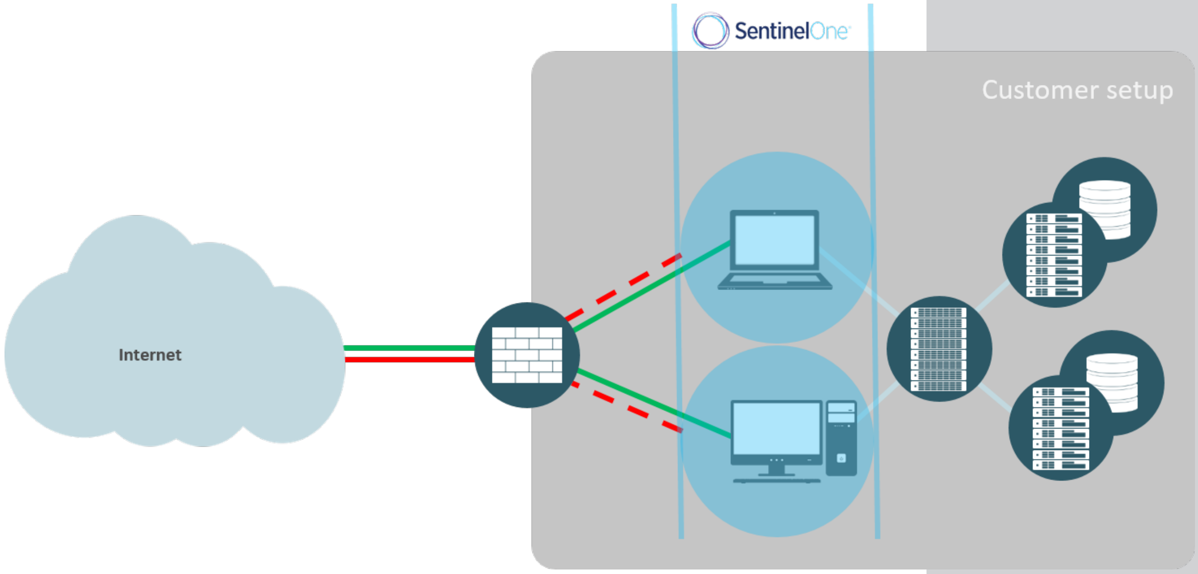
Managed Services

Endpoint Protection

With SentinelOne from noris to a new level



With Endpoint Protection from noris, we offer you a platform that protects you against all kinds of attacks on your end devices. In particular, the detection of fileless malware distinguishes it from conventional virus protection systems.

Benefits

- Malware is intercepted and blocked before reaching the end device
- Detects threats in real time and stops their progress by disconnecting the infected device from the network
- All activities are monitored and the most advanced attacks are detected by machine learning
- Combines dynamic white- and blacklisting with advanced static prevention
- In the variants managed by noris, the certificate corresponds to TSLA and is secured by DNSSEC
- noris network takes over - if desired - the complete operation

Highlights

- Deep File Inspection
- Detection of exploits as well as fileless and sophisticated malware
- Prevention as well as the identification and defence of attacks
- Award-winning machine learning technology
- Certified according to HIPAA and PCI-DSS
- Automatic immunization of other clients
- Dynamic, behavioural threat detection

noris network

Managed Services

Details

In times of ever-increasing threat from cybercrime, it is important to protect your endpoints from attacks. In order to be able to learn from the attacks and to live with the problems, you need a defensive platform that combats any endpoint attacks preventively, recognizes them at an early stage and fights them without errors. noris network therefore offers one of the most advanced platforms for defending against narrow-device attacks, which includes these features.

Our solution distinguishes itself clearly from most other solutions by the following aspects in particular:

- Behavior-based threat detection across all attack vectors
- The Lean Autonomous Agent carries out all prevention and detection measures at the endpoint
- Automated real-time mitigation and resolution
- Auto-immunization of protected devices against new attacks
- real-time forensics
- Significantly lower total cost of ownership than a comparable approach with multiple prevention, detection and response solutions
- Flexible application: Cloud-based or local management server

Here, noris network distinguishes between the three variants OnPremise, Half-Managed and Full-Managed. These differ mainly in the access of the systems, a detailed list of the differences can be found in the table below.

The endpoint protection platform is located within noris network‘s own infrastructure. With the OnPremise variant, we also build the solution on the customer‘s own infrastructure.

The supported operating systems can always be found on the manufacturer‘s page:

https://www.sentinelone.com/platform/

<table>
<tr><th>Variants</th><th>On-Prem</th><th>Half-Managed</th><th>Full-Managed</th></tr>
<tr><td>Access</td><td>full access</td><td>access to the system</td><td>none</td></tr>
<tr><td>Licences</td><td colspan="3">inklusive</td></tr>
<tr><td>Report</td><td>manual setup by the customer</td><td colspan="2">weekly or monthly, set up by noris</td></tr>
<tr><td>Analysis and mitigation of threats by an analyst from noris network</td><td colspan="2">is carried out by customer
(optional support by noris possible)</td><td>optional</td></tr>
<tr><td>Sorting the Clients</td><td>-</td><td colspan="2">optional</td></tr>
<tr><td>Analysis per client by an analyst from noris network</td><td colspan="3">optional</td></tr>
<tr><td>Requirements</td><td>■ at least 1000 clients
■ Certificate for management must be provided
■ VMware on which OVA is installed</td><td colspan="2">none</td></tr>
</table>

Interested?

We look forward to your inquiry!

noris network AG
Thomas-Mann-Straße 16 - 20
90471 Nuremberg, Germany

Phone +49 911 9352-160
Fax +49 911 9352-100

productinquiry@noris.de
www.noris.de

v1.0 20180123