DEEP PACKET INSPECTION

DPI ENABLES COMPLETE NETWORK PERIMETER PROTECTION

R&S®PACE 2 is featured in T-Sense, a monitoring platform able to reveal lurking cyberthreats before the network is compromised

ROHDE&SCHWARZ

Make ideas real

celare
Secured Networks

With the rise of the Internet of Things (IoT) and its interconnected devices—from fridges to wearable gadgets—hackers gain an increasing number of access points to network infrastructures allowing them to infiltrate the network. CELARE, a major provider of network security solutions, has embedded the deep packet inspection (DPI) software R&S®PACE 2 by Rohde&Schwarz into their product to obtain real-time insights into network traffic, revealing potential threats before they strike.

SUMMARY

Business areas

- Network monitoring, network behavior analysis, cybersecurity, cyber intelligence

Challenge

- Improving network behavior analysis and building a contextual layer for research and investigation purposes

Solution

- Embedding the customizable DPI engine R&S®PACE 2, featuring open APIs and plug-ins, to achieve full visibility into IP traffic

Benefits

- High reliability, reduced time to market and the ability to focus on the core product and strategic company decisions

CHALLENGE

Full network traffic visibility to enable network perimeter protection

Newer, increasingly complex technologies are continuously being introduced to the IT market, bringing with them new security challenges for which companies are not yet prepared. Machine-to-machine (M2M) technology, which enables network devices to interact without human intervention, is a good example. A myriad of M2M use cases has become increasingly relevant, as this technology is the underlying concept of IoT. To secure M2M communication, companies make use of industrial control systems (ICS) such as supervisory control and data acquisition (SCADA). These represent an attractive target for cyber attackers who might disguise their malicious code as regular SCADA commands.

To tackle these and similar threats, CELARE, a leading provider of network security solutions, has developed T-Sense, a sophisticated network monitoring platform that detects suspicious activities and reveals cyberthreats before they compromise network functionality. T-Sense combines real-time and big data technologies with a non-intrusive approach that enables complete network perimeter protection from infrastructure to application level. To provide such a wide coverage, T-Sense requires full visibility into all aspects of the network traffic as well as real-time classification capabilities at all times.

CELARE focuses on analyzing network behavior and building a contextual layer for research and investigation purposes. In order to concentrate efforts on their core business and market objectives, they decided not to invest the time and effort required to develop a cutting-edge DPI engine from scratch.

SOLUTION

Application and protocol classification to identify business process flows

Instead, CELARE integrated the advanced DPI engine R&S®PACE 2 by Rohde&Schwarz into their innovative software-based solution T-Sense. The company can now rely on the best-performing OEM DPI software on the market to accurately classify network traffic while concentrating their efforts on further developing their own products. Their main reasons for choosing R&S®PACE 2 are the product's reliability, easy integration, superior service and support. The extension capabilities of R&S®PACE 2 allow T-Sense customers to build their own decoders. Weekly library updates further ensure that the product keeps up with the newest protocols and applications.

R&S®PACE 2 classifies thousands of protocols and applications extremely reliably and offers custom metadata extraction. Its advanced metadata extraction capabilities provide the intelligence needed to make informed and timely decisions. The workflow of T-Sense comprises several stages from the pre-processing of data to detection, extraction, search, analysis and, finally, action based on the information gathered up to this point. R&S®PACE 2 is integrated into the detection and extraction stages. The traffic classification provides the input required to identify business process flows and to build behavioral network profiles accordingly. R&S®PACE 2 also features a SCADA decoder that can detect disguised malicious software. Its custom decoder capability makes it possible to extract additional metadata without the need for extra code. T-Sense makes the most of the DPI capabilities of R&S®PACE 2 by combining them with specific customer knowledge and requirements to achieve the best solution for each use case.

The benefits of licensing R&S®PACE 2

- Weekly signature updates
- Highest classification accuracy in the DPI market
- Classification of encrypted and obfuscated traffic
- Fastest performance in the market with an average of 14 Gbps per core
- Lowest memory footprint in the market
- Individual service and technical support
- Open APIs and plug-ins to add custom decoders and classifiers
- Maximized ROI and reduced TCO by licensing leading-edge technology

RESULT

A reliable network monitoring solution optimized to offer the best performance

Embedding R&S®PACE 2 immediately led to an improved time to market, allowing CELARE to focus on product development and sales. With the highly performant DPI engine by Rohde&Schwarz, T-Sense obtains all the traffic metadata required to simplify network monitoring and to provide full network visibility to their customers within hours. With R&S®PACE 2 embedded, the network monitoring platform T-Sense can now bridge the gap between network interfaces and databases (i.e. between raw and structured data). The intelligence provided by R&S®PACE 2 empowers T-Sense to anticipate system failures, anomalies and security incidents, thus improving traffic management and network security. It features secured and reliable data transfer to external repositories and cloud environments without compromising privacy.

The capabilities of R&S®PACE 2 enable T-Sense to support real-time pattern matching of large amounts of data. The customization of metadata extraction allows for better decision-making based on highly accurate data. The T-Sense reversing platform allows customers to add their own decoders using the R&S®PACE 2 extension framework. It also reduces costs, time and effort thanks to its seamless integration with third-party products. The system overlays the existing network infrastructure, collaborating with conventional security elements such as firewalls or intrusion detection systems (IDS). It is thus a non-intrusive solution that poses no risk to network security. The embedded capabilities of R&S®PACE 2 make T-Sense a scalable software-based sensor for continuous network monitoring optimized to offer the best performance.

> "Our customers are increasingly seeing the need to protect their highly sensitive IT and SCADA-controlled infrastructure against malware and attacks. We chose R&S®PACE 2 because of its technical leadership in DPI and behavioral analysis. We are pleased that Rohde&Schwarz was able to provide the metadata and content extraction functionality we needed to offer the best service and product to our customers."
>
> **Sharon Uziel,**
> **CTO at CELARE**

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

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG
Trade names are trademarks of the owners
PD 3608.6548.32 | Version 01.00 | July 2020
Case study | DPI enables complete network perimeter protection
Data without tolerance limits is not binding | Subject to change
© 2020 Rohde&Schwarz GmbH&Co. KG | 81671 Munich, Germany
© 2020 ipoque GmbH | 04109 Leipzig, Germany

3608654832
3608.6548.32 01.00 PDP 1 en