

Singularity Cloud

Server/VM Workload Detection & Response

Ihr Hybrid Cloud-Geschäft ist komplex. Der Schutz Ihrer Workloads – einschließlich Erkennung und Reaktion – sollte daher einfach bleiben. SentinelOne bietet die kompromisslose EDR-Leistung, die das SOC benötigt, um Linux- und Windows Server-VMs in AWS, Azure, Google Cloud und in Ihrem Rechenzentrum zu schützen.

Server/VM Workload Detection & Response ist Teil der Singularity Cloud-Familie und schützt Workloads in virtuellen Cloud-Instanzen und physischen Servern vor Laufzeitbedrohungen wie Zero-Day-Angriffen und dateiloser Malware. Persistente, korrelierte EDR-Telemetriedaten mit Cloud-Metadaten ermöglichen forensische Transparenz zu kurzlebigen Workloads, um Analysen und Reaktionen sowie die Bedrohungssuche zu unterstützen.



Betriebliche Effizienz

Agenten können automatisiert so bereitgestellt, verwaltet und aktualisiert werden, dass sie sich problemlos in bestehende DevOps-Bereitstellungs- und -Konfigurationsprozesse einfügen.



EDR-Transparenz mit Hybrid Cloud-Kontext

Korrelierte Ereignistelemetriedaten werden den MITRE ATT&CK-TTPs zugeordnet und beinhalten Metadaten wie Konto- und Instanz-IDs, benutzerdefinierte Tags usw.



Leistungsfähige Automatisierung der Sicherheit

Leistungsstarke, aber dennoch intuitive Automatisierungsfunktionen verkürzen die Erkennungs- und Reaktionszeiten, um die Bedürfnisse aller SOC-Teammitglieder vom frischgebackenen Analysten bis zum erfahrenen Threat Hunter zu erfüllen.

146 % mehr Linux-Ransomware mit neuem Code im Jahresvergleich. Verhaltensbasierte KI von SentinelOne kann dieses Risiko für Ihre Server- und VM-Workloads reduzieren.

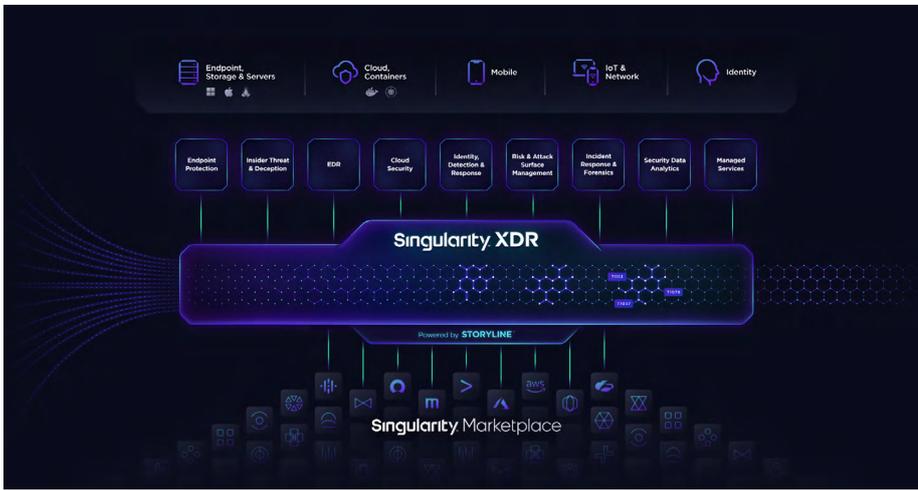
WICHTIGE FUNKTIONEN UND VORTEILE

- + Laufzeit-EDR
- + Unterstützt Cloud-Instanzen in AWS, Azure, Google Cloud und Rechenzentren
- + Unterstützung für 12 große Linux-Distributionen
- + Unterstützung für Windows Server-Versionen von 2022 bis 2003 SP2
- + EINE Multi-Cloud-Verwaltungskonsole für Endpunkte, Server, Workloads usw.
- + Gewährleistet die Unveränderbarkeit von Workloads
- + Integrierte Metadaten vereinfachen Cloud-Operationen



Neben der unerreichten EDR-Leistung in MITRE ATT&CK-Emulationen bietet SentinelOne einzigartige Funktionen wie Storyline™, die die visuelle Darstellung von Angriffen automatisieren und die Vorfall-Triagierung beschleunigen.





Reaktion auf Laufzeitbedrohungen in Maschinengeschwindigkeit

Die Erkennung und Reaktion auf Bedrohungen zur Laufzeit ist die letzte Verteidigungslinie in einer mehrschichtigen Cloud-Sicherheitsstrategie. EDR schützt Workloads vor Bedrohungen wie zur Laufzeit geladene Cryptomining-Malware und Zero-Days wie Log4j, die mit Image-Scans nicht erkannt werden. Weil Bedrohungsakteure (z. B. DarkRadiation) immer häufiger auch Linux angreifen, stellt SentinelOne wirksamere Funktionen für Ihr SOC bereit, die kaum manuellen Aufwand erfordern. Storyline beschleunigt die Vorfall-Triagierung, während automatisierte benutzerdefinierte Reaktionsschritte mit nur einem Klick die SOC-Produktivität steigern und umfangreiche Datenspeicherungsoptionen, Remote Shell, Remote Script Orchestration sowie die intuitive Verwaltungskonsole die Bedrohungssuche erleichtern.

Agil und sicher

- | | | |
|---|--|--|
| <p>✔ Unterstützte Plattformen</p> <ul style="list-style-type: none"> + AWS EC2 + Azure VM + Google Compute Engine | <p>✔ DevOps-freundlich</p> <ul style="list-style-type: none"> + IaC-Automatisierung über VM-Bootstrap + Aktualisierung des Linux-Betriebssystem-Images ohne Kernel-Abhängigkeitsprobleme + Unauffällige Sicherheitsfunktionen im Hintergrund | <p>✔ Leistungsstarke SecOps</p> <ul style="list-style-type: none"> + EDR-Transparenz und Forensik + Automatisierter Kontext von Storyline beschleunigt Triagierung + Wiederherstellung, Rollback mit einem Mausklick (Windows) + Benutzerdefinierte automatisierte Reaktionsmaßnahmen + Bedrohungssuche (Threat Hunting) |
|---|--|--|

UNTERSTÜTZTE LINUX-DISTRIBUTIONEN

- + RHEL
- + CentOS
- + Ubuntu
- + Amazon Linux
- + SUSE
- + Debian
- + Virtuozzo
- + Scientific Linux
- + AlmaLinux
- + RockyLinux
- + Oracle
- + Fedora

UNTERSTÜTZTE WINDOWS SERVER-VERSIONEN

- + Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1
- + Windows Server Core 2019, 2016, 2012
- + Windows Storage Server 2016, 2012 R2, 2012
- + Legacy-Versionen: Windows Server 2008, 2003 SP2+, 2003 R2 SP2+

Innovativ. Vertrauenswürdig. Anerkannt.



Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen



Rekordergebnis bei der ATT&CK-Bewertung

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



99 % der Gartner Peer Insights™

EDR-Analysten empfehlen SentinelOne Singularity



Informationen zu SentinelOne

SentinelOne (NYSE:S) ist ein Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller und genauer als je zuvor. Unsere Singularity XDR-Plattform schützt und stärkt weltweit führende Unternehmen mit einem Echtzeitüberblick über Angriffsflächen sowie mit plattformübergreifender Korrelation und KI-gestützten Reaktionen. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733