SentinelOne
The Future of Endpoint Protection

PRODUCT DATASHEET

Get real-time protection against advanced threats driven by machine learning and intelligent automation.

> **"With the onslaught of malicious actors deploying advanced malware and the limitations of existing antivirus software, SentinelOne is providing a critical solution to this problem. A solution that will benefit the entire industry."**
>
> **Justin Somaini, Chief Trust Officer, Box**

Last year, enterprise organizations collectively faced over three billion cyber attacks. When you consider the growing diversity and sophistication of these attacks, it's only natural to question your ability to detect all of them, and whether or not your organization's response is effective enough.

SentinelOne is recognized as a Visionary on the 2016 Gartner Magic Quadrant for Endpoint Protection Platforms.

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

The truth is, static, AV-based solutions just don't cut it. Today's advanced malware, exploits, and other cyber attacks will blow right by AV-based protection in a fraction of the time it takes to get updated with the latest threat signatures.

Furthermore, vulnerability exists in the gap between detection and response. Even if an attack is successfully detected, lack of integration with incident response tools forces manual attempts to neutralize it. In the meantime, that attack can still proliferate to other areas of your infrastructure.

The key to effective endpoint protection lies in the ability to dynamically analyze and predict any threat's behavior, and respond intelligently at machine speed. This is the essence of SentinelOne.

AV TEST av-test.org 02/2014 APPROVED CORPORATE ENDPOINT PROTECTION

SentinelOne is a certified replacement for AV-based solutions.

Real-time, Unified Endpoint Protection

SentinelOne unifies prevention, detection, and response in a single platform driven by sophisticated machine learning and intelligent automation. It enables you to predict malicious behavior across major threat vectors in real-time, rapidly eliminate threats with fully-automated, integrated response capabilities, and adapt your defenses against the most advanced cyber attacks.

Predict malicious behavior.

Continuous System-level Monitoring

Deployed on each endpoint device, 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 precious user productivity.

Behavioral Detection of Advanced Malware, Exploits and Live Attacks

Endpoint Agents leverage SentinelOne's Dynamic Behavior Tracking (DBT) Engine which uses sophisticated machine learning to predict threats across any vector against a full context of normal behavior.

Real-time Forensic Analysis

SentinelOne dramatically enhances your investigative capabilities with detailed analysis reports, sent from the Agent to the SentinelOne management console in real-time.

Attack Storyline Visualization

SentinelOne shows you a 360-degree view of an attack, mapping out its point of origin and progression across endpoints and other systems for complete forensic insight.

Rapidly eliminate threats.

Zero-Touch Mitigation

SentinelOne's fully integrated, automated response protocol covers all endpoints – local and remote. You can swiftly kill or quarantine malicious processes, making dwell time a thing of the past.

Robust Containment

Upon threat detection, SentinelOne immediately stops its lateral spread cold by disconnecting the infected endpoint device from the network, but still maintains the Agent's connection to the SentinelOne management console.

Full Remediation

Easily reverse attack-driven modifications and restore manipulated files to their last known trusted states.

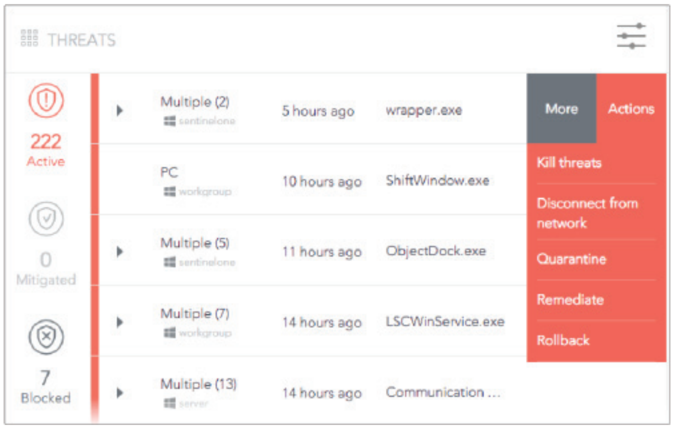
Seamlessly adapt defenses.

Auto-Immunization

Each time the Dynamic Behavior Tracking Engine finds a new, never-before-seen malicious binary, SentinelOne instantly flags it and notifies all Agents on the network, rendering other endpoints immune to the attack.

Cloud Intelligence

SentinelOne further extends your protection by leveraging up-to-the-minute cloud intelligence and data from select reputation services to proactively block known threats.



THREATS

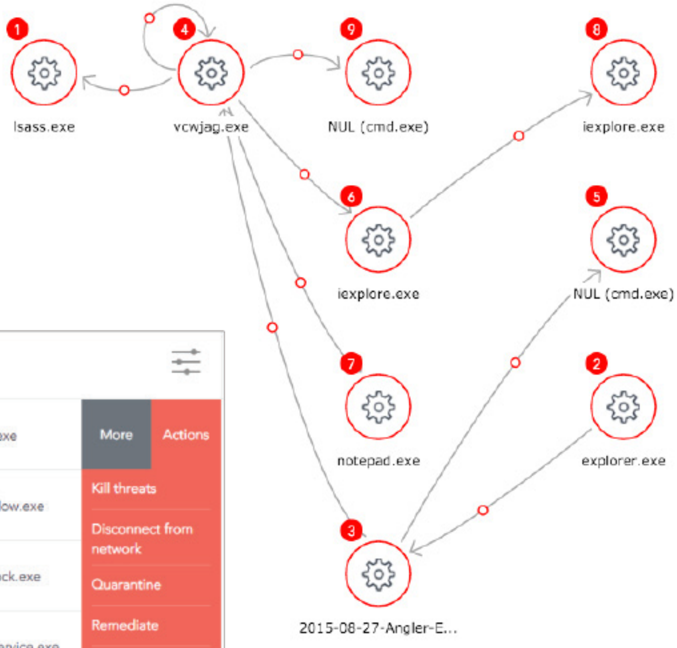
222 Active

0 Mitigated

7 Blocked

▸	Multiple (2) sentinelone	5 hours ago	wrapper.exe
	PC workgroup	10 hours ago	ShiftWindow.exe
▸	Multiple (5) sentinelone	11 hours ago	ObjectDock.exe
▸	Multiple (7) workgroup	14 hours ago	LSCWinService.exe
▸	Multiple (13) server	14 hours ago	Communication ...

Fully integrated mitigation and remediation capabilities



Full-context visualization of attacks

MARY KAY

> **“In today’s threat environment, you’re fooling yourself if you think Antivirus is going to block every attack headed your way. With SentinelOne replacing AV on our endpoints, we’re much better protected not only against malware, but against sophisticated exploits and APTs. On top of that, we’ve experienced zero performance impact to protected devices.”**

Joe Miller, Information Security
Mary Kay Inc.

Microsoft Partner
Virus Information Alliance

The SentinelOne Platform

Protects Major Endpoint Platforms

SentinelOne ensures universal protection across endpoint devices running Windows, OS X, 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.

System Requirements

CLIENTS

Operating Systems:	Windows 7, 8, 8.1, 10
	Windows Server 2008 R2, 2012 R2
	.NET 4.5
	OS X 10.9.x, 10.10.x, 10.11
	Red Hat Linux, CentOS 6.5 and above
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
The Future of Endpoint Protection

For more information about SentinelOne and the future of endpoint protection, please visit: **www.sentinelone.com**