TEVORA™

SentinelOne Endpoint Protection Platform

By David Grazer, Lane Krejcik

22 February 2019

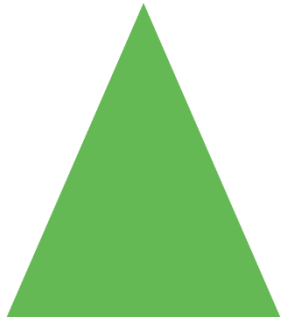

Table of Contents

Endpoint Protection Platform for PCI DSS & HIPAA Compliance

Overview

SentinelOne retained Tevora, a security and risk management consulting firm, and a reputable PCI Qualified Security Assessor (QSA) and HITRUST Assessor, to conduct an independent, in-depth evaluation of SentinelOne's anti-malware Endpoint Protection, Detection, and Response Platform (SentinelOne Platform) and software against PCI DSS version 3.2.1 Requirement 5, and HIPAA Security Rule requirements 164.308(a)(1), 164.308(a)(5)(ii)(B), and 164.308(a)(6)(ii).

This paper describes the functionality of the SentinelOne Platform, and how the solution dynamically prevents, detects, and responds to cyberattacks. SentinelOne performs automated SOC functions such as blocking malware, providing root-cause investigation, correlation and remediation of suspected threats, and performing automated mitigation of cyberattacks. Furthermore, this report outlines the specific ways in which the SentinelOne Platform can bring organizations in line with PCI DSS Requirement 5 and HIPAA's malware protection, and security event response and reporting requirements.

The Current Endpoint Security Marketplace

EPP vs EDR

Over the last decade, the evolution of traditional, signature-based anti-virus (AV) has been slow and incapable of responding to the rapid pace of the threat landscape. In recent years, the rate of innovation is accelerating with next-generation endpoint protection products utilizing new techniques. Typically these solutions are capable of malware prevention using machine learning and are now starting to converge with response capabilities, known as Endpoint Detection and Response (EDR). Next-generation solutions can help satisfy HIPAA and/or PCI DSS requirements and reduce operational overhead.

EPP

EPP solutions rely on two primary features:

1. Background scanning
2. Full system scanning

Background scanning consists of anti-malware software scanning downloaded files, plugged-in hard drives, mounted drives, and other non-volatile storage, searching for malware traces and comparing files and hashes to known virus signatures. This process is known for slowing system speeds due to the intensive processing it requires, especially for hard disk drives.

Full system scans are similar in nature, except they iterate over every file on the endpoint in the hunt for known viruses.

All traditional EPP solutions work in the same way: perform a background or full system scan and compare all against known virus signatures. Frequent updates to the signature databases are required and create user friction during updates and constant risk of missed detections. Traditional EPP solutions neglect to protect against unknown or emerging malware.

EDR

EDR solutions provide an alternative approach to endpoint protection. Leading EDR solutions track system events, identify trends in behaviors, and, if anomalies are detected, provide the tools to create alerts for further investigation and remediation typically performed by an expert analyst in a SOC. Sophisticated EDR solutions can often assume many of the manual remediation responsibilities normally performed by dedicated security operations center (SOC) personnel.

A SOC requires significant overhead often outside of the budget for many enterprises. The SentinelOne Platform eliminates much of the pain with its unified EPP and EDR functionalities, designed to perform prevention, detection, and automated remediation in addition to forensic investigation and threat hunting. Further, while EDR does not adhere to the traditional scheduled

scanning standards set-out in PCI and HIPAA, it does operate in a state of constant-scanning. Real-time visibility and response, coupled with prevention, aligns organizations with compliance standards and a proactive posture towards addressing threats.

SentinelOne Platform: A Compliance Champion

SentinelOne's Platform takes a hybrid approach to achieve the ultimate in endpoint protection and fulfill an organization's compliance requirements. SentinelOne employs four key features:

I. EPP

II. ActiveEDR

III. Suite features like device control, firewall control, and vulnerability management

IV. Advanced threat hunting tools and techniques

SentinelOne applies a methodical approach to threat detection and response, calling each feature at precisely the right moment. EPP features are launched during pre-execution of processes to prevent attacks, and ActiveEDR (powered by patented TrueContext™ technology) is triggered on-execution to track, identify, correlate, contain, and remediate the potential malicious activity.

The SentinelOne Platform also enables full remediation and even a rollback to pre-infected system state. SentinelOne's advanced EDR kicks in for in-depth visibility and hunting, by providing deep visibility into all system behavior activities. This SOC-like functionality determines if the investigated system may be the victim of zero-day attacks, regardless of network connectivity.

How Does SentinelOne Help Customers Meet Compliance Requirements?

Overview

Threat prevention, detection, and response (containment, remediation, investigation, analysis) are integrated through static and behavioral AI engines which 1) constantly monitor all activities on the endpoint to detect malicious activities, and 2) automatically remediate malicious activity – with both processes happening in real time. Today's SentinelOne Platform gives businesses the tools they need to secure their data and systems, using minimal effort to achieve compliance.

Tevora performed an in-depth evaluation of the SentinelOne Platform core features: sophisticated multi-layered protection, detection, visibility, investigation, remediation, and automation.

Protection

The SentinelOne Platform uses autonomous multi-layered prevention to cover diverse threat vectors — known and unknown — even when a system is offline. When a suspected threat is detected, the Platform is capable of automatically responding to eliminate the risk, including rollback of all malicious activity — all viewable as a detailed narrative, and also providing orchestration and investigation data to a supervising SOC. SentinelOne has a robust protection directive which can even disconnect endpoints from the network upon detection of attacks to prevent the spread of malicious activity to the rest of the environment.

Visibility

The SentinelOne Platform has visibility into all activities tracked by the agent, like applications and running processes on configured systems, and even encrypted network traffic.

Real-time alerting is available at the endpoint level and the management console level, to allow end-user and administrator clarity and management capability.

Simplicity

The Platform provides a robust blend of the following features in one autonomous agent with minimal endpoint resource utilization:

- EPP (known and unknown malware intrusion prevention and detection)
- ActiveEDR
- Vulnerability and risk monitoring and management
- Suspected threat detection, monitoring and containment
- Remediation of threat-related operations

- Versatile options for cloud, on-premise or hybrid-hosted management console to fit any business infrastructure.

Automation

A central part of the platform is utilizing intelligent automation to reduce risk and save time. Full endpoint-level automation of responses to suspected threats minimizes response time, reduces negative effect of suspected threats, reduces the need for manual SOC intervention, and minimizes disruption to end-user productivity.

Automation is also facilitated by the over 300 APIs developed by SentinelOne which allows for the integration of its Platform with various SIEM products. With this compatibility framework, logging and monitoring is not only readily available, but it may be configured with ease for businesses with nearly any technical architecture.

Notice

To meet their compliance obligations as organizations processing PCI and/or HIPAA-protected data, it is incumbent on covered businesses to configure SentinelOne to help meet their PCI or HIPAA compliance needs. SentinelOne's obligation is to provide a comprehensive feature set that when configured adequately can support covered organizations to achieve their compliance obligations.

Compliance Requirements

Since SentinelOne introduces anti-threat features that extend beyond traditional EPP performance capabilities, the thought of how to satisfy compliance may come to mind. SentinelOne blends traditional and next-generation malware prevention, detection and remediation, including automated threat management, without losing touch with a business' need to comply with PCI DSS or HIPAA.

Here is how the SentinelOne Platform addresses each applicable PCI DSS and HIPAA requirement:

PCI DSS 3.2.1	SentinelOne Next-Generation Endpoint Protection Platform Features	Meets Requirements?
5.1 – Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	SentinelOne is available on Windows, macOS, Linux and other operating systems commonly used by businesses (See Appendix).	Yes
5.1.1 – Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Malware is detected upon introduction to any computing device within a network protected by the Platform, then it is blocked or automatically quarantined and removed, with all associated operations remediated as well. The latest hashes of known viruses are updated in real time to. ensure that all covered endpoints are protected from all previously known as well as previously unknown viruses.	Yes
5.1.2 – For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	The SentinelOne Platform effectively protects on all major operating systems, allowing business to rest assured their systems, users and data are protected.	Yes

PCI DSS 3.2.1	SentinelOne Next-Generation Endpoint Protection Platform Features	Meets Requirements?
5.2 – Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans, • Generate audit logs which are retained per PCI DSS Requirement 10.7.	Updates are delivered to the SentinelOne Platform immediately, ensuring the Platform is updated in real time on the latest known threats to ensure up-to-date EPP performance. The ability to perform frequent background scans in addition to configurable full system scans surpasses best practices. Logs are also kept for anti-virus activities and configurable to send to all prominent SIEM tools.	Yes
5.3 – Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Anti-tamper mechanism makes it impossible for users to uninstall or deactivate the SentinelOne Platform and as easy to configure as one click. Only designated administrators can change access and administer rights, and all changes to administration rights are logged.	Yes

HIPAA Security	SentinelOne Endpoint Protection Platform Features	Meets Requirements?
§164.308(a)(1) – Policies and procedures to prevent, detect, contain and correct security violations	The SentinelOne Platform effectively prevents, detects, contains, analyzes, rolls back and remediates any security violations associated with malware attacks occurring on covered endpoints.	Partial

HIPAA Security	SentinelOne Endpoint Protection Platform Features	Meets Requirements?
§164.308(a)(5)(ii)(B) – Procedures for guarding against, detecting, and reporting malicious software.	The SentinelOne Platform is available on virtually all operating systems, includes Anti Tamper capabilities, any preferred configuration for management console hosting, and robust threat prevention, detection and reporting via the Platform's management console. Effective integration with most SIEM solutions enables centralized reporting by sharing audit logs to most modern SIEM tools.	Yes
§164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	The SentinelOne Platform identifies both previously known and unknown malware. Once Malware is detected it is automatically quarantined and removed by roll back and remediation. The SentinelOne Platform allows generating a report summarizing the threats and actions for remediation (security incidents).	Yes

Technical Analysis Methodology

Tevora analyzed SentinelOne's Platform to observe the Platform's effectiveness for the following compliance areas:

- PCI DSS Requirement 5
- HIPAA requirements 164.308(a)(5)(ii)(B) and 164.308(a)(6)(ii)

Testing

Methodology

Tevora's primary objective was to assess the efficacy of the SentinelOne Platform in satisfying PCI DSS and HIPAA requirements. To begin, Tevora evaluated how SentinelOne's Platform protects against, detects, contains and removes all known and unknown types of malware. Next, Tevora tested how effective SentinelOne's Platform is against evolving malware threats for systems not commonly considered affected by malware.

Finally, the focus shifted toward testing how the Platform remains current, performs system scans, and generates audit logs. The last test by Tevora was to ensure that end-users could not disable or uninstall the SentinelOne Platform client.

Results

I. Samples of malware were downloaded to a test environment. Upon download to the system, the Platform immediately triggered an alert signaling malware detection, and the payload was quarantined. Activity reports were generated to highlight the complete narrative, including the source and how the malware was introduced to the system, which services it attempted to call upon, what files were launched and targeted and more. After being quarantined, the malware was encrypted with an administrator-defined password, if that file was required to be maintained.

II. While the definition of "systems not considered commonly affected by malware" is at the discretion of each business, this was where the SentinelOne ActiveEDR feature had its time in the spotlight. With its capabilities of identifying anomalous behavior with its automatic SOC functionality, zero-day and uncommonly-known vulnerabilities were detected without needing to rely on virus signatures or definitions. The ActiveEDR functionality also provides automated investigation, orchestration, containment and remediation capabilities with respect to previously unknown and uncommonly known threats.

III. Endpoints report to the Platform's management console every 10 seconds to keep virus hashes as current as possible. Also, background system scans run continuously and may be configured to run at any time interval or even during file downloads or transfers. Numerous auditing options allow owners to specify the granularity of logs and, with over 300 application APIs, virtually every SIEM solution integrates with SentinelOne's Platform.

Logs are available to administrators on the Platform's management console and are encrypted with AES-256 to maintain log integrity.

IV. The management console provides anti-tamper functionality that prohibits deactivation and tampering by default. Tevora verified that this feature prevented the end-user from seeing anything besides the active status of the Platform.

Conclusion

Tevora attests that SentinelOne's Platform meets the intents of prevention, detection, remediation, and reporting requirements covered by the HIPAA Security Rule and HITECH when properly configured. Further, it aligns with HIPAA's Security Rule Requirements §164.308(a)(1), §164.308(a)(5)(ii)(B) and 164.308(a)(6)(ii) for security violations and incidents, and more specifically malware protection.

Tevora further attests that SentinelOne's Platform meets the intents of controls set out in PCI DSS 3.2.1 Requirement 5. The Platform provides the ability to protect, detect, contain, and remove all known and previously unknown types of malware. Additionally, the Platform regularly updates and patches itself to ensure it is frequently maintained for optimal performance. With verbose log capabilities, configurable system scans, Anti Temper mechanism, and hundreds of integrations with SIEM and other information security solutions, the SentinelOne Platform checks all PCI boxes.

Overall, Tevora found that SentinelOne's Endpoint Protection Platform provides a robust endpoint protection solution that is capable of satisfying PCI DSS and HIPAA compliance requirements.

Appendix

Definitions - Compliance Standards

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 requires Covered Entities and Business Associates to comply with general security requirements. More specifically, the Administrative Safeguards in §164.308(a)(1), §164.308(a)(5)(ii)(B) and §164.308(a)6(ii), require Covered Entities and Business Associates to implement and maintain procedures to protect, detect, contain, respond, correct, 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 with the electronic transmission of health information, in part, through several provisions that help 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, 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.

Feature-rich Anti-malware and Anti-threat Platform

SentinelOne EPP is compatible with virtually every operating system a business would use:

Endpoints	Servers	Virtual Environments
Windows XP, 7, 8, 8.1, 10 Mac OSX 10.11 - 10.11.6 macOS 10.12.x, 10.13, 10.14 CentOS 5.5 - 5.11, 6.1 - 6.10, 7.0 - 7.6 Red Hat Enterprise Linux 5.5 - 5.11, 6.0 - 6.10, 7.0 - 7.6 Ubuntu 12.04, 14.04, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10 openSUSE 42.0+ Debian 8 (Jessie), 9 (Stretch)	Windows Server 2003, 2008, 2008 R2, 2012, 2012, 2016 Red Hat Enterprise Linux 6.5, 7.0, 7.2 Ubuntu 12.04, 14.04, 16.04, 16.10 SUSE Linux Enterprise Server 12.0+ (SP1+) Oracle Linux 5.8 - 5.11, 6.5 - 6.9, 7.0+ Amazon Linux (AMI)2016.01+, 2017.01+, 2018.03 Amazon 2 64-bit Virtuozzo 6.8, 7 HP ThinPro 6.2 Fedora 23 - 28	Citrix XenApp, XenDesktop Microsoft Hyper-V Oracle VirtualBox VMware vSphere VMware Workstation VMware Fusion VMware Horizon

About SentinelOne

SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects and responds to attacks across all major vectors. Designed for extreme ease of use, the S1 platform saves customers time by applying AI to automatically eliminate threats in real time for both on premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint. To learn more visit sentinelone.com or follow us at @SentinelOne, on LinkedIn or Facebook.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.

Go forward. We've got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management