SentinelOne
Secure Tomorrow™

SentinelOne Singularity™

Platform Packages, Modules, and Services

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

SentinelOne Singularity unifies and extends detection and response capability across multiple security layers including endpoint, cloud, identity, network, and mobile providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across a large cross-section of the technology stack.

Sentinel Agents are managed via our globally-available multi-tenant SaaS console 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 24×7.

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

Why Choose SentinelOne?

+ With foundation in best-in-breed EPP+EDR, SentinelOne extends native detection and response capabilties across your attack surfaces for global visibility and capability.
+ 95% customer satisfaction
+ 96% of Gartner Peer Insights reviewers 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 platform technologies designed for incident responsers 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 (US, EU, APAC).
- Flexible administrative authentication and authorization: SSO, MFA, RBAC
- Administration customizable to match your organizational structure
- Up to 3 years of threat incident history
- Integrated threat intelligenceand 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

Singularity Core is the foundation of all SentinelOne endpoint security offerings to replace legacy AV or NGAV with a more effective and easily managed EPP. Core includes static and behavioral AI engines, to detect a wide range of attacks. Our autonomous Sentinel agent applies protection and detection right at the endpoint, with or without a cloud connection.

Singularity Control

Singularity Control offers industry-leading endpoint security combined with “security suite” features for endpoint management. Control includes all Core features plus:

Firewall control to control network connectivity to/from devices, including location awareness

Device control of USB devices and Bluetooth/BLE peripherals

Vulnerability management and Application Inventory to provide insight into third party apps with known vulnerabilities, mapped to the MITRE ATT&CK CVE database

Singularity Complete

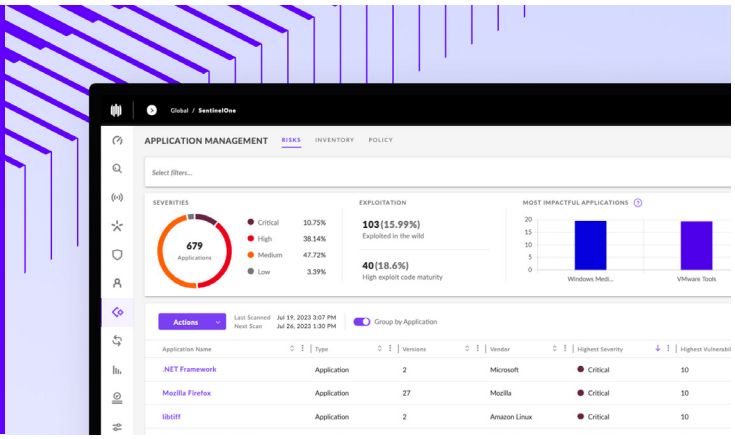
Singularity Complete provides best-in-breed EPP & EDR capabilities in one platform, management console, and agent. Designed for organizations seeking enterprise-grade prevention, detection, and response scalable across the enterprise, coupled with custom automations, Singularity Complete empowers security teams to easily identify and secure every user endpoint on their network.

- Patented Storyline™ for fast RCA and easy pivots
- Complete visibility of both benign and malicious data
- Data retention options to suit every need, upgradeable up to 3 years
- 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™)
- Built-in data collection scripts to enhance visibility and incident investigation
- Timelines, remote shell, file fetch, sandbox integrations, and more

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com



Gartner Peer Insights™

“

Impressive capabilities. Easy to deploy and use EDR.

Director of Cybersecurity
HEATHCARE 1B - 3B USD

Gartner Peer Insights™

“

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

SentinelOne stops ransomware and other fileless attacks with behavioral AI and strong automatic remediation functions.

Vigilance MDR Services Subscription

Vigilance Respond is SentinelOne's global, 24×7 Managed Detection & Response (MDR) service that augments your security team's capacity and offloads the monitoring, review, and triage of every threat to SentinelOne's in-house experts, helping you refocus on more strategic initiatives. Digital forensics analysis and incident response (DFIR) capabilities are available with Vigilance Respond Pro, making it the perfect support service for overstretched IT/SOC teams.

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

SentinelOne GO Subscription

SentinelOne GO is a 90 day guided onboarding and deployment advisory service designed to maximize your success with the Singularity™ Platform. Our customer success team employs a structured methodology to help you get up and running quickly, and equips you with best practices to stay healthy over time. See a model for success with a 30 day trial of Vigilance for fully managed, 24×7 monitoring & triage.

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

Platform Features	Singularity Core Cloud-Native NGAV	Singularity Control Security + Suite Features	Singularity Complete Enterprise Security
Singularity™ Platform Common Features			
Cloud-first multi-tenant SaaS	✓	✓	✓
Fully customizable management experience via multi-site, multi-group architecture	✓	✓	✓
Fully customizable role-based access control and MFA integration	✓	✓	✓
Patented Storyline™ correlation & context	✓	✓	✓
Skylight platform data analytics interface			✓
MITRE ATT&CK® Integration	✓	✓	✓
Data localization	Available	Available	Available
Singularity XDR Features			
Native data ingestion from SentinelOne surface agents (endpoint, cloud, identity, mobile, etc.) – Unmetered and does not decrement the Open XDR ingest quota.	✓	✓	✓
Open XDR data ingestion of 10 GB/day from any external, non-native, non-SentinelOne source. Upgradable to multi-terabyte/day.		✓	✓
Ingested data retention includes both Open XDR & Native data. 14 days default. Upgradable to 3 years.			✓
Singularity XDR Marketplace Apps		✓	✓
Storyline Active Response™ (STAR) Custom Detection Rules. 100 default. Upgradable.		Open XDR data only	✓
Endpoint Surfaces			
Endpoint security for Windows Workstation, macOS, and legacy Windows (XP, 7, 2003SP2+, 2008)	✓	✓	✓
Modern endpoint protection & NGAV utilizing static AI & behavioral AI	✓	✓	✓
Automated or one-click remediation & rollback	✓	✓	✓
Threat triage & investigation: 1 year lookback	✓	✓	✓
Rogue & unsecured device discovery. Requires Ranger Module for remote installation and other network functions.	✓	✓	✓
Mobile endpoint support: iOS, Android, Chrome OS	⊕	⊕	⊕
EPP Suite Control Features: Device Control, Firewall Control, Remote Shell		✓	✓
Application inventory and application CVEs		✓	✓
Built-in data collection scripts			✓
Native EDR data ingestion with Storyline™ and MITRE Engenuity ATT&CK® Mapping			✓
Native EDR threat hunting via Skylight			✓
Native EDR analytics			✓

Platform Features	Singularity Core Cloud-Native NGAV	Singularity Control Security + Suite Features	Singularity Complete Enterprise Security
Cloud Surfaces			
Realtime Cloud Workload Security for Linux VMs, Kubernetes clusters and Windows servers & VMs		✓	✓
Automated or one-click remediation & rollback. Remote shell.		✓	✓
Threat triage & investigation: 1 year lookback		✓	✓
Cloud service provider workload metadata sync		✓	✓
Automated App Control for Kubernetes and Linux VMs		✓	✓
Built-in data collection scripts			✓
Native EDR data ingestion with Storyline™ and MITRE Engenuity ATT&CK® Mapping			✓
Native EDR threat hunting via Skylight			✓
Native EDR analytics			✓
Identity Surface			
Singularity Ranger AD Module: Real-time Active Directory and Azure AD attack surface monitoring and reduction.	⊕	⊕	⊕
Singularity Ranger AD Protect Module: Real-time Active Directory and Azure AD attack surface monitoring and reduction further supplemented with AD domain controller-based Identity Threat Detection and Response.	⊕	⊕	⊕
Singularity Identity Module: Identity Threat Detection & Response for Active Directory and Azure AD and AD domain-joined endpoints.	⊕	⊕	⊕
Singularity Hologram Module: Network-based threat deception that lures in-network and insider threat actors into engaging and revealing themselves.	⊕	⊕	⊕
Platform Module Options			
Singularity Ranger® Attack Surface Management Module: Asset discovery, fingerprinting, and inventory. Automated agent deployment. Suspicious device isolation. Pivot to Skylight threat hunting.		⊕	⊕
RemoteOps Module: Orchestrated forensics, remote investigation, and rapid response at scale.			⊕
Cloud Funnel Data Lake Streaming Module: Replicate telemetry to any cloud for any purpose.			⊕
Binary Vault Module: Automated malicious and benign file upload for additional forensic analysis.			⊕

Service & Support

	Singularity Core Cloud-Native NGAV	Singularity Control Security + Suite Features	Singularity Complete Enterprise Security
Standard Support 5/9	✓	✓	✓
Enterprise Support 24/7/365	⊕	⊕	⊕
Enterprise Support + Technical Account Manager	⊕	⊕	⊕
SentinelOne Guided Onboarding (“GO”) deployment service	⊕	⊕	⊕
Vigilance Respond Managed Detection & Response (MDR) subscription	Limited	Limited	⊕
Vigilance Respond Pro MDR + Digital Forensics & Incident Response (DFIR) subscription	Limited	Limited	⊕
WatchTower Active campaign threat hunting & intelligence reporting	⊕	⊕	⊕
WatchTower Pro Bespoke threat hunting & compromise assessment	⊕	⊕	⊕
Vigilance IR Retainer	⊕	⊕	⊕

Legend: ✓ Included ⊕ Add-on

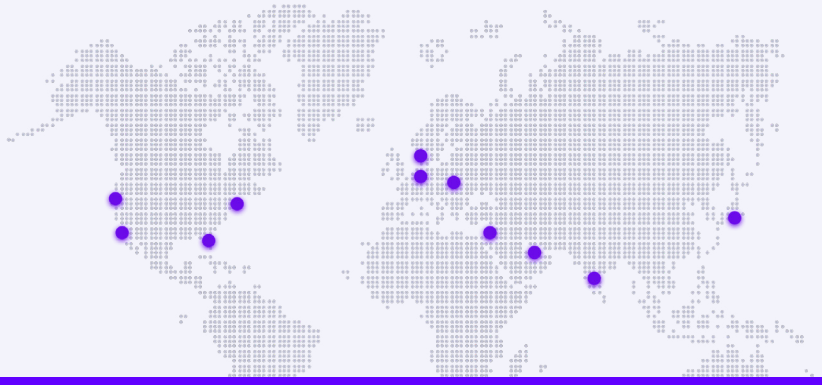
Support Locations

Mountain View, California US (HQ), Amsterdam, Bangalore, Boston, Dubai, Eugene, Fort Lauderdale, Prague, Tel-Aviv, Tokyo

Global Data Centers

US, Frankfurt, Tokyo, AWS GovCloud

Highly 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 11

All Windows Server starting with 2008 R2 SP1 through Server/Core 2019

Mac Sentinel Agent
macOS Ventura, Monterey, Big Sur

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

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

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733