SentinelOne

DATA SHEET

# SentinelOne Endpoint Security

## Singularity Platform Product Bundles

Het SentinelOne Singularity security platform stelt SOC- en IT Operations teams in staat op een efficiëntere manier informatie assets te beschermen tegen de hedendaagse geavanceerde threats.

Singularity biedt en levert gedifferentieerde endpoint protection, Endpoint Detection and Response (EDR), IoT security, cloud security en mogelijkheden voor IT operations - waarbij meerdere bestaande technologieën worden samengevoegd tot één oplossing. We bieden 'resource efficient', autonome Sentinel agens voor Windows, Mac, Linux en Kubernetes en ondersteunen een scala aan 'form factors', inclusief fysieke, virtuele, VDI, customer datacenters, hybride datacenters en cloud service providers.

Sentinels worden beheerd via onze wereldwijd beschikbare multi-tenant SaaS, ontworpen voor gebruiksgemak en flexibel beheer dat aan uw eisen voldoet. Ons Vigilance Managed Detection & Response (MDR) -servicesabonnement is beschikbaar om uw beveiligingsorganisatie 24 uur per dag, 7 dagen per week te ondersteunen.

Deze datasheet beschrijft ons gelaagde productaanbod dat bekend staat als SentinelOne Core, Control en Complete. Elke productbundel bouwt voort op de bundel eronder.

| | |
|---|---|
| **Singularity Complete**<br>Security Operations | Voeg / Vervang EDR om visibility hunting, en IR capabilities te verbeteren |
| **Singularity Control**<br>IT OPS Hygiene | Consolideer naar minder endpoint agents |
| **Singularity Core**<br>Endpoint Protection | Vervang ineffectieve AV & NGAV producten |
| **Singularity Platform** | Global SaaS Platform |

### WHY CHOOSE SENTINELONE?

- We zijn actief in endpoint security en daar zijn we goed in. SentinelOne convergeert echt EPP + EDR zodat u overtollige endpoint agents kunt elimineren en de OPEX kunt verlagen.
- 97% tevredenheid van klantenondersteuning
- 96% van de klanten beveelt SentinelOne aan
- Aanpasbare console met tijdbesparende workflows
- Ransomware opgelost door superieure behavioral AI
- Autonome beschermende reacties worden onmiddellijk geactiveerd
- Tijdbesparende, fatigue-reducerende Storyline™ met ActiveEDRTM ontworpen voor incident responders en threat hunters
- Betaalbare EDR data retentie
- Eenvoudige XDR integraties met andere vendoren

### READY FOR A DEMO?

Bezoek de SentinelOne website voor meer details

# Singularity Platform Features & Offerings

**Alle SentinelOne klanten hebben toegang tot deze 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 de basis van alle SentinelOne endpoint security offerings. Het is ons instapniveau endpoint security product voor organisaties die legacy AV of NGAV willen vervangen met een EPP dat effectiever en beter en eenvoudiger te managen is. Core biedt ook basis EDR-functies die de echte samenvoeging van EPP+EDR mogelijkheden demonstreren.
Threat Intelligence maakt deel uit van ons standaardaanbod en is geïntegreerd via onze AI-functies en Sentinel Cloud. SentinelOne Core-functies zijn onder meer:

- **Built-in Static AI en Behavioral AI analysis** voorkomen en detecteren een breed scala aan aanvallen in realtime voordat ze schade veroorzaken. Core beschermt tegen bekende en onbekende malware, Trojaanse paarden, hacktools, ransomware, misbruik van geheugen, scriptmisbruik, slechte macro's en meer.
- **Sentinels zijn autonoom** wat betekent dat ze preventie- en detectietechnologie toepassen met of zonder cloudconnectiviteit en in realtime beschermende reacties activeren.
- **Herstel is snel** en zorgt ervoor dat gebruikers binnen enkele minuten weer aan het werk zijn zonder re-imaging en zonder scripts te schrijven. Elke niet-geautoriseerde verandering die tijdens een aanval optreedt, kan worden teruggedraaid met 1-Click Remediation en 1-Click Rollback voor Windows.
- **Secure SaaS management access.** Kies uit de US, EU, APAC. Data-driven dashboards, policy management by site en group, incident analysis met MITRE ATT&CK integratie en meer.

## Singularity Control

Control is gemaakt voor organisaties die op zoek zijn naar de beste beveiliging in SentinelOne Core met de toevoeging van "security suite" functies voor endpoint management.

SentinelOne Control-functies omvatten:

- **Alle SentinelOne Core features**
- **Firewall Control** voor controle van de netwerkconnectiviteit van en naar deivces, inclusief location awareness
- **Device Control** voor controle van USB devices en Bluetooth/ BLE randapparatuur
- **Rogue visibility** om devices te ontdekken op het netwerk die SentinelOne agent protectie nodig hebben
- **Vulnerability Management**, in toevoeging op Application Inventory, voor inzicht in 3rd party applicaties waarvan kwetsbaarheden bekend zijn en toegewezen in de MITRE CVE database

**SENTINELONE STOPT RANSOMWARE EN ANDERE FILELESS AANVALLEN MET BEHAVORIAL AI EN STERKE AUTOMATISCHE HERSTELFUNCTIES**

# Singularity Complete

Complete is gemaakt voor enterprises die moderne endpoint protectie en controle nodig hebben plus geavanceerde EDR-features die we ActiveEDR™ noemen. Complete heeft ook de gepatenteerde Storyline™ technologie die automatisch alle OS-procesrelaties [zelfs na reboots] elke seconde van elke dag contextualiseert en ze opslaat voor toekomstige onderzoeken. Storyline™ bespaart analisten vervelende correlatietaken voor gebeurtenissen en brengt ze snel naar de kern. SentinelOne Complete is ontworpen om de belasting van beveiligingsbeheerders, SOC-analisten, threat hunters en incidentele responders te verlichten door telemetrie automatisch te correleren en in kaart te brengen in het MITRE ATT & CK®-framework. De meest veeleisende wereldwijde ondernemingen gebruiken SentinelOne Complete voor hun cybersecurity-eisen. Functies zijn onder meer:

- **Alle SentinelOne Core + SentinelOne Complete features**
- **Gepatenteerde Storyline™** -technologie voor snelle RCA en eenvoudige draaipunten
- **Geïntegreerde ActiveEDR™** zichtbaarheid voor goedaardige en kwaadaardige gegevens
- **14 - 365+ historische EDR dataretentie** + bruikbare querysnelheden op schaal
- **Hunt by MITRE ATT&CK ® Techniek**
- **Markeer goedaardige Storylines** als threats voor handhaving door de EPP-functies
- **Geautomatiseerde Storyline™ Active Response** (STAR) watchlist functies
- Timelines, remote shell, file fetch, sandbox integrations en meer

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 een serviceabonnement dat is ontworpen om de security van klantorganisaties te versterken. Vigilance MDR voegt waarde toe door ervoor te zorgen dat elke dreiging wordt beoordeeld, opgevolgd, gedocumenteerd en geëscaleerd als dat nodig is. In de meeste gevallen interpreteren en lossen we dreigingen in ongeveer 20 minuten op en nemen alleen contact met u op voor dringende zaken. Vigilance MDR stelt klanten in staat om zich alleen te concentreren op de incidenten die ertoe doen, waardoor het de perfecte endpoint add-on-oplossing is voor overbelaste IT / SOC-teams.

**Meer info: https://s1.ai/s1mdr**

## SentinelOne Readiness Services Subscription

SentinelOne Readiness is een adviserende abonnementsservice die is ontworpen om uw team voor, tijdens en na de productinstallatie te begeleiden met een gestructureerde methodologie waarmee u snel aan de slag kunt. Readiness klanten worden begeleid door best practices voor implementatie, krijgen periodieke assistentie bij het upgraden van agents en ontvangen driemaandelijkse ONEscoreTM- 'health check ups' om er zeker van te zijn dat het SentinelOne-domein is geoptimaliseerd.

**Meer 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

| | |
|---|---|
| Technische support via web, telefonisch en e-mail | **Included** |
| In-product resource center / Support portal toegang | **Included** |
| Standaard 9x5 support | **Included** |
| Enterprise support 24x7x365, Follow-the-Sun voor Sev 1 - 2 | Available |
| Toegewezen Technische Accountmanager + Enterprise Support | Available |
| Vigilance Managed Detection & Response (MDR) Subscriptie | Available |
| SentinelOne Readiness Deployment & Ongoing Health Subscriptie | Available |

## OS SUPPORT

SentinelOne ondersteunt een breed scala aan Windows-, Mac- en Linux-distributies, evenals virtualisatie-besturingssystemen. Veelvoorkomende software uitzonderingen worden gedocumenteerd in ons 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 · VB 100 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, opgericht in 2013 en met het hoofdkantoor in Mountain View, Californië, is een softwarebedrijf voor cybersecurity. SentinelOne Singularity is één platform om alle threats op enterprise assets te voorkomen, te detecteren, erop te reageren en erop te jagen.



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

S1-PROD-CCC-260820-1