SentinelOne

SECURING LINUX

Protection & Visibility Across Cloud-Native Workloads

Linux Security Issues

Up until now, Linux security practices have typically included scanning for vulnerabilities and OS/app hardening, but this approach by itself does not cover 0-day risk scenarios. Sometimes EPP & EDR protection products are added though they are often kernel-reliant, do not have a complete feature set, do not accommodate all deployment variations (physical, virtual, containers), are often too reliant on humans to identify attacks, and are too bloated.

SentinelOne Linux Solutions

The SentinelOne Cloud Workload Protection Platform (CWPP) compatible Linux agent is designed to evaluate attacks locally and at machine speed so that adversaries can be identified and expelled in real time. Our SaaS managed agent feature set is broad and integrates security measures like static AI file analysis, behavioral analysis of code execution, EDR artifact collection, and multiple real time protective response mechanisms. SentinelOne supports physical or virtual machines, self-managed Kubernetes, and cloud service provider managed Kubernetes like AWS EKS. SentinelOne provides all this without treading on kernel space and without major impact on CPU and memory.

Cloud Workload Features

SentinelOne Linux CWPP supports Docker, Kubernetes, or AWS EKS dynamic container workload monitoring in these ways:

- Protects containers but does not interfere with them. Protects against container escape.
- One agent per Kubernetes node to reduce the number of managed agents and overhead imposed by the agent.
- Automatically scales as pods and containers are added to the cluster to eliminate AV storms.
- Understand exactly which implementation has been affected or where an EDR historical data search gets a hit. Clear tagging of affected systems using Namespace, Pod, Kubernetes labels, container IDs and image.

[1] Azure AKS, Google GKE, RHEL OpenShift coming soon

Linux Features

Protection

- Static AI Engine, Full Disk Scan
- Dynamic Behavioral AI Storyline Analysis
- Reputation Engine
- Kill, Quarantine

Active Detect & Respond

- Historical EDR Data - Process Events, File Events, Network TCP Events
- Network Isolation
- On Demand File Fetch

Augmentation

- Firewall Control
- Application Inventory
- Bidirectional RESTful API

Container Support

Docker

Kubernetes self-managed

AWS Kubernetes (EKS)

Azure AKS, Google GKE, RHEL

OpenShift coming soon...

Distributions Support

- Ubuntu 14.04, 16.04, 18.04, 19.04
- RHEL/CentOS 6.4+, 7.x, 8.x
- Oracle 6.9, 6.10 (Kernel >3.x), 7.x
- Amazon Linux 2, 2017.03, 2018.03
- HP ThinClient Pro 6.2, 7.1
- Debian 8, 9, 10
- Fedora 25-30
- SLES 12, 15

SentinelOne Differentiators	Significance
Support for dynamic container workloads, physical or virtual machines. Kubernetes aware management information.	Implementation flexibility. Understand affected namespaces, pods, container IDs and more.
Modern SaaS Linux agent management	Not kernel reliant. Load, unload, and update agents without system disruption. Spawn protection on new pods and containers without administrator intervention.
Cloud delivered real time protection and detection • Prevention using patented, local predictive AI models. On write or via disk scan. • Dynamic detection using patented, behavioral AI models	On agent logic reduces attacker dwell time • On agent logic identifies malicious and atypical files including ELF, Windows binaries, PDF, MS Office OLE/XML, and archive file formats • Real time control of run-time environment
Mitigations including kill, quarantine. Protective controls including disconnect device, firewall micro segmentation.	Kill suspicious and threatening processes and let Kubernetes re-spawn them. Augment VPC and Kubernetes namespace segmentation controls to a finer level.
Contextualized 90-day historical EDR data access	SentinelOne Deep Visibility™ with TrueContext™ reveals an entire PID tree relationships in one pivot for easy forensics & hunting
Built-in File Integrity Monitoring (FIM)	Monitor file create, modify, and delete to meet PCI-DSS and other regulatory compliance requirements
Application Inventory	Understand what is installed. Vulnerability scoring coming in 2020.
Bidirectional RESTful API	Pull and push data programmatically via your other tools

About SentinelOne

SentinelOne (www.sentinelone.com), founded in 2013 and headquartered in Mountain View, California, is a cybersecurity software company. Our mission: Defeating every attack every moment of every day. SentinelOne Singularity is one platform to prevent, detect, respond, and hunt in the context of all enterprise assets. See what has never been seen before. Control the unknown.

Real time endpoint protection Active detection & response Cloud delivered IoT discovery & control Native cloud security.

SentinelOne™

www.SentinelOne.com | Sales@SentinelOne.com
+1-855-868-3733 | 605 Fairchild Dr, Mountain View, CA 94043