## Warum EPP & EDR mit SentinelOne?

IT-Netzwerke sind mit Firewall, Sandbox & Co. meist sehr gut im Kern abgesichert, viele Angriffe erfolgen jedoch über das Endgerät, wo User tagtäglich Viren, Würmern und Trojanern ausgesetzt sind. Am Endgerät ist ein intelligenter, verhaltensorientierer Schutz erforderlich. Wir haben nachfolgend beschrieben, warum der traditionelle Antivirus (AV)-Schutz nicht mehr ausreicht, und wie die Endpoint Protection (*EPP*)-Lösung von SentinelOne das Problem löst. Mittels aktiver Endpoint Detection Response (ActiveEDR™) & Deep Visibilty bietet S1 sogar eine „SOC[1]-Analyse“ am Endgerät.


## Traditioneller Antivirus-Schutz (AV) reicht nicht mehr aus.

Der traditionelle (legacy) AV-Schutz basiert auf einer Technologie, welche über 20 Jahre alt ist. Seinerzeit war die Technik ausreichend, heute jedoch gibt es 400.000 neue Bedrohungen – pro Tag.

### Zu wenig Platz auf dem Endgerät für alle Signaturen

Der traditionelle AV-Schutz vergleicht mit bekannten Viren (Signaturen / Hash-Wert), welche schon einmal in Erscheinung getreten sind. SentinelOne (S1) nutzt u.a. einen Reputationsfilter, welcher alle S1 bekannten Viren beinhaltet. Die Filter-Datenbank ist zur Zeit rund zehn Terabyte groß und entspricht damit einer Datenmenge von ca. 1.000 Stunden HD-Videos oder rund 13 Millionen Dokumentenseiten. Soviel Speicherplatz ist auf dem Endgerät nicht für AV-Schutz verfügbar.

### Mutationen bekannter Viren werden nicht zeitnah erkannt

Ein Großteil der Viren sind Mutationen bereits bekannter Viren, welche jedoch für den traditionellen AV-Schutz zunächst unverdächtig erscheinen, da es noch keine Signatur zum Vergleich gibt. Dies wird von Angreifern gerne ausgenutzt, da es für „neue“ Viren keinen Ad-hoc-Schutz gibt (Polymorphe Malware).

### Manipulierte Dokumente nutzen Schwachstellen in Anwendungen (Malicious Documents)

Nicht selten werden von Angreifern mittels digitaler Dokumente gezielt Schwachstellen in populären Anwendungen ausgenutzt und hierüber das Endgerät (das Netzwerk) angegriffen. Solche Angriffe werden von traditionellen AV-Reputationsdatenbanken nicht erkannt.

[1] Als „Security Operations Center“ (SOC) wird die Zentrale der IT-Sicherheit in einem Unternehmen oder einer Organisation bezeichnet. Sie ist im Idealfall 24/7 besetzt und dient dem reibungslosen Ablauf aller Systeme, der Früherkennung und Abwehr von Cyber-Bedrohungen.

### Schadcode ohne verdächtige Anhänge (Fileless Malware) wird nicht erkannt

In den letzten Jahren fokussieren Angreifer die Schwachstelle, dass der traditionelle AV-Schutz nur Angriffe erkennt, welche in Form von Files auf das Endgerät übertragen werden. So sind z.B. sogenannte Power Shell-Angriffe (Skripting) mit einem Legacy AV-Schutz nicht zu entdecken, vgl. auch: https://www.heise.de/security/meldung/Studie-Angreifer-lieben-Powershell-4357396.html

### Verschlüsselter Datenverkehr wird nicht erkannt

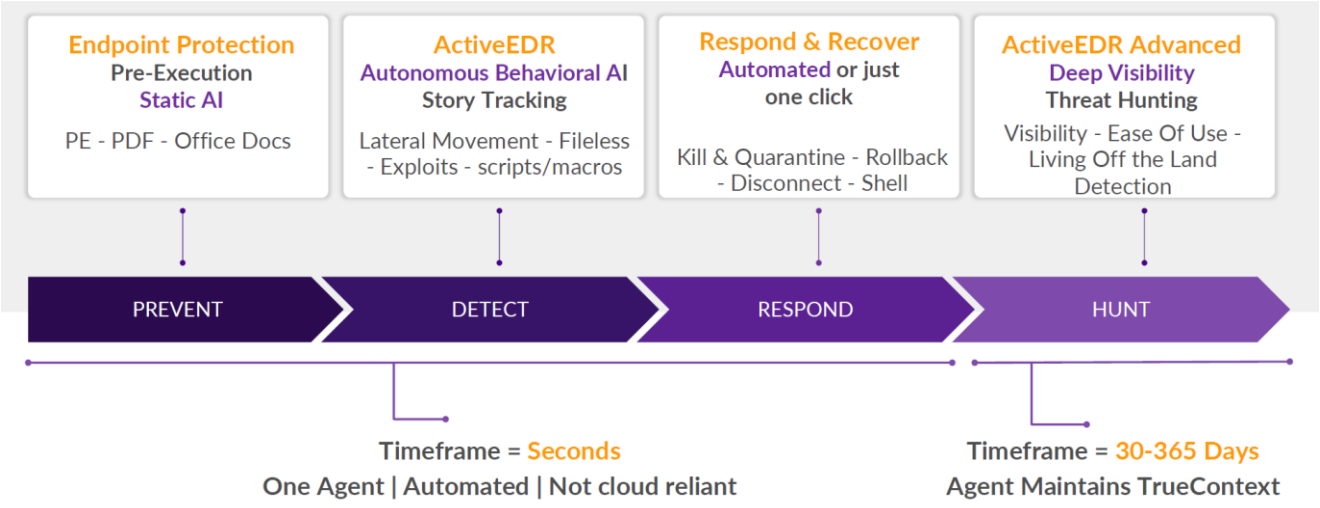
Angreifer nutzen zunehmend die Verschlüsselung ihrer Angriffskommunikation und entziehen sich so einem Zugriff des regulären AV-Schutzes.

## SentinelOne EPP & EDR plus Deep Visibility

Die SentinelOne-Lösung bietet einen Komplett-Schutz gegen Ransomware & Co., auch gegen unbekannte Exploits (ZeroDay) und Memory-only Malware (PowerShell / Skripting). Basierend auf einer einzigen Plattform: zum Schutz, zur Entdeckung, zur sofortigen Reaktion und zur Forensik von Angriffen. Genutzt wird ein homogener Software-Agent, sowohl für Server als auch für Endgeräte: einheitlich für Windows, für MacOS, für Linux, für Virtualization. Mit „machine speed“-Performance und max. 2% CPU-Last:

- Static & Behavioral AI (künstliche Intelligenz, KI)
- keine Pattern-Updates (Signaturen), das Verhalten auf dem Endgerät wird beobachtet
- System-Wiederherstellung per Rollback für Windows-Endgeräte
- Schutz der laufenden Prozesse am Endpoint
- SOC-Analyse & Dokumentation am Endpoint
- API-Schnittstelle zur Integration in bestehende Security-Systeme

**Abbildung:** Workflow der SentinelOne-Lösung.



## Protect & Respond.

## Workflow der SentinelOne-Lösung

SentinelOne nutzt einen Multi-Vektoren-Ansatz und ist unabhängig von Pattern-Updates (Signaturen). Die Abbildung oben verdeutlicht den automatisierten Workflow auf dem zu schützenden Endgerät.

**Endpunktschutz vor der Ausführung mittels Static AI Engine (Künstliche Intelligenz / KI)**

- Bezug zu mehreren Millionen Beispielen von Malware.
- Beispiel: Entdeckung und Quarantäne von neuer Ransomware, welche über einen Email-Link oder über eine Website geladen wurde.

**Endpunktschutz während der Ausführung durch ActiveEDR™ Verhaltensanalyse**

- Stetige Überwachung aller Prozesse sowie der Netzwerk-Kommunikation auf dem Endgerät
- Tracking aller Systemänderungen sowie ein automatisches Logging der beiteiligten Prozesse zu einer archivierenden TrueContext™-ID. Dies ermöglicht ein späteres „Kill & Quarantine“ plus ggf. Rollback, insofern die Prozesse Teil eines Angriffes waren.

**Automatisierte Bereinigung & optionales Rollback**

SentinelOne bereinigt das Endgerät automatisiert per „Kill & Quarantine“. Für Windows-Endgeräte bietet sich die Möglichkeit einer Rücksetzung (Rollback) in den ursprünglichen (sauberen) Zustand vor der Infizierung. Diese Rollback-Funktion wird ermöglicht durch die von SentinelOne patentierte Nutzung der Volume Shadow Copy (VSS) auf den Windows-Endgeräten.

## Forensik – Root Cause Analysis

Die forensische Analyse erfolgt DSGVO-konform mit Hilfe des SentinelOne-Agenten auf dem Endgerät. Dank der TrueContext™-Technologie (welcher Prozess war wann & wie beteiligt?) kann jeder Angriff „post mortem“ nachvollzogen werden (Root Cause Analysis). ActiveEDR™ kennt immer die komplette Geschichte eines Angriffs und löst das Problem in Echtzeit.

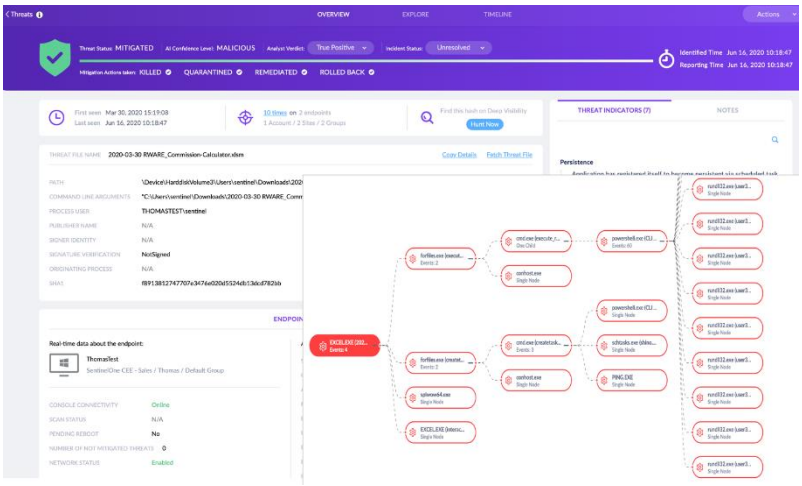



**Abbildung:** ActiveEDR kennt immer den kompletten Angriff

## Vigilance Respond bietet SOC as a Service mit 24/7 Überwachung

SentinelOne bietet mit Vigilance Respond einen Managed Detection & Response Service (MDR). Hierbei überwachen die Cyber Security Analysten von SentinelOne rund um die Uhr Ihre Endgeräte und agieren zeitnah auf Security Events, mit proaktiven Empfehlungen und Support, 24x7.

Der Vigilance Respond Service bietet Unterstützung im Rahmen der gebuchten Lizenzierung, d.h. der Service hat einen Preis, unabhängig von der präferierten Lizenzierung (Core ←→ Control ←→ Complete). Im Rahmen der Complete-Lizenzierung wird also auch ActiveEDR & Deep Visibility genutzt & supportet.

**Abbildung: Workflow von Vigilance**