SentinelOne

DATA SHEET

SentinelOne Endpoint Security

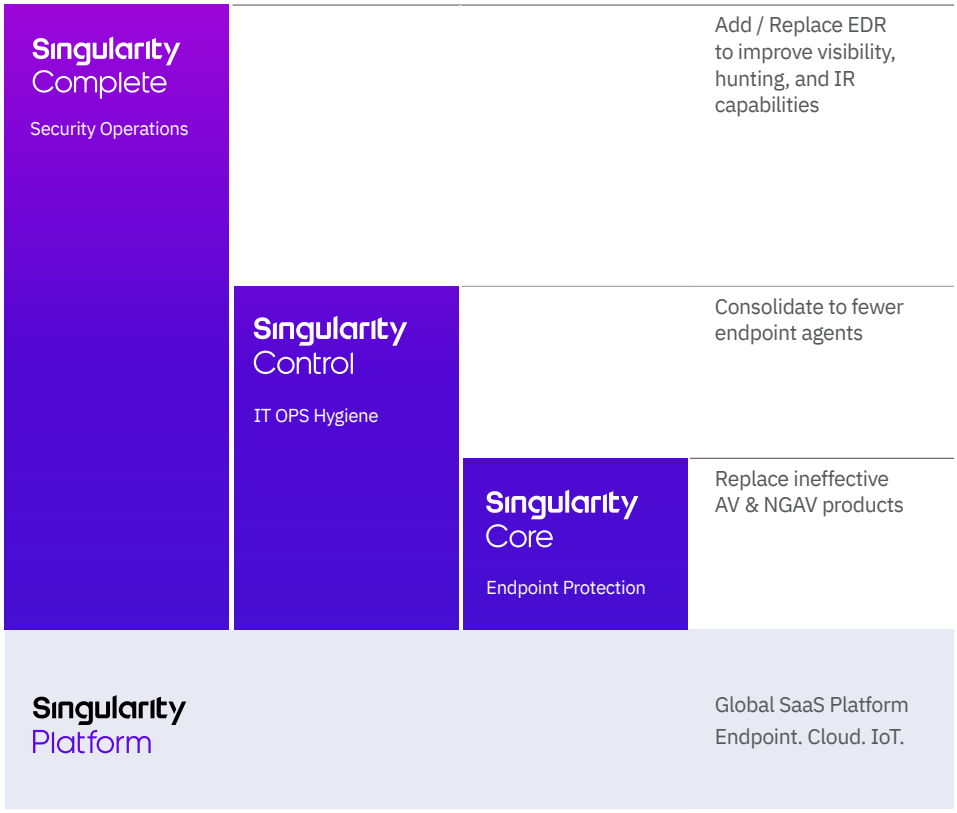
Singularity™ Platform Product Bundles

The SentinelOne Singularity security platform empowers SOC & IT Operations Teams with a more efficient way to protect information assets against today's sophisticated threats.

Singularity delivers differentiated endpoint protection, endpoint detection and response, IoT security, cloud security, and IT operations capabilities - consolidating multiple existing technologies into one solution. We offer resource-efficient autonomous Sentinel agents for Windows, Mac, Linux, and Kubernetes and support a variety of form factors including physical, virtual, VDI, customer data centers, hybrid data centers, and cloud service providers.

Sentinels are managed via our globally-available multi-tenant SaaS designed for ease of use and flexible management that meets your requirements. Our Vigilance Managed Detection & Response (MDR) services subscription is available to back your security organization 24x7.

This datasheet describes our tiered product offerings known as Singularity Core, Control, and Complete. Each product bundle builds on the one below it.



WHY CHOOSE SENTINELONE?

- We do endpoint security and we do it well. SentinelOne truly converges EPP+EDR so that you can eliminate redundant endpoint agents and lower OPEX.
- 97% customer support satisfaction
- 97% of customers recommend SentinelOne
- Customizable console with time saving workflows
- Ransomware solved through superior behavioral AI
- Autonomous protective responses trigger instantly
- Time saving, fatigue-reducing Storyline™ with ActiveEDR® designed for incident responders and threat hunters
- Affordable EDR data retention of 365 days+ for full historical analysis
- Easy XDR integrations to other vendors

READY FOR A DEMO?

Visit the SentinelOne website for more details

Singularity Platform Features & Offerings

All SentinelOne customers have access to these SaaS management console features:

Global SaaS implementation. Highly available. Choice of locality (US, EU, APAC).

Flexible administrative authentication and authorization: SSO, MFA, RBAC

Administration customizable to match your organizational structure

365 days threat incident history

Integrated SentinelOne Threat Intelligence and MITRE ATT&CK Threat Indicators

Data-driven dashboard security analytics

Configurable notifications by email and syslog

Singularity Marketplace ecosystem of bite-sized, 1-click apps

Single API with 340+ functions

Singularity Core

Core is the bedrock of all SentinelOne endpoint security offerings. It is our entry-level endpoint security endpoint security product for organizations that want to replace legacy AV or NGAV with an EPP that is more effective and easy to manage. Core also offers basic EDR functions demonstrating the true merging of EPP+EDR capabilities. Threat Intelligence is part of our standard offering and integrated through our AI functions and SentinelOne Cloud. Singularity Core features include:

- **Built-in Static AI and Behavioral AI analysis** prevent and detect a wide range of attacks in real time before they cause damage. Core protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.
- **Sentinels are autonomous** which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real time.
- **Recovery is fast** and gets users back and working in minutes without re-imaging and without writing scripts. Any unauthorized changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.
- **Secure SaaS management access.** Choose from US, EU, APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.

Singularity Control

Control is made for organizations seeking the best-of-breed security found in Singularity Core with the addition of “security suite” features for endpoint management. Control includes **all Core features plus:**

- **Firewall Control** for control of network connectivity to and from devices including location awareness
- **Device Control** for control of USB devices and Bluetooth/BLE peripherals
- **Rogue visibility** to uncover devices on the network that need Sentinel agent protection
- **Vulnerability Management**, in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database

SENTINELONE STOPS RANSOMWARE AND OTHER FILELESS ATTACKS WITH BEHAVIORAL AI AND STRONG AUTOMATIC REMEDIATION FUNCTIONS

Singularity Complete

Complete is made for enterprises that need modern endpoint protection and control plus advanced EDR features that we call ActiveEDR®. Complete also has patented Storyline™ tech that automatically contextualizes all OS process relationships [even across reboots] every second of every day and stores them for your future investigations. Storyline™ saves analysts from tedious event correlation tasks and gets them to the root cause fast. Singularity Complete is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating telemetry and mapping it into the MITRE ATT&CK® framework. The most discerning global enterprises run Singularity Complete for their unyielding cybersecurity demands. Complete includes all Core and Control features **plus**:

- **Patented Storyline™** for fast RCA and easy pivots
- **Integrated ActiveEDR® visibility** to both benign and malicious data
- **Data retention options to suit every need**, from 14 to 365+ days
- **Hunt by MITRE ATT&CK ® Technique**
- **Mark benign Storylines as threats** for enforcement by the EPP functions
- Custom detections and automated hunting rules with **Storyline Active Response (STAR™)**
- Timelines, remote shell, file fetch, sandbox integrations, and more

Gartner peerinsights™

"Impressive capabilities. Easy to deploy and use EDR.

Director of Cybersecurity - Heathcare
1B - 3B USD

Gartner peerinsights™

"Single platform the SOC can rely on.

Security & Risk Management - Finance
50M - 250M USD

IT Central Station
Unbiased reviews from the tech community

"Increased efficiency. We've absolutely seen an ROI.

Global InfoSec Director - Manufacturing
10B - 25B USD

Vigilance MDR Services Subscription

SentinelOne Vigilance Managed Detection & Response (MDR) is a service subscription designed to augment customer security organizations. Vigilance MDR adds value by ensuring that every threat is reviewed, acted upon, documented, and escalated as needed. In most cases we interpret and resolve threats in about 20 minutes and only contact you for urgent matters. Vigilance MDR empowers customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC Teams.

More info:
www.sentinelone.com/global-services/services-overview/

SentinelOne Readiness Services Subscription

SentinelOne Readiness is an advisory subscription service designed to guide your Team before, during, and after product installation with a structured methodology that gets you up and running fast and keeps your installation healthy over time. Readiness customers are guided through deployment best practices, provided periodic agent upgrade assistance, and receive quarterly ONEscore™ health check-ups to ensure your SentinelOne estate is optimized.

More info:
www.sentinelone.com/global-services/readiness/

Bundled Features

	Singularity Complete	Singularity Control	Singularity Core
Global SaaS Platform. Secure Access, High Availability, Hierarchical Policy Administration, EDR Incident Response & Threat Hunting, Analytics, IoT Control (with Ranger option), CWS	✓	✓	✓
Security Operations EDR Features			
Deep Visibility ActiveEDR® with Storyline™ context	✓		
MITRE ATT&CK® Integration	✓		
Storyline Active Response (STAR) Custom Detection Rules	✓		
Storyline Active Response (STAR) Pro Custom Detection Rules	+		
Binary Vault Live Malware Upload Repository	+		
File Integrity Monitoring	✓		
14-day EDR Hunting Data Retention	✓		
Extended EDR Hunting Data Retention up to 365 days	+		
Cloud Data Lake Streaming	+		
Secure Remote Shell	✓	✓	
IT OPS / Security Hygiene & Suite Features			
OS Firewall control with location awareness (Win, Mac, Linux)	✓	✓	
USB device control (Win, Mac)	✓	✓	
Bluetooth® / Bluetooth Low Energy® control (Win, Mac)	✓	✓	
Rogue Device Discovery	✓	✓	
App Vulnerability (Win, Mac)	✓	✓	
Base Endpoint Protection Features			
Autonomous Sentinel agent Storyline™ engine	✓	✓	✓
Static AI & SentinelOne Cloud file-based attack prevention	✓	✓	✓
Behavioral AI fileless attack detection	✓	✓	✓
Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)	✓	✓	✓
Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)	✓	✓	✓
Autonomous Rollback Response / 1-Click, no scripting (Win)	✓	✓	✓
Quarantine device from network	✓	✓	✓
Incident Analysis (MITRE ATT&CK®, timeline, explorer, team annotations)	✓	✓	✓
Agent anti-tamper	✓	✓	✓
App Inventory	✓	✓	✓

Optional Packages

	Co pee		
Network Asset Inventory			
Network Attack Surface Control			
Agent Auto-Deploy (Coming Soon)			
Hunt Device-Based Threats			
Cloud Workload Security for Kubernetes and VMs			
Cloud Provider Metadata Integration			
Automated App Control for Kubernetes			
Automated App Control for Linux VMs			
CIS Benchmarks for Workloads (Coming Soon)			

OS SUPPORT

SentinelOne supports a wide variety of Windows, Mac and Linux distributions as well as virtualization OSes. Common software exceptions are documented in our support portal.

Windows Sentinel agent
All Windows workstation starting with 7 SP1 through Windows 10
All Windows Server starting with 2008 R2 SP1 through Server/Core 2019

Mac Sentinel agent
macOS Big Sur, Catalina, Mojave

Linux Sentinel agent
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Windows Legacy agent
XP, Server 2003 & 2008, POS2009

Supported Container Platforms
Self-managed and Managed Kubernetes Services (EKS, AKS, GKE), OpenShift

Virtualization & VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V

Innovative. Trusted. Recognized.

ISO 27001 CERTIFIED by schellman