SentinelOne Endpoint Security Platform

Protects major endpoint and server platforms

SentinelOne ensures universal protection across user endpoints and servers running Windows, Mac OS X, iOS and Linux.

Integration with enterprise security infrastructure and tools

SentinelOne offloads indicators using industry standard formats (CEF, STIX, OpenIOC) for seamless integration with SIEMs, firewalls, and leading network security solutions.

Flexible deployment

Deploy SentinelOne to best fit your organization's needs: as an on-premise solution, or use as a cloud-based service.

SentinelOne is a certified AV replacement for Windows and MacOS.

System Requirements

USER ENDPOINT CLIENTS

Operating Systems:	Windows 7, 8, 8.1, 10 Mac OSX 10.9.x, 10.10.x, 10.11 Red Hat Linux, CentOS 6.5 and above

SERVER ENDPOINT CLIENTS

Operating systems:	Windows Server 2088 R2, 2012 R2 Windows Server 2016 .NET 4.5 CentOS 6.5 or higher, Ubuntu 14.04 (64-bit) Ubuntu 16.04, 16.10
Virtual Environments:	vSphere Microsoft Hyper-V Citrix Xen Server, Xen Desktop, Xen App
Hardware:	1 GHz Dual-core CPU or better 1 GB RAM or higher if required by OS (recommended 2 GB) 2 GB free disk space

MANAGEMENT SERVER (ON-PREMISE)

Operating System:	Linux Ubuntu 14.04 LTS Server
Hardware:	4-core Intel Xeon E5-2680v2, 2.8 GHz or better 8 GB RAM 500 GB free disk space

SentinelOne

For more information about SentinelOne and the future of endpoint security, please visit: www.sentinelone.com or follow us on Twitter: @SentinelSec

SentinelOne

Dealing with today's cyber threats requires a fundamentally different approach.

The truth is, legacy AV and prevention-only solutions don't cut it. Today's advanced malware, exploits, and other cyberattacks will blow right by AV-based solutions in a fraction of the time it takes to get updated with the latest threat signatures. Prevention should never be your last line of defense, no matter how sophisticated your static analysis claims to be.

Furthermore, vulnerability exists in the gap between detection and response. Even when an attack is detected, that attack can still proliferate to other areas of your infrastructure while security personnel scramble to fully eliminate it from the environment.

The key to effective endpoint security lies in the ability to intelligently uncover and behaviorally detect advanced threats, and respond at machine speed.

This is the essence of SentinelOne.

SentinelOne is recognized as a Visionary on the 2017 Gartner MQ.

Ransomware protection. SentinelOne covers customers up to $1,000/endpoint (up to $1M total) to recover files in the event of an undetected ransomware attack.

Unified Next-Generation Endpoint Security

SentinelOne unifies prevention, detection and response in a single platform driven by sophisticated machine learning and intelligent automation.

It enables you to prevent and detect attacks across all major vectors, rapidly eliminate threats with fully automated, policy-driven response capabilities, and gain complete visibility into your endpoint environment with full-context, real-time forensics.

Protect endpoints across *every* threat vector.

Deep system-level monitoring

Deployed on each endpoint, SentinelOne's lightweight autonomous agent monitors all activity in both kernel and user space (including files, processes, memory, registry, network, etc.). The agent is virtually silent and will never degrade user productivity.

Intelligent, signature-less static prevention

As a first line of defense, SentinelOne's Deep File Inspection (DFI) engine expertly uncovers and blocks known and unknown file-based malware, leveraging advanced machine learning algorithms instead of signatures.

Behavioral detection of advanced attacks

SentinelOne broadens protection against advanced threats through cutting-edge behavior-based detection. SentinelOne's Dynamic Behavior Tracking (DBT) Engine detects any type of malicious activity—from polymorphic malware to sophisticated exploits to stealthy insider attacks—against a full context of normal system activity.

"In today's threat environment, you're fooling yourself if you think antivirus is going to block every attack headed your way. Seeing that malware and other attacks can easily get by AV, you need endpoint security that uses behavior-based detection instead of signatures."

Joe Miller
Security Engineering Team LeadC
Global Cosmetics Manufacturer

Respond automatically.

Zero-touch mitigation and containment

SentinelOne's fully integrated, policy-driven mitigation covers all endpoints—local and remote—allowing for decisive incident response that makes dwell time a thing of the past.

Upon detection, SentinelOne immediately stops lateral threat spread cold by swiftly killing malicious processes, quarantining infected files, or disconnecting the infected endpoint device from the network while still maintaining the agent's connection to the man-agement console.

Full remediation

Easily reverse malware-driven modifications to registry and system settings.

Single-click rollback

Instantly restore any compromised files back to their previous trusted states (requires enablement of Windows VSS).

Auto-immunization

Each time SentinelOne finds a new, never-before-seen malicious binary, it instantly flags it and notifies all agents on the network, rendering other endpoint devices immune to the attack.

Visualize attacks in high-definition.

Full-context forensics in real time

SentinelOne dramatically enhances your investiga-tive capabilities with detailed forensic data generated in real time. It shows you an intuitive 360-degree view of an attack, mapping out its point of origin and progression across endpoints and other systems for complete forensic insight.

Deploy, scale, and manage with ease.

SentinelOne puts the industry's most innovative prevention, detection, and response capabilities at your fingertips through a single management console that can be flexibly deployed either in the cloud or on-premise. Effortlessly scale to protect user endpoints and servers across physical, virtual, and cloud environments.

The SentinelOne Platform