TEVORA™

SentinelOne Singularity™ Platform

By Adoriel Bethishou

December 16, 2020

PCI Qualified Security Assessor

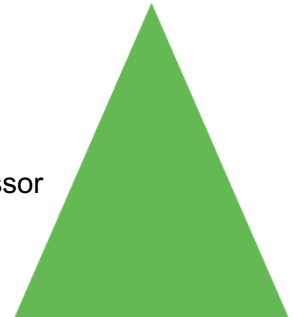

Table of Contents

Endpoint Protection Platform for PCI DSS 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 the SentinelOne's anti-malware Endpoint Protection, Detection, and Response Platform (SentinelOne Singularity™ Platform) and software against PCI DSS version 3.2.1 Requirements 5, 10.8, and 11.5.

This paper describes the functionality of the SentinelOne Singularity Platform and how it dynamically prevents, detects, and responds to cyberattacks. The SentinelOne Singularity Platform is used by IT Teams and SOC Teams to protect their organizations from the negative effects of attacks. In its capacity as an anti-virus/next-gen anti-virus (AV/NGAV) replacement, the SentinelOne Singularity Platform prevents malware and fileless attacks with static and behavioral AI technology coupled with machine-speed response capabilities. The SentinelOne Singularity Platform enables a variety endpoint control including USB and Bluetooth® device control, firewall control, and application vulnerability.

SOC Teams use the SentinelOne Singularity Platform for its EDR capabilities including root-cause investigation, MITRE ATT&CK®-integrated proactive and *ad hoc* threat hunting, incident response, and cyberattack remediation. Singularity Ranger®, another SentinelOne Singularity Platform feature, aids in overall security initiatives by providing real time asset inventory and protection from suspicious devices and compromised IoT. The SentinelOne Singularity Platform provides deep feature parity across many OSes including Windows workstations, Windows servers, Mac devices, Linux, virtual machines, cloud service provider workloads, and cloud-native containerized workloads. All functions are managed from a single, RBAC-enabled, multi-tenant console that is fully customizable to a customer's organizational needs across global geos.

This report outlines the specific ways in which the SentinelOne Singularity Platform can bring organizations in line with PCI DSS Requirement 5 and 11.5.

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 using new techniques. Typically these solutions are capable of malware prevention via machine learning and are now starting to converge with response capabilities, known as Endpoint Detection and Response (EDR). Next-generation solutions can help satisfy 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, creating user friction during updates and constant risk of missed detections. Traditional EPP solutions neglect to effectively 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 Singularity Platform eliminates much of the pain with its unified EPP and EDR functionalities, together referred to as “endpoint protection.” Endpoint protection (EP) is designed to perform prevention, detection, and automated remediation in addition to forensic investigation and threat hunting.

While EDR does not adhere to the traditional scheduled scanning standards set-out in PCI, 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 Singularity Platform: A Compliance Champion

The SentinelOne Singularity Platform takes a hybrid approach to achieve the ultimate in EP and fulfill an organization's compliance requirements by employing four key features:

I. EPP

II. ActiveEDR™

III. Suite features including USB and Bluetooth device control, firewall control, and vulnerability management

IV. Advanced threat hunting tools and techniques

The SentinelOne Singularity Platform 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 Storyline™ technology and coupled with behavioral AI models) is triggered on-execution to track, identify, correlate, contain, and remediate the potential malicious activity.

The SentinelOne Singularity Platform also enables full remediation and a rollback to a pre-infected system state. SentinelOne's Deep Visibility™ EDR, part of the SentinelOne Singularity Platform "Complete" product bundle, kicks in for in-depth automated or human-driven hunting activities and incident response by providing insightful visibility into system behavior activities. This SOC functionality determines if the investigated system may be the victim of a zero-day or any other type of attack. Investigations can move forward regardless of the device's location and irrespective of its online or offline status. SOC analysts have multiple tools at their disposal to cross correlate data and control the situation all with efficiency and ease-of-use at the forefront.

How Does SentinelOne Singularity Platform Help Customers Meet Compliance Requirements?

Overview

Threat prevention, detection, and response (containment, remediation, investigation, analysis) are integrated through static and behavioral AI engines which constantly monitor all activities on the endpoint to detect malicious activities and automatically remediate malicious activities in real time. The SentinelOne Singularity 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 Singularity Platform and its core features: sophisticated multi-layered protection, detection, visibility, investigation, remediation, and automation.

Protection

The SentinelOne Singularity 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 SentinelOne Singularity Platform automatically responds to eliminate the risk, including rollback of all malicious activity — all viewable as a detailed incident narrative, and provides orchestration and investigation data to a supervising SOC. The SentinelOne Singularity Platform has a robust protection directive which can disconnect endpoints from the network upon detection of attacks to prevent the lateral spread of malicious activity to the rest of the environment.

Visibility

SentinelOne's Singularity Platform has visibility into all activities tracked by the agent, including applications and running processes on configured systems, and 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 SentinelOne Singularity 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 SaaS cloud management, on-premise or hybrid-hosted management console to fit any business requirement.

Automation

The SentinelOne Singularity Platform uses 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 a single API with over 360 functions developed by SentinelOne to enable integration of the SentinelOne Singularity Platform with multiple Technology Alliance partner product types including threat intelligence enrichment, sandbox dynamic analysis, SIEM, SSO, cloud assisted security brokers (CASB), messaging (e.g. Slack), Kafka datalake streaming, reporting tools, and more. The SentinelOne Marketplace integrations, coupled with Storyline Active Response (STAR), form the basis for XDR functionality and multi-platform workflow all in the name of faster, unmitigated responses and overall risk reduction.

Notice

To meet their compliance obligations as organizations processing cardholder data, it is incumbent on covered businesses to configure the SentinelOne Singularity Platform to help meet their PCI 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 the SentinelOne Singularity Platform introduces anti-threat features that extend beyond traditional EPP performance capabilities, the thought of how to satisfy compliance may come to mind. The SentinelOne Singularity Platform 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.

As a service provider, SentinelOne is under-scope of PCI requirement 10.8 that requires organizations to have the capacity to detect, identify, and resolve failure of security mechanisms or security incidents.

PCI DSS 3.2.1	SentinelOne	Meets Requirements?
10.8 – Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • **Firewalls** • **IDS/IPS** • **FIM** • **Anti-virus** • **Physical access controls** • **Logical access controls** • **Audit logging mechanisms** • **Segmentation controls (if used)**	For the purposes of PCI DSS 10.8, SentinelOne has implemented processes to detect, identify, and address security incidents and any failures of security mechanisms. The integrity of the product is monitored and processes are in place to contain security threats. In the event that security incidents effect customer data, SentinelOne has defined processes to notify customers with next steps and recommendations to secure their environment. These processes are under scope of SentinelOne's ISO 27001 certification.	Yes

Here is how the SentinelOne Singularity Platform addresses each applicable PCI DSS 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).	The SentinelOne Singularity Platform is available on Windows, macOS, Linux, Kubernetes cloud workloads, and other operating systems commonly used by businesses (See Appendix).	Yes

PCI DSS 3.2.1	SentinelOne Next-Generation Endpoint Protection Platform Features	Meets Requirements?
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 being introduced to the endpoint. This notifies both the user and the administrator, who can set parameters prior which will quarantine and kill the virus, and then add the virus hash to a policy blacklist. The antivirus was also proven to identify malware based on behavior alone.	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 Singularity Platform effectively protects all major operating systems, allowing business to rest assured their systems, users, and data are protected.	Yes
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 Singularity Platform immediately, ensuring it 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. Scans can also be user initiated on folders and external USB storage with a right-click. Logs are also kept for anti-virus activities and configurable to send to all prominent SIEM tools.	Yes

PCI DSS 3.2.1	SentinelOne Next-Generation Endpoint Protection Platform Features	Meets Requirements?
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.	The anti-tamper mechanism makes it impossible for users to uninstall or deactivate the SentinelOne Singularity Platform and can be configured in a single click. Only designated administrators can change access and administer rights, and all changes to administration rights are logged.	Yes
11.5 - Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	File Integrity Monitoring (FIM) capabilities are in place using the Deep Visibility function within the SentinelOne Singularity Platform. This allows users to monitor devices using queries and report on changes to any file integrity. FIM scans in real-time and alerts according to user preferences.	Yes

Technical Analysis Methodology

Tevora analyzed the SentinelOne Singularity Platform to observe its effectiveness for the following compliance areas:

- PCI DSS Requirement 5
- PCI DSS Requirement 10.8
- PCI DSS Requirement 11.5

Testing

Methodology

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

The focus shifted toward testing how the SentinelOne Singularity 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 Singularity Platform client. Additionally, Tevora tested Deep Visibility's ability to act as a File Integrity Monitoring (FIM) solution.

Results

I. Samples of malware were downloaded to a virtual machine in a test environment. The malware was identified by both the SentinelOne agent and the administrator console and then removed in a timely manner. Logs of the event were generated. Different sets of malware were introduced and quarantined right away or after the virus behaved suspiciously.

II. While the definition of "systems not considered commonly affected by malware" is at the discretion of each business, the SentinelOne ActiveEDR feature performed above and beyond. 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 SentinelOne Singularity Platform management console every ten seconds to keep virus hashes as current as possible. Background system scans run continuously and may be configured to run at any time interval, even during file downloads or transfers. Numerous auditing options allow owners to specify the granularity of logs and, with over 360 application APIs, virtually every SIEM solution integrates with the SentinelOne Singularity Platform. Logs are available to

administrators on the SentinelOne Singularity Platform 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. End-users are unable to see or configure SentinelOne Singularity Platform features.

V. Deep Visibility queries were written to look for specific file creation activity in various folders and with various additional parameters (e.g. filetypes, dates) to certify against the File Integrity Monitoring capability of the SentinelOne Singularity Platform. These were written to custom Deep Visibility rules and set to run and notify immediately. Results returned aligned with the queries and were returned at the schedule set when making the rule.

Conclusion

Tevora attests that the SentinelOne Singularity Platform meets the intents of controls set out in PCI DSS 3.2.1 Requirement 5, 10.8, and 11.5. The SentinelOne Singularity Platform provides the ability to protect, detect, contain, and remove all known and previously unknown types of malware. Additionally, the SentinelOne Singularity Platform regularly updates and patches itself to frequently maintain optimal performance. The ability of Deep Visibility to target and monitor filepaths on endpoints for activity and alert immediately ensures sufficient File Integrity Monitoring. With verbose log capabilities, configurable system scans, anti-tamper mechanisms, and hundreds of integrations with SIEM and other information security solutions, the SentinelOne Singularity Platform checks all PCI boxes.

Appendix

Definitions - Compliance Standards

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 Endpoint Protection (EPP+EDR) is compatible with virtually every operating system a business would use:

Windows Modern

Windows (32/64-bit): 10, 8.x, 7 SP1+

Supported without Agent UI: Windows 10 IoT Enterprise

Windows Server: 2019, 2016, 2012 R2, 2012, 2008 R2 SP1

Windows Server Core: 2019, 2016, 2012

Windows Storage Server: 2016, 2012 R2, 2012

Windows Legacy

Windows (32/64-bit): XP SP3+ (requires KB968730), Windows Server 2003 SP2+ or R2 SP2+ (requires KB968730), Windows 2008 (Pre-R2)

Windows Embedded POSReady 2009 (with unofficial support for other versions)

Mac Agent

macOS 11 (Big Sur) "kextless"

macOS 10.15.x (Catalina)

macOS 10.14 (Mojave)

macOS 10.13 (High Sierra)

Linux Agent

Ubuntu 14.04, 16.04, 18.04, 19.04, 19.10, 20.04

RHEL 6.4+, 7.1-7.8, 8.0-8.2

CentOS 6.4+, 7.1-7.8, 8.0-8.1

Oracle 6.9, 6.10, 7.x

Amazon AMI 2, 2017.03, 2018.03

SUSE Linux Enterprise Server 12.x, 15.x

Fedora 25-30, 31 kernel 5.5.x+

Debian 8, 9, 10

Virtuozzo 7

Scientific Linux 6, 7

Supported Container Platforms

Kubernetes self-managed v1.13+

CSP Managed K8s Service: AWS EKS, Azure AKS, Google Cloud GKE

Docker

Supported Cloud Service Provider VMs

AWS EC2

Azure VM

Google Compute Engine

Virtualization & VDI

Citrix XenApp

Citrix XenDesktop

Oracle VirtualBox

VMware vSphere

VMware Workstation

VMware Fusion

VMware Horizon (Agent version 2.6.x)

Microsoft Hyper-V (requires the VHD file)

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology scales people through automation and with features like AI-based prevention and detection, automated interpretation and response, better EDR visibility and overall frictionless threat resolution. To learn more, visit www.sentinelone.com or follow us on Twitter 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