SentinelOne for AWS

Protection, Detection, and Response for Endpoints and AWS Cloud Workloads

Why SentinelOne?

- **Built-in Static and Behavioral AI**
  Prevent and detect threats at machine speed, delivering high-quality detections without human intervention.
- **In-Depth Visibility**
  Monitor all concurrent OS processes, malicious or benign, in real time across all major OSes and cloud workloads with Storyline technology
- **Cloud Workload Security**
  Deliver enterprise-grade protection and EDR directly to Amazon EC2, EKS, and ECS. Application Control preserves workload immutability - NO allow-lists to maintain or ML training
- **Cloud Metadata Integration**
  Review VM and Kubernetes metadata tags right within the SentinelOne console. Group instances by tags, apply security policies by groups, and more.
- **Streamlined Threat Hunting**
  Simplify queries of EDR telemetry with Deep Visibility™. Build your own hunting queries or use our hunt pack library
- **Get Users Back in Business Fast**
  Recover user endpoints in moments without re-imaging or writing scripts, surgically unwinding unauthorized changes in just 1 click.

Product overview

The speed, sophistication, and scale of threats have evolved, leaving first generation prevention and EDR solutions behind. When attackers pierce prevention measures, endpoint detection and response needs to happen autonomously, in real-time across endpoints, cloud workloads and IoT.

Product features

Storyline: Connects the dots automatically

Every millisecond of every day, Storyline observes all concurrent processes within all major OSes and cloud workloads, connects the dots, and builds context. Distributed intelligence watches each Storyline to drive instantaneous protection against advanced attacks.

Each Storyline is preserved in AWS cloud storage to fuel EDR activity. Plus, 1-click recovery and response surgically unwinds unauthorized changes to get your organization back in business with minimal fuss

Enterprise-grade EDR for VMs and Containers

Singularity Cloud delivers full-featured EDR directly to your AWS workloads. Pivot and hunt from an attack Storyline by MITRE ATT&CK® technique.

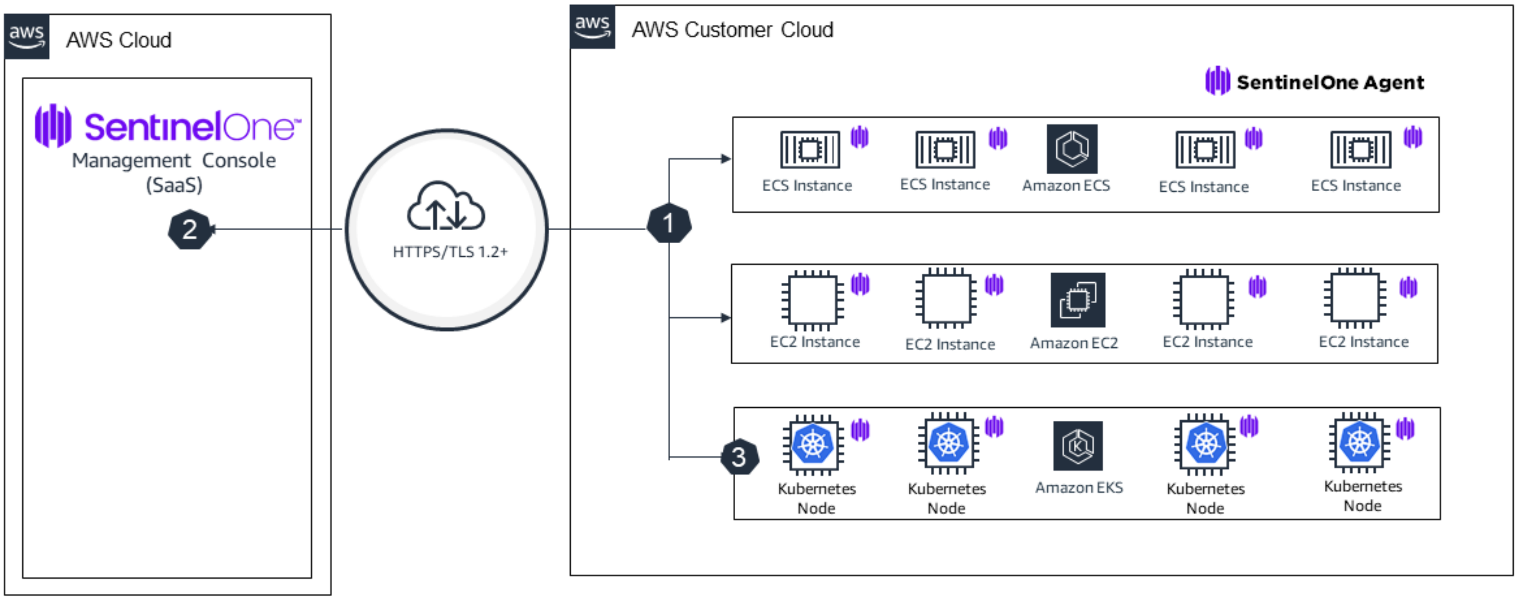
Query endpoint telemetry securely stored in the SentinelOne Cloud built upon AWS with industry-leading historical EDR data retention options. Mark findings as threats and resolve with one click. Leverage a single API with 350+ functions provides a basis for further automation.

DevOps Friendly

Auto-deployed as a DaemonSet, a single, resource-efficient Kubernetes Sentinel agent protects the K8s worker, its pods, and 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 freedom to update your AMI at will without fear of conflicting with the Sentinel agent.

How it works

Singularity Cloud, an optional add-on to Singularity Complete, extends security and visibility to assets running in public clouds, private clouds, and on-premises data centers. Security teams can manage both Linux and Windows servers in Amazon EC2 and Docker & Kubernetes containers from the same console where they manage user endpoints. A single featherweight Sentinel agent delivers autonomous runtime protection, detection, and response at machine speed across the hybrid cloud estate. The Kubernetes Sentinel brings ActiveEDR® to Amazon EKS and Amazon ECS, with automated kill and quarantine, Application Control, and cloud metadata integration.



1. Workload telemetry, Cloud metadata, and detection alerts are sent from OS agent to the SentinelOne SaaS service
2. The SentinelOne Management Console provides C2, analysis and visibility
3. Mitigation action is initiated from the SentinelOne console and pushed to the workload OS agent

Differentiators

- One product for consolidated, autonomous protection - prevention, detection, remediation and hunting
- Patented 1-Click Remediation & Rollback
- Powerful Threat Hunting platform with full context and flexible data retention (14 days - 1 year)
- MITRE Engenuity ATT&CK 2020: 100% visibility and zero missed detections
- Coverage for Windows/Mac/Linux as well as cloud and container workloads
- Single cloud-delivered platform with true multi-tenant capabilities to address the needs of global enterprises and MSSPs
- Frictionless Ecosystem Integration

What our customers are saying

> *SentinelOne has changed the way we do cybersecurity.*
> **- Tony Tuffe, IT Support Specialist, Norwegian Airlines**

Data Points

353%
Return on Investment

3
Month Payback

97%
Customer Satisfaction

4.9
Rating on Gartner Peer Insights

Additional Resources

- [Total Economic Impact of SentinelOne]
- [Singularity Complete]
- [Singularity Cloud Workload Security]
- [Gartner Peer Insights]
- [MITRE Engenuity ATT&CK 2020]

SentinelOne Singularity Key Capabilities

Additional information about SentinelOne Singularity can be found here.

Endpoint Protection & Control	✓
Endpoint Detection and Response (EDR)	✓
Cloud Workload Security	+
Network Attack Surface Management	+

Solution available in AWS Marketplace