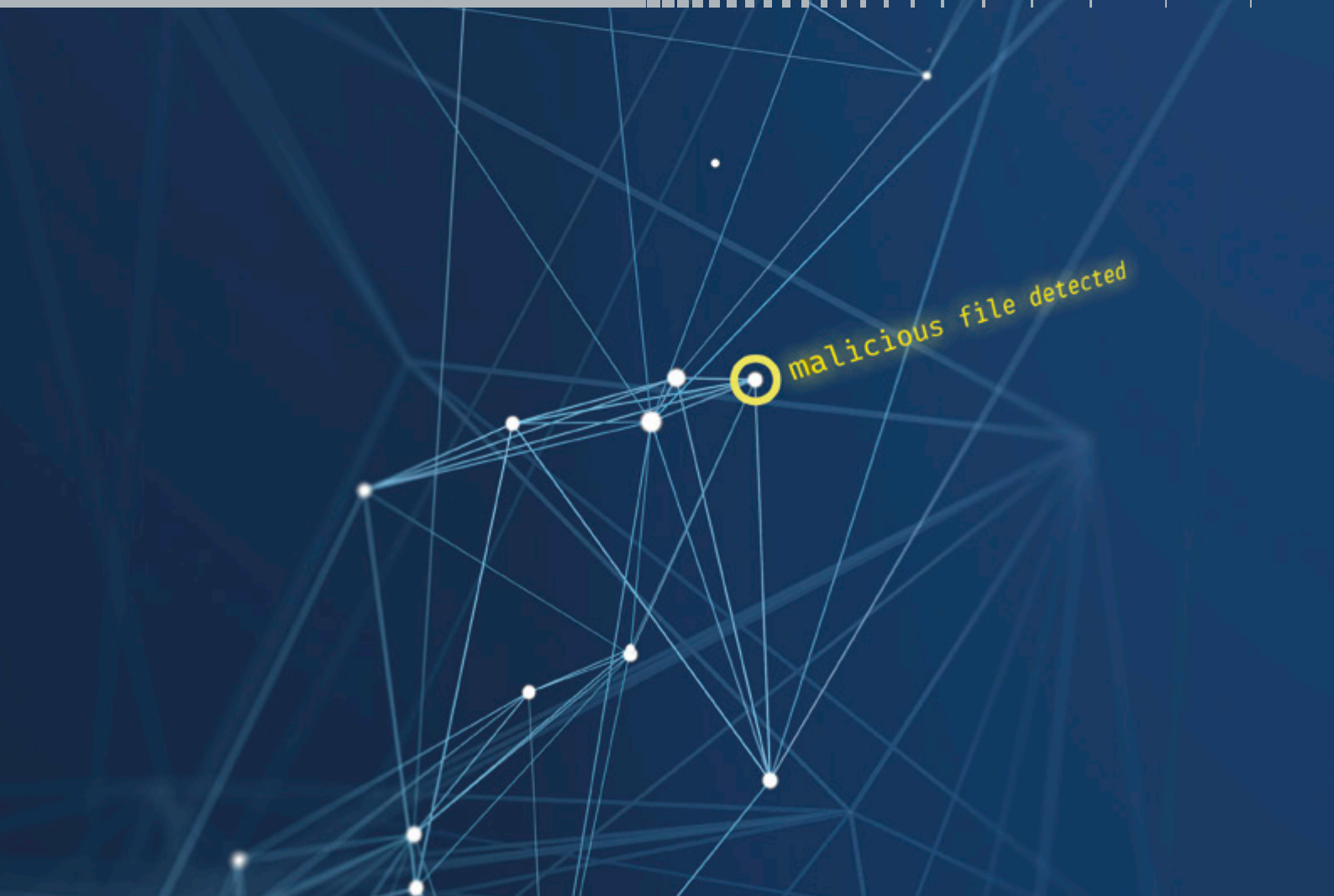
Deep Packet Inspection for Threat Analysis

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

Secur|Ty made in Germany

ROHDE&SCHWARZ
Cybersecurity



Challenge & Solution

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, judge and block malicious activity.

Summary

Area of Business

- IT security vendor, providing malware and behavior analysis services as well as network protection solutions against malicious attacks

Challenge

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

Solutions

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

Benefits

- Fast and reliable detection of malicious threats and mitigation of data breaches
- Maximized return on investment and reduced cost of ownership and time-to-market by sourcing R&S®PACE 2

Challenge

Advanced persistent threats (APTs) are stealthier and more spiteful than ever. Sophisticated techniques are used to quietly breach organizations and deploy customized malware, which potentially remains undetected for months. Such attacks are caused by cybercriminals who target individual users with highly evasive tools. Legacy security approaches are bypassed to steal sensitive data from credit card details to intellectual property or government secrets. Traditional cybersecurity solutions, such as email spam filters, anti-virus software or firewalls are ineffective against advanced persistent threats. APTs can bypass such solutions and gain hold within a network to make organizations vulnerable to data breaches.

With its network-based advanced malware response solution, MNX, Saint Security offers a product that can intercept possible APTs at any point in a network. By leveraging artificial intelligence (AI), machine learning and big-data-based profiling technologies, MNX identifies and blocks various types of malware that existing security solutions cannot detect – even if they have never been seen before or belong to a new family of malware. To fingerprint malicious activity and to unlock the full potential of its AI-based analysis methodologies, Saint Security required a deep understanding of the observed network traffic. More specifically, MNX's technology needed real-time extraction of file content for the identification of potentially dangerous executables caused by APTs in order to set up advanced security and traffic management policies.

Solution

With Rohde & Schwarz Cybersecurity's DPI software R&S®PACE 2 integrated in MNX, Saint Security was able to gain granular visibility of network traffic – enabling the differentiation of good traffic from bad.

High Performance DPI Engine

R&S®PACE 2 is a DPI software used by network security vendors to extract file content and 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.

Extraction of Files for Threat Analysis

By extracting content, such as files attached to emails (e.g. .pdf, .exe, .docx, etc) or sent through file transfers from within the traffic, Saint Security gets a detailed understanding of network transactions and file movements. This empowers Saint Security to enhance MNX to detect any type of malware more precisely and to actively filter possible threats.

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 content and 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:

- Get full insight into IP network communication
- Increase capabilities to detect executable files within network traffic
- Extract traffic metrics for AI-based anomaly detection
- Uncover multi-stage, persistent attacks moving laterally across a network
- Protect customers against advanced security threats

Result

As R&S®PACE 2 embedded in the malware protection solution MNX proved its value in delivering granular visibility of IP traffic, Saint Security was able to unlock the full potential of its AI-based analysis methodologies.

Added Benefits of R&S®PACE 2:

- Weekly signature updates
- Highest classification accuracy in the DPI market
- Fast performance and low memory foot print
- Service and technical support tailored to your needs
- On-demand protocol and application development
- VPN, Anonymizer and Tunneling Detection (DNS, HTTP)

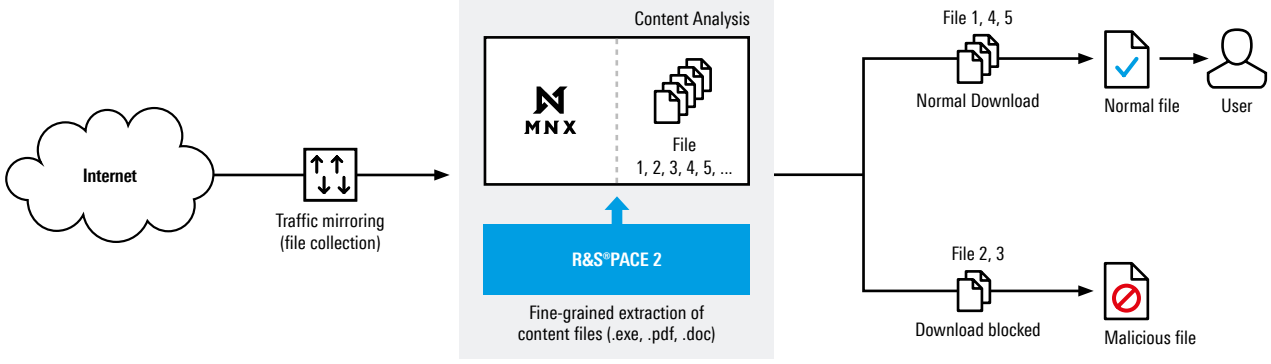
> "The content and metadata extraction functionality provided by the DPI engine R&S®PACE 2 allows us to extract fine-grained information of file content. The information helped us to better identify and investigate malicious activity which in turn enhanced our product's quality. Our customers can now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

The ability of extracting file content extended the functionality 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 can be quickly and accurately discovered.

By coupling artificial intelligence and machine learning enabled by R&S®PACE 2, Saint Security now provides the technology and services to be predictive and preventive against cyberattacks. As a result, customers using MNX enjoy the comfort and knowledge that there is an extensive decrease of threats within their networks.

Additionally, by sourcing R&S®PACE 2 instead of building its own DPI, Saint Security not only sped up its time-to-market but also reduced development time, cost and resource requirements whilst focusing on its core competencies.

DPI-enabled AI-based malware protection



Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-223
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

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

PD 5215.5036.32 | Version 01.00 | September 2017 (sch)
Deep Packet Inspection for Threat Analysis
Data without tolerance limits is not binding | Subject to change

5215503632

5215.5036.32 01.00 PDP 1 en