Next Generation Endpoint Protection

Buyer's Guide

SentinelOne

Contents

INTRODUCTION 3
Today's Security Landscape
Why Traditional Security is Not Working
Is Antivirus Dead?
Sandboxing as a Defense?

A NEW APPROACH TO ENDPOINT SECURITY 5
Next Generation Endpoint Protection
Next Generation Endpoint Protection as an Antivirus Replacement
Six Things Your NGEP Must Do

EVALUATING NEXT GENERATION ENDPOINT PROTECTION VENDORS 7
Evaluation Questions
Licensing

WHY SENTINELONE? 8
A Brief History
SentinelOne Endpoint Protection Platform
AV-Test Certification
Testimonials
Next Steps

SentinelOne

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 to the right 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

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).

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 disc-based 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

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 behavior-based approach. Instead of looking for something known or it's variant like signature-based detection, next-generation endpoint security is looking at the system behavior to identify suspicious activity. 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 next-generation 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 attack lifecycle.

Six Things Your NGEP Must Do

Your Next Generation Endpoint Protection (NGEP) solution needs to address six core pillars that, when taken together, can detect and prevent the most advanced attack methods at every stage of their lifecycle:

1

Known Attack Prevention.

We explored above how only looking for known threats won't protect against variants or unknown attacks, but coupling it with additional security layers can pre-emptively stop known threats before they can execute on endpoints. However, instead of relying on a single vendor's intelligence, make sure your NGEP uses a vast collection of reputation services to proactively block threats and bad sources. Be sure the NGEP vendor uses data from the cloud, indexing files for passive scanning or selective scanning to keep it lightweight, instead of performing resource-intensive system scans.

2

Dynamic Exploit Detection.

Hackers often use exploits to target code-level vulnerabilities so they can breach systems and execute malware. Drive-by downloads are a common vector for carrying out exploit attacks. NGEP should provide anti-exploit capabilities to protect against both application and memory-based attacks. This should be achieved by detecting the actual techniques used by exploit attacks - for example: heap spraying, stack pivots, ROP attacks and memory permission modifications - not by using methods that are dependent on static measures, like shellcode scanning. This approach is much more reliable in detecting unknown attacks, since the exploitation techniques themselves are not as easy to change or modify as the shellcode, encoder, dropper and payload components used in malware.

3

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.)

4

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.

5

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.

6

Forensics.

Since no security technology claims to be 100% effective, the ability to provide real-time 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. 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)?
2. How, in technical methods, does the product detect attacks from each vector - including malware, exploits, and live/insider threats?
3. How frequently are updates made available? Are updates pushed or pulled to the endpoint? Do the updates require any user intervention (i.e. reboot?)
4. Can the product prevent threats if the endpoint is offline from the network?
5. How scalable is the product? How many clients can be supported by each management console?
6. Is the management server cloud-based or on-premise?
7. What is done to prevent false positives and learn benign system behavior? What is the current false positive rate?
8. Do they integrate with SIEM systems for incident management?
9. Are there prevention policies to protect against threats in real-time?
10. What levels of contracted support does the endpoint protection vendor provide? Are software updates and upgrades part of the licensing fee?

LICENSING

Typically, endpoint protection products are purchased as licenses per user or per endpoint, often in 1-year, 2-year or 3-year increments. Vendors typically offer volume discounts for larger environments. License costs vary, but are usually $30 to $70 each, depending on the vendor and number of licenses purchased. The cost can be deceptive, as some endpoint protection products may provide narrow functionality that requires additional products to be installed. Weight the cost in terms of functionality and how many products you have to install for total endpoint security.

Why SentinelOne?

A BRIEF HISTORY

SentinelOne was formed by an elite team of cyber security engineers and defense experts who joined forces to reinvent endpoint protection. With decades of collective experience, SentinelOne founders honed their expertise while working for Intel, McAfee, Checkpoint, IBM, and elite units in the Israel Defense Forces. They came together in 2013 to build a new security architecture that could defeat today's advanced threats that come from organized crime and nation state malware.

SENTINELONE ENDPOINT PROTECTION PLATFORM

SentinelOne's Endpoint Protection Platform is an all-in-one endpoint security solution that provides protection against known and unknown attacks by identifying and mitigating malicious behaviors at machine speed. 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:

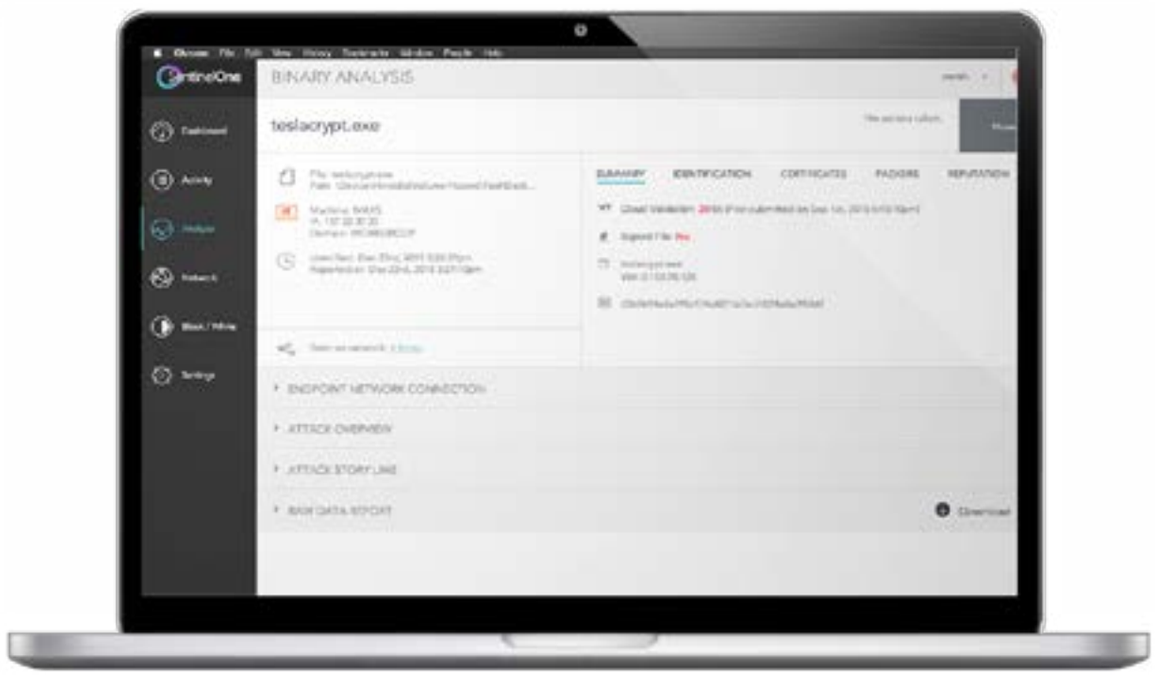
Mitigation - Easy-to-configure policies that kill the process, quarantine or delete malicious binaries and all associated remnants, and remove the endpoint from the network.

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.



TESTIMONIALS

"Protecting endpoint devices from increasingly sophisticated threats is a critical point of focus, since many of these can now bypass traditional signature-based security approaches. I am really impressed with SentinelOne's ability to monitor all processes on a device, whether it is on or off the corporate network, and detect malware based on its behavior. I believe this new model is needed to protect against advanced malware that is invisible to outdated anti-virus systems."

—Ben Carr, *Director of Information Security, VISA*

citibank

"SentinelOne is bringing true innovation to endpoint protection. I am continuously on the lookout for advanced IT security technologies. Their ability to replace aging signature-based anti-virus with dynamic execution inspection that can detect and protect against advanced malware and zero day threats represents a major advancement for endpoint security."

— Doug Shean, *Senior Vice President, Citibank*

CONDE NAST

"The amount of malware is continuing to increase while existing anti-virus software is struggling to provide effective protection. SentinelOne's new approach is helping solve a widespread problem which the industry has been grappling with for some time. Knowing SentinelOne is certified by third-party AV testing organization AV-TEST gives me the confidence that it represents a viable option to replace anti- virus solutions."

— Craig Holland, *CISO Conde Nast*

LCRA
ENERGY • WATER • COMMUNITY SERVICES

"The SentinelOne EPP solution delivers much needed innovation to endpoint protection in an industry that has struggled to keep pace with the amount of new malware and variants. My confidence in SentinelOne has deepened given their unique approach doesn't rely on signatures, and they are certified by the well-respected AV-TEST Institute."

— Larry Whiteside Jr., *Chief Security Officer, Lower Colorado River Authority*

AV TEST

AV-TEST CERTIFICATION

AV-TEST, a leading independent anti-virus research institute, has awarded SentinelOne EPP the Approved Corporate Endpoint Protection certification for both Windows and OSX, which validates its effectiveness for detecting both advanced malware and blocking known threats. This validation now enables enterprises to replace their existing corporate antivirus suites with SentinelOne EPP and still meet compliance requirements, such as PCI DSS. SentinelOne EPP is the only next generation endpoint protection vendor to obtain this certification.

NEXT STEPS

To request a SentinelOne Endpoint Protection Platform evaluation, fill out the Contact Us form and a customer representative will get back to you shortly.

For more information on SentinelOne, please visit **www.sentinelone.com**.