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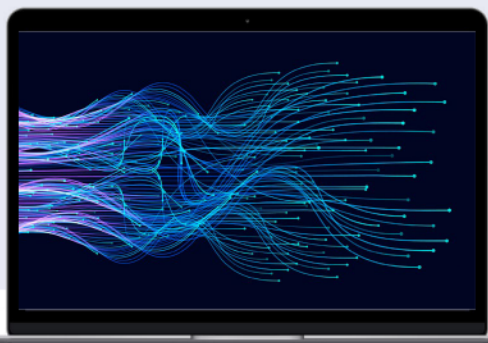
In addition to unmatched EDR performance in MITRE ATT&CK emulations, SentinelOne provides unique capabilities such as Storyline™ to automate attack visualization and accelerate incident triage.

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