SentinelOne

DATA SHEET

SentinelOne Endpoint Security

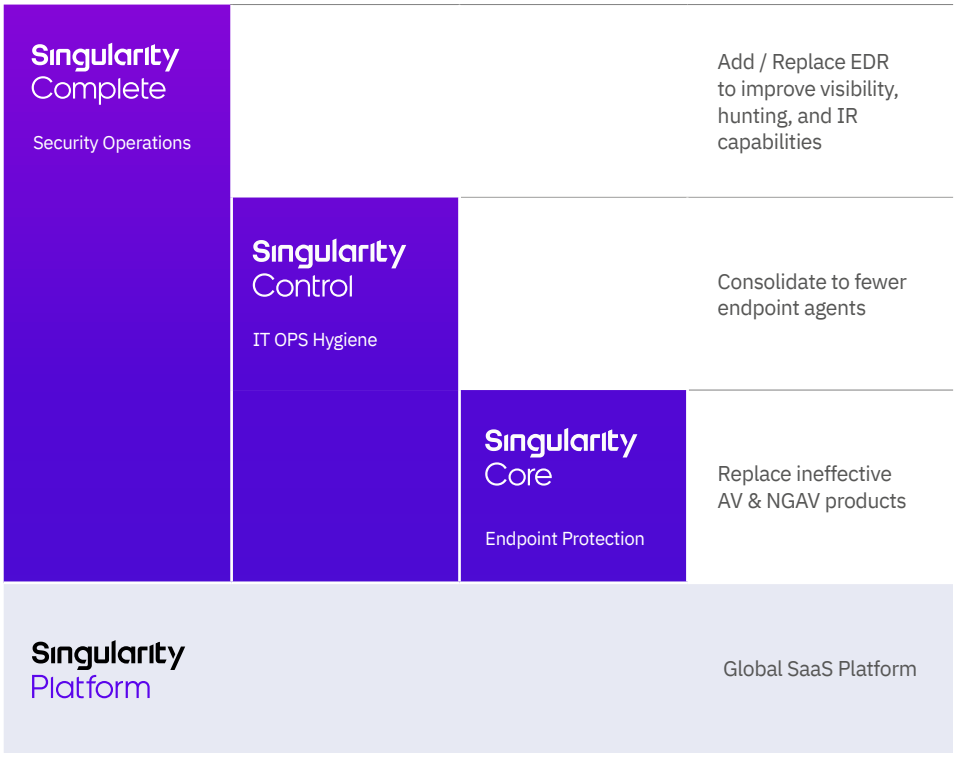
Singularity Platform Product Bundles

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 SentinelOne 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
- 96% 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
- 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 API-driven XDR integrations (SIEM, sandbox, Slack, 3rd party Threat Intel, etc)
- Single API with 340+ functions

Singularity Core

Core is the bedrock of all SentinelOne endpoint security offerings. It is our entry level 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 Sentinel Cloud. SentinelOne 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 SentinelOne Core with the addition of “security suite” features for endpoint management. SentinelOne Control features include:

- **All SentinelOne Core features**
- **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. SentinelOne 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 SentinelOne Complete for their unyielding cybersecurity demands. Features include:

- **All SentinelOne Core + SentinelOne Control features**
- **Patented Storyline™ tech** for fast RCA and easy pivots
- **Integrated ActiveEDR™ visibility** to both benign and malicious data
- **14 - 365+ historical EDR data retention** + usable query speeds at scale
- **Hunt by MITRE ATT&CK ® Technique**
- **Mark benign Storylines as threats** for enforcement by the EPP functions
- **Automated Storyline™ Active Response** (STAR) watchlist functions
- Timelines, remote shell, file fetch, sandbox integrations, and more

Gartner peerinsights™

> “Very flexible management capabilities in additional to strong EPP/EDR features.
>
> **Gov’t/PS/ED 5,000 - 50,000 Employees**
> Mar 13, 2020

> “Good Riddance Ransomware... SentinelOne Smokes The Competition!
>
> **Retail 1B - 3B USD**
> Mar 20, 2020

> “Configuration and rollout was extremely easy. The cloud dashboard is simple to use.
>
> **250M - 500M USD**
> Jul 2, 2020

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: https://s1.ai/s1mdr

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: https://s1.ai/ready

Bundled Features

	Singularity Complete	Singularity Control	Singularity Core
Global SaaS Platform. Secure Access, High Availability, EPP Policy Administration, EDR Incident Response & Threat Hunting, Analytics, IoT Control (with Ranger option)	✓	✓	✓
Security Operations EDR Features			
Deep Visibility ActiveEDR™	✓		
Deep Visibility Storyline™ pivot	✓		
Deep Visibility hunt by MITRE ATT&CK ® technique	✓		
Automated Storyline™ Active Response (STAR) watchlist	✓		
Manual / Auto file fetch (Windows, Mac, Linux)	✓		
Deep Visibility Mark Benign finding as Threat for enforcement response	✓		
Extended EDR Historical Data Storage (available 14-365 days)	✓		
Secure Remote Shell (Windows Powershell. Mac & Linux bash)*	✓	✓	
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 & Sentinel 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	✓	✓	✓

* included with Singularity Control for a limited time

Global Support & Service Offerings

Technical support by phone, web, and email	**Included**
In-product resource center / Support portal access	**Included**
Standard 9x5 Support	**Included**
Enterprise Support 24x7x365, Follow-the-Sun for Sev 1 & 2	Available
Designated Technical Account Manager + Enterprise Support	Available
Vigilance Managed Detection & Response (MDR) Subscription	Available
SentinelOne Readiness Deployment & Ongoing Health Subscription	Available

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 Catalina, Mojave, High Sierra

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
Kubernetes self-managed v1.13+ (self-managed, AWS Kubernetes (EKS), Azure AKS)

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

AWS GovCloud · SE Labs AAA Enterprise Endpoint Protection · VB100 VIRUS virusbtn.com · MITRE ATT&CK · TEVORA HIPAA Attestation · TEVORA PCI DSS Attestation · ISO 27001 CERTIFIED by schellman · Gartner peerinsights customers' choice 2020

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

96%

96% of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97%

Customer Satisfaction (CSAT) is ~97%

Net Promoter Score in the "great" to "excellent" range

About SentinelOne

SentinelOne founded in 2013 and headquartered in Mountain View, California, is a cybersecurity software company. SentinelOne Singularity is one platform to prevent, detect, respond, and hunt in the context of all enterprise assets.

© SentinelOne 2020

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733

S1-PROD-CCC-140820-1