SentinelOne™

Optimally Armed against Progressive Cyber Attacks: Endpoint Protection at noris network AG

The Challenge: Protecting Against Advanced Threats

In times of sophisticated cybercrime, where ransomware can bring entire productions to a standstill within a few hours or where millions of sensitive data can be stolen with just a few mouse clicks, mediocre security strategies and reactive security solutions are no longer an adequate option. Especially in terms of endpoint protection, next-generation solutions already offer security-conscious companies the opportunity to counter advanced cyber threats with equally advanced technologies and to leave the defensive or reactive position. Against this backdrop, the leading ICT service provider noris network has opted for the Endpoint Protection Platform from SentinelOne.

Founded in Nuremberg, Germany in 1993, the owner-managed noris network AG is today one of the German pioneers in the field of modern IT services. Renowned customers such as adidas, Puma, Küchen Quelle, Flughafen Nürnberg GmbH and Consorsbank rely on the tailor-made ICT solutions from noris network in the areas of IT outsourcing, managed services, cloud services and colocation. The technological basis for these services is a high-performance IT infrastructure with its own

CHALLENGES

- Increasingly sophisticated techniques to disguise known malware as well as memory-based transmission

SOLUTION

- SentinelOne Endpoint Protection Platform

BENEFITS

- Reduction of false positive
- High detection rate
- GDPR compliant

noris network

high-performance backbone and several high-security data canters – including the award-winning data centers Nuremberg South and Munich East, two of the most modern and energy-efficient data centers in Europe. For its consistent quality and security in service and information security management, the company is certified in accordance with ISO 9001, ISO 20000-1, ISO 27001, the ISO 27001 certificate on the basis of basic IT protection, and also in accordance with industry-specific standards such as PCI DSS. The environmental management is certified according to ISO 14001.

Michael Ibe
Head of the Security Operations Center at noris network

"Even though we have always been successful in defending ourselves against malware, we were aware that the increasing sophistication that cybercriminals have shown in the development of malware will require us in an even more complex way in the future. We had previously relied on traditional antivirus solutions, but now it was time to switch to next-generation endpoint technology. "

Starting point: Endpoint Security in Times of WannaCry & Co.

Companies that place their ICT infrastructure trustingly in the hands of external service providers expect not only individual solutions but above all system stability and absolute security of their sensitive data. However, large-scale cyber-attacks such as WannaCry, targeted data theft and, not least, new security guidelines as part of the forthcoming General Data Protection Regulation of the EU (GDPR) are putting increasing pressure on IT and managed security service providers and are creating increasing security requirements. In endpoint protection in particular, the security strategy needs to be realigned, as hackers are using increasingly sophisticated techniques to disguise known malware as well as memory-based transmission mechanisms to which traditional endpoint solutions such as antivirus, firewalls, intrusion prevention systems (IPS) or attack detection systems (IDS) are helplessly confronted.

noris network AG keeps a constant eye on both the current threat landscape and all new security solutions appearing on the market. For this reason, the company has decided to break new ground with SentinelOne when it comes to endpoint protection. "Even though we have always been successful in defending ourselves against malware, we were aware that the increasing sophistication that cybercriminals have shown in the development of malware will require us in an even more complex way in the future," says Michael Ibe, Head of the Security Operations Center (SOC) at noris network. "We had previously relied on traditional antivirus solutions, but now it was time to switch to next-generation endpoint technology. As we are continuously planning our technical and organizational solutions in the course of our security management systems, the time for the introduction of this new solution could be planned very quickly ".

Challenge: Maximum Malware Protection with low CPU Utilization

Following an extensive research, which focused mainly on integrating various functionalities into a single product, and a three-month test phase, the company finally decided in September 2017 to choose SentinelOne's endpoint protection platform. The main reason for this was the use of innovative protection technologies, because unlike traditional signature-based security products, the SentinelOne platform is based on dynamic behavioral analysis techniques in combination with machine learning and intelligent automation.

In this way, even infections with unknown or stealthy malicious code can be identified and automatically blocked within a few seconds on the basis of its execution behavior, even before damage occurs. At the same time, machine-learning skills ensure that behavioral analysis techniques are constantly being learnt and continuously optimized thanks to the continuous flow of information about threats. In addition, the solution can be used for all common systems (Windows, OSX, Linux derivatives).

Michael Ibe
Head of the Security Operations Center at noris network

“Many solutions are not easy to use because their updates require a lot of bandwidth in the local network and cause CPU peaks on the computer with resource-intensive scans, resulting in an unpleasant full load on the client. As a leading ITC service provider with demanding customers, we could not afford such failures or delays for our customers' users," explains Ibe. “The slim client and low memory and CPU utilization of the platform convinced us immediately.”

In addition to maximum malware protection, those responsible at noris network also had an eye on resource friendliness. “Many solutions are not easy to use because their updates require a lot of bandwidth in the local network and cause CPU peaks on the computer with resource-intensive scans, resulting in an unpleasant full load on the client. As a leading ITC service provider with demanding customers, we could not afford such failures or delays for our customers' users," explains Ibe. “The slim client and low memory and CPU utilization of the platform convinced us immediately.”

Business Benefit: Relief of Employees and GDPR-compliant Data Protection

Since using SentinelOne Endpoint Protection Platform, the security teams at noris network have been relieved in the long term. This is mainly due to the fact that the solution combines a wide range of functionalities in one platform, so that the teams do not lose valuable time in merging different product solutions. In addition, the client is fast and reliable.

The central management server cluster for each noris network customer is designed intuitively and clearly arranged. It is hosted in the highly secure, certified data centers of noris network AG in Germany – an environment in which the confidentiality of log and analysis data with regard to current data protection and data security requirements can be fully guaranteed. There is no such thing as "calling home" to the manufacturer as with other next generation scanning solutions. Nevertheless, the central management provides an up-to-date database. If SentinelOne detects a potential attack at an endpoint, the signature is immediately forwarded to the other clients via the management station so that they can raise their shields against this new threat at an earlier stage than previously possible

Since SentinelOne uses its intelligent "Next Generation" technology to identify malicious code based on its execution behavior, the number of false positives (i. e. reporting activities that look dangerous but are not) is also reduced. This in turn means that administrators are able to focus on the analysis of real threats. This attack analysis is particularly effective thanks to the provision of collected forensic data on the management station, including all file information, paths, system names, IP addresses, domains etc., and enables those responsible to quickly disclose the modus operandi and the attacker's intentions.

With the SentinelOne platform, noris network was also able to achieve a new level of security in terms of data protection. Solutions for which data protection and data security is relevant are always operated in the company's own noris network data centers in Germany, such as here at the SentinelOne management station. This remains important because companies continue to look for the "safe harbor" in Germany on the basis of legal regulations and data protection precautionary measures – which are for example important for banks/financial service providers, lawyers, tax consultants, insurance companies, health companies, public administrations etc.

The new General Data Protection Regulation requires effective protection of the processed data from loss of confidentiality, integrity, availability and above all resilience. “With the SentinelOne platform, we feel perfectly prepared for the strict GDPR requirements," explains Michael Ibe. “In this way, we can not only effectively protect our data and the data entrusted to us from theft and misuse, but can also easily comply with the obligations imposed by the EU.”

.

Michael Ibe
Head of the Security Operations Center at noris network

“Colleagues from all areas of the company are enthusiastic about the exceptionally high detection rate of the system as well as the performance and reliability of the client," says Michael Ibe. "In our opinion, the solution is at least 1.5 years ahead of the market.”

As the platform provides the noris network´s security officers with a clear real-time audit trail, enabling them to gain a 360-degree insight into any attacks, the company is able to quickly assess the scope of a possible attack and the extent of the data potentially affected, to react appropriately and at the same time to document the defensive measures in a GDPR-compliant manner.

The implementation of the solution took about six weeks and could be completed smoothly thanks to the successful cooperation between the noris network specialist departments and the seamless support provided by the SentinelOne team. “Colleagues from all areas of the company are enthusiastic about the exceptionally high detection rate of the system as well as the performance and reliability of the client," says Michael Ibe. "In our opinion, the solution is at least 1.5 years ahead of the market.”

SentinelOne™

For more information about SentinelOne Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com.

ProteQtor IT Security is reseller van SentinelOne. Wij leveren u de software, helpen met de implementatie en geven u advies.

Vragen of opmerkingen? Neem gerust contact met ons op!

BEL ONS
+31 (0)88 066 0770

VIND ONS
Industrieweg 20-7
3846 BD Harderwijk

MAIL ONS
info@proteqtor.nl