SentinelOne
The future of endpoint security

The value of SentinelOne

The key to effective endpoint protection lies in the ability to dynamically detect malicious behavior across all attack vectors and respond intelligently at machine speed, all through a single, easy-to-manage platform.

This is the essence of SentinelOne.

We defeat advanced threats across all major vectors of attack. If today's threat landscape were comprised only of file-based malware, then signature-based antivirus and other static prevention solutions might be considered adequate protection. However, advanced threats extend far beyond attacks involving executable files; organizations must also protect against memory-only malware, document and browser-based exploits, and script-based attacks that can be initiated by insiders. Simply put: if the attack is file-less, legacy and next-generation AV leaves you defenseless.

SentinelOne's Endpoint Protection Platform (EPP) protects against all major types of cyberattacks. Our technology doesn't depend on signatures or heuristic analyses, which is only eective on files. SentinelOne detects threats dynamically, based on behavior. We watch the endpoint system from the perspective of processes, and can identify any major type of cyberattack, regardless of how it is launched.

SENTINELONE EPP PROTECTS AGAINST:

Advanced malware

Ransomware, trojans, worms, backdoors

File-less attacks

Memory-based malware

Exploits

Document- and browser-based

Script-based attacks

Powershell, Powersploit, WMI, VBS

Credential stealing attacks

Credential-scraping, Mimikatz, tokens

Our multi-faceted approach to protection addresses the entire threat execution lifecycle.

When it comes to protecting user endpoints and critical servers against today's sophisticated attacks, prevention-based solutions alone don't cut it. The best next-generation endpoint protection approaches are ones which address the entire threat execution lifecycle with a combination of prevention, detection, and response capabilities. The SentinelOne EPP unifies all of these critical capabilities within a single platform. With SentinelOne, reducing the overall attack surface through whitelisting and blacklisting, and blocking known threats using nextgeneration static prevention, is just the beginning.

In addition to thwarting attacks pre-execution, SentinelOne EPP dynamically detects advanced malware, exploits, and insider/ script-based attacks, and oers fully integrated, intelligent mitigation and remediation capabilities. Organizations can set customized response policies to execute automatically upon attack detection, eliminating threats almost instantaneously from the environment.

We enable complete endpoint and server visibility and intuitive 360-degree attack views.

You can't expect to adequately protect an endpoint device if you can't see exactly what's actually running on it. SentinelOne's lightweight, autonomous agent performs full system-level monitoring of both kernel and user space. Because we see everything that's happening, we can eectively detect the stealthiest attacks on execution, against a full context of normal application and system behavior.

We take everything we monitor and render detailed forensics in real time, complete with an intuitive Attack Storyline that provides critical insights into all events that took place during an attack from its point of origin to its progression across endpoints and other systems.

We protect the broadest range of user endpoint and server platforms — physical and virtual.

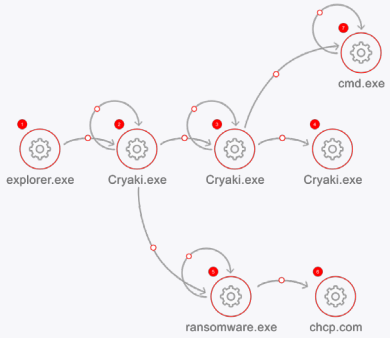
Today's IT environments are comprised of a wide variety of operating systems and endpoint device types. SentinelOne's industry-leading protection extends across Windows, Mac OS, and Linux-based endpoints, and scales easily to protect hundreds of thousands of user endpoints and critical servers across the entire enterprise.

SET MITIGATION POLICIES TO AUTOMATICALLY:

- Alert security personnel
- Kill malicious processes
- Quarantine infected files
- Disconnect compromised endpoints from the network

REVERSE ANY ATTACK-DRIVEN MODIFICATIONS BY:

- Remediating individual endpoint systems
- Rolling back files to pre-attack states



SENTINELONE PROTECTS USER ENDPOINTS AND CRITICAL SERVERS RUNNING:

- Windows 7, 8, 8.1, 10
- Windows Server 2008 R2, 2012 R2
- Mac OS X 10.9.x, 10.10.x, 10.11
- Red Hat Linux, CentOS 6.5 and above, Ubuntu 12.04 and 14.04 LTS

VIRTUAL PLATFORMS

- vSphere
- Microsoft Hyper-V
- Citrix Xen Server, Xen Desktop, Xen App

We deliver TCO up to 5x lower than that of a multi-solution NGEP approach.

Deploying a collection of next-generation endpoint protection solutions that address prevention, detection, and response functions individually involve multiple agents and management consoles, require a greater number of security personnel to manage, and introduce greater overall risk of interoperability issues that threaten productivity. SentinelOne EPP seamlessly combines all critical NGEP capabilities in a single, easy-to-manage platform that involves only one lightweight endpoint agent. SentinelOne EPP's total cost of ownership is up to 5x less than other approaches involving a collection of solutions.

Our solution is backed by our Cyber Guarantee.

SentinelOne is the only Endpoint Protection vendor to financially back its technology. We oer all customers a Ransomware Cyber Guarantee, which mitigates the financial risks (up to $1,000 per endpoint, up to $1M total) of paying ransom to recuperate data in the unlikely event that a ransomware attack can't be prevented or detected by SentinelOne, or if the system cannot be successfully rolled back to its pre-attack state.

CYBER SentinelOne GUARANTEE

SentinelOne
The future of endpoint security

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