are spreading fast and are highly sophisticated.

For many years, the Cyber Kill Chain offered a way to beat back security threats at various points. The illustration below shows a set of steps followed by hackers, which offered a path for security vendors to follow for thwarting the attacks and protecting the network. Each step was an opportunity to stop a targeted attack—the earlier the better. When this Kill Chain was the primary method for stopping or mitigating a threat, each step of the way had some associated tasks to complete to combat the threat. This legacy Cyber Kill Chain is no longer sufficient as a model for threat detection. First, it focuses on malware. Many attacks now happen because of human errors, insecure configurations of remote access points and more. Malware is just one possible cause of attack. Second, the Cyber Kill Chain aligns with the perimeter-centric mindset that does not apply to today's distributed environments.

Now, with BYOD, SaaS applications and apps demanding high bandwidths, for example for voice and video communication, there is an almost infinite number of intrusion vectors. Signature-based intrusion detection systems no longer work either, because each new attack means a new signature. Network security vendors must change their approach to threat detection to take these aspects into account.

> "Unknown threats are spreading fast and are highly sophisticated. Network security vendors need to change their approach to gain a holistic network view in order to stay ahead of threats."

THE CYBER KILL CHAIN

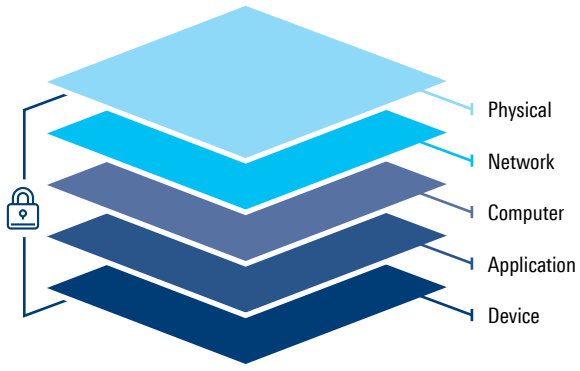
3. BUILDING THE RIGHT CYBERSECURITY SOLUTION

With today's key challenges and rapidly increasing traffic, devices and users, how can network security vendors stay ahead of threats and prepare for the future? There are new technologies and models available that can ensure sophisticated enterprise security.

3.1 In-depth security requires a layered model

As networks change and businesses adopt new technologies, it has become impossible to achieve security by deploying security equipment at a single point in the network, like the perimeter method of the past. Instead, security techniques and tools have to be implemented on multiple layers, integrating them with all software and devices.

THE LAYERED SECURITY MODEL



This layered approach is necessary for security tools to be able to generate intelligence on every layer, aggregating and combining information for a holistic approach to analyzing security. That way, network security teams can know that they are seeing the full picture of their infrastructure's security status.

3.2 Understanding new responsibilities and processes

It has become clear that security vendors have to look at network security differently than in the past. This requires more than just slightly updated products. It's not enough to install tools, network security requires properly set up roles and processes to handle and respond to incidents, investigate security issues and more.

This means creating a culture where everyone is involved in security, including end users. Everyone must be aware of security risks and understand how to help prevent them. This requires a change in mindset so that users understand that the choices they make can have a huge effect on their company's overall security. Training and awareness exercises can be effective in preventing breaches, whether due to device use, file downloads or sharing information insecurely. Network security teams and others working to combat cyber threats also have to realize that they are now responsible for knowing what is under their control, even when applications and office locations are distributed and network perimeters are a thing of the past.

3.3 Avoid breaches: Design networks with a zero-day approach

Forward-looking network security vendors have to consider secure network design in a cloud-driven world. While signature detection and confirmation may have sufficed before, that is no longer enough for real security. Data breaches come in all shapes and sizes, from multiple sources and methods. Here are just a few of the actual breaches that have affected enterprises recently:

- A company's employee is contacted via Facebook Messenger by a new, malicious buddy and accepts a ransomware file transfer.
- An attacker tries to write a new configuration to a sensor within an industrial control network. (This sensor normally only gets regular requests to provide its data.)
- A corporate employee uses the corporate Internet connection to share illegal content over the BitTorrent peer-to-peer file-sharing service. BitTorrent actively obfuscates behavior on the protocol level to circumvent firewalls.
- Advanced ransomware uses a vulnerability in the Windows sharing service SMB to gain system access. Malformed protocol requests caused the vulnerability in the first place. Post-infection, the malware tries to use the Tor network for command and control (C&C).
- A large enterprise's facilities are compromised, and the attacker then tries to transfer sensitive information using the ICMP protocol.
- In an industrial control system, an attacker spoofs Modbus protocol messages to get information about network elements and their capabilities.

These breaches show the range and depth of attacks today, and the type of information that attackers are able to

extract and use. Perimeter security alone could not stop these breaches.

State-of-the-art security design has to be built for intrusions using unknown threats or malware (zero-day). Tools such as next-generation firewalls are a fundamental part of protecting enterprise networks. When considering modern security methods, the key to getting ahead of the competition is to gain visibility and a holistic network view. For that to happen, network security vendors need to understand network traffic and user communication patterns, making sure that customers can:

- Get an understanding of current network status and usage patterns
- Create powerful network and user profiles as a foundation for anomaly detection

Creating user profiles is a first step towards building a security baseline. User profiles can include the following information:

- User activity and communication. Which applications do users access? When do they access these applications?
- System activity and communication. When is a system turned on and communicating? With which other network elements does the system communicate?
- Network activity and communication. Which devices and services are active or inactive within the network and when?

To create these profiles, network security vendors can use artificial intelligence (AI) and then continuously check network activity against this "normal" state in order to find unusual events that might indicate an infection or attack.

3.4 Include automated remediation and mitigation

By using the knowledge acquired through deep analysis of the network traffic and usage patterns within the network, network security vendors can provide fine-grained network access control (NAC) to reduce access from and to the internet and internal network resources to the minimum required. They can also engineer their solution to automatically provision security rules to remediate an infection or to isolate infected network elements.

> "Ensure sophisticated enterprise security through applying a layered security approach, creating user profiles and fine-gained network access control (NAC)."

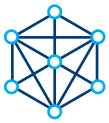
DPI ENABLES PROFILE-BASED ANOMALY DETECTION

User

User activity*
User communication*
Downloads, uploads, file transfers

System

Device activity*
Device communication



Network

Devices
Device activity*
Communication patterns*
Network service activity

* DPI increases network-based visibility on activities and communications

4. WHY DPI IS NECESSARY FOR MODERN NETWORK DESIGN

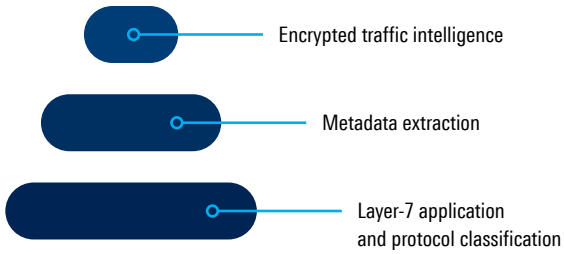
For network security vendors, deep packet inspection is the missing piece that creates the visibility that is essential today. The old shallow, or stateful, packet inspection (SPI) just looked at the header information. With some of the modern challenges mentioned above, like encryption or obfuscation, SPI misses hugely important details of a packet. By adding DPI software into network security solutions, cybersecurity vendors can see beyond the header. Looking at packet payload brings a wealth of network data that enterprises need today: be it data on malicious content, application-specific issues, or to detect general usage trends.

However, building custom DPI solutions is a considerable task for a network security vendor today. It is complicated, requires significant investment and does not get any easier over time, because a DPI engine needs to be constantly updated with new signatures. Buying DPI software is a lot cheaper, because it only requires licensing costs and can be easily deployed as part of a solution. Licensed DPI software is updated automatically with new signatures, and comes with an advanced toolkit for challenges such as obfuscated or encrypted applications. A powerful DPI engine is never done. Instead, it is updated as often as possible (ideally weekly) to add newly found signatures and incorporate thousands of protocols and applications, with the goal of understanding patterns and behavior. That keeps the DPI capabilities ahead of hackers.

Incorporating DPI adds IP traffic analytics capabilities to network security devices and provides granular information on applications and protocols for proper classification. It looks into every packet traversing the network and examines the payload of the packet (content) to find illegal statements and match predefined criteria. DPI also extracts metadata.

> "Deep packet inspection is the missing piece that allows for the visibility that's essential today."

DPI FUNCTIONALITIES



The graphic above reflects the way that DPI offers a complete technology for gaining network visibility. Layer 7 classification pinpoints the application layer so that the correct information gets through to IT teams without any clutter or unnecessary data. Next, the metadata extraction features offer structured data insights into various categories, including the host, location, certificates, element types and version type. Finally, the analytics and metrics collected via DPI include packet size, packet timing, entropy, jitter, latency and throughput. DPI can also see and help to enforce QoS categories to prioritize business applications.

DPI is very lightweight, so hardware or software that integrates DPI can run continuously, even in production environments. It analyzes packets up to layer 7, beyond simply the header, footer and payload included by legacy network monitoring. DPI looks at all the IP packets of a connection—which makes sense particularly as more and more network traffic is handled via IP.

DPI can even gather information about encrypted or obfuscated applications and protocols. For instance, it can classify applications and get essential information on their type, such as if a voice call or chat is taking place. More specifically, the heuristic methods used by DPI solutions can compare packet timings, packet sizes and other parameters over time, correlating them over different flows of a network connection. In addition, the statistics and heuristics provided by DPI are not restricted to SSL or TLS-based connections. They also work for the detection of applications that are obfuscated or actively hiding, such as anonymizers or VPNs.

5. HOW DPI EMPOWERS NETWORK SECURITY

One of the essential strengths of DPI that makes it such a good fit for modern enterprise networks is its flexibility. Network equipment and security vendors are licensing and incorporating DPI into their products to ensure their customers can block a huge variety of threats in their distributed environments.

DPI can solve many security challenges by enabling:

- Fine-grained application control to block malicious file transfers
- Whitelisted commands based on patterns and semantics
- Detection of obfuscated connections, such as BitTorrent file sharing
- Consideration of protocol message content to identify connections, extract the relevant request data and block specific connections like Tor
- Detection of suspicious protocol usage in user profiles to prevent stolen or leaked information
- File extraction to identify unusual communication patterns

Deep packet inspection brings intelligent analytics to modern network security products. The following success stories offer some details on how DPI plays an essential part in detecting potential threats through full network visibility.

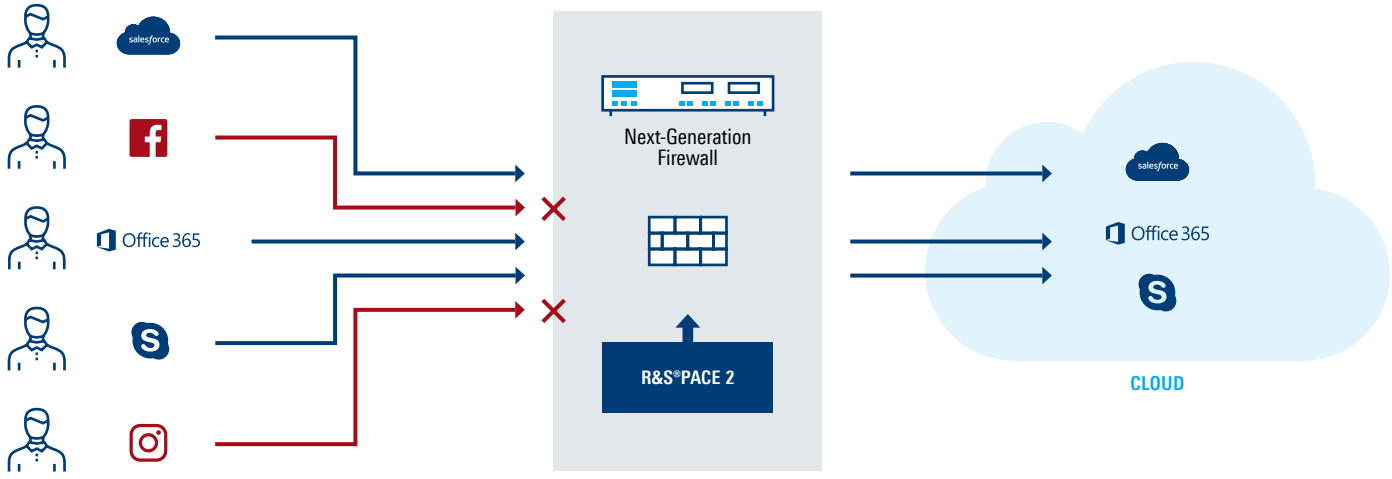
5.1 Building a better next-generation firewall

One large Rohde&Schwarz customer, a provider of next-generation firewalls, needed to fully protect enterprise networks delivering cloud and SaaS applications and supporting mobile devices. The customer's IT team also needed to maintain application security policies, combat shadow IT and get regular application and protocol updates without spending a lot of money.

By embedding the R&S®PACE 2, the DPI engine from Rohde&Schwarz, in next-generation firewalls, the provider can detect and classify thousands of applications and attributes. These next-generation firewalls, deployed in enterprise network infrastructures, are able to maintain bandwidth even when identifying VoIP protocols—all in real time. Users can refine corporate policies and decide which applications are assigned to which QoS category once they have the detailed information provided by the DPI engine.

This DPI software provides the most accurate classification on the market. It also allowed the vendor's customers to manage network traffic volumes quickly, detect encrypted applications and speed up the most important apps.

DPI-ENABLED APPLICATION CONTROL



5.2 Advanced malware protection using DPI

In another case, a provider of advanced malware response solutions uses the DPI engine R&S®PACE 2 to combat advanced persistent threats (APT). These threats have grown more powerful and dangerous, and legacy security tools cannot keep up with new advances. To provide a full-scale solution using its AI-based analysis capabilities, this customer needed to include DPI. The DPI engine's real-time file content extraction from Rohde&Schwarz allowed the customer to find and block the possibly dangerous .exe files often used by persistent threat actors.

Thanks to DPI, this customer could achieve granular visibility of network traffic, so that they could then guarantee full network visibility to their customers. They are now able to set up advanced security and traffic management policies to prevent attacks. With embedded DPI, this malware response solution provider can detect malicious threats quickly and mitigate data breaches. In addition, they have achieved a faster time to market. Lastly, adding the DPI engine allowed this vendor to fully use their AI methodologies. DPI allows them to extract traffic metrics to then detect anomalies using AI to identify and block new types of malware that could not even be seen before. They sped up their time to market and saved money by licensing the DPI engine R&S®PACE 2.

5.3 DPI and advanced threat protection

In the case of another product, a network intrusion detection system, machine learning creates behavioral models for users and devices and then analyzes how they all interact. The product incorporates DPI and thwarts threats by monitoring all raw network data continuously in real time, even in cloud environments. It delivers alerts that contain metadata and connection metrics, going beyond the basics to offer real-time, prioritized information for IT teams to use for their decision-making.

This use of DPI results in a lightweight product that can self-learn and work at scale for enterprise networks, extracting only relevant metadata. It detects threats and anomalous behaviors, including those that traditional security tools cannot find, without any prior threat knowledge. And it does so quickly, finding attacks in progress and alerting on any issues that might be coming. The product can correlate connection patterns, which helps users to see devices that show the same behavior as affected devices, such as downloading the same information or performing a software update. The product can also be deployed as a virtual appliance in virtualized environments and capture all traffic among VMs. It integrates easily into security stacks through a flexible syslog output.

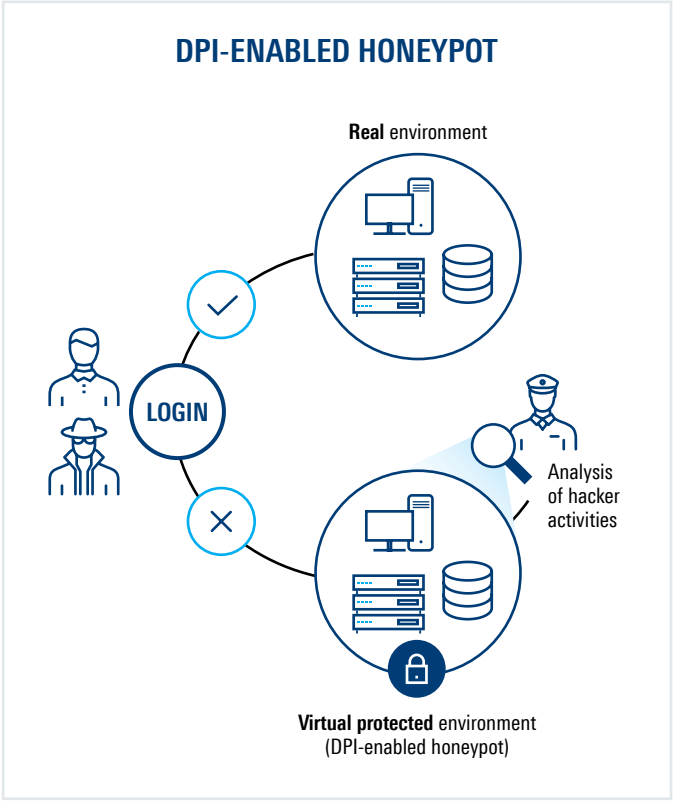
This threat protection solution is deployed on a TAP or SPAN port for ease of installation, and then performs similarity clustering and anomaly monitoring with the data ingested from that port. All in all, this product is the first to use machine learning at scale in a production network.

5.4 How DPI enables deception-based security

Deception technology is a method of securing the network that automates the creation of traps, decoys or lures. These are IT assets that either use real licensed operating system software or emulate such devices. They are mixed in among and within existing IT resources to provide a layer of protection and stop attackers that have already penetrated the network.

Traps can use emulations imitating medical devices, ATMs, retail point-of-sale systems, switches, routers and much more. Lures are generally real information technology resources (files of varying kinds), which are placed on actual IT assets.

For this type of deception-based security, DPI can add important capabilities to strengthen products offered by network security vendors. It provides fine-grained analytics of traffic to and from the honeypot by creating network profiles and device profiles. In addition, DPI can be used to extract files transferred to the honeypot in order to provide them to the analytics system.



6. CONCLUSION AND OUTLOOK

With all this in mind, what should drive decisions around network security? It will help to understand that the role of network security vendors is changing—and has already changed, in many cases. These vendors are becoming data science organizations, as the influx of data from devices and networks continues. They are constantly gathering, aggregating and analyzing data to meet customer needs. Using that data wisely gives vendors a leading edge.

As the role of data and analytics grows, network security vendors have to choose their core competency and, on many fronts, decide whether to build or buy the new tools and features they need to serve customers.

AI-powered security analytics are the future and network analytics are the foundation of this future. With IP traffic constantly growing, that becomes a key source of both challenges and potential for advancement.

AI is complex, however, and is not an overnight project. As network security vendors transform into data science organizations, their approach to data will mature. The pyramid depicted below explains the prerequisites that need to be satisfied before network security vendors can implement anomaly detection and other AI-based techniques.

Start by collecting the necessary data (note that DPI is a must-have to collect data for high-quality user and network profiles) and then ensure that it is possible to move and store that data.

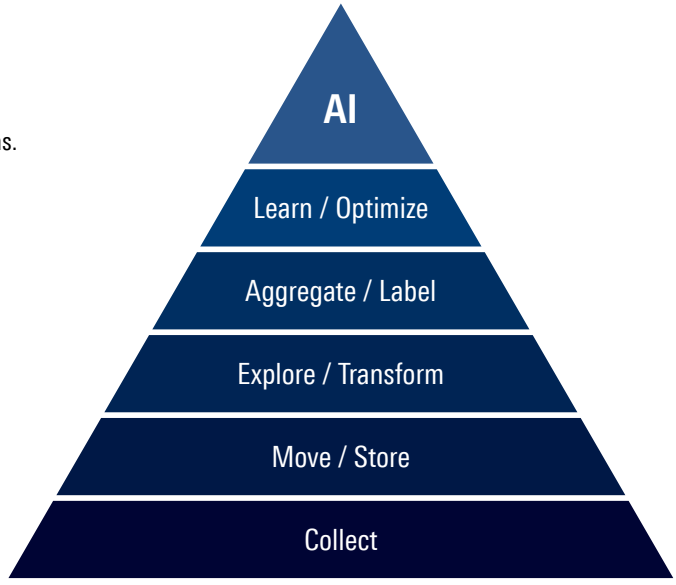
The next step is data exploration and transformation, which involves data cleaning, such as deduplicating redundant data, finding different versions or inconsistencies in data. From there, the next level of the hierarchy is the aggregation and labeling of data. In this step, it is necessary to define which metrics to track as well as their sensitivity to various factors, such as seasonal increases, along with applying simple segmentation policies to the data. This step also includes creating training data and labeling data.

Getting closer to the top, the learning and optimizing step takes place once the experimentation framework and A/B testing are in place to gauge incremental changes in the data model. At this point, there are defined simple, baseline user profiles and simple machine learning algorithms can be applied. These simple heuristics are hard to beat, because they are easier to debug than hyper-tuned machine learning black boxes with hidden parameters. Finally, network security vendors reach the AI peak when they are taking advantage of complex machine learning algorithms.

DATA SCIENCE HIERARCHY OF NEEDS*

Network security vendors become data science organisations. This hierarchy shows the prerequisites for anomaly detection and other AI-based techniques.

Conclusion:
1. Data collection is key
2. Data has to be moved / stored
3. Data is transformed into baselines & profiles



*DPI is mandatory to collect data for high-quality user and network profiles

This pyramid represents the complex data science tasks needed to reach full integration of AI. When network security vendors source DPI solutions, such as R&S®PACE 2 from Rohde&Schwarz, they can focus on the higher steps of the hierarchy of prerequisites. Embedding the DPI engine allows the integration of an essential technology, allowing vendors to move ahead in the market without getting bogged down in building DPI from scratch.

Companies have to protect themselves against all kinds of attacks, from a huge range of potential sources. But an attacker only needs a single successful attempt. With those odds, it is not enough to try to prevent attacks from happening. Instead, network security vendors need to detect them, which is why comprehensive network visibility built into their products is crucial. In today's complex, demanding IT landscape, security without a stringent inspection of data is impossible. For businesses moving to a comprehensive enterprise security model, DPI is here to make its mark. Data collection is essential for successful threat detection, and DPI is a critical enabler to remove the traffic inspection blind spots that plague networks today.

For network security vendors, deep packet inspection is the missing piece that creates the visibility that is essential today. The legacy shallow, or stateful, packet inspection (SPI) just looked at the header information. As encryption and obfuscation are becoming more prevalent, SPI misses hugely important details of a packet. Adding DPI software to network security solutions makes it possible to go beyond the header. Seeing into the packet payload brings a wealth of network data that enterprises need today to detect malicious content, application-specific issues, illegal statements, general trends and to match custom criteria. In addtion, DPI software can extract metadata.

Deep packet inspection software, such as R&S®PACE 2 from Rohde&Schwarz, offers visibility into network traffic to eliminate the blind spots that have been created as SaaS apps, remote users and distributed locations all proliferate. Incorporating DPI adds IP traffic analytics capabilities to network security devices and provides granular information on applications and protocols for proper classification.

"Data collection is essential for successful threat detection, and DPI is a critical enabler to remove the traffic inspection blind spots that plague networks today."

7. DPI ENGINE BY ROHDE&SCHWARZ

The lightweight DPI engine from Rohde&Schwarz includes powerful capabilities for layer 7 application and protocol classification, metadata extraction and metrics. It contains a software library which is updated constantly with new signatures as they are detected in the overall threat landscape.

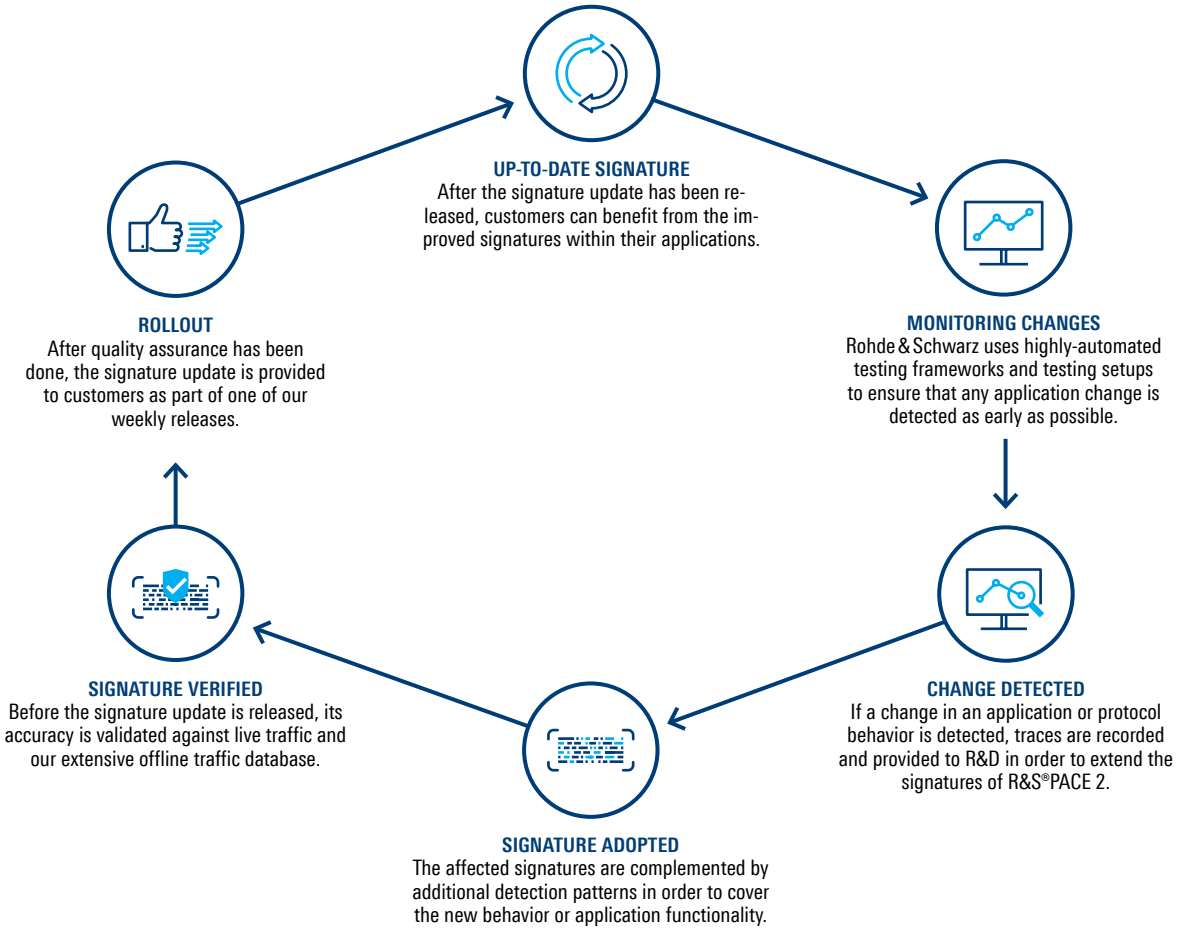
The DPI engine R&S®PACE 2 is equipped to handle the challenges faced by modern network management teams: QoS and QoE analytics for performance improvements on demanding applications, third-party network support for cloud-based, distributed environments, TCP reassembly for fragmented and out-of-order packets and bidirectional network support, among others.

R&S®PACE 2 can help to create leading-edge network security products that address the following use cases: (based on Gartner's Magic Quadrant for Unified Threat Management)

- Application control
- Network-based anomaly detection (NBAD)
- Advanced threat prevention
- Vulnerability assessment
- Malware protection
- Data loss and leakage prevention

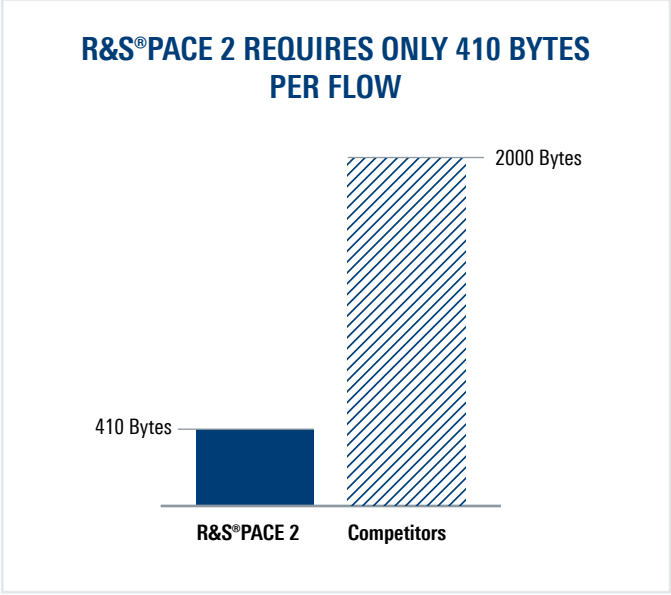
The DPI engine R&S®PACE 2 features API integration, fast and efficient memory handling, metadata extraction from voice and video apps and an easy OEM deployment. It is delivered as a software development kit and uses a polling API for seamless adoption.

ROHDE&SCHWARZ ENSURES UP-TO-DATE SIGNATURES



R&S®PACE 2 offers the industry's smallest processing footprint with the most efficient memory and simplest CPU integration. It requires only 410 bytes of memory per flow, uses very little processing power (CPU load) and does not need any memory allocation during run time.

Customers using the DPI engine R&S®PACE 2 in their security products find compelling results, including:
- Regained network visibility
- Secured networks in a post-perimeter world
- Improved application performance
- Improved WiFi and other network performance



Customers also find many benefits from sourcing R&S®PACE 2:
- Weekly protocol and application signature updates
- Highest classification accuracy in the DPI market
- Focus on core competencies to become more efficient and profitable
- Speed up time-to-market by optimizing the development schedule
- Reduce and optimize development costs by outsourcing DPI
- Maximized return on investment (ROI)

Rohde&Schwarz is recognized globally as a leading developer of DPI software. It has more than 10 years of expertise in optimizing the performance of network equipment and IT security solutions with embedded DPI. With customers in over 60 countries worldwide in the areas of network analytics, traffic management and network security, its objective is customer satisfaction throughout the entire product lifecycle.

ipoque

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

Rohde & Schwarz

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

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

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

PD 5215.9225.52 | Version 02.01 | September 2021
White paper | Why network security requires Deep Packet Inspection
Data without tolerance limits is not binding | Subject to change

5215922552
5215.9225.52 02.01 PDP 1 en