SentinelOne
Core

SentinelOne
Control

SentinelOne
Complete

Executive Summary

SentinelOne offers a single autonomous agent combining EPP and ActiveEDR in three different tiers for customized requirements.

SentinelOne Core has all the endpoint security essentials including prevention, detection, and response.

SentinelOne Control adds desired security suite features, like device control and endpoint firewall control. It also adds full remote shell execution to ease IT overhead and provide uncharacteristic levels of granular control for managing endpoints.

SentinelOne Complete adds the Deep Visibility Threat Hunting module for advanced forensic mapping, visibility, and nuanced response capability for the enterprise SOC or interested technology professional.

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

SentinelOne™

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043

SentinelOne

Core

Made for every organization that wants top-notch protection without the hassle of complex management or the need for highly skilled security analysts. SentinelOne consolidates attack prevention, detection, response, and recovery into a single agent that protects Windows, Mac and Linux. SentinelOne "Core" is the bedrock of our platform.

SentinelOne Core features include:

- **Endpoint Prevention (EPP)** to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start
- **ActiveEDR Basic** for **Detection & Response (EDR)** works in real time with or without cloud connectivity. ActiveEDR detects highly sophisticated malware, memory exploits, script misuse and other fileless attacks as they attempt to do damage. **ActiveEDR** responds at machine speed to autonomously contain damage
- **ActiveEDR** recovery gets users up and running in minutes and includes 100% remediation as well as rollback for Microsoft Windows

SentinelOne

Control

Made for organizations seeking best-of-breed security found in SentinelOne Core with the addition of security suite features that streamlines granular endpoint management.

SentinelOne Control features include:

- All **SentinelOne Core** features
- **Device Control** for policy-based control of all USB device peripherals
- **Firewall Control** for policy-based control of network connectivity to and from assets, including location awareness
- **Vulnerability Management**, in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database
- **Full Remote Shell** capability for direct endpoint access by incident responders and forensics personnel

SentinelOne

Complete

Made for enterprises that need modern endpoint security and control plus threat hunting options for the SOC. SentinelOne Complete fulfills the needs of security administrators, SOC analysts, and Incident Responders. The most discerning global enterprises run SentinelOne Complete for their unyielding cybersecurity demands.

SentinelOne Complete features include:

- All **SentinelOne Core** + **SentinelOne Control** features
- **ActiveEDR Advanced** adds visibility of all benign data
- **ActiveEDR Advanced** adds enterprise threat hunting. SentinelOne differentiates with ease-of-use personified by the active nature of the solution in autonomously responding to attacks. All OS stories are automatically contextualized with S1's patented TrueContext function, saving analysts tedious event correlation tasks and getting them to the root cause fast.

SentinelOne's MDR - Vigilance

We know that managing enterprise assets and the threats against them takes a toll on your team. SentinelOne's Vigilance is an optional and supplemental Managed Detect and Respond (MDR) services
offering. Vigilance complements your team and SOC, providing 3 levels of 24x7x365 service:

- **Vigilance Monitor:** Empower and accelerate your security team with expert advice
- **Vigilance Respond:** Ensure business continuity and network hygiene in near real-time
- **Vigilance Deploy:** Designed for customers seeking a quick start, Vigilance Deploy spans the first 90 days of your SentinelOne deployment

FEATURE		Core	Control	Complete
Endpoint Protection	Static AI	✓	✓	✓
	Behavioral AI	✓	✓	✓
	Documents, Scripts	✓	✓	✓
	Fileless, Exploits	✓	✓	✓
	Lateral Movement	✓	✓	✓
Response	Remediation and Rollback	✓	✓	✓
	Network Quarantine	✓	✓	✓
	Full Remote Shell		✓	✓
ActiveEDR		Basic	Basic	Advanced
Suite Features	Device Control		✓	✓
	Firewall Control		✓	✓
	Vulnerability Management		✓	✓
EDR/Threat Hunting	Attack Storyline	Basic	Basic	Advanced
	Deep Visibility (Including Encrypted Traffic)			✓
	TrueContext Threat Hunting			✓