SentinelOne™

# Solving the AV Problem

## AUTONOMOUS ENDPOINT PROTECTION THAT SAVES YOU TIME

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

## Cloud Infrastructure is on the Rise, Security is Lagging Behind

The traditional concept of 'antivirus software', which arose with the first heuristic AV products released in 1987, entered obsolescence sometime early this decade. Industry leaders first began noticing the decline around 2012 when the volume of new malware samples began to outstrip the ability of AV vendors to write new signatures. Both the volume and sophistication of malware has continued to increased exponentially.

By 2014, an executive at a prominent endpoint protection firm famously declared that antivirus was "dead." At the time, contemporaries scoffed at the remark. After all, signature-based endpoint protection products are still on the market, but a look at the trend in malware samples from 2016 shows that things have gotten dramatically worse.

By November 2016, nearly six hundred million unique malware samples had been registered—an increase of 300 million since the year antivirus "died." This increase in malware samples totally outstrips the industry's ability to write individual signatures. What's more, advanced techniques from nation-state actors have begun to filter into the mainstream of the hacking community, and malware authors have begun to spin off their own unique solutions to get around endpoint protection. The volume and sophistication of malware have decisively smothered traditional endpoint protection methods.

In response, several new and established companies have spun off new methodologies, such as endpoint protection and response (EDR), next-gen antivirus (NGAV), and next-gen endpoint protection (NGEP). However, not all of these approaches can fully encompass what's necessary to defend the enterprise the full range of modern threats. Any product that attempts to protect the endpoint in this era of vulnerability can't just target present threats—it must also be future-proof.

SentinelOne™

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043

# The Threats Keep Coming

A common truism in the information security industry is that most hackers are "script kiddies." That is to say, most common hackers are just following directions that other, more advanced users have set out for them. This may be true, but now even the script kiddies have become powerful, armed with novel tools and techniques. More sophisticated hackers have become yet more powerful in turn, and are now employing code inherited from nation-state intelligence agencies. Some of these techniques are simply amplifications of existing methods. For example:

- **Polymorphic malware** - If a malware is recognized by defenders by its hash, name or signature, then it is simple for attackers to generate a new malicious file on every attempt by adding a few bytes to the file. This way, the sample becomes unknown to reputation engines.
- **Supply chain attacks** - threat actors will always look for the easy way in such as by attacking existing proprietary or open-source software on the victim's machine. For example, in September 2017, a backdoored version of CCleaner infected over 2.27 million computers.
- **Packers to compress code** - these obfuscate malware data so it can't be read by security researchers or endpoint protection programs. Many packers are often commercially available. One such packer, Themida, was recently used in malware that was able to take over ATMs and turn them into skimmers.
- **File-less malware** - malicious code that does not require using an executable file on the endpoint's file system besides those that are already there. This makes it far more difficult for traditional AV and other endpoint security products to detect or prevent because of the low footprint and the absence of files to scan.

All of these techniques have been seen in the wild, but new advancements in criminal technology have made them even deadlier. It's best to think of malware authors as a sort of render farm, cranking out iterations of malicious code at rates far faster than enterprises can match. The firm AV-TEST, which is responsible for the chart in the introduction, registers almost 350,000 new malware samples per day.

Each sample represents a unique piece of code, which requires a signature to match. A large AV firm might employ a few hundred engineers to write these signatures—but they could work until the heat death of the universe and still not catch up with the volume. Worse still, these variants are ephemeral. Most malware blinks in and out of existence—shows up, infects, and disappears—before a sample can be written.

- In addition to these techniques, we have seen a reduction in the time between a vulnerability becoming public and the time it is seen in the wild. Highly effective cyber attacks like WannaCry and the use of the leaked EternalBlue occurred within two months of the vulnerability being announced and patched.

- This phenomenon is exacerbated by the rise of the 'dark web', which makes it easy for threat actors to share malware, stolen data and hacking services with little risk of detection. Market places that sell malware, RATS, and ransomware as a service are booming on the dark web, with an estimated 10,000 legitimate ads for such services placed across 25 different shadow trading platforms, according to a study published in 2018.

# Industry Responses

Faced with this avalanche of threats,  the security industry has adopted a number of methodologies in an attempt to address these problems. Each of these recognizes that the idea of finding malware based on its signature is, at best, ancillary to the process of detection, mitigation, and response. Each technique attempts to find a workaround—but not every approach is sufficient. In order to succeed, novel anti-malware techniques can't just protect against present threats. They need to anticipate the future.

## Static AI

This can be an effective method to prevent file execution for known threats, but it has limitations and cannot be relied on as a sole defense. Not only is file-based malware easily adapted to evade existing detection rules, but static AI does not address the increasing problem of fileless malware such as the macroless DDE vulnerability found in MS Outlook and MS Word.

## Server-Side Detection

Some products use client-side monitoring and make all decisions regarding detection and mitigation on the server or in the cloud. This approach has the same disadvantages as any response that does not happen on the endpoint: it requires connectivity. Prevention is impossible because the agent has to wait for the server to respond before acting.

## Tailored Rules (Yara)

Customised 'Yara rules' have allowed some "next generation" security vendors to create various patches in order to claim the ability to address unknown threats. The reality is detecting malicious activity based on only few indicators may be sufficient to demonstrate detection in a controlled test, but there is a real risk of false detections in live deployments.

## Endpoint Detection and Response (EDR)

EDR is now widely recognized as an essential requirement for enterprise networks, with an increasing number of security solutions offering visibility on corporate assets. However, many of these solutions are seen as difficult and complicated to manage by enterprise customers. Equally problematic is the fact that EDR solutions will need more and more human intervention as time goes by because they don't currently protect against more advanced forms of malware, not to mention other types of cyber attacks, such as exploits or script-based attacks. As an example, 38% of all attacks now employ PowerShell, but not all EDR products are able to detect PowerShell-based attacks. EDR products also cannot detect file-less malware, a threat category that has been steadily rising in prominence. Lastly, EDR products attempt to quarantine malware by trapping it inside VMs—but there is already plenty of malware that can escape sandboxes.

In short, key features of EDR are already running behind the present-day reality of malware. With the number and type of threats on the increase, and the lack of highly-trained personnel to deal with them, the modern enterprise needs a solution that can be managed and automated into existing security flows.

## Next Generation Anti Virus

Some security vendors have developed a different approach to shutting down the inherent weaknesses in signature-based detection, with so-called 'Next Generation Antivirus'. This capability is provided by limited machine-learning algorithms to analyze compressed files. If the algorithm suggests that a file will unfold itself into malicious software, then the program takes steps to automatically mitigate and remediate.

Like EDR, this solution fails to take into account more advanced threats such as the rise of file-less malware, and it relies on an outdated understanding of the threatscape. If there are no files to unpack or analyze, this solution would allow attackers to do a seamless end-run around these "next-gen" capabilities. Additionally, the algorithm itself requires constant fine-tuning, which requires manpower.

In the end, both 'Next Generation Antivirus' and EDR run into the same problems. They require too much manpower in an age of limited resources. The only conclusion is that the next generation of malware is already outrunning the next generation of antivirus. A different approach is needed.

# The SentinelOne Solution

## Behavior, Not Identity

**So what can be done to mitigate the ever changing attack landscape?**

The key is to prevent anything that can be prevented pre-execution and to deal with what cannot by looking at the behavior of processes executing on the endpoint.

This is effective because, despite the large and increasing number of malware variants, they operate in very similar ways. The number of malware behaviors is considerably smaller than the number of ways a malicious file might look, making this approach suitable for prevention and detection.

An effective solution needs to cover malware of every variety and description. To be threat-agnostic, multiple layers of prevention and detection are required, backed with the ability to rollback and to provide visibility into any activity on the agent - and to do it cross-platform.

### Broad Protection Against Diverse Modes of Attack

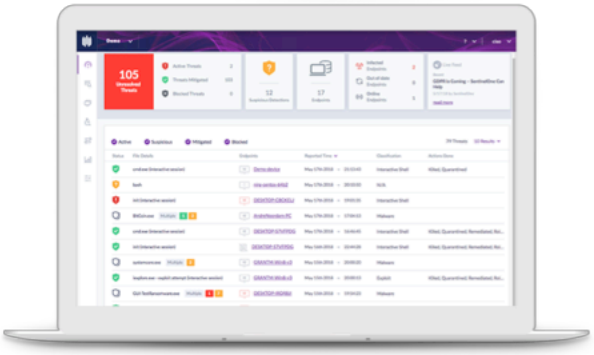
| MALWARE | | EXPLOITS | | LIVE/INSIDER | |
|---|---|---|---|---|---|
| **Executables** Trojans, malware, worms, backdoors, payload-based | **Fileless** Memory-only malware, no-disk-based indicators | **Documents** Exploits rooted in Office documents, Adobe files, macros, spear phishing emails | **Browser** Drive-by downloads, Flash, Java, Javascript, VBS, IFrame/HTML5, plug-ins | **Scripts** Powershell, WMI, PowerSploit, VBS | **Credentials** Mimikatz, credentials scraping, tokens |

# The SentinelOne Solution - How it Works

An effective, streamlined security solution such as offered by SentinelOne combines the tenets of defense-in-depth in a single product—incorporating mechanisms that deal with malware before it executes, while it's executing, and after it has executed. It also lowers costs and improves efficiency, allowing the business to grow without interruption.

## Pre-Execution

SentinelOne's single agent technology uses a Static AI engine to provide pre-execution protection. The Static AI engine replaces traditional signatures and obviates recurring scans that kill end-user productivity.

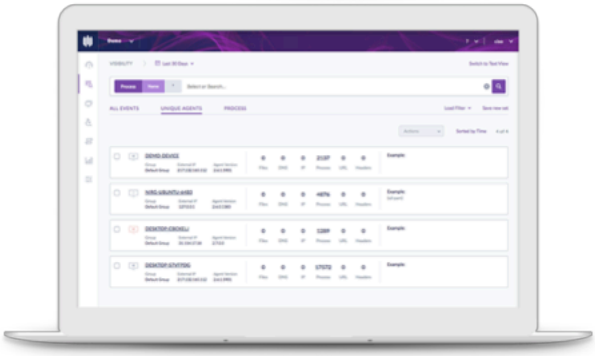


## On-Execution

SentinelOne's Behavioral AI engines track all processes and their inter-relationships regardless of how long they are active. When malicious activities are detected, the agent responds automatically at machine speed.
Our Behavioral AI is vector-agnostic—it doesn't care whether the threat is file-based malware, scripts, weaponized documents, lateral movement, file-less malware, or even zero-days.

## Post-Execution

SentinelOne's Automated EDR provides rich forensic data and can mitigate threats automatically, perform network isolation, and auto-immunize the endpoints against newly-discovered threats. As a final safety measure, SentinelOne can even rollback an endpoint to its pre-infected state.



# The Future is Already Here

## Threat Actors Will Continue to Look for Quick Wins

**Built to stop cutting-edge malware, SentinelOne will remain a relevant security tool–no matter what the future may hold.**

Of course, no one can predict what will happen next, and the only thing known with certainty is that threats will continue to develop as the economics of cyber attacks is in favor of the attackers. This was vividly demonstrated in March 2018, when cyber criminals demanded $52,000 after a crippling ransomware attack on Atlanta City. The city did the right thing, refusing to pay the ransom, but at a cost to taxpayers estimated at over $2.5 million. Few businesses can afford to take that kind of loss, as the criminals well know.

It is not only new and emerging threats that we must be on guard for, but also creative uses of known ways to bypass traditional defenses such as using IOT and other devices connected to the network to gain access and to run code. In short, threat actors will continue improving their techniques and their ability to evade traditional defense.

On top of this, with businesses and users transitioning to the cloud to improve connectivity and ensure maximum productivity, the modern network is built on principles such as Google's BeyondCorp, which shifts access control away from vulnerable firewalls onto endpoint devices. This, however, allows opportunities to utilize endpoint vulnerabilities in order to gain access.

This means enterprises need to be proactive and not just wait for the next security breach to happen. It also means investing in a security layer that exists on the last mile. Such protection should have the following:

- Support all your existing OSs, including cloud and VDI because the attacks are always looking at your weakest link
- Include several types of technologies which can detect in parallel, to achieve separate security layers
- Not rely on a person to run it effectively, including preventing threats
- Integrate with other security solutions on your network - by contributing to others and be contributed from
- Allow visibility to all your assets, because a single view of a device is always weaker than a historical view across your network
- Backup your assets, and test that it's working

With SentinelOne, administrators have access to a single product that provides deep expertise in multiple areas. A single product, it is both a jack of all trades and a master of all trades. SentinelOne protects **Windows**, **MacOS**, and **Linux** systems alike, and, as protection can be carried out by an autonomous agent independent of internet connectivity, it can even protect air-gapped systems. Administrators who choose SentinelOne will have access to a versatile multi platform product which encompasses multiple layers of defense.