SentinelOne

DATA SHEET

# Singularity™ Cloud

## Kubernetes Workload Detection & Response

**Kubernetes is the de facto standard for container orchestration.** While good practice, image scanning alone is insufficient as it fails to protect workloads from runtime threats. A cloud defense-in-depth strategy which includes EDR is recommended.

Kubernetes Workload Detection & Response, part of the Singularity Cloud family, defends containerized workloads running in Kubernetes clusters from runtime threats such as zero-day attacks and fileless malware. A single, no-sidecar agent protects the K8s worker, all its pods, and all their containers, for maximum resource efficiency. Persistent, correlated EDR telemetry with cloud metadata delivers forensic visibility into ephemeral workloads to fuel analytics, response, and threat hunting.

### Operational Efficiency

Easy to deploy, manage, and update agents in an automated fashion that fits into existing DevOps provisioning and configuration management practices.

### EDR Visibility with K8s Context

Correlated event telemetry that is mapped to MITRE ATT&CK TTPs and which includes K8s metadata such as pod name, image ID, and much more.

### Convenient Customer Experience

Manage security of containerized microservices from the same SentinelOne console you already use to manage user endpoints, servers, VMs, and more.

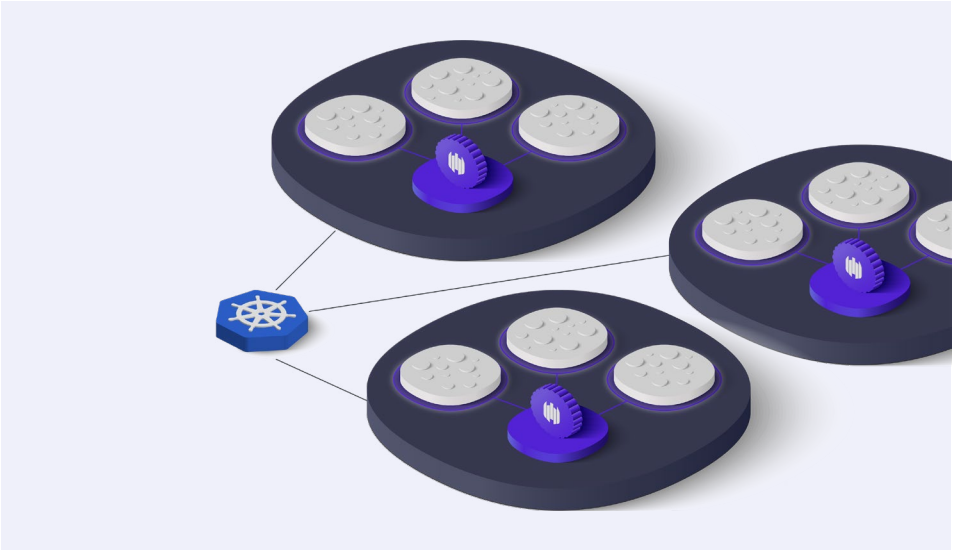
With support for 13 leading Linux distributions and both managed and self-managed Kubernetes services across AWS, Azure, and Google Cloud, SentinelOne delivers leading EDR performance to a wide array of K8s deployments.

kubernetes aws Azure docker Google Cloud

**94%** of organizations have experienced at least one Kubernetes security incident in the last year. Kubernetes Workload Detection & Response from SentinelOne can reduce that risk.

## KEY FEATURES & BENEFITS

+ Automated deployment as DaemonSet
+ Auto-scaling protection
+ Runtime EDR
+ User space agent for maximum stability
+ Supports managed K8s services from AWS, Azure, and Google Cloud
+ Supports 13 leading Linux distributions
+ Integrated metadata simplifies cloud ops

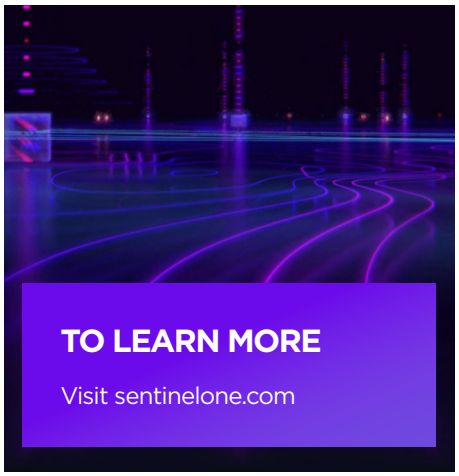


## SUPPORTED LINUX DISTRIBUTIONS

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

# The Last Line in Defense-In-Depth

Runtime threat detection and response is your backstop in a robust, multi-layered cloud security strategy, to protect against threats such as crypto mining malware loaded at runtime and zero-day threats like log4j. With Linux increasingly targeted by threat actors (eg., DarkRadiation), extensive data retention options and integrated K8s metadata from SentinelOne equips your SOC with the forensic visibility needed for threat hunts.



## TO LEARN MORE

Visit sentinelone.com

# Agile and Secure

### Supported Platforms

+ AWS EKS, EKS-Anywhere
+ Azure AKS
+ Google GKE
+ OpenShift
+ Docker, containerd, cri-o runtimes
+ K8s v1.13 or later

### DevOps Friendly

+ IaC automation via HELM charts
+ Update host OS image without kernel dependency hassles
+ Security that doesn't get in the way

### Powerful SecOps

+ EDR visibility for ephemeral workloads
+ Custom automated response actions
+ Maximum stability, uncompromising performance

## Innovative. Trusted. Recognized.

Gartner

**A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms**

MITRE ENGENUITY

**Record Breaking ATT&CK Evaluation**

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights 4.9

**99% of Gartner Peer Insights™**

EDR Reviewers Recommend SentinelOne Singularity

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

**About SentinelOne**

SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity XDR platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

**sentinelone.com**

sales@sentinelone.com
+ 1 855 868 3733