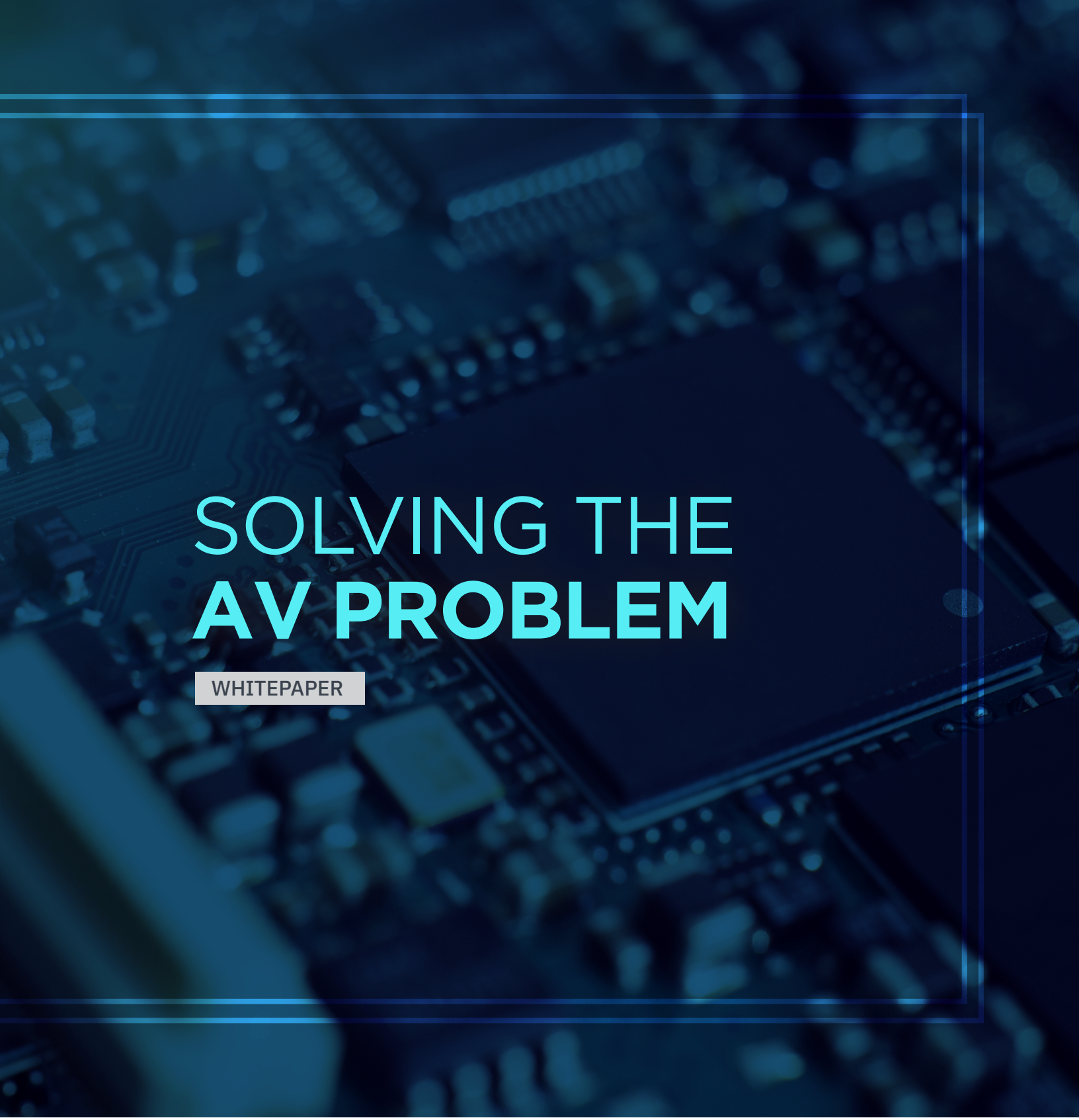


SOLVING THE AV PROBLEM

WHITEPAPER

SentinelOne™

Contents

History **of the AntiVirus**

1987

The traditional concept of antivirus software with the first heuristic AV products released.

2012

The decline of Antivirus effectiveness. The volume of malware samples begins to outstrip the ability of AV vendors to write new signatures.

2014

Top executive at a prominent endpoint protection firm famously declares “Antivirus is dead”.

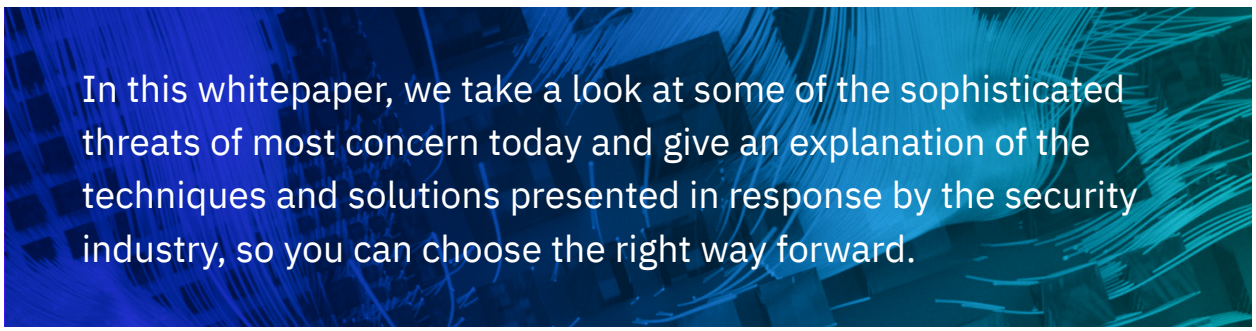
2016

Total unique malware samples exceed six hundred million registered, an increase of 300 million since 2014.

Today....

- The increase in malware samples easily outstrips the industry’s ability to write individual signatures.
- Advanced techniques from nation-state actors filter into the mainstream.
- Malware authors develop unique solutions to get around endpoint protection.
- The volume and sophistication of malware have decisively smothered traditional endpoint protection methods.

In response, several new methodologies and product categories have appeared. These new product categories include endpoint protection and response (EDR), next-gen antivirus (NGAV), and next-gen endpoint protection (NGEP). With so much choice now, how can security professionals easily tell the difference, trust which solution is right and have confidence that history will not repeat itself in the near future.



The threats keep coming, **faster and increasingly novel**

How many times have you heard “most hackers are just script kiddies.”? This phrase makes it sound like there is nothing to worry about. Youngsters practicing their basic skills or following an instruction manual that other, more advanced users have set out.

The reality is that the majority can now arm themselves with novel tools and techniques. The speed of which we see nation-state TTP’s filter down through sophisticated hackers to the masses is accelerating, exacerbated by the rise of the ‘dark web’. Now there is a hidden market place for threat actors to share malware, stolen data and hacking services with little risk of detection. Imagine a dark Ebay, selling malware, remote access trojans, and ransomware as a service. Business is 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.

Some techniques once considered advanced now commonplace include:

- 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.

As there is a marketplace for nefarious digital services, there is now a supply chain for the strategy, manufacture and delivery of attacks. Malware authors can focus on the manufacture and selling of what they are good at - churning 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. Even with 1000 engineers working round the clock, even the largest Antivirus firm cannot catch up with the volume.

In addition to these tools and 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.

Response from **security vendors**

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 (the known). They need to anticipate the future (the unknown).

Static AI Engine

This can be an effective method to prevent file execution for known threats as it can determine if new files are threats before they can execute. Static AI engines do have 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 a 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 EDR solutions offering visibility on corporate assets. Many of these solutions, however, come with drawbacks and can be difficult and complicated to manage by enterprise customers.

EDR solutions need more and more human intervention as time goes by. They don't currently protect against more advanced forms of malware and other types of cyber-attacks, such as exploits or script-based attacks. With direct-to-memory attacks now accounting for over 57 percent of hacks, not all EDR products are able to detect such activity. With PowerShell based attacks and file-less malware rocketing to prominence, attackers can cut the expense and hassle of using malware and glide by defences. EDR products also attempt to quarantine malware by trapping it inside VMs, but this may be bolting the door after the horse has bolted as there is already a vast array of malware that can escape sandboxes.

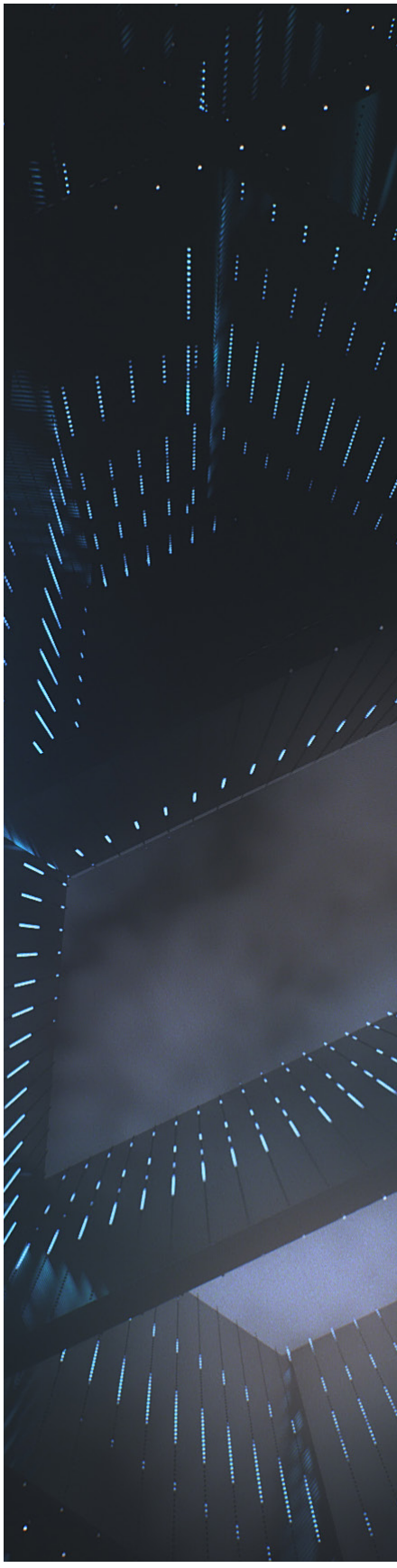
Key features of EDR may be already running behind the present-day reality of threat and poised to cause more problems. With the volume and variety of threats on the increase, and the lack of highly-trained personnel to deal with them, the modern enterprise needs a solution that can be managed and automated into existing security flows.

Next Generation Antivirus (NGAV)

Some security vendors have developed a different approach to the terminal situation in signature-based detection and named it '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.

As with EDR, this solution fails to take into account more advanced threats, it relies on an outdated understanding of the threatscape and can add to the human management overhead. With the rise of direct-to-memory attacks and file-less malware, there are no files to unpack or analyse. NGAV can now allow attackers free reign to run around these "next-gen" capabilities. Buyers should also note that, the algorithm itself requires constant fine-tuning, which requires manpower.

In conclusion, both 'Next Generation Antivirus' and EDR run into similar problems and 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.



Tomorrow's threats require a **new enterprise security paradigm**

SentinelOne | Autonomous AI Platform

One platform to prevent, detect, respond, and hunt in the context of all enterprise assets. See what has never been seen before. Control the unknown. All at machine speed.

REAL TIME
Endpoint Protection

Multiple patented AI algorithms protect against the widest array of threat vectors. Eliminate dependency on connectivity, cloud latency, and human intervention. On-device AI prevents known and unknown threats in real time.

ACTIVE
Detection & Response

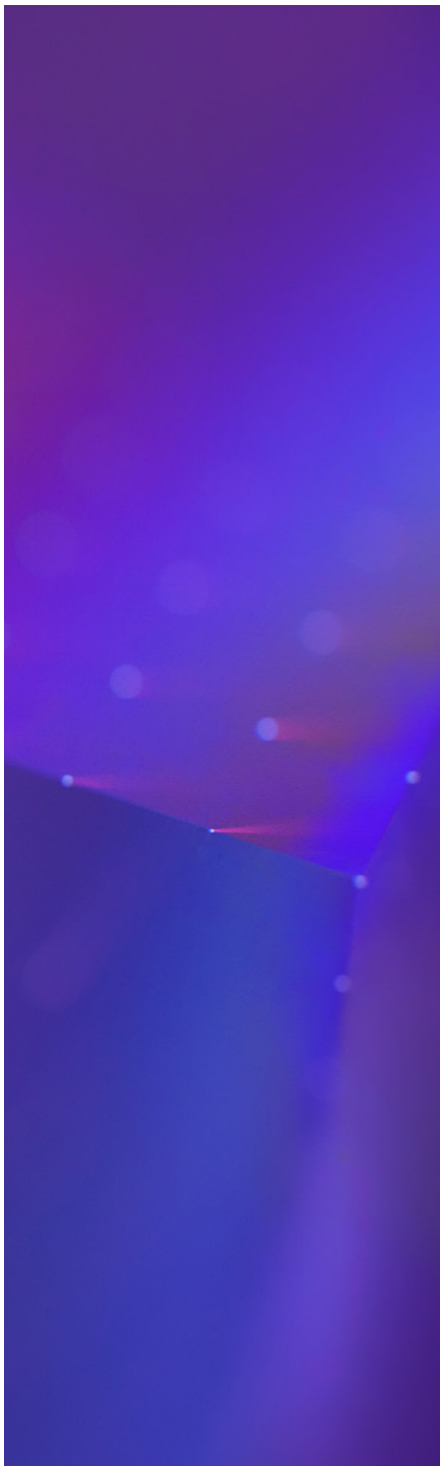
Devices self defend and heal themselves by stopping processes, quarantining, remediating, and even rolling back events to surgically keep endpoints in a perpetually clean state. Hunt more and pivot less.

CLOUD DELIVERED
IoT Discovery & Control

SentinelOne Ranger transforms every device into a sentinel, mapping and enforcing the enterprise IoT footprint. Hunt rogue devices, ensure vulnerability hygiene, and segment devices with dynamic policies.

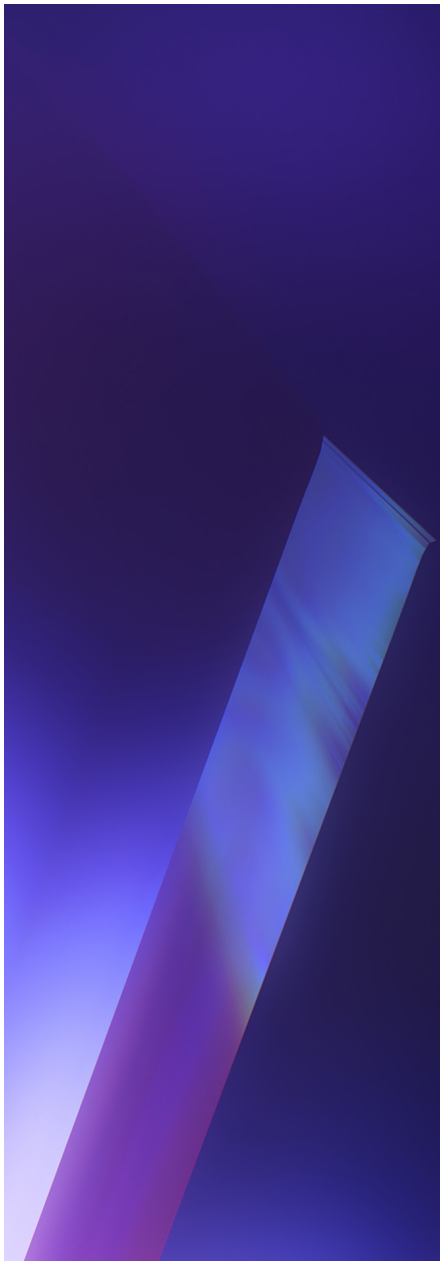
NATIVE
Cloud Security

Deploy autonomous CWPP across cloud, container, and server workloads. The building blocks of your secure cloud transformation are visibility, file integrity monitoring, protection, and compliance.



SentinelOne singularity platform **unite endpoint protection, detection, response and remediation**

Confront the entire threat lifecycle to thwart the impact of attacks on endpoints. The SentinelOne platform delivers the defences you need to prevent, detect and undo known and unknown threats.



Pre-Execution

SentinelOne's single agent technology uses a Static AI engine to provide pre- execution protection. The Static AI engine replaces traditional signatures avoiding 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 is able to 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, invaluable for threats like Ransomware.

Broad Endpoint Protection Against Diverse Modes of Attack

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

The Future is Already Here.

SentinelOne™

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