SentinelOne

Enterprise Protection Platform for PCI DSS & HIPAA Compliance

SentinelOne

SentinelOne was founded in 2013 with a vision to develop new and groundbreaking, next generation endpoint protection solutions for enterprises.

Audience

- **Organizations**
- **PCI DSS QSAs**
- **HIPAA Internal or External Auditors**

Overview

SentinelOne partnered with Tevora, a security and risk management consulting firm, a known PCI Qualified Security Assessor (QSA) and HITRUST Assessor, to conduct a detailed evaluation and assessment against their next generation ant-virus software to ensure it meets or exceeds the various compliance requirements facing organizations today.

This paper outlines SentinelOne's functionality and how it meets the applicable PCI DSS 3.1 and HIPAA Security Rule requirements.

This paper describes how SentinelOne's Enterprise Protection Platform software satisfies the application of PCI DSS 3.1 Requirement 5 and HIPAA Security Rule requirement 164.308(a)(5)(ii)(B), decreases organizational risk by evaluating malware based on system behavior, and reduces malware exposure to organizations.

Failures of Traditional AV

"Today's advanced malware, exploits, and other cyber attacks will blow right by AV-based protection in a fraction of the time it takes to get updated with the latest threat signatures."

Traditional verses Next-Gen Anti-Virus

Over the past two decades there has not been a significant evolution in traditional anti-virus solutions and how they handle malicious software. Most traditional solutions are vague in their claims to be the best at protecting against zero days and obfuscated malicious software.

At the core of every anti-virus solution there are typically three stages that aid in the detection of malicious software:

Three Phases of Traditional Virus Detection:

- Background Scanning
- Full System Scanning
- Virus Definitions

Background Scanning

With traditional AVs, there is a severe degradation in end user experience, is when a system or person opens a file, plugs in a USB drive, mounts a volume, or downloads a file. Pass this phrase through a search engine and the top results will lead you to why background scanning is no longer necessary, or how to disable it. In its core essence background scanning does exactly what the name implies. It performs a rescan of the entire end point with current anti-virus signatures.

Full system scanning

When configured correctly, system scanning is performed as a low priority task. These scans are on demand and check updated anti-virus signatures against system memory, programs loaded at startup, backups, hard drives, removable storage and network drives.

Virus Definitions

These signatures are what tie background scanning and full system scans together. These reputations based methods have become better over the years. However, the way the signatures analyze binaries to determine whether malicious or not have been found to not be very effective. This typically involves some form of static and dynamic analysis being used in conjunction to emulate the execution of an application within a sandbox.

So What's Different About SentinelOne Enterprise Protection Platform?

Enterprise Protection Platform uses multiple AI engines to protect you against threats. This signature-less approach requires no daily/weekly updates, recurring scans and performs better. SentinelOne's Static AI Engine analyzes files pre-execution and quarantines the ones that are classified as threats. This classification is done without the use of traditional signatures.

SentinelOne's behavioral AI engine gains insight into every process on the system at the kernel level to extract all relevant operations data. This includes system calls, network, IO, registry, and more. This allows the behavioral engine to monitor the behavior of every process that executes on the system. Having this insight allows SentinelOne to provide many response options that can be tailored to each organization's incident response plan.

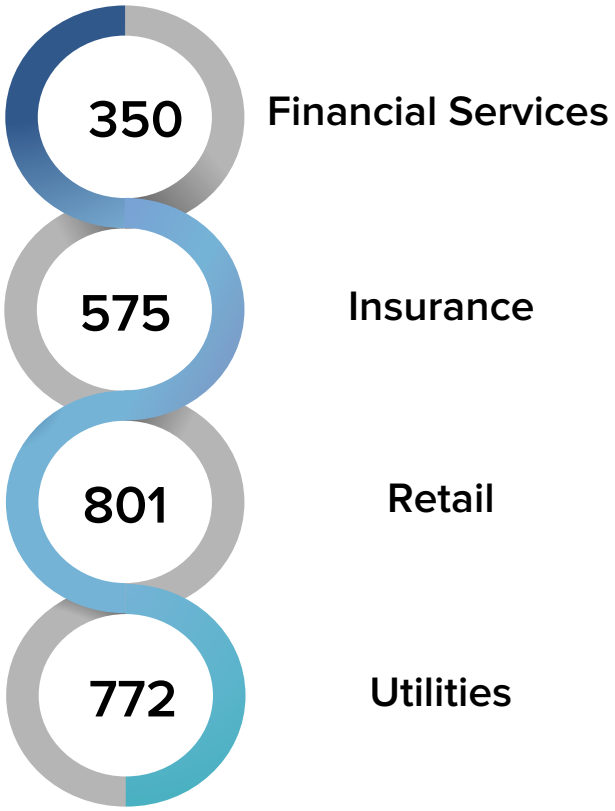
Compliance Challenges

Various compliance standards necessitate some very specific language in terms of requirements for anti-virus solutions. This is why it is more common to see the phrase "endpoint protection solutions" as an offering. However, when one digs into the feature sets of a next generation endpoint protection offering, they typically find one requirement such as the inability update virus definitions barring their organization from really choosing a solution that suits their needs. Instead traditional anti-virus solutions are then chosen that have been proven to be less than 50% effective.

70-90%

Of malware samples are unique to an organization

Weekly average number of malware events per industry:



HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that Covered Entities must take strong measures to protect the privacy and security of health information. At the endpoint, this translates to ensuring the host is protected from malware. Specifically, the HIPAA Security Rule Administrative Safeguards - §164.308(a)(5)(ii)(B), requires Covered Entities and Business Associates to implement and maintain procedures to protect, detect, and report on malicious software throughout the environment.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

PCI DSS

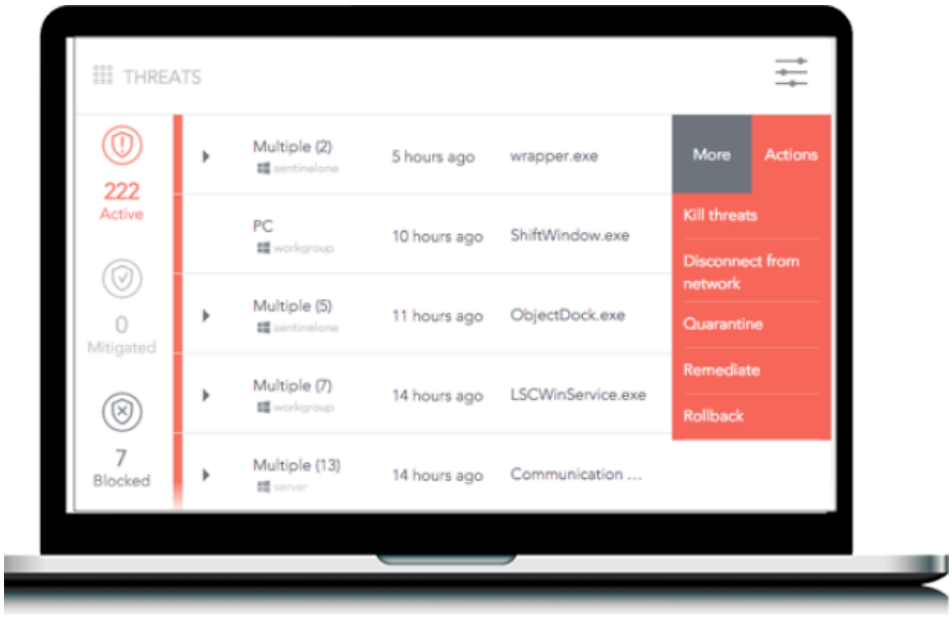
The Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data wherever it resides to ensure that members, merchants, and service providers maintain the highest information security standard. PCI DSS is a set of comprehensive requirements for enhancing payment account data security. The standard was developed by the founding payment brands of the PCI Security Standard Council, in an effort to help facilitate the broad adoption of consistent data security measures on a global basis. PCI DSS Requirement 5 requires the protection of all systems against malware.

Did You Know?

The HHS civil rights office, or OCR, is authorized to impose penalties of more than $50,000 per HIPAA violation.

SentinelOne Enterprise Protection Platform Overview

Enterprise Protection Platform's Static and Behavioral AI engines, system level monitoring, endpoint forensics, and cloud intelligence design delivers strong protection against both known and unknown malware, to effectively defend organizations from today's advanced threats. Endpoint Protection Platform effectively detected, prevented, and removed all malware infection attempts during the assessment. Tevora evaluated the four primary features of the platform: Detection, Protection, Reporting and Features in the Platform during the assessment.

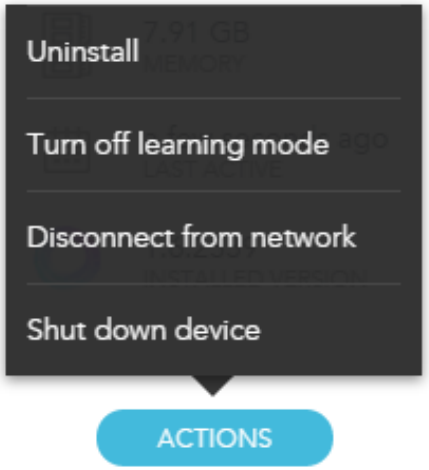


Detection

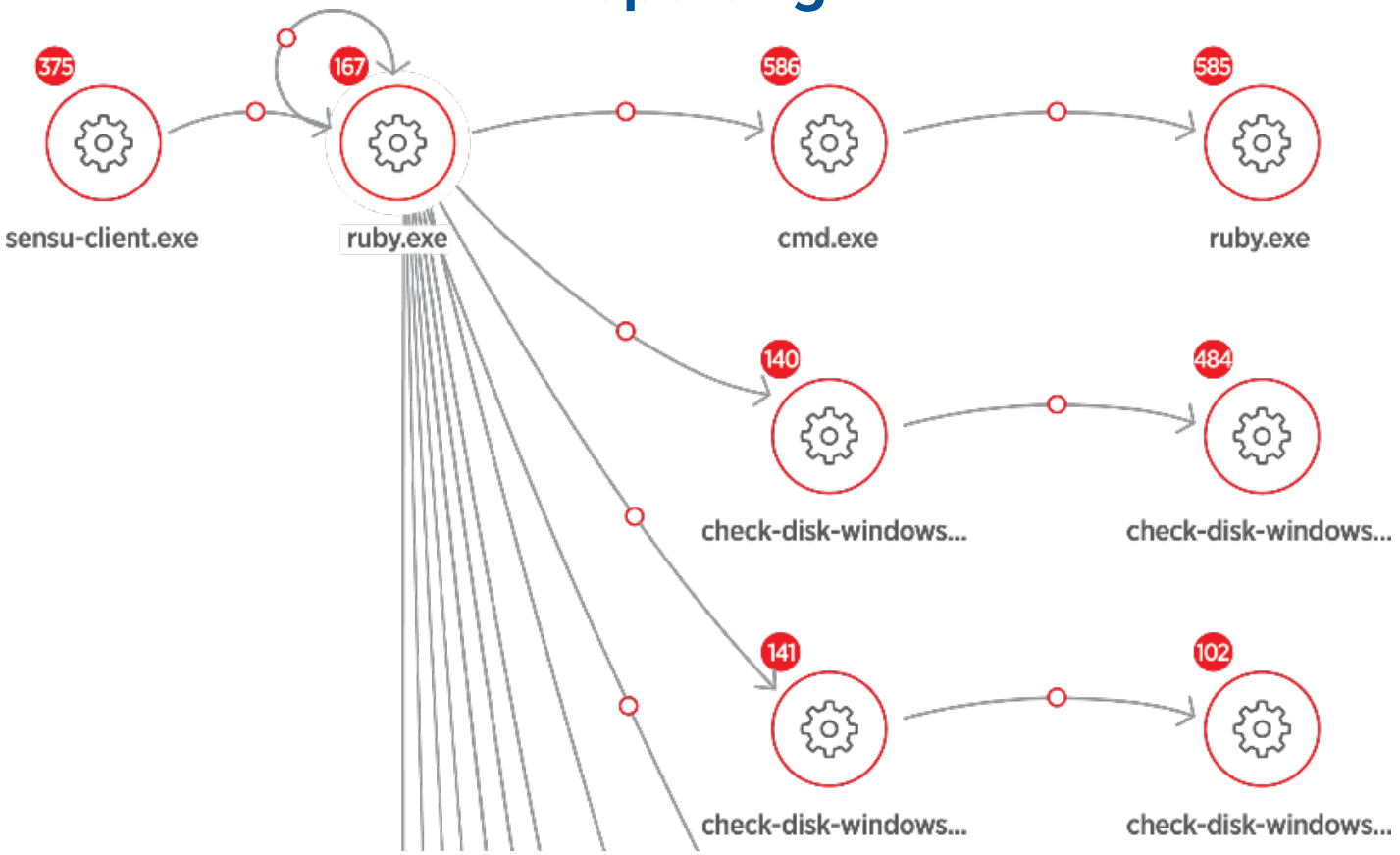
With behavior learning and cloud intelligence, Enterprise Protection Platform quickly and easily identifies both known and unknown malware and suspicious software.

Protection

With system level monitoring, Enterprise Protection Platform prevents malware from accessing system resources and stops the execution flow of malicious payloads. Based on policies, Enterprise Protection Platform can perform automated containment and mitigation of threats including proactively disconnect a host from the network to prevent malware from infecting other hosts or kill, quarantine threats.



Reporting



The management console provides real-time reporting for active threats, running processes, configurations changes, and network activity. Additionally, Enterprise Protection Platform provides email and SMS notifications, and log forwarding for SIEM integration.

Feature Rich Platform

With additional features not found in traditional endpoint protection solutions, such as whitelisting, blacklisting, and rollback mitigation actions, Endpoint Protection Platform provides more than just compliance; it provides one of the most robust endpoint protection solutions on the market.

Technical Analysis Methodology

Tevora leveraged a series of industry-accepted tools, techniques and virus databases to evaluate the SentinelOne Enterprise Protection Platform. The below sections identify the sources and technical evaluation used to validate the platform meets or exceeds the PCI DSS v3.1 and HIPAA Security Rule requirements.

Malware used to launch DoS attacks jumped from #8 to #2 in threat action variety in 2015

Testing Overview

Tevora's analysis of SentinelOne Enterprise Protection Platform consisted of assessing the solution with the following considerations in mind:

- Testing of all PCI DSS section 5 requirements regarding the protection of all systems against malware and regularly updated anti-virus software or programs
- Testing of all applicable HIPAA Security Rule requirements regarding the protection of all systems against malware and regularly updated anti-virus software or programs
- Review and testing of any PCI DSS and HIPAA Security Rule requirements regarding the implementation and use of anti-virus software within the environment.

Solution Effectiveness

Tevora assessed SentinelOne Enterprise Protection Platform for overall malware protection effectiveness, product scalability, and ease of management.

The following malware sources were utilized to assess SentinelOne Enterprise Protection Platform effectiveness to stop both known and unknown malware:

- Malware provided by SentinelOne
- Malware samples provided from FireEye
- Various malware repositories
- Various common payloads such as Meterpreter using common encoding techniques such as Shikata ga nai

SentinelOne Enterprise Protection Platform was assessed on the following operating systems to determine feature parity, scalability, and ease of management:

- Windows Operating Systems 7, 8.1, and 10
- Mac OS X (10.11) El Capitan

Testing Results

Since anti-virus is often used as a preventative control for user decisions, Tevora wanted to track the effectiveness of SentinelOne's Enterprise Protection Platform against new malware samples that were received from various sources.

Tevora began testing to ensure that SentinelOne was capable of detecting, removing, and protecting against all known types of malicious software. Testing efforts focused on the Alert, Kill, and Quarantine Action Mode's in the setting interface. It was found that all malware samples were detected. While Quarantine mode behaved most like a traditional anti-virus solution, immediately identifying malicious files and isolating them from the test system. We found during testing that all action modes resulted in the ability to detect, remove, and protect against all sampled malware.

The next portion of the testing was to check and ensure that all anti-virus mechanisms are able to be kept current, perform periodic scans, and generate audit logs. In a time where anti-virus solutions are found to be less than 50% effective, SentinelOne ensures that it is always up to date, checking file hashes against reputable sources such as VirusTotal. Using this method, SentinelOne's platform does not suffer the traditional time lapse in needing to push out new definitions. This process tends to create a vulnerable gap in organizations who deploy traditional anti-virus solutions. It was however found during testing that SentinelOne does not have the capability of performing periodic scans, but instead offers a continuous monitoring approach that constantly inspects the operating system for changes. SentinelOne will introduce a system scan capability in 2017.

SentinelOne is capable of generating reports and utilizes Syslog to send the reports in a variety of formats to make integration into an organization's SIEM a breeze. Additionally, these logs are not sent over traditional insecure channels such as UDP, which is insecure. Organizations who use SentinelOne have the additional capability to transmit these logs over SSL, which fulfill another PCI-DSS requirement in ensuring the integrity of the files.

Our final test was to ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users. Testing started with a local administrator account and attempted to bypass the built in anti-tamper protections using methods that would be most commonly found in an enterprise environment. After being unsuccessful in disabling SentinelOne, we attempted to uninstall the software. SentinelOne agents are able to be removed via online and offline methods. The online method would send a request to the administrator who is able to approve the request to have the agent removed. The offline method requires a verification key. Both attempts to remove the software were unsuccessful.

PCI & HIPAA Control Requirements

PCI DSS 3.1	SentinelOne Endpoint Protection Platform
Requirement 5.1: Deploy anti-virus software on all systems commonly affected by malicious software	With a wide range of supporting agents, SentinelOne's Endpoint Protection Platform supports many modern operating systems that are commonly found in organizations. Supported operating systems include: Windows 7, 8, 8.1, 10 Windows Server 2008 R2, 2012 R2 OS X 10.9.x, 10.10.x.
Requirement 5.1.1: Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	SentinelOne capabilities include the ability to guard against malicious software by leveraging leading cloud reputation services and kernel level monitoring. When malicious files are detected, alerts are generated on the end point are reported to the management console. Utilizing a behavioral engine and organizations policies, SentinelOne can take automated or manual mitigation actions upon detection. Administrators can select from a variety of methods for addressing malicious software including: quarantining, killing malicious processes, blacklisting, and rollback mitigation.
Requirement 5.2: Ensure all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs which are retained per PCI DSS requirement 10.7.	SentinelOne is kept up to date by leveraging leading cloud reputation services which are sent hashes of suspected suspicious files. The continuous monitoring function, paired with other protection features, goes above and beyond the original intent of performing periodic system scans. Audit logs are generated by the agents and sent to the centralized server to provide real-time endpoint forensics. Logs can be sent to an organizations SIEM allowing for further investigation. In 2017, SentinelOne will introduce the ability to initiate full disk scans from the console and also do this on a scheduled basis.
Requirement 5.3: Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically	Agent anti-tamper safeguards actively protect against unauthorized uninstallation or disabling of SentinelOne Endpoint Protection Platform.
HIPAA Security	**SentinelOne Endpoint Protection Platform**
§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software	SentinelOne capabilities include the ability to guard against malicious software by leveraging leading cloud reputation services and kernel level monitoring. When malicious files are detected, alerts are generated on the end point are reported to the management console. The reports generated by the agent are stored on an encrypted file system on the management server and can be easily forwarded to an organization's SIEM for further investigation. Additionally, SentinelOne includes the capability to alert administrators by both e-mail and SMS text message.

Assessor's Conclusion

Tevora attests that SentinelOne's Enterprise Protection Platform meets all detection, prevention, and reporting requirements for the HIPAA Security Rule and HITECH when properly implemented within an organization's environment. In addition to being 100% complaint with HIPAA Security Rule Requirements for malware protection.

Tevora also found that SentinelOne's Enterprise Protection Platform meets most PCI DSS 3.1 requirements. SentinelOne provides the ability to detect, remove, and protect against all known types of malicious software. Additionally, it has the ability to be kept current and generate audit logs, as well as deploys anti-tampering mechanisms to ensure that users are not able to disable or alter SentinelOne agents.

Tevora assessed SentinelOne's ability to continuously monitor system events as Enterprise Protection Platform does not provide the ability to perform periodic, full system scans. The continuous monitoring function paired with other protection features, such as their whitelisting feature, goes above and beyond the original intent of performing periodic system scans. Utilizing a behavioral engine, preventative detection, along with whitelisting will detect and take automated mitigation actions on known and unknown threats that can be tailored to an organizations policy.

Overall Tevora found that SentinelOne's Enterprise Protection platform provides a robust endpoint protection solution to meet the information security needs of any organization.

SentinelOne