SentinelOne

Singularity™ EPP+EDR

Einheitliche Funktionen für Prävention, Erkennung, Untersuchung und Reaktion

DATENBLATT

Gartner

Gartner stuft SentinelOne als „Leader“ ein
Gartner Magic Quadrant
„Endpoint Protecion Platform 2020“

Bedrohungen werden immer schneller, raffinierter und umfangreicher, sodass Präventions- und EDR-Lösungen der ersten Generation nicht Schritt halten können

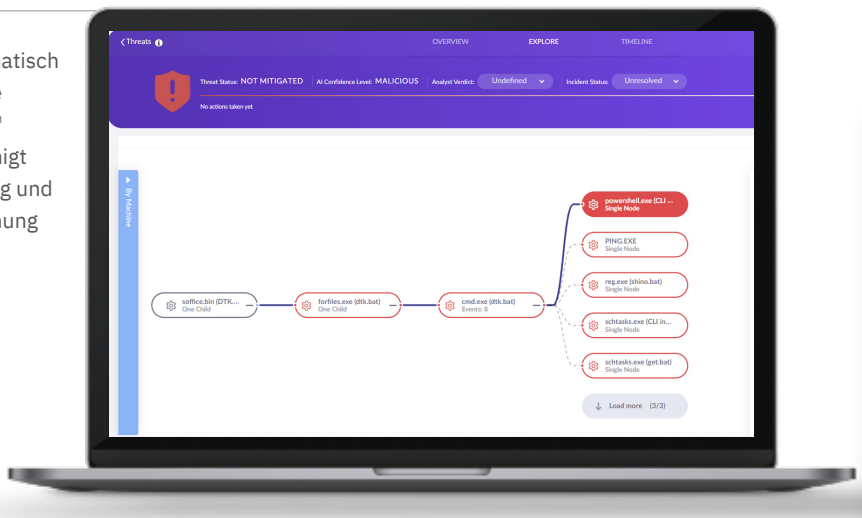
Wenn Angreifer Schutzmaßnahmen überwinden, müssen Endpoint Detection and Response auf dem Endpunkt autonom und in Echtzeit erfolgen – und zwar mit und ohne Netzwerkverbindung. SentinelOne Singularity EPP+EDR kombiniert Präventions- und EDR-Funktionen der nächsten Generation in einem einzigen Sentinel-Agenten, um den autonomen Betrieb der EPP in Maschinengeschwindigkeit zu gewährleisten.

Auf Basis von Deep Visibility™ und ActiveEDR™

ActiveEDR verwendet verhaltensbasierte KI zur Identifizierung gerade laufender schädlicher Prozesse und Kennzeichnung korrelierter Ereignisse. Außerdem wird automatisch eine Storyline™ zum Angriff erstellt, die die Ereignisse visualisiert und die Untersuchung beschleunigt. Im Schutzmodus identifiziert der Sentinel-Agent nicht nur den Angriff, sondern wehrt zudem automatisch den Eindringling ab. Anschließend macht ein Analyst mit der patentierten 1-Klick-Wiederherstellung nicht autorisierte Änderungen rückgängig. Dafür sind keine Skripte erforderlich.

Robuste Forensik, intuitive Einfachheit

EDR darf nicht mehr nur exklusiv für wenige zur Verfügung stehen. Um die mittlere Reparaturdauer (Mean Time to Repair, MTTR) zu verkürzen und die Produktivität zu maximieren, muss EDR 2.0 die Erkennung und Reaktion vereinfachen. KI überwacht kontinuierlich alle Ereignisse auf allen Betriebssystemen und in allen Umgebungen, ganz gleich ob das ein Rechenzentrum, Cloud-Service-Provider, Büro oder Homeoffice ist. Deep Visibility ermöglicht die Suche nach Bedrohungen und deren Untersuchung ohne Lernkurve, sodass Incident Response und Threat Hunting von mehr Sicherheitsmitarbeitern durchgeführt werden können.



Die automatisch generierte Storyline™ beschleunigt Triagierung und Untersuchung

SINGULARITY EPP+EDR

Autonome, KI-gestützte Präventions- und EDR-Funktion in Maschinen-geschwindigkeit

WICHTIGSTE FUNKTIONEN

+ Konsolidierte, autonome EPP/EDR-Funktionen
+ Reines EPP, reines EDR und kombinierte Modi – im gleichen Produkt
+ Linux, macOS, Windows, Kubernetes und Docker
+ Online/Offline-Schutz, Erkennung und Reaktion
+ Automatisierte Ereignis-korrelation in Storylines
+ Patentierte 1-Klick-Funktionen für Wiederherstellung und Rollback
+ Vollständige Abstimmung mit MITRE ATT&CK®-Framework
+ Flexible EDR-Datensicherung: 14 Tage bis mehr als 365 Tage wählbar
+ Remote-Forensikfunktionen für jedes Betriebssystem

Gartner peerinsights™

“

Hervorragender Kundendienst, noch besseres Produkt.

★★★★★

SENIOR DIRECTOR, IT
Gesundheitswesen

Wichtigste Eigenschaften

- **Autonome Echtzeit-Funktionen** zur Erkennung und Behebung komplexer Bedrohungen ohne menschliche Interaktion.
- **Kompromissloser Schutz** für Windows, Linux und macOS – physische und virtuelle Systeme, Container, Cloud, Rechenzentrum, überall.
- **Beschleunige Triagierung und Ursachenanalyse** mit Erkenntnissen zu Zwischenfällen und der marktweit besten Abstimmung mit MITRE ATT&CK® – mit und ohne MDR. Untersuchungen in Sekunden mit automatisierten Korrelationen und Storylines.
- **Wiederherstellung und Rollback mit nur einem Mausklick** vereinfacht die Reaktion und verkürzt die mittlere Reparaturdauer (MTTR).
- **Intuitive Benutzerführung** bei Deep Visibility, S1QL und STAR™ (Storyline Active Response) verringert die Komplexität des Threat Huntings.
- **Datenspeicherungsoptionen** für jeden Bedarf – von 14 Tagen bis mehr als 365 Tage.
- **Schnelle, reibungslose Implementierung** dank Interoperabilitätsfunktionen.
- **Integrierte Threat Intelligence** zur Erkennung und Anreicherung führender Drittanbieter-Feeds sowie eigener proprietärer Quellen.

WICHTIGSTE VORTEILE

+ Kürzere Verweildauer von Bedrohungen
+ Beschleunigte Incident Response
+ Verkürzte mittlere Reparaturdauer
+ Weniger „Warnmeldungs-müdigkeit“
+ Höhere Produktivität für die Analysten
+ Eine Komponente der Singularity-Plattform

BEREIT FÜR EINE DEMO?

Weitere Details finden Sie auf der SentinelOne-Website.

MANAGED DETECTION AND RESPONSE

Da sich Kunden mit Vigilance MDR auf die relevanten Zwischenfälle konzentrieren können, ist das die perfekte Add-on-Lösung für überlastete IT/SOC-Teams.

Weitere Informationen finden Sie unter **https://s1.ai/s1mdr**.

ATT&CK®

2020 MITRE ATT&CK

- Geringste False-Negative-Rate
- Meiste Korrelationen
- Umfassendste Datenanreicherung

Gartner

2020 GARTNER MAGIC QUADRANT FÜR EPP

- Als „Leader“ eingestuft
- Höchste Bewertung für „wichtige Funktionen“ bei allen drei von Gartner definierten Kundenprofiltypen

FORRESTER®

2020 FORRESTER WAVE™ EDR

„Strong Performer“

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

Hervorragender EPDR-Innovator

Bei SentinelOne haben Kunden höchste Priorität

Durch kontinuierliche Auswertung und Verbesserung können wir die Erwartungen unserer Kunden übertreffen.

Gartner peerinsights customers' choice™

97 %

der Gartner Peer Insights™ „Voice of the Customer“-Bewerter empfehlen SentinelOne

97 %

Kundenzufriedenheit (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

AAA MAY 2020

TEVORA

PCI DSS-Bestätigung
HIPAA-Bestätigung

Gartner peerinsights 4,9 ★★★★★

Informationen zu SentinelOne

Mehr Funktionen, weniger Komplexität: SentinelOne ist ein innovativer Anbieter für Cybersicherheit mit autonomer, verteilter Endpunkt-Threat Intelligence, der das Sicherheitskonzept vereinfacht, ohne Kompromisse zu verlangen. Unsere Technologie lässt sich automatisieren und ermöglicht die reibungslose Behebung von Bedrohungen. Sind Sie bereit?

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733

S1-SNGL-EPP-EDR-10022020