SentinelOne CDW

DATA SHEET

Singularity™ Cloud

Server/VM Workload Detection & Response

Your hybrid cloud business is complex, workload protection, detection, and response shouldn't be. SentinelOne offers the uncompromising EDR performance the SOC needs to protect Linux and Windows Server VMs running across AWS, Azure, Google Cloud, and your data center.

Server/VM Workload Detection & Response, part of the Singularity Cloud family, defends workloads running in virtual cloud instances and physical servers from runtime threats such as zero-day attacks and fileless malware. 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 Hybrid Cloud Context

Correlated event telemetry that is mapped to MITRE ATT&CK TTPs and includes metadata such as Account and Instance IDs, custom tags, and more.

Powerful Security Automation

High-powered yet intuitive, automation capabilities compress detection and response times, to meet the needs of every SOC team member, from entry-level analyst to sophisticated threat hunter.

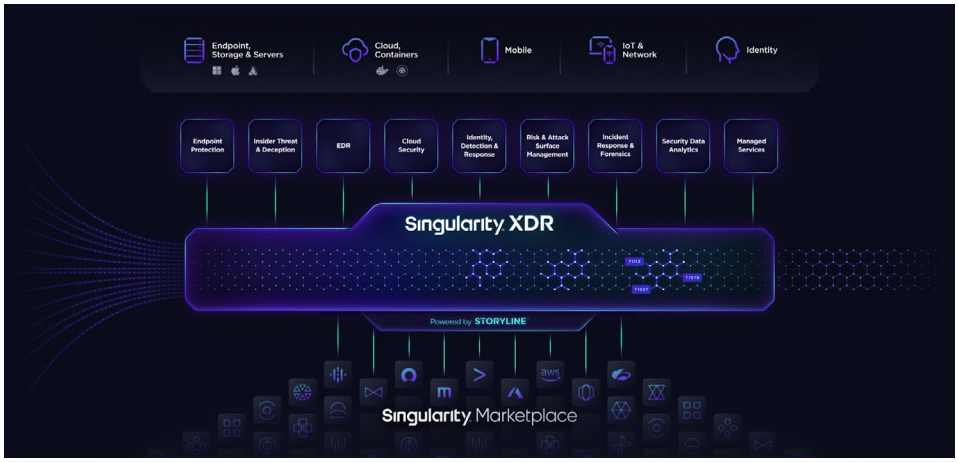
In addition to unmatched EDR performance in MITRE ATT&CK emulations, SentinelOne provides unique capabilities such as Storyline™ to automate attack visualization and accelerate incident triage.

aws Azure docker Google Cloud

146% YoY increase in Linux ransomware with new code. Behavioral AI from SentinelOne can reduce that risk to your server and VM workloads.

KEY FEATURES & BENEFITS

+ Runtime EDR
+ Supports cloud instances on AWS, Azure, Google Cloud, and data center
+ Support for 12 major Linux distros
+ Windows Server version support from 2022 back to 2003 SP2
+ ONE multi-cloud management console for endpoint, server, workloads, and more
+ Preserves workload immutability
+ Integrated metadata simplifies cloud ops



Machine-Speed Response for Runtime Threats

Runtime threat detection and response is the last line of defense in a multi-layered cloud security strategy. EDR protects workloads from threats such as crypto mining malware loaded at runtime and zero-days like log4j that image scanning alone would miss. With Linux increasingly targeted by threat actors (e.g., DarkRadiation), SentinelOne equips your SOC with the capabilities to achieve more with less manual drudgery. Storyline accelerates incident triage; 1-click and automated custom response actions amplify SOC productivity; and extensive data retention options, remote shell, remote script orchestration, and intuitive management console fuel threat hunts.

Agile and Secure

Supported Platforms

+ AWS EC2
+ Azure VM
+ Google Compute Engine

DevOps Friendly

+ IaC automation via VM bootstrap
+ Update Linux OS image with no kernel dependency hassles
+ Security that doesn't get in the way

Powerful SecOps

+ EDR visibility and forensics
+ Storyline automated context accelerates triage
+ 1-click remediation, Rollback (Windows)
+ Custom automated response actions
+ Threat hunting

SUPPORTED LINUX DISTRIBUTIONS

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

WINDOWS SERVER SUPPORT

+ 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1
+ Windows Server Core 2019, 2016, 2012
+ Windows Storage Server 2016, 2012 R2, 2012
+ Legacy Windows Server 2008, 2003 SP2+, 2003 R2 SP2+

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 · AV-Comparatives · 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

CDW
www.cdw.com
866.782.4239