SentinelOne

DATA SHEET

Cloud Workload Security

EPP+EDR for Cloud VMs and Containers

Whether running in public cloud or private cloud, on servers or in containers, organizations of all sizes are looking for means of securing their cloud workloads in a manner that preserves agility.

Dozens if not hundreds of accounts, spread across multiple clouds. Developers updating containerized microservices daily, even hourly. And so many VMs. Your multi-cloud footprint is always changing. No wonder security is often the #1 concern when using cloud infra-structure. The speed and scale of change is a double-edged sword. SentinelOne can help.

SentinelOne Cloud Workload Security extends distributed, autonomous endpoint protection, detection, and response to compute workloads running in public clouds, private clouds, and on-prem data centers. With SentinelOne, security teams can manage Linux and Windows servers, Docker containers and Kubernetes clusters, all from the same multi-cloud, multi-tenant Singularity™ Platform over 4,000 customers use to manage user endpoints.

Your hybrid cloud business is complex. Cloud workload protection shouldn't be.

AUTONOMOUS CWS

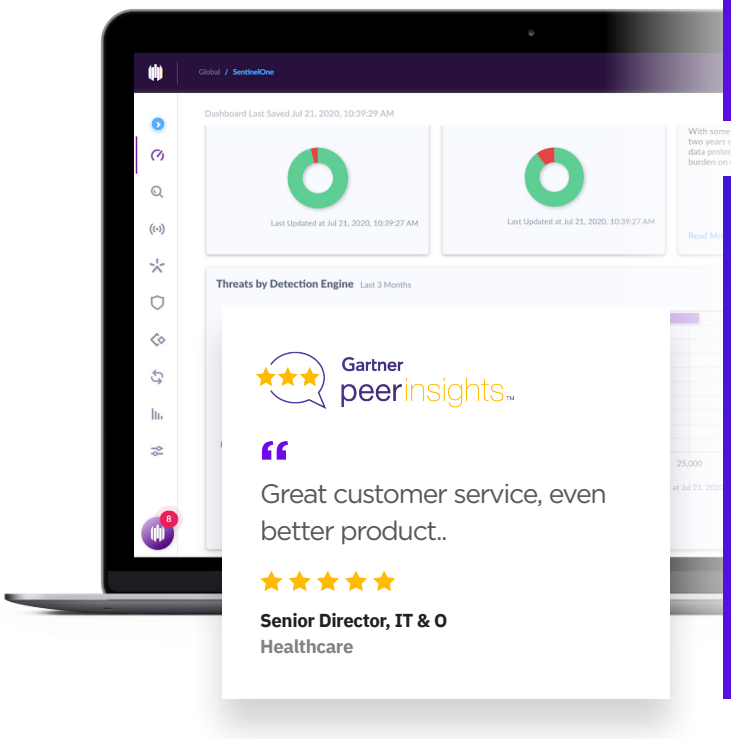
EPP + EDR for cloud VMs and containers

KEY FEATURES

+ Cloud VM security (Linux, Windows)
+ Runtime container security for EKS, AKS, GKE, and self-managed K8s
+ App Control for containers (K8s, Linux)
+ App Control for VMs (COMING SOON)
+ ONE multi-cloud, multi-tenant console

BENEFITS

+ Multi-cloud visibility
+ Autonomous real-time EPP+EDR at the cloud VM
+ Runtime protection for Docker & Kubernetes
+ Reduced MTTR
+ Accelerated IR
+ Less alert fatigue



Key Capabilities

- **Autonomous, real-time** detection and remediation of complex threats at the VM and K8s pod level with no need for human intervention.
- **Runtime protection** of containerized workloads that identifies and kills unauthorized processes such as malware, cryptojacking, and more. Contextualized EDR telemetry with key container details such as cluster, node, pod, and image name and container ID.
- **Enterprise-grade EPP+EDR** proven across thousands of customers worldwide to thwart malware, accelerate response, and transform hunting.
- **Complete forensics** into any VM or K8s pod via fully capable remote shell.
- **Resource-efficient Kubernetes agents** deployed 1 per worker node, with runtime protection for every pod in the node without any extra instrumentation.
- **Accelerated incident response** (IR) with automated event correlation into Storylines mapped to MITRE ATT&CK techniques.
- **Multi-cloud, multi-tenant** SentinelOne console streamlines hybrid and multi-cloud administration.
- **1-Click Remediation & Rollback** simplifies response and slashes MTTR (Mean Time to Repair).

Gartner peerinsights™

"Wow... get S1 now, or just be 1 year older when you do.

★★★★★

Cloud DevOps I&O
MISC, 1B - 3B USD

Gartner peerinsights™

"Easy and effective EPP+EDR in one.

★★★★★

Security Analyst
MANUFACTURING, 3B - 10B USD

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights™ 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS · TEVORA PCI DSS Attestation HIPAA Attestation

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?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

SentinelOne

DATA SHEET

Singularity | RANGER

Cloud-Delivered Network Visibility & Control

The proliferation of IoT use in business, open BYOD policies, and a global remote workforce exponentially increases the quantity of unmanaged IP-enabled devices directly neighboring enterprise infrastructure. One compromised printer can become an adversary's home base for reconnaissance, lateral movement, and a breach.

SentinelOne addresses this risk with Ranger, an integral component of our Singularity XDR Platform that turns endpoint Sentinel agents into distributed network sensors. Sentinel Rangers enable control of the enterprise network attack surface in real time by discovering, identifying, and containing any device-based threat. Your endpoints can now autonomously protect compute infrastructure from IoT attacks, compromised devices, and vulnerabilities. No hardware. No network changes. Simply enable Ranger in the endpoint policy and the Sentinel agents get it done.

Key Benefits

- Global networked device inventory
- Detect & alert on new devices
- Isolate device-based threats
- Hunt suspicious device activity
- Quantify exposure to Ripple20
- Proactive attack surface management

Challenging Problem. Minimal Friction Solution.

Singularity Ranger is designed to add global network visibility and control in one place with minimal friction. Ranger is part of our Sentinel agent. Just toggle it on. Ranger eliminates the need for additional specialty agents, SPAN and TAP ports, and network gear dedicated to network visibility. Plus forget about tedious manual traffic capture and upload for analysis. Ranger makes it automatic.

RANGER

Ranger is the easy button for network attack surface control

RANGER KEY DIFFERENTIATORS

+ 1-Click network visibility
+ Peer-to-peer agent deployment with Ranger Pro option
+ 1-Click control over unknown and IoT network devices
+ ML device fingerprinting via active & passive scanning
+ Highly configurable per subnet
+ No added software
+ No new hardware
+ No network changes

IT Central Station

"

Ranger gives exceptional visibility where we had none.

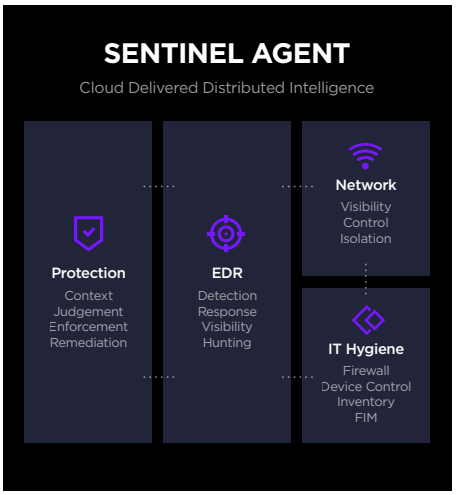
★★★★★

Security Architect
Global Services, 10B - 25B USD

Proactive Attack Surface Control

SentinelOne's Singularity Platform delivers cloud managed distributed intelligence. Our differentiated endpoint protection, endpoint detection and response, cloud workload security, and IT operations capabilities consolidate multiple existing technologies into one solution. Singularity Ranger adds network and IoT control to the mix within the same agent. Ranger is designed to address customer requirements like these:

- Monitor changes to configuration management database (CMDB) in real-time
- Investigate devices and device activity
- Pivot from a suspicious device and hunt lateral movement activity
- Isolate device-based threats with 1-Click
- Identify and close gaps in SentinelOne deployment coverage
- Close coverage gaps with Ranger Pro



Rogues™	Singularity Core	Singularity Control	Singularity Complete
Find supported user endpoints with automated network sweeps	✓	✓	✓
Find agent deployment gaps	✓	✓	✓
Singularity RANGER	**Rogues** plus the following capabilities:		
Live global asset inventory	+	+	+
Advanced ML device fingerprinting with flexible active + passive scanning	+	+	+
Isolate suspicious and malicious devices		+	+
Watch and react to suspicious device behavior with Storyline Active Response (STAR™)			+
Hunt device-based threats in Deep Visibility™			+
Singularity RANGER PRO	**Rogues** and **Ranger** plus the following capabilities:		
Close agent deployment gaps with configurable p2p job automation	+	+	+

SIMPLIFY ROLLOUT

Rogues finds your user endpoints that are missing a Sentinel agent. Ranger Pro simplifies closing those gaps, with configurable peer-to-peer agent deployment jobs to go along with all the network control capabilities that make Ranger so useful.

LEGEND	
	✓ Included
	+ Available

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights™ 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · AAA Cyber Security Ratings · ISO 27001 CERTIFIED by schellman · VB100 VIRUS virusbtn.com · AAA Cyber Security Ratings · TEVORA PCI DSS Attestation HIPAA Attestation

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?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

SentinelOne

SOLUTION BRIEF

SentinelOne Singularity XDR

The cybersecurity threat landscape is rapidly evolving and expanding. As attack vectors multiply, from endpoints to networks to the cloud, many enterprises address each vector with a best-in-class solution to protect those specific vulnerabilities. However, these point tools don't connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect. Besides, the manual investigation process can often be slow and cumbersome, causing security teams to fall behind in containing and remediating threats.

Singularity XDR

SentinelOne Singularity XDR unifies and extends detection and response capability across multiple security layers, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, automated response across the complete technology stack. With Singularity XDR, customers can get unified and proactive security measures to defend the entire technology stack, making it easier for security analysts to identify and stop attacks in progress before they impact the business.

Key Capabilities

01 | Eliminate blind spots with cross-stack visibility

Singularity XDR enables enterprises to seamlessly ingest structured, unstructured, and semi-structured data in real-time from any technology product or platform, breaking down data silos and eliminating critical blind spots. The solution empowers security teams to see data collected by disparate security solutions from all platforms, including endpoints, cloud workloads, IoT devices, networks, and more, within a single dashboard. Singularity XDR lets analysts take advantage of insights derived from aggregating event information from multiple different solutions into a single contextualized "incident". It also provides customers with a central enforcement and analytics layer point hub for complete enterprise visibility and autonomous prevention, detection, and response, helping organizations address cybersecurity challenges from a unified standpoint.

02 | Uncover stealthy attacks with cross-stack correlation

SentinelOne patented Storyline™ technology provides real-time, automated machine-built context and correlation across the enterprise security stack to transform disconnected data

SOLUTION BENEFITS

Increased SOC Efficiency and Productivity

No context switches or multiple dashboards in response minimizes delays. One platform and one workflow reduces the number of alerts, eliminates blind spots and data gaps, and reduces the number of interfaces that security must access during a response.

Rapid Time to Value

Out-of-the-box integrations across multiple different products. Enables you to maximize value from your existing cybersecurity investment rapidly.

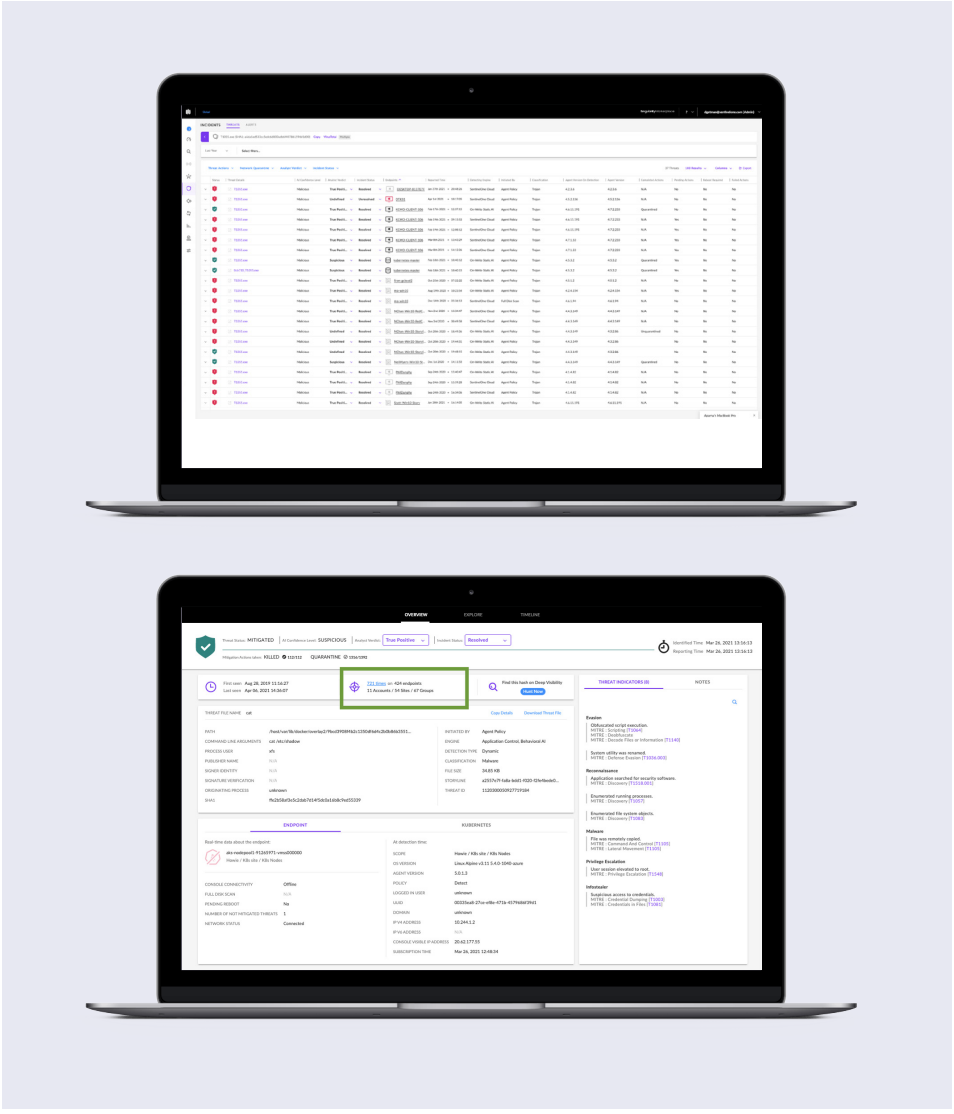
Streamlined Operations & Workflows

Achieve single-pane visibility & analysis for siloed data streams.

Reduced Total Cost of Ownership (TCO)

Reduce the costs associated with configuring and integrating multiple point solutions with a fully integrated cybersecurity platform.

into rich stories and lets security analysts understand the full story of what happened in their environment. Storyline automatically links all related events and activities together in a storyline with a unique identifier. This allows security teams to see the full context of what occurred within seconds rather than needing to spend hours, days, or weeks correlating logs and linking events manually. SentinelOne's behavioral engine tracks all system activities across your environment, including file/registry changes, service start/stop, inter-process communication, and network activity. It detects techniques and tactics that are indicators of malicious behavior to monitor stealth behavior, effectively identify fileless attacks, lateral movement, and actively executing rootkits. Singularity XDR automatically correlates related activity into unified alerts that provide campaign-level insight and allows enterprises to correlate events across different vectors to facilitate triage of alerts as a single incident.



03 | Auto-enrich threats with integrated threat intelligence

Singularity XDR integrates threat intelligence for detection and enrichment from leading 3rd party feeds and our proprietary sources that auto-enrich endpoint incidents with real-time threat intelligence. It empowers security teams to get additional contextual risk scores on Indicators of compromise (IoCs) such as IPs, hashes, vulnerabilities, and domains. For example, with our Recorded Future integration, threats are auto enriched from 800,000+ sources,

KEY INTEGRATIONS

ENDPOINT

IOT

CLOUD

THREAT INTEL

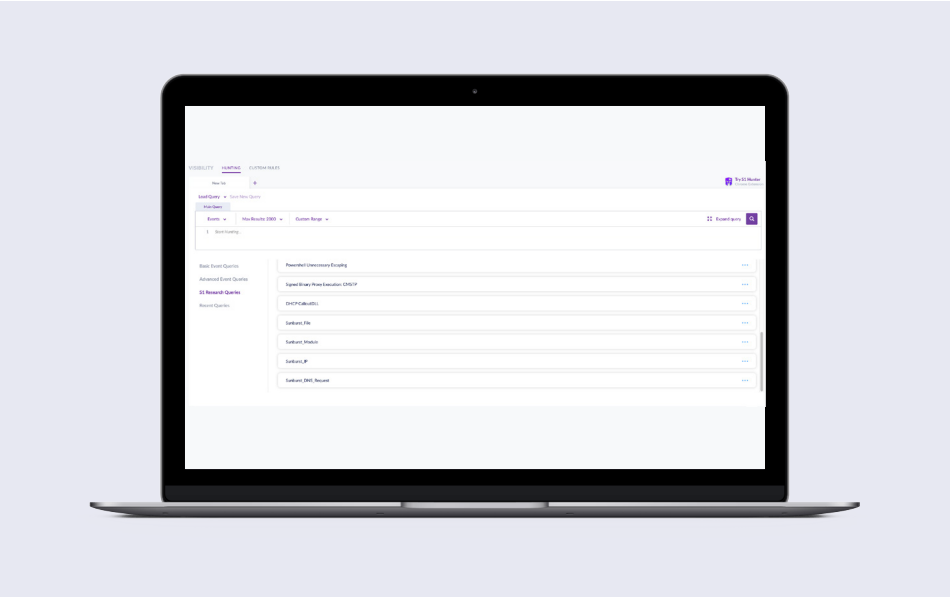
IDENTITY

EMAIL

NETWORK

SASE

enabling customers to accelerate threat investigation and triage capabilities. Customers can also leverage a query library of hunts curated by SentinelOne research which continually evaluates new methodologies to uncover new IOCs and Tactics, Techniques, and Procedures (TTPs).



04 | Automate response across different domains

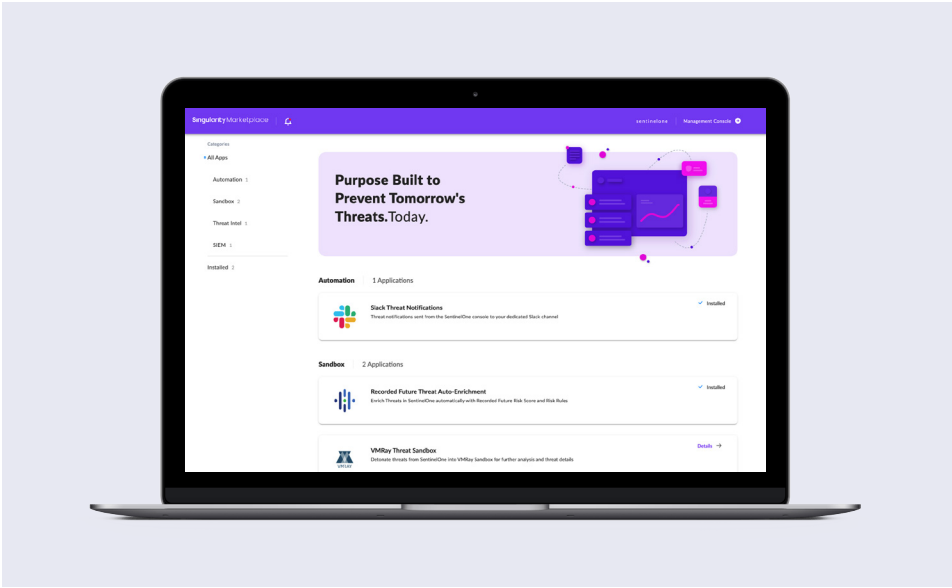
Singularity XDR enables analysts to take all the required actions to automatically resolve threats with one click, without scripting, on one, several, or all devices across the estate. With one click, the analyst can execute remediation actions such as network quarantine, auto-deploy an agent on a rogue workstation, or automate policy enforcement across cloud environments.

Singularity XDR also lets customers leverage the insights Storyline delivers to create custom automated detection rules specific to their environment with Storyline Active-Response (STAR). STAR lets enterprises incorporate their business context and customize the EDR solution to their needs. With Storyline Active-Response (STAR) custom detection rules, you can turn queries into automated hunting rules that trigger alerts and responses when rules detect matches. STAR gives you the flexibility to create custom alerts and responses specific to your environment; for example, auto-kill a process to automatically and rapidly detect and contain threats across your environment.

05 | Frictionless integration with leading SOAR tools

As you may have other security tools and technologies deployed in your SOC, SentinelOne offers a growing portfolio of integrations to third-party systems like SIEM and SOAR via Singularity Marketplace. Singularity Apps are hosted on our scalable serverless Function-as-a-Service cloud platform and joined together with API-enabled IT and Security controls with a few clicks. Singularity Marketplace is part of our platform, so once the integration is set up, the effect becomes immediately visible within the product - removing the barriers of writing complex code, making automation simple and scalable between vendors. Security teams can easily navigate the best course of action to remediate and defeat high-velocity threats by driving a unified, orchestrated response among security tools in different domains.

> “
>
> Data ingest is a major challenge for most vendors. To accommodate the volume, velocity, and variety of security data, XDR technologies must be anchored by a modern data pipeline that can collect and process security data at scale across hybrid IT.
>
> XDR technologies should also be able to provide automated machine-built context and correlation to provide the security team with automated insights across the enterprise security stack.
>
> **Dave Gruber**
>
> SR. ANALYST, ENTERPRISE STRATEGY GROUP



06 | Scale your security team and increase SOC efficiency

Singularity XDR provides a single, unified platform extended threat detection, investigation, response, and hunting with:

- Single source of prioritized alerts that ingests and standardizes data across multiple sources.
- Single consolidated view to quickly understand the progression of attacks across security layers.
- Single platform to rapidly respond and proactively hunt for threats.

SOLUTION HIGHLIGHTS

Seamlessly Ingest Data From Many Sources

Ingest structured, unstructured, and semi-structured data in real-time from any technology product or platform.

Uncover Attack Campaigns Across Your Enterprise Stack

Gain real-time, automated machine-built context and correlation across the enterprise security stack to transform disparate data into rich stories.

Quickly Contain Attacks With Actionable, Automated Response

Resolve threats automatically, with 1-click—without scripting on one, several, or all devices across the enterprise.

Accelerate Investigation & Threat Hunting

Provide a common query capability across a central data repository to proactively uncover advanced adversaries.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS · TEVORA PCI DSS Attestation HIPAA Attestation

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?

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733