SentinelOne
The future of endpoint security

Next-Generation Endpoint and Server Protection

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 protection lies in the ability to intelligently uncover and behaviorally detect advanced threats, and respond at machine speed.

This is the essence of SentinelOne.

SentinelOne provides the lowest TCO and highest ROI according to NSS Labs.

CYBER SentinelOne WARRANTY

Ransomware protection. Guaranteed.

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 Protection

SentinelOne Endpoint Protection Platform (EPP) 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.

Joe Miller
Security Engineering Team Lead
Global Cosmetics Manufacturer

"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 protection that uses behavior-based detection instead of signatures."

Protect endpoints across every threat vector

Deep system-level monitoring

Deployed on each endpoint, SentinelOne EPP'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 EPP'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

EPP 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.

Respond automatically

Zero-touch mitigation and containment

SentinelOne EPP'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 EPP 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 management 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 EPP finds a new, never-beforeseen 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

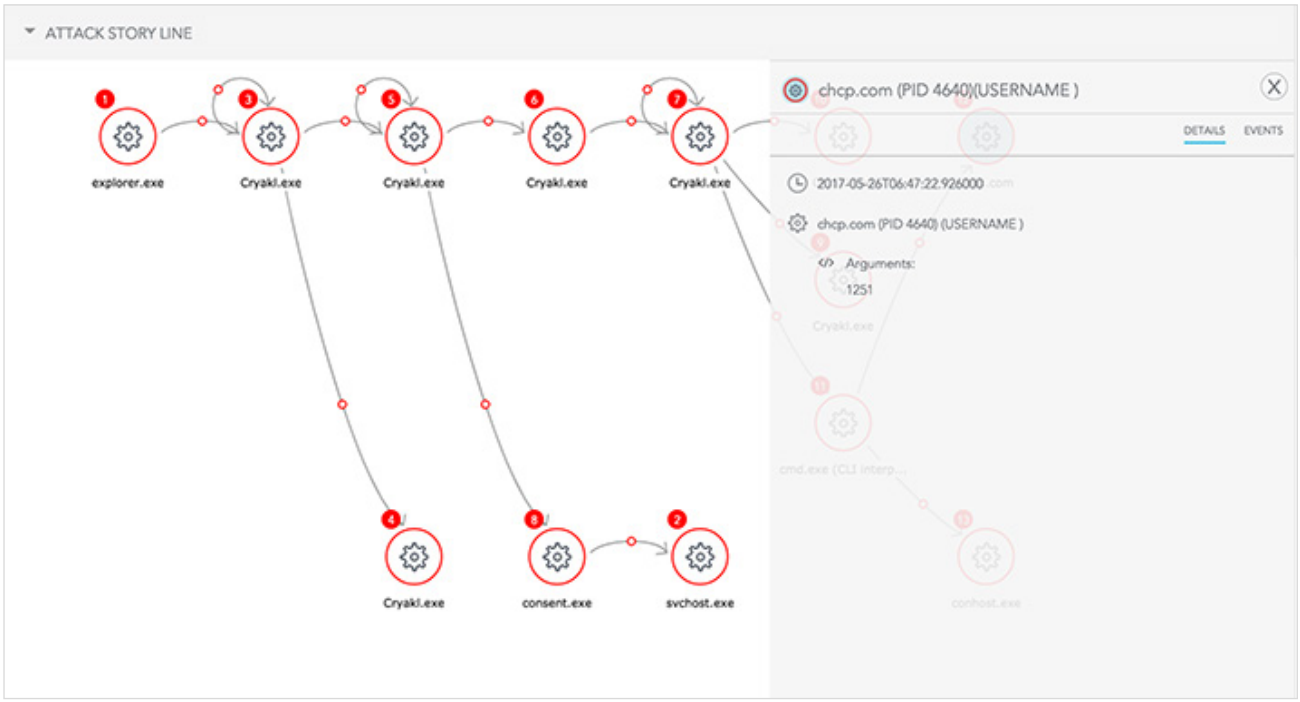
Full-context forensics in real time

SentinelOne EPP dramatically enhances your investigative capabilities with detailed forensic data generated in real time. EPP 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 EPP 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 Endpoint Protection Platform



Protects major endpoint and server platforms

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

Integration with enterprise security infrastructure and tools

SentinelOne loads 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

USER ENDPOINT CLIENTS

Operating Systems

Windows XP, 7, 8, 8.1, 10
Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x
macOS 10.13 (High Sierra)
CentOS 6.5, 7.0, 7.2
Red Hat Enterprise Linux 6.5, 7.0, 7.2
Ubuntu 12.04, 14.04, 16.04, 16.10
openSUSE 42.2

SERVER ENDPOINT CLIENTS

Operating Systems

Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016
CentOS 6.5, 7.0, 7.2
Red Hat Enterprise Linux 6.5, 7.0, 7.2
Ubuntu 12.04, 14.04, 16.04, 16.10
SUSE Linux Enterprise Server 12SP1
Oracle Linux 6.5 - 6.9, 7.0+
Amazon Linux (AMI) 2016.09+, 2017.03+

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 Systems

Ubuntu 14.04.x LTS Server
Red Hat Enterprise Linux 7.x

Hardware:

4-core Intel Xeon E5-2680v2, 2.8 GHz or better
8 GB RAM
1 TB free disk space

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com

SentinelOne is a certified AV replacement for Windows and MacOS.

SentinelOne
The future of endpoint security