Next Generation Endpoint Protection

Buyers guide
version 2

SentinelOne™

SentinelOne™

Next Generation Endpoint Protection

Introduction

Today's security landscape

In the past two decades of tech booms, busts, and bubbles, two things have not changed – hackers are still finding ways to breach security measures in place, and the endpoint remains the primary target. And now, with cloud and mobile computing, endpoint devices have become the new enterprise security perimeter, so there is even more pressure to lock them down.

Companies are deploying piles of software on the endpoint to secure it – antivirus, anti-malware, desktop firewalls, intrusion detection, vulnerability management, web filtering, anti-spam, and the list goes on. Yet with all of the solutions in place, high profile companies are still being breached. The recent attacks on large retail and hospitality organizations are prime examples, where hackers successfully used credit-card-stealing-malware targeting payment servers to collect customer credit card information.

Why traditional security is not working

There is a fundamental problem with the security that leaves us basically in the same spot: it is looking for something known - a known hash, IP address, vulnerability, behavior. Ultimately hackers are able to use enough masking techniques to bypass the security software, leaving the server or laptop once again the victim of an attack. It's very easy to alter this malicious code with downloaded or created tools to bypass security measures. Anyone who has basic coding skills can do it. The diagram shows a few attack masking techniques, which are often used in conjunction with each other to take a known binary and cause it to appear completely new, unknown, and benign on the surface.

Along with masking techniques, hackers are using different vectors or paths to deliver the malicious code and carry out their attacks. Top attack vectors are listed to the right. Attacks can be single-vector or part of a multi-vector, more sophisticated attack.

Attack Masking Techniques

Packers
Designed to ensure code runs only on a real machine (anti-virtual machines, sleepers, interactions, anti-debug)

Variations/Obfuscators
Alters known malicious code to make it appear new/different

Malware
The code that runs on the victim's machine

Targeting
Allows code to run only on a specific targeted machine or device with specific configuration

Wrappers
Designed to turn code into a new binary

Is antivirus dead?

Antivirus has been around now for 25 years, yet has not innovated to protect against attacks that use unknown threat techniques. It continues to look for a known hash, and small changes to the hash can bypass the system. Antivirus also overlooks the fact that attacks can be file-less, infecting the memory and writing directly to RAM rather than file systems.

In addition, antivirus is known to not be user-friendly, hogging bandwidth with updates, and spiking CPU with resource-intensive scans. This not only leads to downtime, but often causes users to get frustrated and take strides to disable the software or ignore security warnings.

Sandboxing as a defense?

Approximately 5 years ago, network-based sandboxes began entering the scene. They, in essence, "emulate" the execution of unknown files inside a virtual machine residing on the network and monitor file behavior throughout its execution inside the "protected" environment. While these solutions have been able to increase detection rates of new threats, they are far from being 100% effective.

Attackers quickly realized while their current packing techniques could not be used to bypass the sandbox environment, they just needed to detect the environment, which could easily be done by noticing limited emulation time, lack of user interaction, and only a specific image of the OS. Once the environment is identified, they ensure their malicious code will not run in the emulated environment, will be flagged as benign, and will continue its route to the end device and only run there (where the endpoint antivirus can do little to stop it).

Math-based next-gen AV

There is an abundance of noise around “Next-Generation Antivirus” point products that claim to be developed with ‘predictive mathematics’, ‘machine learning’, and ‘artificial intelligence’. Regardless of whether or not the underlying technology constitutes true A.I., the overall approach (from a security standpoint) is flawed. The industry’s most hyped math-based prevention product is one that will not come close to solving your overall endpoint protection challenges. .

With the new threat landscape, a new model that uses a different approach is needed.

Attack vectors

Malware

Executables

Malware, Trojans, Worms, Backdoors, Payload-based

Fileless

Memory-only malware
No discbased indicators

Exploits

Documents

Exploits rooted in Office documents, Adobe, Macros. Spearphishing emails

Browser

Drive by downloads, Flash, Java, Javascript, vbs, iframe/html5,plug-ins

Live/Insider Threats

Scripts

Powershell, WMI, PowerSploit, VBS

Credentials

Credentials scraping, Mimikatz, Tokens

Five reasons to look beyond math-based AV

1. File-based malware-only half the battle

PE and DLL-based attacks ONLY represent 50% to 60% of new malware observed each week. Prevention-only products will be completely ineffective towards threats that use multiple vectors, especially when they don't even use files, such as:

- Memory-based malware
- Exploits
- Script-based attacks from the inside

2. Some things can't be predicted

The true nature of a file (benign or malicious) can be predicted through statistical analysis of predefined attributes is FAULTY malware is driven by human behavior which makes it nearly impossible to predict what new tactics and techniques attackers will develop next.

3. 99% is not enough

When 99% pertains only to file-based malware, that isn't enough. Even if 99% of file-based malware is blocked, what will you do with the 1%?

If you are being threatened by 100 variants of malware then 99.9% prevention sounds pretty good, but what if there are literally millions?

One new zero-day attack is discovered almost every week, and there are almost 1 million new malware variants released EACH week.

Just ONE of these attacks could cause tremendous financial and reputational damage to an organization.

4. Teaching the A.I. takes time

On initial deployment, there's substantial overhead where security and IT teams need to spend time telling the system what's safe (versus what's not), as the product doesn't use definition files.

It's up to the admin to investigate files based on MD5 hashes and threat intelligence reports, too.

Depending on the environment and the number of IT resources dedicated to the security project, this process could be extremely timeconsuming.

5. No on-prem management option

If your organization adheres to stringent data privacy policies that require it to own its own data, then the industry's most hyped math-based next-generation AV isn't an option for you.

It is strictly cloud-based, with no option to deploy as an on- premise management server.

A new approach to endpoint security

Next generation endpoint protection

In the past couple of years, a new type of technology emerged designed to detect and prevent threats at the endpoint using a unique behaviorbased approach. Instead of looking for something known or it's variant like signature-based detection, next-generation endpoint security is analyzing file characteristics (to uncover known and unknown file-based malware) as well as the entire endpoint system behavior to identify suspicious activity on execution. Endpoint detection and response (EDR) monitors for activity and enables administrators to take actions on incidents to prevent them from spreading throughout the organization. Next-Generation Endpoint Protection (NGEP) goes a step further and takes automated actions to prevent and remediate attacks.

Until recently, administrators have been hesitant to use the protection capabilities because of false positives associated with flagging unusual behavior that isn't malicious. Skype, for example, defies many rules of a 'normal' application, jumping ports and protocols, yet it's a legitimate application often used for business use. The NGEP must have the ability to learn the local systems and environment so it doesn't flag benign behavior.

Next generation endpoint protection as an antivirus replacement

If you're evaluating next-generation endpoint security solutions, you may be thinking it's yet another tool to install and potentially bloat your endpoint (as well as your budget.) And if you're in a regulated industry, you may be required to keep your antivirus and install endpoint protection as an additional layer to protect against new and unknown attacks. Many next-generation endpoint security vendors would actually not claim that they can be an Antivirus replacement. But if the nextgeneration vendor has been tested and certified as meeting Antivirus requirements (and passing the detection test), you can consider replacing your Antivirus with next-generation endpoint security.

To completely replace the protection capabilities of existing legacy, static-based endpoint protection technologies, NGEP needs to be able to stand on its own to secure endpoints against both legacy and advanced threats throughout various stages of the threat lifecycle - pre-execution, on-execution and post-execution. Your Next Generation Endpoint Protection (NGEP) solution needs to address four core pillars that, when taken together, can detect and prevent the most advanced attack methods at every stage of their lifecycle:

Advanced malware detection

Your NGEP must be able to detect and block unknown malware and targeted attacks - even those that do not exhibit any static indicators of compromise. This involves dynamic behavior analysis - the real-time monitoring and analysis of application and process behavior based on low-level instrumentation of OS activities and operations, including memory, disk, registry, network and more. Since many attacks hook into system processes and benign applications to mask their activity, the ability to inspect execution and assemble its true execution context is key. This is most effective when performed on the device regardless of whether it is on or offline (i.e. to protect even against USB stick attacks.)

Mitigation

Detecting threats is necessary, but with detection only, many attacks go unresolved for days, weeks, or months. Automated and timely mitigation must be an integral part of NGEP. Mitigation options should be policy-based and flexible enough to cover a wide range of use cases, such as quarantining a file, killing a specific process, disconnecting the infected machine from the network, or even completely shutting it down. Quick mitigation during inception stages of the attack lifecycle will minimize damage and speed remediation.

Remediation

During execution, malware often creates, modifies, or deletes system file and registry settings and changes configuration settings. These changes, or remnants that are left behind, can cause system malfunction or instability. NGEP must be able to restore an endpoint to its pre-malware, trusted state, while logging what changed and what was successfully remediated.

Forensics

Since no security technology claims to be 100% effective, the ability to provide realtime endpoint forensics and visibility is a must. Clear and timely visibility into malicious activity throughout an organization allows you to quickly assess the scope of an attack and take appropriate responses. This requires a clear, real-time audit trail of what happened on an endpoint during an attack and the ability to search for indicators of compromise.

Evaluating next generation endpoint protection vendors

Evaluation questions

Now that you know what to look for in a next-generation endpoint protection solution, you'll need to start evaluating vendors on your shortlist. Request an evaluation from the vendor, and make sure it's full production software so that you can see how it will actually perform in your environment and against the security test you've outlined. For your evaluation, take the following considerations into account:

1. Is the EPP and EDR solution combined in a single agent to be deployed via traditional software deployment tool and managed/operated via a single central management console?
2. Does the software offer a multi tenancy functionality for endpoints both on premise and in the cloud? For example if a company has two different IT teams that need to manage diverse entities or subsidiaries in different countries, can the software support this and manage the endpoints?
3. For endpoints (including mobile devices, if supported), which operating systems and major operating system versions are supported? For each of these, what are the performance requirements (CPU, memory, storage)?
4. How, in technical methods, does the product detect and prevent attacks from each vector - including malware, exploits, and live/insider threats?
5. How frequently are updates made available? Are updates pushed or pulled to the endpoint?
6. Do the updates require any user intervention (i.e. reboot?)
7. Can the product prevent threats if the endpoint is offline from the network?
8. How scalable is the product? How many clients can be supported by each management console?
9. Is the management server cloud-based or on-premise?
10. What is done to prevent false positives and learn benign system behavior?
11. What is the current false positive rate?
12. Do they integrate with SIEM systems for incident management?
13. Are there prevention policies to protect against threats in real-time?
14. What levels of contracted support does the endpoint protection vendor provide?
15. Are software updates and upgrades part of the licensing fee?

Why SentinelOne?

A brief history

SentinelOne was founded by a group of international defense and intelligence experts who saw the need for a dramatic new approach to endpoint protection. Today, our growing global team remains dedicated to constant innovation.

SentinelOne endpoint protection platform

SentinelOne's The SentinelOne Endpoint Protection Platform (EPP) offers organizations real-time, unified endpoint protection that unifies prevention, detection and response in one platform managed via a single console. SentinelOne EPP leverages advanced machine learning and intelligent automation to protect Windows, OS X, and Linux-based endpoint devices from threats across all major vectors: advanced malware (file- and memory-based), exploits and stealthy script-based attacks. It closely monitors every process and thread on the system, down to the kernel level. A view of system-wide operations - system calls, network functions, I/O, registry, and more - as well as historical information, provides a full context view that distinguishes benign from malicious behavior. Once a malicious pattern is identified and scored, it triggers an immediate set of responses ending the attack before it begins.

Responses include:

Mitigation

Easy-to-configure policies that kill the process, quarantine or delete malicious binaries and all associated remnants, and remove the endpoint from the network.

Immunization

As soon an attack is prevented, details are immediately shared to other endpoints within the network, immunizing those systems that might be part of a coordinated attack.

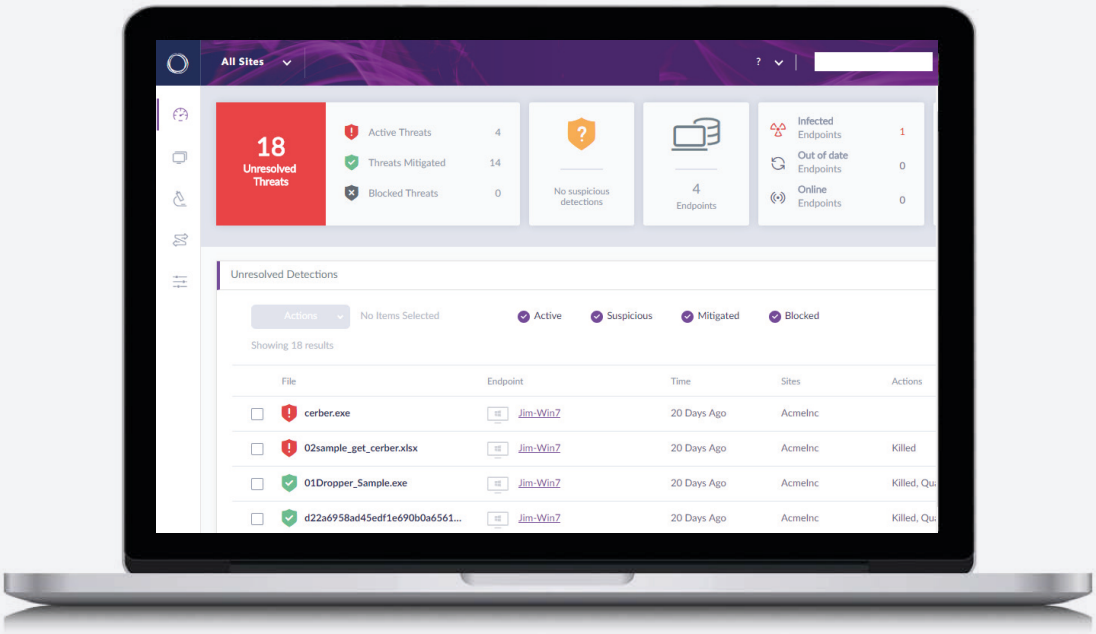
Remediation

Automatically restore deleted or modified files to their pre-attack state.

Forensics

A 360-degree view of the attack including file information, path, machine name, IP, domain, and more (available within SentinelOne or through your SIEM)

In addition, SentinelOne EPP is a single, lightweight solution that uses an average of 1-2% CPU, so endpoints are able to do what they're supposed to do - be a laptop, desktop, mobile device, or server. As it focuses on what's right for each system, no signature updates/active scans are needed, and endpoints are always protected, whether you're on or off the network. SentinelOne EPP is supported on major mobile, desktop/ laptop, and server operating systems.



Certified antivirus replacement

AV-TEST, a leading independent anti-virus research institute, has awarded SentinelOne EPP the Approved Corporate Endpoint Protection certification for both Windows and OS X, which validates its effectiveness for detecting both advanced malware and blocking known threats. SentinelOne EPP is the only next generation endpoint protection vendor to obtain this certification on both platforms.

SentinelOne EPP has also been validated against PCI-DSS and HIPAA by third-party compliance assessor, Tevora. This validation now enables enterprises to replace their existing corporate antivirus suites with SentinelOne EPP and still meet PCI and HIPAA compliance requirements.

SentinelOne™

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