DEEP PACKET INSPECTION

Orsec Technologies boosts its AI-based threat detection solution with R&S®PACE 2

DPI-POWERED MACHINE LEARNING FOR NETWORK MONITORING SOFTWARE

ROHDE&SCHWARZ

Make ideas real

ORSEC
Technologies

Protecting your company's information from data breaches is an ever-present security concern, all the more serious for small and medium companies who cannot afford a dedicated IT security team. oorigin® by Orsec Technologies incorporates the analytics capabilities of R&S®PACE 2 for a faster and more efficient detection of cyberthreats.

SUMMARY

Area of business

- Cybersecurity vendor, AI-based analytics to detect cyberthreats in a network

Challenge

- Full traffic visibility to recognize user and device patterns
- Information in real time to detect threats as soon as they infiltrate the network
- High efficiency to keep TCO low

Solution

- Incorporating the DPI engine R&S®PACE 2 to achieve full visibility into IP traffic and extract a rich set of metadata

Benefits

- Supply real-time intelligence to the AI to enhance analytics
- Streamline the investigative flow, making threat detection faster and more accurate
- Saving on development costs and speeding up the development schedule by licensing leading-edge DPI technology

CHALLENGE

Real-time data for speedy threat detection

The constant development in modern IT means that new cyberthreats are arising every week, hand in hand with new technologies and use patterns. Cloud deployment, remote working or trends such as bring your own device (BYOD), meaning that employees access the corporate network from their private devices, make protecting corporate infrastructures an increasingly complex task. At the same time, hackers' methods benefit from the newest technological developments and are becoming all the more sophisticated. Cyberthreats can remain undetected for months and end up causing major data leakage, with the subsequent loss of money and reputation for those affected.

Even large corporations and governments, who employ highly specialized teams and expensive security tools, regularly fall victim to cyberattacks. For small and medium companies, it is even harder to implement an efficient and affordable cybersecurity policy.

With these businesses in mind, Orsec Technologies brought oorigin® to the market, an AI-based advanced analytics solution that hunts cyberthreats to tackle them before they affect the network. oorigin® empowers IT administrators to proactively search for malware or attackers lurking in the network and so discover shadow IT. Even after an incident has occurred, oorigin® manages to reduce investigation time by providing system administrators with detailed data on how the structure was infiltrated and what data was compromised.

To detect threats effectively, oorigin® needs to have an overview of everything that is happening in the network at all times. To make the most of its machine learning features, Orsec requires insight into traffic patterns, as well as a deep understanding of the detected data. Especially when it comes to attacks employing new techniques or technologies, it is of paramount importance to introduce new classification parameters quickly.

SOLUTION

Accurate and granular insight into traffic metadata

R&S®PACE 2 is a market-leading deep packet inspection (DPI) engine that provides advanced protocol and application classification with metadata extraction. It is optimized to offer fast performance, an efficient memory usage and the highest classification accuracy in the industry, thanks to its weekly updates that include the newest protocols and applications.

By embedding the state-of-the-art DPI engine by Rohde & Schwarz into its network monitoring software, Orsec Technologies is able to gain full, real-time visibility into network activity. R&S®PACE 2 provides extremely reliable classification of thousands of protocols and applications up to layer 7, with virtually no false positives – regardless of whether advanced obfuscation, encryption or port hopping techniques are being used. The intelligence delivered by R&S®PACE 2 feeds the machine learning features of oorigin®, achieving better user and device behavior analytics. The insight into a rich set of traffic metadata allows oorigin® to work with a smaller amount of more relevant information to identify devices, servers and virtual machines. Similarly, R&S®PACE 2 can detect executables, such as email attachments and executable files transferred within the network, which in turn enables Orsec's technology to detect any hidden malware.

oorigin® benefits from the intelligence delivered by the DPI technology. Investigative flows are streamlined so that the solution can pick up on an extensive range of anomalies, which reduces the time needed to detect a threat.

Key benefits of R&S®PACE 2

- Weekly signature updates
- Highest classification accuracy on the DPI market
- Content and metadata extraction
- Classification of encrypted and obfuscated traffic
- Fast performance with low memory footprint
- Service and technical support tailored to the customer's individual needs
- On-demand protocol and application development

RESULT

A proactive, intelligence-driven security solution

The unique classification precision of R&S®PACE 2 fosters an accurate and swift detection of cyberthreats before they affect the network. Rohde & Schwarz provides a reliable DPI technology that is platform-independent and easy to integrate. By sourcing R&S®PACE 2 instead of developing DPI in-house, Orsec Technologies considerably reduces the maintenance costs while strongly reducing development efforts. R&S®PACE 2 is tailored to suit the specific needs of each customer, plus its application and protocol library is continuously updated to include the latest developments. In the case of oorigin®, this means that the software improved its analytics capacities with minimal internal effort. Thus, Orsec Technologies is able to offer a high-class product at a price affordable for small and medium companies.

The AI on which oorigin® is based is boosted by the highly performant R&S®PACE 2 engine, which has the smallest processing footprint as well as the most efficient memory usage on the market. Hence, the next-generation cybersecurity solution has improved its threat hunting capabilities – all while recording smaller forensic datasets than those required by full packet capture (FPC).

Based on the combination of machine learning and real-time traffic classification, Orsec Technologies offers an intelligence-driven, proactive network monitoring software that logs all network activity in search of potential cyberthreats. In this way, oorigin® is a first-class cybersecurity option for a wide range of use cases, from device inventory to post-investigation of cyberincidents.

> "The traffic metadata extracted by R&S®PACE 2 provides a rich information feed that can be used to boost our machine learning and to obtain priceless intelligence for investigation following a cyberincident. The analytics capabilities of R&S®PACE 2 empower oorigin® to function like a security camera in the network to detect any suspicious traffic behavior indicative of a cyberthreat"
>
> **Jean-Luc Rouinvy, CTO and founder of Orsec Technologies SAS.**

ipoque

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

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
Info: + 49 (0)341 59403 0
E-Mail: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 3608.4980.32 | Version 01.00 | April 2020
Case study | DPI-powered machine learning for network monitoring software
Data without tolerance limits is not binding | Subject to change