SentinelOne

DATENBLATT

# Singularity™ XDR

## Eine einzige Plattform für Transparenz, Erkennung und Reaktion für alle Endpunkte, Cloud-Umgebungen und Identitäten

Cybersicherheitsbedrohungen entwickeln sich exponentiell weiter – sowohl in Bezug auf Geschwindigkeit als auch auf den Umfang. Gleichzeitig können die meisten Sicherheitsteams mit den ihnen zur Verfügung stehenden Ressourcen kaum mit neuen Bedrohungen Schritt halten. Häufig fehlen Unternehmen der globale Überblick und der Kontext aus allen Sicherheitslösungen, was zu Lücken in der Erkennung führt. Zudem nutzen Analysten Einzellösungen für jeden einzelnen Vektor und müssen Daten daher isoliert analysieren und manuell untersuchen. Sicherheitsteams benötigen heute jedoch eine proaktive Lösung zur Identifizierung, Eindämmung und Behebung neuer Bedrohungen.

SentinelOne Singularity XDR vereinheitlicht und erweitert Erkennungs- und Reaktionsfunktionen für mehrere Sicherheitsebenen, einschließlich Endpunkte, Cloud-Umgebungen, Identitäten, Netzwerke und Mobilgeräte. Dies bietet Sicherheitsteams unternehmensweite zentrale und umfassende Transparenz, leistungsstarke Analysen sowie automatisierte Reaktionen für einen Großteil der Sicherheitstechnologien.

### Verarbeitung von Daten aus mehreren Quellen

Mit Singularity XDR können Unternehmen strukturierte, unstrukturierte und halbstrukturierte Sicherheitsdaten in Echtzeit aus jedem Produkt und jeder Plattform nahtlos erfassen und damit Datensilos aufbrechen sowie blinde Flecken beseitigen. Die Lösung kann Daten aus getrennten Sicherheitslösungen und allen Plattformen (z. B. Endpunkte, Cloud-Workloads, IoT-Geräte, Netzwerke uvm.) visualisieren.

### Aufdeckung von Angriffskampagnen in allen Unternehmenstechnologien

Sie erhalten in Echtzeit automatisierte und maschinell erstellte Kontext- und Korrelationsinformationen für alle Ihre Unternehmenstechnologien, sodass aus den einzelnen Daten ein umfassendes Bild entsteht. Die verhaltensbasierte KI bewertet Bedrohungen (z. B. dateilose Angriffe, laterale Bewegungen und aktive Rootkits), sobald diese auftreten, sodass auch ohne manuelle Eingriffe detaillierte Erkennungen möglich sind. Einzelne Ereignisse werden automatisch zu einer Storyline mit umfassendem Kontext korreliert, sodass ein Angriff von Anfang bis Ende nachvollzogen werden kann.

### 1-Klick-Funktion für Wiederherstellung und automatisierte Reaktion

Dank Singularity XDR können Analysten alle nötigen Maßnahmen ergreifen, um Bedrohungen automatisch oder mit einem Klick auf einem, mehreren oder gar allen Geräten in der Unternehmensumgebung zu beheben – ohne dass manuell Skripte ausgeführt werden müssen. Mit nur einem Schritt kann ein Analyst Wiederherstellungsaktionen wie Netzwerkquarantäne, die automatische Bereitstellung von Agenten auf nicht autorisierten Workstations oder die automatisierte Richtliniendurchsetzung für Cloud-Umgebungen veranlassen.

## WICHTIGE FUNKTIONEN UND VORTEILE

+ **Sehen**
  Maximale Transparenz in allen Winkeln Ihres Unternehmens

+ **Schützen**
  Absicherung mit beispielloser Geschwindigkeit, Abdeckung und Effizienz

+ **Beheben**
  Automatisierte Reaktion im gesamten vernetzten Sicherheitsökosystem

---

+ Beschleunigte Untersuchung und Threat Hunting mithilfe von MITRE ATT&CK® und proaktiven, benutzerdefinierten STAR™-Hunting- und Reaktionsregeln

+ Optimierte Geschäftsabläufe und verbesserte Sicherheitsworkflows

+ Kürzere mittlere Reaktionsdauer durch einfache, schnelle und relevante Automatisierung

+ Höhere Produktivität der Analysten

+ Schnelle Einsatzbereitschaft für Ihre Analysten

+ Kombination von Native XDR und Open XDR, damit Kunden die nötige Flexibilität erhalten, ohne sich auf eine einzige Lösung beschränken zu müssen

# Automatische Anreicherung mit integrierten Bedrohungsdaten

Singularity XDR integriert Bedrohungsdaten, um die Erkennung zu verbessern und Daten zu Zwischenfällen automatisch mit Erkenntnissen aus führenden Drittanbieter-Feeds und proprietären Quellen anzureichern. Auf diese Weise erhält das Sicherheitsteam einen umfassenderen Überblick über die Situation sowie zusätzliche kontextbezogene Risikobewertungen zu Kompromittierungsindikatoren (Indicators of Compromise, IOCs) wie IP-Adressen, Hashes, Schwachstellen und Domänen. Zudem ordnet die Plattform Ereignisse dem MITRE ATT&CK-Framework zu und erleichtert dem Team die Analyse und Untersuchung. Außerdem können Kunden eine Bibliothek mit Threat Hunting-Abfragen nutzen, die von Forschern und Threat Huntern kuratiert wird. Diese bewerten neue Methoden und identifizieren neue IOCs und TTPs (Taktiken, Techniken und Prozeduren).

## Erweitern Sie Ihr Team mit einer intuitiven Plattform

Singularity XDR stellt eine zentrale einheitliche Plattform zur erweiterten Erkennung, Untersuchung und Abwehr von Bedrohungen sowie für Threat Hunting bereit und bietet folgende Vorteile:

- Eine zentrale Quelle für priorisierte Warnungen, die Daten aus mehreren Quellen erfasst und standardisiert.
- Eine zentrale, konsolidierte Ansicht, damit Sie den Fortschritt von Angriffen auf allen Sicherheitsebenen schnell nachvollziehen können.
- Eine zentrale Plattform, mit der Sie Bedrohungen schnell abwehren und proaktiv danach suchen können.

## REIBUNGSLOSE INTEGRATION IN SICHERHEITS-ÖKOSYSTEME FÜHRENDER ANBIETER

Dank Singularity Marketplace kann die SentinelOne Singularity XDR-Plattform mit kleinen 1-Klick-Anwendungen erweitert werden, die Unternehmen die Vereinheitlichung von Prävention, Erkennung und Reaktion für alle Angriffsflächen erleichtern.

Gartner peerinsights

“Insgesamt ist dies die einfachste Lösung zur Abwehr von Bedrohungen, die ich je genutzt habe, und eine der unkompliziertesten Software-Bereitstellungen, die ich je erlebt habe. Der Service ist hervorragend.

★★★★★

**SICHERHEITS- UND RISIKOMANAGER**
Bauunternehmen

Singularity Platform

## HABEN SIE INTERESSE AN EINER DEMO?

Weitere Informationen finden Sie auf der SentinelOne-Website.

## Innovativ. Vertrauenswürdig. Anerkannt.

**Gartner**

**Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen**

**MITRE ENGENUITY**

**Rekordergebnis bei der ATT&CK-Bewertung**

- 100 % Schutz. 100 % Erkennung.
- Höchste analytische Abdeckung 3 Jahre in Folge
- 100 % Echtzeit und keinerlei Verzögerungen

Gartner peerinsights 4,9 ★★★★★

**99 % der Gartner Peer Insights™**

EDR-Analysten empfehlen SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

**Informationen zu SentinelOne**

SentinelOne ist Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller, umfangreicher und genauer, als das mit ausschließlich manuellen Technologien möglich ist. Die Singularity XDR-Plattform bietet Ihnen Echtzeit-Transparenz und intelligente KI-gestützte Reaktion. Nutzen Sie mehr Optionen mit geringerer Komplexität.

**sentinelone.com**

sales@sentinelone.com
+ 1 855 868 3733