SentinelOne

DATA SHEET

Kubernetes Sentinel Agent

A component of SentinelOne Cloud Workload Security

Achieve runtime protection and EDR for containerized workloads.

Cloud-native containerized workloads need runtime security protection and EDR just like any other compute. SentinelOne delivers these capabilities to SecOps and DevSecOps teams. Kubernetes Sentinel agents supplement pre-production CI/CD container scanning with real-time protection for live, in-production containers. Runtime protection is vital to identify and stop previously unknown threats that pre-production scans miss. K8s Sentinels also remove a blind spot for the SOC by enabling EDR threat hunting visibility into container operations. Our efficient one agent per node architecture supports self-managed Kubernetes and managed Kubernetes services including AWS EKS, Azure AKS, and Google Cloud GKE.

Kubernetes Sentinel enforcement points are managed within the same multi-tenant console alongside other Sentinels for Windows, macOS, and Linux. Administration is flexible, distributed, and managed via role-based access controls that match your organization's structure. Kubernetes Sentinels offer compatibility and ongoing support for popular Linux families without the risk of kernel module instability or container interference.

MANAGED K8S SERVICE

SELF-MANAGED K8S

Kubernetes Sentinel enables the SOC to protect cloud-native workloads across multiple cloud service providers via one simple SaaS solution.

KUBERNETES SENTINEL FEATURES

Operations

+ Support for all major Linux distributions
+ Stable. No kernel modules required.
+ Installation ease via Helm
+ Lightweight. One agent per k8s node. Auto scales as workloads grow and shrink.
+ ONE console for multi-tenant management and RBAC
+ Clear tagging of K8s attributes: Clusters, Namespaces, Controllers, Pods, Containers and Container Images

Container Prevention

+ On-agent intelligence means no cloud latency impact on protection
+ On-agent Static AI blocks & quarantines malware in real time in ELF, Windows and Mach-O binaries
+ On-agent Behavioral AI stops previously unknown fileless threats in real time
+ On demand disk scan
+ Application Control

Container ActiveEDR®

+ Storyline™ automatic PID tree context creation and re-linking
+ Storyline Threat Hunting
+ Storyline Active Response automation
+ 14 - 365+ days EDR data retention options
+ MITRE ATT&CK technique integration
+ Integrity Monitoring

Container Response

+ Secure remote shell
+ Node firewall control
+ Network isolation
+ File fetch

Storyline™ Makes SentinelOne a Better Choice

SentinelOne pioneered Storyline technology to reduce threat dwell time and to make EDR searching and hunting operations far easier. Storyline automatically correlates all software operations in real time at the endpoint and builds actionable context on the fly for every linked process across all process trees every millisecond of every day. Automated responses are triggered on-agent in real time, via Storyline Active Response (STAR™), our XDR cloud engine, or manually by analysts.

For endpoint protection (EPP), Static and Behavioral AI engines continually examine thousands of concurrent OS stories and seek out-of-bounds files and processes warranting immediate protective responses. For endpoint detection & response (EDR), Sentinels do the correlation heavy lifting to save the analyst time and headache. Storyline context of both malicious and benign data is maintained during long term storage (14 to 365+ days) within the Singularity platform so that it is available instantly when the analyst needs it.

Never build another PID tree again. We do it for you.

CLOUD-NATIVE DIFFERENTIATION

The Kubernetes Sentinel for containerized workloads offers more real time prevention, detection, response, and visibility features than any other vendor.

KUBERNETES SENTINEL SUPPORTS THESE LINUX DISTROS

- RHEL
- CentOS
- Ubuntu
- Oracle
- Amazon
- SLES Worker Nodes
- Fedora
- Debian
- Virtuozzo
- Scientific Linux

READY FOR A DEMO?

Visit the SentinelOne website for more details.

Kubernetes Sentinel Supports These Running Environments

KUBERNETES SELF-MANAGED

AWS EKS

MICROSOFT AZURE AKS

GOOGLE CLOUD PLATFORM GKE

RED HAT OPENSHIFT

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9

97% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP

ISO 27001 CERTIFIED by schellman

VB 100 VIRUS virusbtn.com

TEVORA PCI DSS Attestation HIPAA Attestation

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733