APPLICATION AWARENESS

DEEP PACKET INSPECTION FOR THREAT ANALYSIS

Saint Security uses R&S®PACE 2 to enhance its AI-based malware protection solution

ROHDE&SCHWARZ

Make ideas real

SAINT SECURITY

Saint Security uses the deep packet inspection (DPI) engine R&S®PACE 2 in its network-based advanced malware response solution MNX to identify, analyze, assess and block malicious activity.

SUMMARY

Area of business

- IT security vendor providing malware and behavior analysis services as well as solutions to protect networks against malicious attacks

Challenge

- Guaranteeing full visibility of network traffic in order to fingerprint malicious activities
- Setting up advanced security and traffic management policies to prevent cyberattacks

Solution

- Embedding the DPI engine R&S®PACE 2 in the malware protection solution MNX to extract metadata in real time

Benefits

- Fast and reliable detection of malicious threats and mitigation of data breaches
- Granular visibility of application data in real time

CHALLENGE

Advanced persistent threats (APTs) are stealthier and more perfidious than ever. Cybercriminals use targeted, highly evasive tools to infiltrate organizations unnoticed and deploy customized malware that potentially remains undetected for months to steal sensitive data ranging from credit card details and intellectual property up to government secrets. Traditional cybersecurity solutions, such as email filters, anti-virus software or firewalls, are ineffective against APTs. With its network-based advanced malware response solution MNX, Saint Security offers a product that can intercept APTs at any point in a network. By leveraging artificial intelligence (AI), machine learning and big-data-based profiling technologies, MNX identifies and blocks malware that existing security solutions cannot detect, including threats that the system has never seen before or new families of malware. To fingerprint malicious activities and to unlock the full potential of its AI-based analysis methodologies, MNX needs to be capable of classifying traffic accurately in real time.

SOLUTION

By integrating the DPI software R&S®PACE 2 by Rohde&Schwarz into MNX, Saint Security gained granular visibility of network traffic – enabling the distinction of good traffic from bad.

High-performing DPI engine
R&S®PACE 2 is a DPI software employed by network security vendors to extract metadata from IP traffic. R&S®PACE 2 operates in real time at multiple Gbps speeds, providing insight into network behavior and application usage. The software is optimized for fast performance, efficient memory usage and classification accuracy.

Reliable classification for threat analysis
Thanks to reliable classification, Saint Security obtains the ability to pre-filter traffic with the highest possible accuracy, allowing for targeted advanced security checks. This empowers Saint Security to enhance MNX to detect any type of malware more precisely and to filter out possible threats proactively.

Full IP traffic visibility for artificial intelligence
In addition to identifying and extracting various types of executables from network traffic, R&S®PACE 2 also offers a variety of other extracted metadata. This data can be used to establish helpful baselines in order to identify malicious or unusual user behavior and detect unknown threats with AI-based, heuristic and statistical methods.

Benefits

By embedding R&S®PACE 2, Saint Security is able to:

- Gain full insight into IP network communication
- Increase its capabilities to detect executable files in network traffic
- Extract traffic metrics for AI-based anomaly detection
- Uncover multi-stage APTs moving laterally across a network
- Protect customers against advanced security threats

RESULT

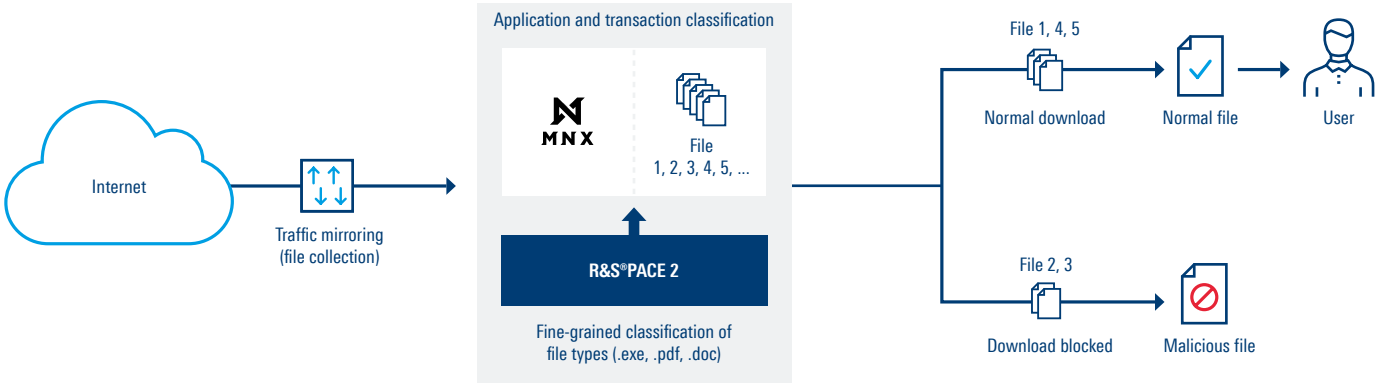
R&S®PACE 2 embedded in the malware protection solution MNX has proven its value in delivering granular visibility of IP traffic. Saint Security has been able to unlock the full potential of its AI-based analysis methodologies. The ability to classify traffic accurately has extended the capabilities of MNX to analyze all network traffic, services and protocols across all ports with extremely fine granularity. Multi-stage, advanced persistent threats such as malicious emails, ransomware or Trojans are discovered quickly and accurately. By coupling artificial intelligence and R&S®PACE 2, which is enabled by machine learning, Saint Security is now able to provide the technology and services to predict and prevent cyberattacks. As a result, customers using MNX enjoy the comfort and reassurance that threats within their networks are in decline. Additionally, by sourcing R&S®PACE 2 instead of building its own DPI, Saint Security was not only able to speed up its time-to-market, but also to reduce development time, cost and resource requirements whilst focusing on its core competencies.

> "The metadata extraction functionality provided by the DPI engine R&S®PACE 2 allows us to gather fine-grained information on activities in the network. The information helps us to better identify and investigate malicious activity, which in turn enhances our product's quality. Our customers can now rely on a sophisticated security solution that even detects previously unknown or unseen threats."
>
> **Kihong KIM, CEO of Saint Security**

Added benefits of R&S®PACE 2:

- Weekly signature updates
- Highest classification accuracy in the DPI market
- Fast performance and low memory footprint
- Service and technical support tailored to your needs
- On-demand protocol and application development
- Detection of VPN, anonymizers and tunneling such as PsiPhon and Ultrasurf

DPI-ENABLED AI-BASED MALWARE PROTECTION



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 raw IP data into network 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 more than 85 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
Info: + 49 (0)341 59403 0
E-Mail: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 5215.5036.32 | Version 02.00 | October 2021
Deep Packet Inspection for Threat Analysis
Data without tolerance limits is not binding | Subject to change

5215503632
5215.5036.32 02.00 PDP 1 en