SentinelOne

DATENBLATT

Singularity™ Cloud

Kubernetes Workload Detection & Response

Kubernetes ist der De-facto-Standard für die Container-Orchestrierung. Image-Scans sind eine gute Wahl, reichen aber allein nicht aus, weil sie Workloads nicht vor Laufzeitbedrohungen schützen können. Daher wird eine Cloud-Verteidigungsstrategie in der Tiefe empfohlen, die auch EDR beinhaltet.

Kubernetes Workload Detection & Response ist Teil der Singularity Cloud-Familie und schützt in Kubernetes-Clustern ausgeführte Container-Workloads vor Laufzeitbedrohungen wie Zero-Day-Angriffen und dateiloser Malware. Ein einziger Agent ohne Sidecar schützt den K8s-Worker, alle seine Pods und alle Container darin, um maximale Ressourceneffizienz sicherzustellen. 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 K8s-Kontext

Korrelierte Ereignistelemetriedaten werden den MITRE ATT&CK-TTPs zuordnet und beinhalten K8s-Metadaten wie den Pod-Namen, die Image-ID usw.

Komfortable Kundenerlebnisse

Verwalten Sie die Sicherheit der containerisierten Microservices über dieselbe SentinelOne-Konsole wie die Benutzerendpunkte, Server, VMs usw.

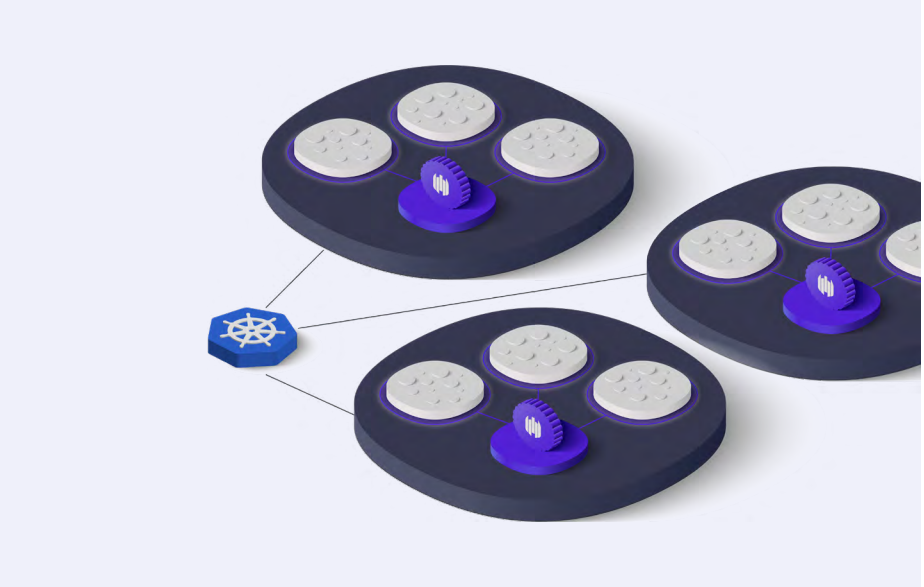
SentinelOne unterstützt 13 führende Linux-Distributionen sowie verwaltete und selbstverwaltete Kubernetes-Services in AWS, Azure sowie Google Cloud und bietet damit eine hervorragende EDR-Leistung für verschiedenste K8s-Bereitstellungen.

kubernetes aws Azure docker Google Cloud

94 % aller Unternehmen haben im letzten Jahr mindestens einen Kubernetes-Sicherheitsvorfall verzeichnet. Kubernetes Workload Detection & Response von SentinelOne kann dieses Risiko verringern.

WICHTIGE FUNKTIONEN UND VORTEILE

+ Automatisierte Bereitstellung als DaemonSet
+ Automatisch skalierter Schutz
+ Laufzeit-EDR
+ Benutzerbereich-Agent für maximale Stabilität
+ Unterstützung für verwaltete K8s-Services in AWS, Azure und Google Cloud
+ Unterstützung für 13 führende Linux-Distributionen
+ Integrierte Metadaten vereinfachen Cloud-Operationen

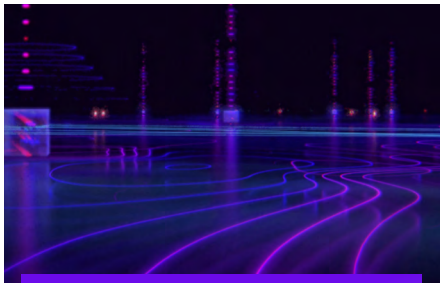


UNTERSTÜTZTE LINUX-DISTRIBUTIONEN

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

Die letzte Verteidigungslinie in der Tiefe

Die Erkennung und Reaktion auf Bedrohungen zur Laufzeit ist Ihre letzte Absicherung in einer robusten, mehrschichtigen Cloud-Sicherheitsstrategie. Damit sind Sie vor Bedrohungen wie zur Laufzeit geladene Crypomining-Malware und Zero-Day-Bedrohungen wie Log4j geschützt. Da Bedrohungsakteure (z. B. DarkRadiation) immer häufiger auch Linux angreifen, erhält Ihr SOC mit den umfassenden Datenspeicherungsoptionen und integrierten K8s-Metadaten von SentinelOne die erforderliche forensische Transparenz für die Bedrohungssuche.



WEITERE INFORMATIONEN

Besuchen Sie uns unter sentinelone.com

Agil und sicher

Unterstützte Plattformen

+ AWS EKS, EKS-Anywhere
+ Azure AKS
+ Google GKE
+ OpenShift
+ Docker, Container, CRI-O
+ K8s v1.13 oder höher

DevOps-freundlich

+ IaC-Automatisierung über HELM-Diagramme
+ Aktualisierung des Hostbetriebssystem-Images ohne Kernel-Abhängigkeits-probleme
+ Unauffällige Sicherheitsfunktionen im Hintergrund

Leistungsstarke SecOps

+ EDR-Transparenz für kurzlebige Workloads
+ Benutzerdefinierte automatisierte Reaktions-maßnahmen
+ Maximale Stabilität und hohe Leistung ohne Kompromisse

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 % BEI 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 (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