SentinelOne EPP and EDR Next Generation Endpoint Protection

The increasing success rate of cyber attacks and ineffectiveness of traditional security solutions demands a new model to protect endpoints from advanced malware and zero-day threats.

In an era where attackers can automatically generate tailored payloads on a per target basis, using static methods to determine whether a file is malicious or benign is futile. A new, disruptive approach, that focuses on the malware's core functionality, which cannot be changed as easily as its hash or other static indicators, is needed.

SentinelOne delivers comprehensive next generation endpoint protection that profiles, tracks, assembles a context, and identifies malicious patterns of behaviors across the entire lifecycle of execution of malware, in real time, on the end device.

SentinelOne Solutions Datasheet

Portfolio

SentinelOne provides next generation enterprise endpoint protection that detects, mitigates, and remediates advanced malware, APT's, and zero-day attacks. To meet the requirements of different organizations SentinelOne offers: SentinelOne EPP, which is designed to completely replace existing corporate Anti-Virus (AV)/endpoint protection solutions, and SentinelOne EDR which augments traditional AV/endpoint tools with next generation detection and response capabilities.

SentinelOne EPP

Replace AV: SentinelOne EPP is a next generation AV replacement suite that delivers complete protection against targeted attacks, advanced malware, and zero-day threats by tracking malicious behavior, in real-time, across multiple endpoints.

SentinelOne EDR

Augment AV: SentinelOne EDR stops advanced threats and zero-day attacks, and is designed to augment and be deployed alongside existing endpoint protection solutions. Using dynamic execution inspection, SentinelOne EDR detects advanced threats, provides automated mitigation and generates real-time forensics.

SentinelOne EDR co-exists with traditional corporate AV/endpoint protection solutions, and supports multiple endpoint platforms (desktops, servers, and mobile devices).

SentinelOne Solutions Datasheet

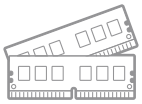
Next Generation Endpoint Protection Capabilities

The following next generation endpoint protection capabilities form the core of SentinelOne solutions.

Prevention*

Blocks known in-the-wild threats by leveraging up to the minute cloud intelligence and select reputation services to proactively block threats before they can execute on endpoints.

Dynamic Exploit Detection



Prevents attacks that use memory and application exploits by detecting their execution techniques (e.g., heap spraying, stack pivots, ROP attacks, and memory permission modifications) and not relying on static measures like shellcode scanning.

Dynamic Malware Detection

Stops targeted and zero day attacks using real-time execution monitoring and analysis to assemble true behavioral context without the need for static measures. SentinelOne performs monitoring and analysis of application and process behaviors at low-level instrumentation of OS activities and operations, including memory, disk, registry, network, and more. The ability to inspect and assemble the true execution context is critical to stop attackers since they have learned to take advantage of hooking into system processes and benign applications.

*- SentinelOne EPP only

SentinelOne

SentinelOne Solutions Datasheet

Mitigation

Beyond just detection, manual or fully automated mitigation options can be configured via policy and include various actions such as: killing malicious processes, quarantining threats or isolating infected machines.

Remediation

Remediation action deletes malware and any related dropped files or remnants.

Endpoint Forensics

Media-rich reports generated during attacks can track malicious activity and provide clear visibility in real time so security staff can timely respond and communicate across the organization to minimize the impact of attacks.

SentinelOne

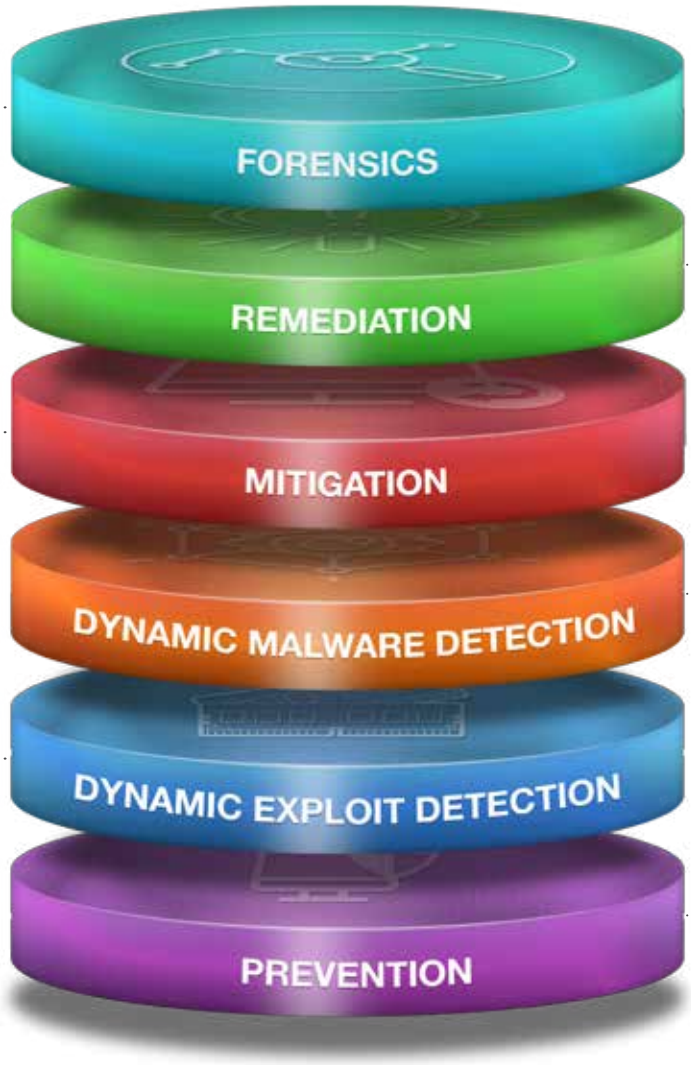
SentinelOne Solutions Datasheet

Next Generation Endpoint Protection Capabilities

Real-time analysis & root cause forensic investigation

Automatic Mitigation Quarantine files and endpoints

Dynamic Exploit Detection - Protect from app and memory based exploits, drive by downloads



Rollback & Immunize - Automatic remediation to undo system changes

Dynamic Execution Inspection - Full system monitoring to protect from evasive, packed malware , social engineering/spearphising

Reputation-based preemptive block & prevention polices - Protect from known threats

SentinelOne Solutions Datasheet

Key Features

Features
Learning mode – establishes a baseline of legitimate applications running on endpoints to minimize false positives.
Cloud intelligence – proactively blocks known threats by leveraging cloud intelligence and select reputation services.
Auto immune – instantly shares new threat intelligence across endpoints to prevent lateral movement and further infection.
Anti-exploitation detect and prevent application and memory-based exploits based on the techniques themselves without relying on static measures.
Dynamic execution inspection – continuously monitors and tracks activity on endpoints to analyze behavior and detect unknown threats.
Automated mitigation – fully automates remediation and threat removal, including killing processes, and quarantining threats or endpoints.
Remediation – recovers deleted files or restores modified files back to their state prior to malware execution, effectively reversing any malware-driven modifications.
Endpoint forensics – graphical reports generated during attacks deliver sandbox equivalent investigative capabilities.
Multi-platform support – protects endpoints across multiple operating systems (Windows, OS X, Android, Linux*, IOS*)
Always on protection – autonomous agent analyzes and stops threats without the need to offload any data, regardless if endpoints are on/off network or whether they are connected to the Internet.
Seamless integration – offload indicators using industry standard formats (CEF, STIX, OpenIOC) to seamlessly integrate with SIEMs, firewalls, and leading network security solutions.

*- Coming soon

System requirements (Clients):

Operating systems
- Windows 7, 8, 8.1
- Windows Server 2008 R2, 2012 R2
- .NET 4.5
- OS X 10.9.x, 10.10.x
- 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)
- 1 GB free disk space

SentinelOne

What is Next Generation Endpoint Protection?

Certifications and Awards

SentinelOne EPP is the first AV-TEST INSTITUTE certified next generation endpoint protection platform

SentinelOne Endpoint Protection Platform (EPP) receives FIVE STARS in SC Magazine review *"Strong zero-day capabilities"* and *"Some of the best forensics we've seen"*
- Peter Stephenson

The 10 Coolest Security Startups Of 2014

Best business antivirus of 2015

About SentinelOne

SentinelOne is a startup formed by an elite team of cyber security engineers and defense experts who joined forces to reinvent endpoint protection. With decades of collective experience, SentinelOne founders honed their expertise while working for Intel, McAfee, Checkpoint, IBM, and elite units in the Israel Defense Forces. They came together in 2013 to build a new security architecture that could defeat today's advanced threats and nation state malware.

2513 E. Charleston Rd
Mountain View, CA 94043

SentinelOne
www.sentinelone.com

contactus@sentinelone.com
support@sentinelone.com
sales@sentinelone.com