

SentinelOne
core

SentinelOne
Control

SentinelOne
complete

Executive Summary

SentinelOne offers a single autonomous agent combining EPP and EDR 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 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 all network connectivity to and from assets regardless of location
- **Vulnerability Management**, in addition to Application Inventory, for insight into 3rd party apps that have known CVE vulnerabilities
- **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 Core features include:

- All **SentinelOne Core** + **SentinelOne Control** features
- **ActiveEDR Advanced** adds visibility of all begin information
- **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 VIGILANCE MDR

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			✓



SentinelOne
core



SentinelOne
complete

Executive Summary

SentinelOne offers a single autonomous agent while providing two packages to cover deployments of different sizes and security requirements. The SentinelOne Core has all endpoint security essential feature in place, including; prevention, detection, and response. Everything you need to keep your assets safe.

The SentinelOne Complete adds on top of the SentinelOne Core the more advanced capabilities, like threat hunting and Deep Visibility (EDR).



- 100% Endpoint Protection Capabilities
- Detection/Threat Hunting **Basic**
- 100% Remediation
- Suite Features



- 100% Endpoint Protection Capabilities
- Detection/Threat Hunting **Advanced**
- 100% Remediation
- Suite Features

Endpoint Protection

Multi-layered AI-powered protection to replace Anti-Virus products

FEATURE	core	complete
Static AI Pre-execution protection for known and unknown file base malware	✓	✓
Behavioral AI Agent side behavioral tracking covering any attack vector, including unknown exploits and bypasses of traditional AV attempts	✓	✓
Documents, Scripts Behavioral AI engine build to detect and mitigate using documents and scripts to run malicious code	✓	✓
Fileless, Exploits Behavioral AI engine capable of protecting from file-less and exploits attempts.	✓	✓
Lateral Movement Behavioral AI engine focused on discovering attempts coming from another device over the network	✓	✓
PUP macOS engines to protect from probably unwanted program	✓	✓






Response

The ability to automatically respond to malicious activity







FEATURE	core	complete
Remediation Clean all artifacts of a malicious attempt, including registry, scheduled tasks and more	✓	✓
Rollback Revert an endpoint to its pre-infected state	✓	✓
Network Quarantine Disconnect a device from the network to ensure the impact is contained	✓	✓

EDR/Threat Hunting

Rich forensic data and can action threats automatically, including mitigation and even a complete rollback to pre-encrypted states

FEATURE	core	complete
Attack Storyline Visual diagram representing an execution flow, helping IR teams to quickly evaluate the impact of any threat		
Deep Visibility Deep Visibility into every operation on the agent, including the ability to search for historic data		
Encrypted Traffic Visibility Visibility into the encrypted network traffic without pushing certificates or the need for expensive SSL appliances/blades		
File Integrity Monitoring Monitor any file and get notified upon access or change		

Suite Features

FEATURE	core	complete
Device Control Apply policy and control USB and peripheral device connected to your assets		
Firewall Control Manage the personal firewall on your devices		
Disk Encryption Manageability Manage your disk encryption status and keys using the SentinelOne console		

AUTONOMOUS ENDPOINT PROTECTION THAT SAVES YOU TIME

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™ | Core

- Endpoint Protection Platform (EPP)
- Active EDR **Basic**
- Response **Basic**
100% Remediation + Rollback
- Suite Features **Basic**

SentinelOne™ | control

- Endpoint Protection Platform (EPP)
- Active EDR **Basic**
- Response **Basic**
100% Remediation + Rollback
- Suite Features **Advanced**

SentinelOne™ | Complete

- Endpoint Protection Platform (EPP)
- Active EDR **Advanced**
- Response **Advanced**
100% Remediation + Full Remote Shell
- Suite Features **Advanced**
- Visibility
- Threat Hunting