SentinelOne

End User Guide

What Sets Us Apart

Immunity with simplicity: for people and organisations, zero day and everyday. **That's what sets us apart.**

SentinelOne liberates you from the suffocating complexity of cyber security, while keeping you safe from cyber attack. And we free your people to work how they want, where they want, with the tools they choose, while protecting them from cyber harm.

The most powerful, simple, and complete endpoint security guaranteed

Look beyond endpoint prevention. SentinelOne uniquely delivers immunity from file AND fileless malware. Plus, we generate massive time savings through the automation of detection and remediation. Protection, detection, and response are delivered in one autonomous agent.

IMMUNITY—
PURE AND SIMPLE

- On every endpoint
- On the widest range of operating systems (including MacOS and Linux)
- Against every type of attack
- At every stage in the threat lifecycle

Tried, tested

Gartner calls SentinelOne a visionary, and Gartner customers that use our product give it an average rating of 94%. NSS Labs' 2018 report says SentinelOne has the lowest TCO of all advanced endpoint protection solutions. We can help you build a compelling business case very easily, and road-test our technology in your environment without disruption. Most that test it, keep it.

Solving your real world problems

NEVER ENOUGH TIME. NEVER THE RIGHT EXPERTISE. Each new generation of cyber technology has added to the global shortage of cyber skills. Your resources are stretched to their limits, every day. We end that trend. SentinelOne's AI-driven automation brings unique simplicity. It saves you time, safeguards resources, and puts expert power and insight within reach of non-specialists.

You're not keeping pace with threat evolution.

The standard approach to evolving threats creates layer upon layer of detection and reporting, leaving you to join the dots. Your critical response times are extending, giving attackers an open window of opportunity.

SentinelOne cuts out the log jam by automating the detection, response and remediation of threats.

You need the freedom to transform

Digital transformation is a huge opportunity, as well as a serious challenge. Cyber security doesn't need to add to your problems.

We offer immunity from file and fileless malware, ransomware and all other exploits, on all endpoints, from day zero. And we make it very simple to live with. With those guarantees, what can't you achieve?

Your end users need freedom of choice

They're employed for their innovation and creativity. They'll choose the tools that let them do their best work, given the chance.

We can cut them loose: with immunity for them, and less work for you. No more whitelisting, for example. Plus, we offer the best end user experience on the market.

Alleviating the pain and suffering of legacy endpoint AV

You're wasting effort on legacy solutions that are a nightmare to manage, users hate, and can only reliably stop known threats.

SentinelOne is a single suite, deployed as a single agent, certified to replace legacy AV. It monitors every process and threat at machine speed, with automated responses to accelerate response and remediation.

Technology – The essential differences

- Two AI engines at the endpoint: a static AI engine to scan files before they've run plus a unique behavioural AI engine to analyse code and processes in action
- Powerful automation driving a three-step process of threat prevention, detection, and remediation
- Unique system roll-back, from the management console, to a clean, unencrypted version of files and content - in seconds
- Deep visibility* - including encrypted traffic visibility - for threat hunting, automated forensics, and auditing
- One, lightweight agent (...not two or sometimes as many as five)
- Parity of protection offline and online
- Deploy from the cloud, on-premise, or in a hybrid infrastructure

THE BIG ADVANTAGES OF AI-DRIVEN BEHAVIORAL ANALYSIS

Use of a static AI is not uncommon. It's a great tool for detecting malicious code, even on day zero. But code is only one attack vector.

The second, **behavioural AI** is unique to SentinelOne. It analyses all running code **and system processes**, using machine learning to benchmark and detect suspicious behaviour, over both short-term and extended timescales.

That makes SentinelOne truly threat agnostic. Some endpoint protection solution are great with particular vectors, but we're expert with all of them.

Moving beyond detection, the behavioural AI automates the response to threats and their remediation at machine speed. Plus it records everything it sees, putting forensic-levels of visibility and detailed reporting at the fingertips even of non-specialists.

Behavioural AI makes it extremely unlikely that a threat will penetrate the endpoint. (But for those rare occasions, there is our equally unique system rollback feature.)

Benefits checklist

Here's a full list of the most important benefits delivered by SentinelOne. See how it compares with your current vendor:

- Complete immunity from ransomware, malware, exploits, fileless malware
- Significant savings in time and skills through automation of threat analysis, response, and system administration
- Consequently, the lowest TCO for endpoint protection (NSS Labs 2018)
- On-demand, deep visibility powered by automated forensics, plus powerful reporting
- Protects endpoints at parity offline and online
- Simply the best end user experience - undetectable in operation, plus greatest level of end user freedom, without compromising security or compliance
- Widest range of Linux, MacOs, Windows and VDI environments supported
- Minimises false positives
- Deploy from the cloud, on-premise, or in a hybrid architecture
- Strengthened GDPR compliance

AV-TEST av-test.org

Leading the Pack in Protection and Performance Over Legacy Players such as McAfee, Symantec and Avast. More

NSS LABS

SentinelOne achieved the 'Recommended' rating from NSS Labs. More

4.7/5 Gartner peerinsights

Hugely positive recommendations in Gartner Peer Reviews

Don't take our word for it; read some of the SentinelOne reviews here