TEVORA™

SentinelOne Singularity™ Platform

By Adoriel Bethishou

17 December 2020

HITRUST External Assessor

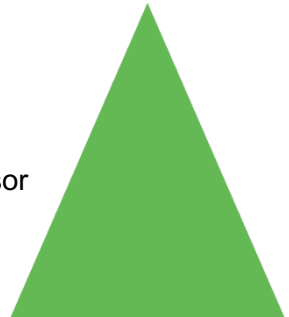

Table of Contents

Endpoint Protection Platform for 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 Singularity™ Platform) and software against 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 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. 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 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 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 HIPAA 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 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 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 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 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

The SentinelOne 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 HIPAA-protected data, it is incumbent on covered businesses to configure The SentinelOne Singularity Platform to help meet their 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 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 HIPAA.

Here is how the SentinelOne Singularity Platform addresses each applicable HIPAA requirement:

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 Singularity Platform effectively prevents, detects, contains, analyzes, rolls back, and remediates any security violations associated with malware attacks occurring on covered endpoints.	Yes
§164.308(a)(5)(ii)(B) – Procedures for guarding against, detecting, and reporting malicious software.	The SentinelOne Singularity Platform is available on virtually all operating systems, includes anti-tamper capabilities, preferred configuration for management console hosting, and robust threat prevention, detection, and reporting via the SentinelOne Singularity Platform's management console. The SentinelOne Singularity Platform integrates with most SIEM solutions to allow more accurate log aggregation and alerting.	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 Singularity Platform identifies both previously known and unknown malware. Once Malware is detected, it is automatically quarantined, removed, and the hash of the virus saved as a policy blacklist. The SentinelOne Singularity Platform allows generating a report summarizing the threats and actions for remediation.	Yes

Technical Analysis Methodology

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

- 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 Singularity Platform in satisfying HIPAA requirements. 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 affected by malware.

Finally, 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.

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's 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'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. End-users are unable to see or configure SentinelOne Singularity Platform features.

Conclusion

Tevora attests that the SentinelOne Singularity Platform meets the intents of prevention, detection, remediation, and reporting requirements covered by the HIPAA Security Rule and HITECH when properly configured. Furthermore, 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 malware protection. Testing verified that the SentinelOne Singularity Platform is capable of identifying, isolating, and resolving threats posed by malware and maintains accurate log information on said events. The SentinelOne Singularity Platform gives insight into endpoint activity down to the file-level and can be configured to alert depending on specific user or machine behaviors.

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.

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