

Linux Sentinel Agent

A component of SentinelOne Cloud Workload Security

Achieve runtime security and EDR for Linux servers without sacrificing stability.

Security teams require protection, detection, response, visibility, and threat hunting across all OSes. Linux is no exception. Unlike legacy AV and first-generation EDR, SentinelOne offers the advanced security features the SOC needs to protect Linux across multiple clouds via one simple SaaS solution built for performance and automation.

Linux Sentinel agents are designed to run on physical or virtual machines in your data center or at AWS, Azure and Google Cloud. Linux Sentinels are the security enforcement point and are managed within the same multi-tenant console alongside other Sentinels for Windows, macOS, and Kubernetes.

Administration is flexible, distributed, and managed via role-based access controls that match your organization's structure. Linux Sentinel offers compatibility and ongoing support for many popular Linux families without the risk of kernel module instability.

LINUX SENTINEL DIFFERENTIATORS

- A wide array of supported Linux families
- Operational stability. No kernel modules.
- Real time prevention for file-based and fileless attacks
- Full EDR visibility + massive data retention
- Deep response capabilities

RUNNING CLOUD-NATIVE CONTAINERIZED WORKLOADS?

We also offer Kubernetes Sentinel differentiated by runtime protection, EDR capabilities, and unique container focused solutions.



LINUX SENTINEL FEATURES

Operations

- + Support for all major Linux distros
- + Stability. No kernel modules required.
- + Installation ease across physical, virtual, and cloud service providers
- + ONE console for multi-tenant management and RBAC
- + Application inventory

Prevention

- + On-agent intelligence means no cloud delay 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
- + AppCtrl for containerized workloads
- + AppCtrl for Cloud VMs (Coming Soon)

Enterprise-grade ActiveEDR™

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

Response capabilities

- + Secure remote shell
- + 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.**

Linux Sentinel supports these running environments



PHYSICAL
OR VIRTUAL



AWS EC2



MICROSOFT AZURE



GOOGLE CLOUD
PLATFORM

Just because it is a Linux agent does not mean it lacks features. Linux Sentinels offer the features the SOC needs for Linux prevention, detection, response, and visibility.

LINUX SENTINEL SUPPORTS DESKTOPS AND SERVERS FOR MANY DISTRIBUTIONS AND CAN BE OPERATIONALIZED VIA ANSIBLE, CHEF, PUPPET, AND AZURE VM EXTENSIONS:

- **Ubuntu** 14.04, 16.04, 18.04, 19.04, 19.10, 20.04
- **RHEL** 6.4+, 7.1-7.9, 8.0-8.3
- **CentOS** 6.4+, 7.1-7.8, 8.0-8.2
- **Oracle** 6.9, 6.10, 7.7, 8.0-8.2
- **Amazon AMI 2**, 2017.03, 2018.03
- **SUSE Linux Enterprise Server** 12.x, 15.x
- **Fedora** 25-30, 31 kernel 5.5.x+, 32
- **Debian** 8, 9, 10
- **Virtuozzo** 7
- **Scientific Linux** 6, 7

ATT&CK®

2020 MITRE ATT&CK

- Fewest Misses
- Most Correlations
- Best Data Enrichment Coverage

FORRESTER®

2020 FORRESTER
WAVE™ EDR

"Strong Performer"

kuppingercole
ANALYSTS

2020 KUPPINGERCOLE
MARKET COMPASS

Featured EPDR Innovator

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.



97 %

Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97 %

Customer Satisfaction (CSAT)



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?