SentinelOne | aws

SOLUTION BRIEF

SentinelOne Singularity Cloud Workload Security for Amazon Web Services

Real-Time Protection, Detection, and Response for AWS Cloud Workloads

SentinelOne: Securing Workloads on AWS with SentinelOne

The speed, sophistication and scale of cyber threats have evolved. When attackers pierce prevention measures, detection and response must happen autonomously, in real time. Cloud-specific metadata and telemetry are required to help businesses map threat vectors, attack paths, and decrease overall time to recovery.

Singularity Cloud Workload Security, SentinelOne's cloud workload protection (CWPP) solution, provides runtime protection and OS-level visibility for workloads running on Amazon EC2, ECS, and EKS, as well as VMs, containers, and Kubernetes clusters in a private cloud or on-prem data center. With support for 13 major Linux distributions, the cloud-native CWPP agent is built upon the eBPF framework and operates entirely in user space for maximum operational stability and agility - no kernel dependency hassles, and no kernel panics. SentinelOne delivers both real-time detection and automated response to protect you against machine speed attacks on your hybrid cloud workloads.

AWS Services Supported, and Key Integrations

- Amazon Elastic Compute Cloud (EC2) - including AWS Graviton and Amazon Linux 2022
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
- Amazon Elastic Kubernetes Service Anywhere (EKS-A)
- Amazon Elastic Container Service Anywhere (ECS-A)
- AWS Security Hub
- AWS Disaster Recovery
- AWS Backup
- Amazon Security Lake
- ... and more

KEY BENEFITS

- **Real-Time Cloud Workload Protection**
- **Deployment in Minutes**
- **Built-in Static and Behavioral AI Engines**
- **Streamlined Threat Hunting**
- **Hybrid Cloud Friendly**
- **Integration with AWS Services**

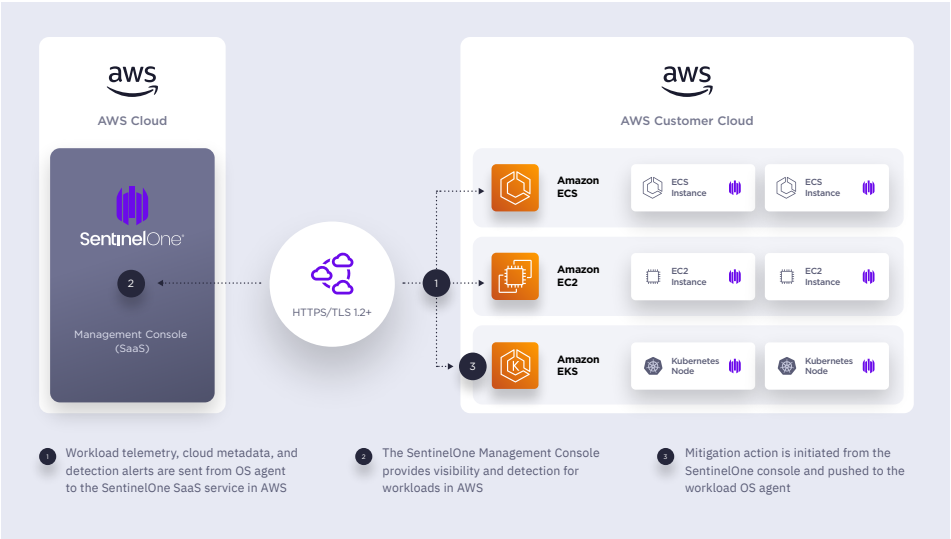
aws PARTNER

- Public Sector
- Amazon Linux Ready
- AWS Graviton Ready
- Security Software Competency
- Containers Software Competency

Key Benefits

01 | Workload resilience and integrity for Amazon EC2 and Containers

Singularity Cloud Workload Security delivers full-featured cloud workload protection directly to your AWS workloads. Gain the power of multiple detection engines in one lightweight and stable agent, including Static AI, Behavioral AI, and Application Control Engines. Real-time workload defense at runtime, with protection from, and detection of, ransomware, zero-day exploits, cryptomining, memory injection, and more. Protect your mission-critical workloads regardless of age or OS. Broad OS support including 13 Linux distributions including Amazon Linux 2022, 20 years of Windows Server, and support for the popular container runtimes Docker, containerd, and cri-o.



02 | DevOps Friendly: Quick time to protection with minimal overhead

Built using the eBPF framework, with minimal impact on compute and no impact to kernels, Singularity Cloud Workload Security is simple to deploy and manage, and prioritizes your resource efficiency along with security.

Auto-deployed as a DaemonSet, a single, resource-efficient Kubernetes CWPP agent protects the K8s worker, all its pods, and all their containers without any container instrumentation to gum up the works. Plus, our agent operates entirely in user space: no tainted kernels, no kernel panics, and no messy kernel dependencies.

03 | Enhanced visibility and threat hunting

Accelerate investigations and incident response with unmatched runtime telemetry. You'll gain forensic visibility even for ephemeral workloads. Singularity Cloud will act as your Workload Flight Data Recorder™, with Skylight™ providing forensic visibility and Storyline™ auto-correlating, enriching, & visualizing the attack.

CASE STUDY

LARGE NORTH AMERICAN INFORMATION SERVICE PROVIDER

CHALLENGES

+ The information service provider had hundreds of Linux servers, Amazon EC2 and Amazon EKS instances in production. They were struggling with cloud compliance challenges and gaps in workload protection after an incident triggered a compliance audit.

SOLUTION

+ Deploying the SentinelOne Linux agent to resources running in EC2, and the SentinelOne Kubernetes agent to workloads in EKS, protecting thousands of AWS workloads within a few hours.

RESULTS

+ Gained visibility and control over their AWS workloads, providing superior protection against ransomware and malware. Automated detection and response frees security resources. Automated deployment protects new resources, and DevOps can update AMIs without worrying about kernel conflicts.

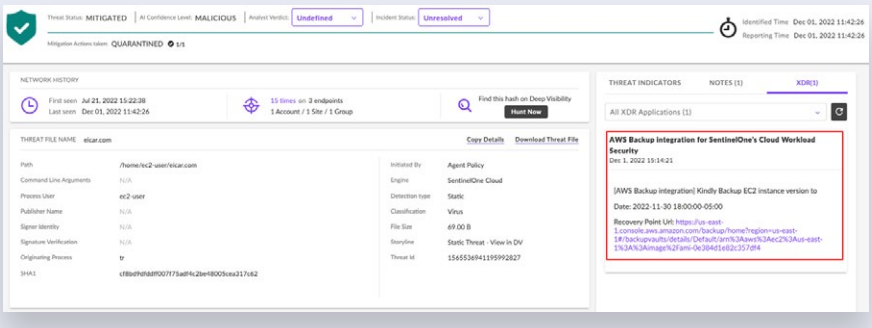
Optimized for AWS

Hosted in multiple AWS regions around the world including GovCloud, Singularity Cloud Workload Security is optimized for AWS users. With a shared focus on customer excellence and security in the cloud, SentinelOne jointly innovates with AWS on new services, offerings, and integrations to help customers innovate quickly and securely on AWS.

Key Integrations

Singularity Cloud Workload Security has security-focused integrations including:

1. **AWS Backup and AWS Elastic Disaster Recovery Service** to support customers in business continuity and incident response.
2. **AWS Security Hub** to provide high-fidelity threat information from SentinelOne agents running on AWS workloads to AWS Security Hub.
3. **Amazon Security Lake** to ingest customer logs into the Singularity Platform for threat hunting, forensics, and to help investigate and establish root causes of security alerts.



SentinelOne Integration with AWS Backup: Helping Customers Recover Quickly

Singularity Cloud Workload Security, as well as other SentinelOne solutions, including our market-leading Endpoint Detection and Response, are available for purchase and fulfillment through AWS Marketplace, making it easier than ever to get started with leading cloud workload workload protection.

Available in
AWS Marketplace

GET STARTED WITH SENTINELONE SOLUTIONS ON AWS

Visit **AWS Marketplace** or **s1.ai/AWS** to request a demo.

SentinelOne®

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 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 Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne (NYSE:S) 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 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