SentinelOne

Singularity™ Cloud

Cloud Workload Security for Containers

Containers are popular because they are easy to build, test, and run across a wide range of infrastructure (public and private clouds, dev laptops), container runtimes (Docker, containerd, cri-o), and with or without orchestration (e.g., Kubernetes). This flexibility can complicate security operations and attract threat actors.

Singularity Cloud Workload Security for Containers is real-time CWPP that protects containerized workloads from runtime threats like ransomware, zero-days, and more. With or without orchestration, SentinelOne delivers AI-powered threat detection and machine-speed response to defend containerized workloads across AWS, Azure, Google Cloud, and private data centers. A forensic history of workload telemetry recorded to our Singularity Data Lake provides security analysts the visibility needed to investigate incidents, slash response time, and inform threat hunting.

Workload Detection and Response

Real-time detection of machine speed attacks. Automated recovery, for maximum workload availability..

Hunting and Forensics

Accelerate investigations and IR, power threat hunts. Workload Flight Data Recorder™.

Stability and Performance

Accelerate innovation with runtime security that does not get in the way. No kernel dependencies. Low CPU and memory overhead.

96%

of developers use AI coding tools

Key Features And Benefits

+ eBPF architecture, for stability & performance
+ Supports Docker, containerd, cri-o runtimes
+ Auto-scaling protection
+ Real-time CWPP
+ Supports self-managed and managed K8s services
+ Supports 14 leading Linux distributions including Amazon Linux 2023
+ Integration with Snyk (purchased separately)

With support for 14 major Linux distributions, 3 container runtimes, and both managed and self-managed Kubernetes services from AWS, Azure, and Google Cloud, SentinelOne delivers real-time protection to a wide array of containerized workloads, on-prem or in public cloud.

kubernetes aws Google Cloud docker

aws PARTNER

- Public Sector
- Security Software Competency

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 first and last line of defense in a robust, multi-layered cloud security strategy, to protect against threats such as container escapes, ransomware, 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 IR and threat hunting.

Agile and Secure

Supported Platforms

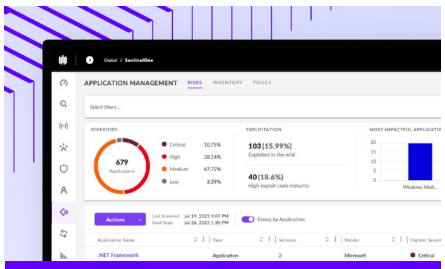
+ Amazon EKS, ECS
+ Azure AKS
+ Google GKE
+ Docker, containerd, cri-io runtimes
+ K8s, OpenShift

DevOps Friendly

+ IaC automation
+ No kernel modules or dependency hassles
+ Integrates with Snyk to help prioritize and fix vulnerabilities

Powerful SecOps

+ Forensic visibility for ephemeral workloads
+ Real-time threat detection
+ Customized auto-response actions



Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · Virus 100 · SE Labs Best Innovator Winner 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com
sales@sentinelone.com
+1 855 868 3733