XDR - Endpoint Security

SentinelOne Singularity™ Platform Products

SentinelOne Singularity delivers differentiated endpoint protection, endpoint detection and response, IoT security, cloud security, and IT operations capabilities by consolidating multiple existing technologies into one solution.

Offering 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.

The Secure ISS Security Event Monitoring service is available to back your organisation to ensure threats are mitigated 24 x 7. This datasheet describes the tiered product offerings known as Singularity Core and Complete. Each product package builds on the one below it.

Singularity Complete

Security Operations

Add / Replace EDR to improve visibility, hunting, and IR capabilities

Singularity Core

Endpoint Protection

Replace ineffective AV & NGAV products

Singularity Platform

Global SaaS Platform
Endpoint. Cloud. IoT.

Why Choose SentinelOne

- 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.
- Customisable 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.

Singularity Platform Features & Offerings

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

- ✓ Global SaaS implementation. Highly available. Choice of locality
- ✓ Flexible administrative authentication and authorisation: SSO, MFA, RBAC
- ✓ Administration customisable to match your organisational structure
- ✓ 365 days threat incident history
- ✓ Single API with 340+ functions
- ✓ 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

Singularity Core

Core is the bedrock of all SentinelOne endpoint security offerings. It is an entry-level endpoint security product for organisations 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 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 unauthorised changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.
- **Secure SaaS management access.** Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.

Singularity Complete

Complete is made for organisations that need modern endpoint protection and control plus advanced EDR features. Complete also has patented Storyline™ tech that automatically contextualises 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. Complete includes all Core features **plus:**

- **Patented Storyline™** for fast RCA and easy pivots, and for enforcement by the EPP functions and custom detections and automated hunting rules.
- **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.**
- Timelines, remote shell, file fetch, sandbox integrations, and more.
- **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.

	Singularity Core	Singularity Complete
Global SaaS Platform. Secure Access, High Availability, Hierarchical Policy Administration, EDR Incident Response & Threat Hunting, Analytics, IoT Control	✓	✓
Security Operations EDR Features		
Deep Visibility ActiveEDR® with Storyline™ context		✓
MITRE Engenuity ATT&CK® Integration		✓
Storyline Active Response (STAR™) Custom Detection Rules		✓
File Integrity Monitoring		✓
14-day EDR Hunting Data Retention		✓
Secure Remote Shell		✓
Remote Script Orchestration		+
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)		✓
App Vulnerability (Win, Mac)		✓
Rogue Device Discovery	✓	✓
Base Endpoint Protection Features		
Autonomous Sentinel agent Storyline™ engine	✓	✓
Static AI & SentinelOne Cloud Intelligence 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	✓	✓