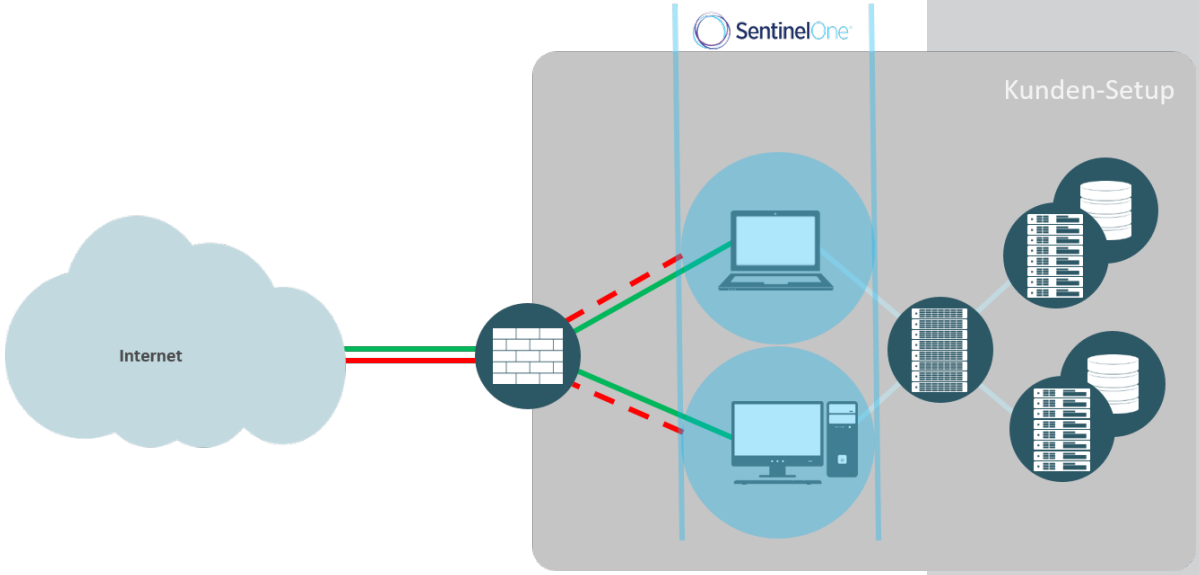
Endpoint-Protection

Mit SentinelOne von noris auf ein neues Level



Mit Endpoint-Protection von noris bieten wir Ihnen eine Plattform, die Sie vor jeglicher Art von Angriffen auf Ihre Endgeräte schützt. Vor allem durch die Erkennung von Fileless Malware hebt es sich von herkömmlichen Virenschutz-Systemen deutlich ab.

Vorteile

- Malware wird bereits vor dem Erreichen des Endgerätes abgefangen und geblockt
- Bedrohungen werden in Echtzeit erkannt und deren Fortschritt gestoppt, indem das infizierte Gerät vom Netzwerk getrennt wird
- Alle Aktivitäten werden überwacht und die fortschrittlichsten Angriffe mit Hilfe von maschinellem Lernen erkannt
- Kombiniert dynamisches White- und Blacklisting mit fortschrittlicher statischer Vorbeugung
- In den durch noris gemanagten Varianten entspricht das Zertifikat TSLA und ist gesichert durch DNSSEC
- noris network übernimmt - wenn gewünscht - den kompletten Betrieb

Highlights

- Deep File Inspection
- Erkennung von Exploits sowie fileloser und ausgeklügelter Malware
- Prävention sowie die Identifizierung und Abwehr von Attacken
- Preisgekrönte Machine-Learning-Technologie
- Zertifiziert nach HIPAA und PCI-DSS
- Automatische Immunisierung anderer Clients
- Dynamische, verhaltensorientierte Bedrohungserkennung

noris network

Details

In Zeiten von stetig wachsender Gefahr durch Cyber-Kriminalität ist es wichtig, seine Endgeräte vor Angriffen zu schützen. Um nicht erst im Nachhinein aus den Angriffen lernen zu können und mit den Problemen leben zu müssen, benötigt man eine Abwehr-Plattform, die jegliche Endpoint-Attacken präventiv bekämpft, frühzeitig erkennt und fehlerfrei bekämpft. noris network bietet daher eine der fortschrittlichsten Plattformen zur Abwehr von Endgerät-Attacken an, die diese Features beinhaltet.

Unsere Plattform hebt sich vor allem durch folgende Aspekte von den meisten anderen Lösungen deutlich positiv ab:

- Verhaltensbasierte Erkennung von Bedrohungen über alle Angriffsvektoren hinweg
- Der schlanke autonome Agent führt alle Präventions- und Erkennungsmaßnahmen am Endpoint durch
- Automatisierte Mitigation und Behebung in Echtzeit
- Auto-Immunisierung von geschützten Endgeräten gegen neue Angriffe
- Echtzeit-Forensik
- Deutlich niedrigere Gesamtbetriebskosten als bei einem vergleichbaren Ansatz mit mehreren Lösungen für Prävention, Erkennung und Reaktion
- Flexibel einsetzbar: Cloud-basierter oder lokaler Management-Server

Dabei unterscheidet noris network die drei Varianten On-Prem, Half-Managed und Full-Managed. Diese unterscheiden sich vor allem im Zugriff der Systeme, eine detaillierte Auflistung der Unterschiede findet sich in der Tabelle anbei.

Die Endpoint-Protection-Plattform liegt innerhalb der noris network-eigenen Infrastruktur. Bei der Variante OnPremise bauen wir die Lösung auch auf der Kunden-eigenen Infrastruktur auf.

Die unterstützten Betriebssysteme finden sich immer aktuell auf der Seite des Herstellers:
https://www.sentinelone.com/platform/

Varianten	On-Prem	Half-Managed	Full-Managed
Zugriff	Vollzugriff	Zugang zum System	keiner
Lizenzen	inklusive		
Report	manuelle Einrichtung durch den Kunden	wöchentlich oder monatlich, eingerichtet durch noris	
Analyse und Mitigation von Bedrohungen durch einen Analysten von noris network	wird durch Kunden durchgeführt (optionale Unterstützung durch noris möglich)		optional
Einsortierung der Clients	-	optional	
Analyse pro Client durch einen Analysten von noris network	optional		
Voraussetzungen	■ min. 1000 Clients ■ Zertifikat für das Management muss bereitgestellt werden ■ VMware auf der das OVA installiert wird	keine	

Interessiert?

Wir freuen uns auf Ihre Anfrage!

noris network AG
Thomas-Mann-Straße 16 - 20
D-90471 Nürnberg

T +49 911 9352-160
F +49 911 9352-100

produktanfrage@noris.de
www.noris.de

v1.2 20180405

noris network