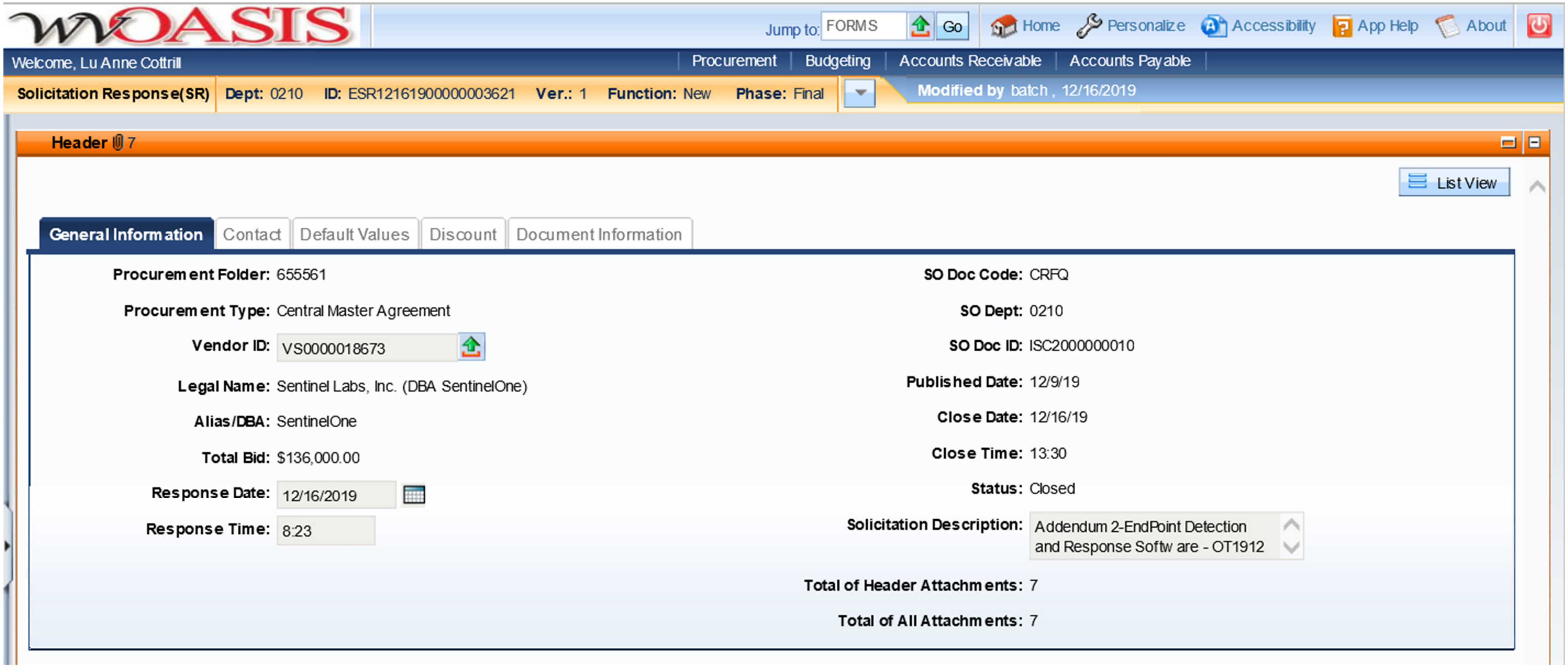
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) **Dept:** 0210 **ID:** ESR12161900000003621 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 12/16/2019

Header 7

Procurement Folder:	655561
Procurement Type:	Central Master Agreement
Vendor ID:	VS0000018673
Legal Name:	Sentinel Labs, Inc. (DBA SentinelOne)
Alias/DBA:	SentinelOne
Total Bid:	$136,000.00
Response Date:	12/16/2019
Response Time:	8:23
SO Doc Code:	CRFQ
SO Dept:	0210
SO Doc ID:	ISC2000000010
Published Date:	12/9/19
Close Date:	12/16/19
Close Time:	13:30
Status:	Closed
Solicitation Description:	Addendum 2-EndPoint Detection and Response Softw are - OT1912
Total of Header Attachments:	7
Total of All Attachments:	7

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 655561

Solicitation Description : Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-12-16 13:30:00	SR 0210 ESR12161900000003621	1

VENDOR

VS0000018673

Sentinel Labs, Inc. (DBA SentinelOne)

SentinelOne

Solicitation Number: CRFQ 0210 ISC2000000010

Total Bid : $136,000.00 **Response Date:** 2019-12-16 **Response Time:** 08:23:44

Comments: Yearly discounts applied on bid response for 1-4 years

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature on File **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA	$16.000000	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$16.000000	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$16.000000	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$20.000000	$40,000.00

Comm Code	Manufacturer	Specification	Model #
43233204			

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

SentinelOne RFP Response
State of West Virginia
November 19, 2019

SentinelOne™

Table of Contents

Contact Information

This RFP is being submitted by:

Lane Vargo

703-608-6223

lanev@sentinelone.com

Executive Summary

Thank you for this opportunity to respond to this RFP. SentinelOne thanks you for your interest and welcomes any questions or inquiries.

Company

SentinelOne, founded in 2013 and headquartered in Mountain View, California, is a cybersecurity software company. Our 2,500+ customers, including 3 of the Fortune 10, come from many verticals including aviation, healthcare, finance, energy, entertainment, cosmetics, retail, government, law, manufacturing, services, and many others. SentinelOne is excited to have been chosen by Gartner as a Customer Choice award recipient in 2019's EDR (endpoint detect and respond) category and in 2018's EPP (endpoint protection platform) category.

The Business Problem

Most organizations are re-thinking their security stack because the scourge of threats worsen each year. At the same time, organizations are competing for cybersecurity talent within a limited pool of candidates. We find that customers seek protection and visibility that keeps up with clever adversaries, but they also want solutions that are simpler to operate, not more complex. Organizations simply want more value. At SentinelOne, we build products that support these themes:

- Lowering total cost of ownership (TCO) with better technology that’s simpler to operate by fewer staff thereby saving labor costs
- Reducing risk by handling today’s newest threat vectors proactively. Our product protects data with prevention, detection, responses and threat hunting in one package.
- API integration of multi-vendor security tools to promote inter-tool automation and orchestration thereby providing faster, more consistent responses

- Making threat hunting easier by reducing guess work. With SentinelOne, hunting becomes an activity that even novice investigators can successfully execute. This is important in a tight IT personnel market.
- Providing assistance to the security operations center (SOC) through our optional Vigilance SOC service. Providing incident response services when needed.
- Compliance with global standards including GDPR and ISO 27001
- Flexibly management options. We offer Cloud, on-premise, or hybrid infrastructure options with clear policy settings.
- ActiveEDR threat hunting and response for autonomous (no cloud reliance) protection from file-based and file-less attacks

It is widely understood that legacy endpoint protection approaches that use static signature-based technology, are no match for today's advanced cyber threats. Furthermore, the lack of protection mechanisms alongside traditional incident response tools leaves a huge gap between detection and remediation during which organizations are highly vulnerable.

Furthermore, Security Operations Center (SOC) Teams are drowning in massive quantities of raw data produced by EDR-centric solutions that lack good protections. There is simply not enough time to investigate everything. Likewise, System Operations/Administration teams deal with the administration of multiple security agents as well as potential issues created by conflicting agent versions. This can cause missed detections and infections resulting in the user having to physically send their laptops back to the IT depot for repair and re-imaging. End user productivity suffers because their machines are bogged down by these agents or in extreme cases, not having a machine to work with at all while it's being repaired.

Offering Overview

SentinelOne offers a fundamentally new, groundbreaking approach to server and workstation security. Built in-house from the ground up, the SentinelOne platform unifies prevention (EPP), detection & response (ActiveEDR), fast recovery, incident response threat hunting and security suite features into a single-agent solution for modern Windows, legacy Windows, Mac, and Linux. Customers use SentinelOne to protect user workstations and servers running natively or within VDI infrastructure or the cloud. Though SentinelOne is primarily a SaaS solution with data centers situated within AWS on three continents (North America, Europe, and Asia), an on-premise management solution is also offered for customers with closed networks. Our solution offers protection, visibility, simplicity and automation for all business or governmental organizations. SentinelOne use cases include:

- Replacement of legacy AV or sub-standard “nextgen” EPP
- Replacement of passive EDR products for customers buried in the alerts and the data these products produce
- Agent consolidation projects aimed at reducing the quantity of agents currently used at the endpoint

- Cloud workload implementations
- As a complementary security control alongside other security stack components

SentinelOne's products identify and neutralize malware and fileless cyber threats while adding visibility and ease-of-use for threat hunters. SentinelOne solves these organizational business challenges:

- Protection and response automation to drastically reduce attacker dwell time
- Fast, automated remediation and recovery to get affected users working again in minutes
- Fewer alerts and more context for IT staff and Security personnel fatigued by their current products
- Threat hunting ease of use to aid in the overall shortage of highly skilled threat hunters
- Agent consolidation
- The ability to support containerized cloud workloads
- API integration with other products

When you take a look at SentinelOne, you will see that our product addresses these types of problems with an effective combination of EPP+EDR. First, SentinelOne is the most effective platform at system protection. Second, we offer a variety of responses including the unique ability to rollback Windows machines remotely, taking the chore of re-imaging off of everyone’s already full plate. Third, when you need detection and visibility for activities like threat hunting and Indicator of Compromise (IoC) identification, it’s there for you with our ActiveEDR feature that pre-correlates benign data at the endpoint. Pre-correlation makes hunting far simpler because related events maintain a contextual relationship making it easier for analysts to see attack flows.

SentinelOne’s core value is summarized as a proven ability to keep unauthorized, destructive code out of your environment while providing detailed “what if” searching capabilities for hunters and responders all in one agent.

Services

SentinelOne supplements its products with a full menu of optional services including Managed Detect and Respond (MDR) to supplement customer Secure Operations Centers (SOC), Incident Response (IR) assistance, a variety of technical support plans and Technical Account Managers (TAM) for focused customer attention. SentinelOne is the fastest growing endpoint vendor on the market today.

Differentiators

Based on the technical knowledge and understanding of our engineering team, SentinelOne continues to innovate the endpoint protection (EPP) and endpoint protection and response (EDR) market space to reflect customer requirements on both the technical and business fronts. Some of our innovations include the following:

#1 SentinelOne is a Comprehensive Security Platform

We deliver EPP + EDR + Security Suite features in a multi-tenant, multi-site platform with simple licensing. We offer SaaS, on prem and hybrid-cloud implementation. Our single agent, single code base architecture offers enterprises critical features allowing for the elimination of other product agents.

#2 SentinelOne Agents are Smarter and Faster at Prevention, Detection, and Response

SentinelOne agents feature exceptional tamper resistance and have their prevention, detection, and response logic local to the agent itself shrinking attack dwell time significantly. Our approach is in contrast to our competitors whose agents upload raw data to their clouds, process it for detections, then send a response command. All of this processing takes too much time and in some cases the adversary has pivoted and moved on. SentinelOne is not cloud reliant for detection and response. We encourage customers to perform sophisticated efficacy testing both online and offline.

#3 Quick Recovery

SentinelOne's patented Remediation and Rollback capabilities get users working again with minimal downtime. We offer one-click remediation to reverse unwanted system changes and one-click Windows rollback to restore any affected data. This ease of use also aids overworked IT staff. Less re-imaging. Less tedious work. Fewer user complaints.

#4 SentinelOne Aids Analysts by Eliminating Tedious Work

Analysts are drowning in alerts and Threat Hunters can't piece together evidence fast enough. SentinelOne's approach delivers context quickly by automatically grouping related data and alerts. The result is faster situational awareness. SentinelOne's ActiveEDR hunting capability is engineered for experienced threat hunters that want to hunt on 90 days of historical benign data. Related benign data is stamped with a unique TrueContext ID at the agent before it is stored in our cloud for future customer use. TrueContext pre-correlation is a notable EDR technology evolution making it easier for analysts to pivot from an artifact of interest to a pre-correlated set of related events. This advancement is different from our competitors that simply upload a multitude of atomic, independent, non-correlated benign events requiring the analyst to have knowledge and intuition of what they should do next.

#5 SentinelOne Vigilance (optional) Managed Detect & Respond Service

Sleep better at night and handle the details in the morning. SentinelOne offers its Vigilance Managed Detect and Respond service but it is not required. This is in contrast to other vendors that require the purchase of their MDR service because it is their core detection capability. SentinelOne Vigilance complements our customer's SOC with monitoring, response assistance and deployment help.

#6 SentinelOne's Powerful API Enables 3rd Party Integration

SentinelOne can be run as a dedicated security point product or it can be integrated with your other tools to create a security machine. SentinelOne provides more ways to integrate with 3rd party products than our competitors. We include a single, well documented 2-way RESTful API with 300+ functions to automate almost every action found in the console. SentinelOne offers pre-built integrations or you can build your own with the tools we provide.

4.1.1.1 Containment and Remediation

4.1.1.2 The Vendor must provide a software and/or sevice that is capable of supporting 2000 endpoints throughout the State of West Virginia

Yes

SentinelOne is more than capable of supporting 2000 endpoints on the platform. SentinelOne's SaaS solution can support up to 150,000 endpoints within a single cloud instance per cluster environment.

4.1.1.3 The Vendor must provide a software and/or sevice that can be centrally managed by a West Virginia Office of Technology Administrator

Yes

SentinelOne's solution provides a central management console for the management of all State of West Virginia endpoints. Customer consoles, accessed via a web browser, are hosted in AWS on highly available infrastructure.

4.1.1.4 The Vendor must provide a software and/or service that shall feature the following

4.1.1.4.1 Automatically restrict potentially malicious activity to within an isolation container

Yes

The SentinelOne solution is capable of automating the process of detection and network isolation based on policy configured.

4.1.1.4.2 Automatically isolate applications interacting with untrusted content from more trusted portions of the device outside the container

While SentinelOne does not utilize application level isolation, the solution has a variety of automated and/or manual Response capabilities to control and remediate detected file-based and fileless attacks:

Alert

Isolate host from network. Only the console can interact with the device.

Kill offending process or processes

Quarantine malicious code

Remediate (reverse unwanted system changes related to an incident, including artifact removal, droppers removed, registry keys restored, and scheduled tasks restored.

Windows Rollback (restore affected data from Windows vss snapshot)

Remote Shell for Incident Responders

Administrators have the ability to execute system commands remotely via the console or the API. These are examples of remote commands:

Get configuration

Configure firewall logging

Decommission

Disconnect from network / reconnect to network

Fetch logs

File fetch (any file)

Initiate scan / abort scan

Move to another site

Reboot

Remote shell

Search on Deep Visibility

Send message to agent OS UI

Show applications

Show agent passphrase

Shut down

Uninstall

Update software

View threats

4.1.1.4.3 Automatically detect and isolate potentially malicious code behavior

Yes

SentinelOne offers real time detection and response to malicious events that occur on endpoints, including malicious scripts, abnormal PE execution, fileless malware, application and OS exploits, abnormal process activities, memory and credential scrapes, reverse shells, zero-day exploits, memory only attacks, and other attacks.

Local Agent Logic is Not Cloud Reliant

SentinelOne agent prevention, detect, and response logic is performed locally at the agent therefore our agents are not cloud reliant. Unlike other vendors, the agent does not have to upload data to the cloud to look for indicators of attack (IoA) nor does it need to send code to a cloud sandbox for dynamic analysis. Other vendor's cloud-centric approaches introduce a large time gap between infection to cloud detection to response at which point an infection may have spread. For example, certain Wannacry variants are shown to spread to 1000's of computers within 1 minute. SentinelOne's agent evaluates threats locally and can take automatic local responses at machine speed.

ActiveEDR

To identify and stop attacks, SentinelOne pioneered "ActiveEDR" that utilizes patented behavioral AI models for on-execution malicious behavioral analysis. The primary design goal of ActiveEDR is to detect evil in real time at the endpoint so that a protective response can be taken automatically. Our approach reduces attacker dwell time to milliseconds in contrast to other products that are cloud reliant for detection. SentinelOne ActiveEDR tracks and monitors all processes that load directly into memory as a set of related "stories." By maintaining story context through the life of the software execution, the agent can determine when processes turn malicious then execute the response specified in policy. ActiveEDR utilizes independent behavioral engines for different vectors including:

Anti-exploitation & Fileless Attacks

Abnormal PE execution

Lateral movement

Abnormal macros & scripts execution

Intrusion detection

Cryptominer Detection

SentinelOne's approach to memory-based attack detection, unlocks a whole new class of attack-detection techniques. At RSA 2019, SentinelOne announced a partnership with Intel Corporation to combat cryptomining. Our partnership integrates Intel's Accelerated Memory Scanning techniques with the SentinelOne single-agent architecture. The primary design goal of faster, more efficient detection of memory anomalies is accomplished by offloading SentinelOne agent processing power from the CPU to the Intel integrated graphics processor unit (6th generation GPU or newer). By using the GPU, detection code can be even more sophisticated than what the industry is used to thus opening the door for the detection of cryptominers and other novel attacks all without latency or degradation of endpoint performance.

4.1.1.4.4 Continuosly detect and isolate threats based on machine learning, behavior analytics, and custom detection rules

Yes

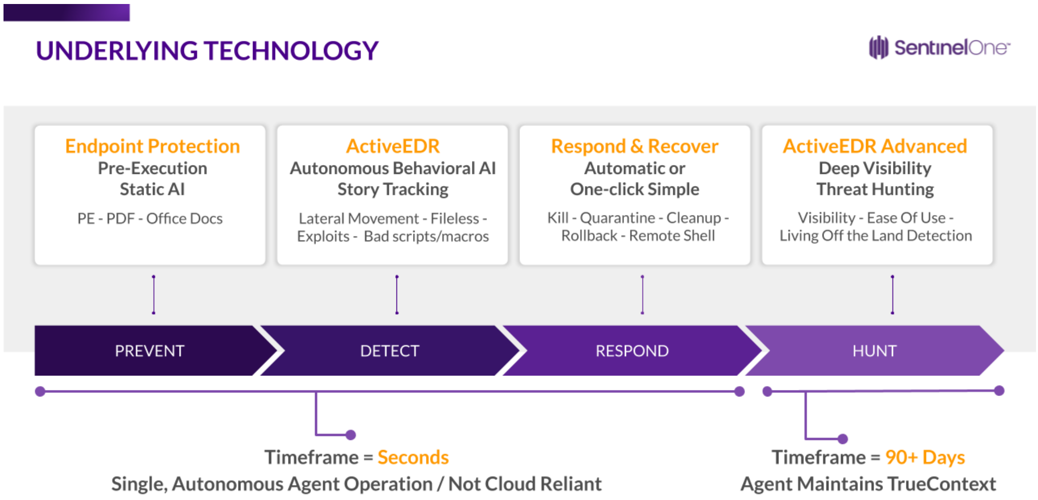
Detection Flow

SentinelOne utilizes multiple cascading engines: reputation, StaticAI, and ActiveEDR capabilities to prevent and detect different types of attacks at different phases. At a high level the agent processes in this order:

SentinelOne's agent will perform a simple hash lookup to the SentinelOne intelligence cloud if the agent is online. This lookup is computationally inexpensive and fast but we do not rely on cloud reachability. If the intelligence cloud is not available, Steps 2 and 3 below form the bulk of the prevention and detection mechanisms.

SentinelOne's Endpoint Prevention (EPP) component uses StaticAI Prevention to analyze (online or offline) portable executable (PE) files pre-execution and takes the place of traditional signatures. This engine also performs analysis on PDF, Microsoft OLE documents (legacy MS Office) and MS Office XML formats (modern MS Office). The goal of StaticAI in the product is to detect commodity and some novel malware with a compact, on-agent machine learning model that serves as a substitute for large signature databases as seen used in legacy AV products.

SentinelOne's ActiveEDR behavioral engine incorporates logic to detect on-execution techniques and tactics used across Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, and Command & Control. The goal of ActiveEDR behavioral in the product is to detect atypical OS story flows that are indicators of maliciousness.



UNDERLYING TECHNOLOGY

SentinelOne

Endpoint Protection
Pre-Execution
Static AI
PE - PDF - Office Docs

ActiveEDR
Autonomous Behavioral AI
Story Tracking
Lateral Movement - Fileless - Exploits - Bad scripts/macros

Respond & Recover
Automatic or
One-click Simple
Kill - Quarantine - Cleanup - Rollback - Remote Shell

ActiveEDR Advanced
Deep Visibility
Threat Hunting
Visibility - Ease Of Use - Living Off the Land Detection

PREVENT

DETECT

RESPOND

HUNT

Timeframe = Seconds
Single, Autonomous Agent Operation / Not Cloud Reliant

Timeframe = 90+ Days
Agent Maintains TrueContext

The Role of Machine Learning

SentinelOne develops machine learning models in-house as a mechanism for predicting when certain file types and OS story trees have exceeded what we know to be normal. Machine learning design goals:

Accurately predict whether something is "bad" even if its building blocks and/or tools, tactics, and procedures are net new and never before seen

Accurately predict what is truly bad while not simultaneously inaccurately tagging benign files and/or OS activities as bad (false positives)

Allow for ML modularity within the agent itself so that new, evolved models can be integrated with ease

SentinelOne Data Science Team creates ML models using structured techniques that balance efficacy increases while simultaneously keep FP rates the same or lower. Data Science achieves this using these these methods:

Good samples of diverse file types from multiple sources like Reversing Labs, VirusTotal, VirusShare, and dark arts colleagues. We also procure legitimate software and FP-prone problematic software for integration into training sets.

High variance, low bias training sets representative of what's in the wild. The more sources we use, the less bias we introduce.

To increase variance, we cluster similar samples, remove duplicates, balance malicious and benign, and ensure all types are represented

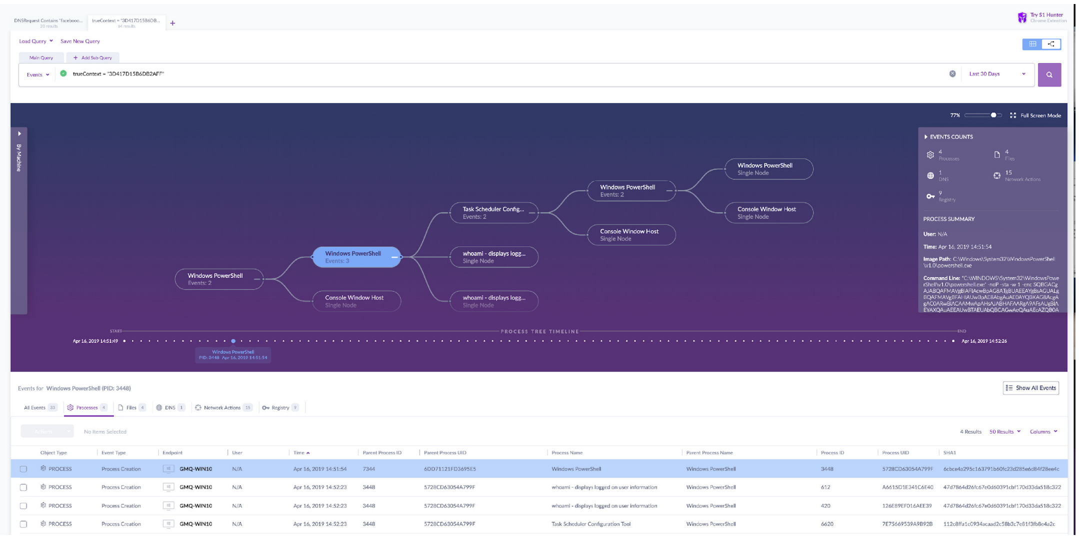
Good feature selection is a must and requires deep knowledge legitimate coding practices. SentinelOne employs thousands of features that help to form statistically accurate ML models.

MITRE ATT&CK

If an exploit or other fileless attack is used to attack a system, indicators of how the system was exploited will be provided. The SentinelOne indicators are also mapped to MITRE ATT&CK TTPs, which will provide an additional layer intelligence, allowing security personal to understand the attack more quickly.

If the attack is researched in our ActiveEDR Advanced tool, attack storylines will indicate which components are related to attacks found by our Static AI and Behavioral AI functions.

In addition to this, if an application was exploited within the attack, the SentinelOne agent takes a realtime inventory of all software installed including their versions. This data is correlated against MITRE's CVE database to provide insight into a system's risk level to the environment and show which applications pose the most risk on those endpoints.



trueContext = "3D417D15B6DB2AFF"

EVENTS COUNTS

4 Processes
4 Files
1 DNS
15 Network Actions
9 Registry

PROCESS SUMMARY

User: N/A

Time: Apr 16, 2019 14:51:54

Image Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Command Line: "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBIAFIAcwBpAG8ATgBUAEEAYgBsAGUALgBQAFMAVgBFAHIAUwBpAE8AbgAuAE0AYQBKAG8AcgAgAC0ARwBIACAAMwApAHsAJABHAFAARgA9AFsAUgBIAEYAXQAuAEEAUwBTAEUAbQBCAGwAeQAuAEcAZQB0A

Events for Windows PowerShell (PID: 3448)

All Events 33 | Processes 4 | Files 4 | DNS 1 | Network Actions 15 | Registry 9

	Object Type	Event Type	Endpoint	User	Time	Parent Process ID	Parent Process UID	Process Name	Parent Process Name	Process ID	Process UID	SHA1
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:51:54	7344	6DD71121FD3695E5	Windows PowerShell	Windows PowerShell	3448	5728CD63054A799F	6cbce4a295c163791b60fc23d285e6d84f28ee4c
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	612	A6615D1E341C6E40	47d7864d26fc67e0d60391cbf170d33da518c322
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	420	126E89EF016AEE39	47d7864d26fc67e0d60391cbf170d33da518c322
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	Task Scheduler Configuration Tool	Windows PowerShell	6620	7E75669539A9B92B	112c8ffa1c0934acaad2c58b3c7e81f3fb8e4a2c

4.1.1.4.5 Automatically capture necessary event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plug-ins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness

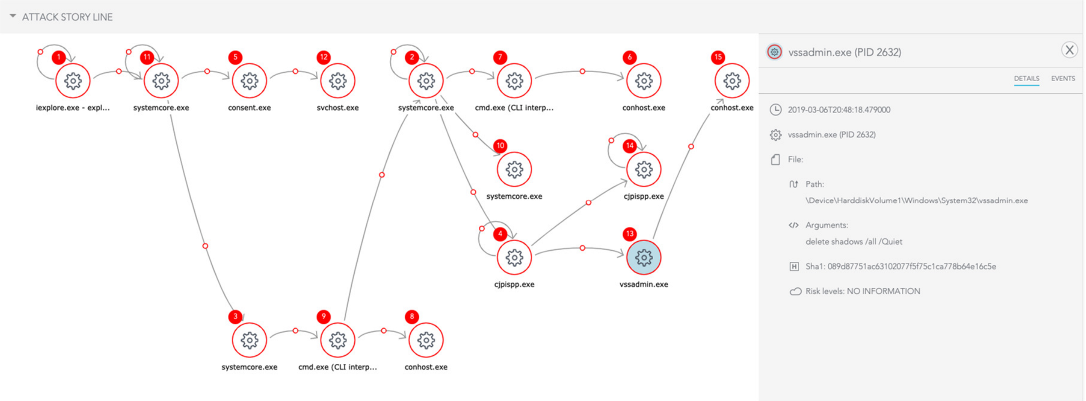
Yes

All benign, suspicious, and malicious activity is monitored and logged by the SentinelOne agent. Suspicious and Malicious activity, as well as forensic data is always sent up to the management console for review. With ActiveEDR Advanced capabilities, all benign activity that occurs on an endpoint is also sent up to the console for both manual and automated Threat Hunting. All data can either be viewed in a more raw format or can be visualized in a storyline (shown below).

SentinelOne automatically links all related events and activity together in a storyline with a TrueContext ID. This allows security teams to pivot and see the full context of what occurred within seconds rather than needing to spend hours, days, or weeks correlating logs and linking events manually.

Detected Threat Storyline

(Note that this style will be changed to the "Active EDR Advanced Storyline" style in August 2019)



vssadmin.exe (PID 2632)

2019-03-06T20:48:18.479000

vssadmin.exe (PID 2632)

File:

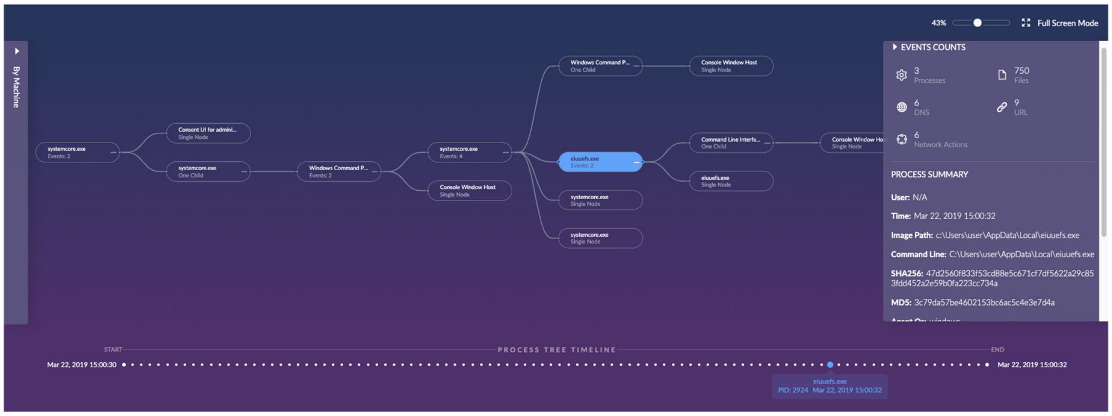
Path:
\Device\HarddiskVolume1\Windows\System32\vssadmin.exe

Arguments:
delete shadows /all /Quiet

Sha1: 089d87751ac63102077f5f75c1ca778b64e16c5e

Risk levels: NO INFORMATION

Active EDR Advanced Storyline



PROCESS SUMMARY

User: N/A

Time: Mar 22, 2019 15:00:32

Image Path: c:\Users\user\AppData\Local\eiuuefs.exe

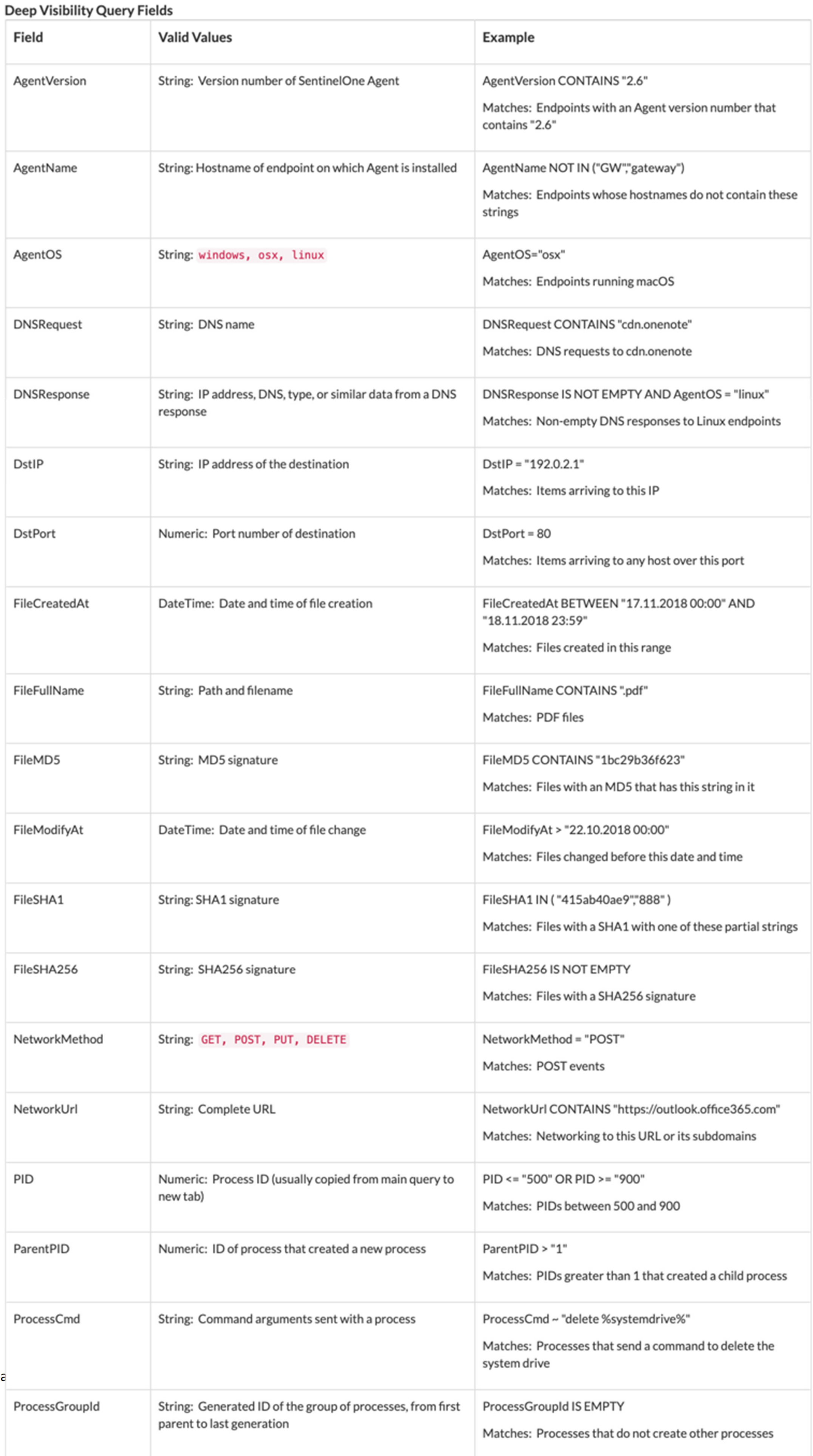
Command Line: C:\Users\user\AppData\Local\eiuuefs.exe

SHA256: 47d2560f833f53cd88e5c671cf7df5622a29c85 3fdd452a2e59b0fa223cc734a

MD5: 3c79da57be4602153bc6ac5c4e3e7d4a

Benign Data Attributes

List current as of May 2019. More attributes added quarterly.



Deep Visibility Query Fields

Field	Valid Values	Example
AgentVersion	String: Version number of SentinelOne Agent	AgentVersion CONTAINS "2.6" Matches: Endpoints with an Agent version number that contains "2.6"
AgentName	String: Hostname of endpoint on which Agent is installed	AgentName NOT IN ("GW","gateway") Matches: Endpoints whose hostnames do not contain these strings
AgentOS	String: `windows, osx, linux`	AgentOS="osx" Matches: Endpoints running macOS
DNSRequest	String: DNS name	DNSRequest CONTAINS "cdn.onenote" Matches: DNS requests to cdn.onenote
DNSResponse	String: IP address, DNS, type, or similar data from a DNS response	DNSResponse IS NOT EMPTY AND AgentOS = "linux" Matches: Non-empty DNS responses to Linux endpoints
DstIP	String: IP address of the destination	DstIP = "192.0.2.1" Matches: Items arriving to this IP
DstPort	Numeric: Port number of destination	DstPort = 80 Matches: Items arriving to any host over this port
FileCreatedAt	DateTime: Date and time of file creation	FileCreatedAt BETWEEN "17.11.2018 00:00" AND "18.11.2018 23:59" Matches: Files created in this range
FileFullName	String: Path and filename	FileFullName CONTAINS ".pdf" Matches: PDF files
FileMD5	String: MD5 signature	FileMD5 CONTAINS "1bc29b36f623" Matches: Files with an MD5 that has this string in it
FileModifyAt	DateTime: Date and time of file change	FileModifyAt > "22.10.2018 00:00" Matches: Files changed before this date and time
FileSHA1	String: SHA1 signature	FileSHA1 IN ("415ab40ae9","888") Matches: Files with a SHA1 with one of these partial strings
FileSHA256	String: SHA256 signature	FileSHA256 IS NOT EMPTY Matches: Files with a SHA256 signature
NetworkMethod	String: `GET, POST, PUT, DELETE`	NetworkMethod = "POST" Matches: POST events
NetworkUrl	String: Complete URL	NetworkUrl CONTAINS "https://outlook.office365.com" Matches: Networking to this URL or its subdomains
PID	Numeric: Process ID (usually copied from main query to new tab)	PID <= "500" OR PID >= "900" Matches: PIDs between 500 and 900
ParentPID	Numeric: ID of process that created a new process	ParentPID > "1" Matches: PIDs greater than 1 that created a child process
ProcessCmd	String: Command arguments sent with a process	ProcessCmd ~ "delete %systemdrive%" Matches: Processes that send a command to delete the system drive
ProcessGroupId	String: Generated ID of the group of processes, from first parent to last generation	ProcessGroupId IS EMPTY Matches: Processes that do not create other processes

4.1.1.4.6 Be configurable to control the ability of applications running within the isolation container to access only specified system resources

No

SentinelOne's architecture differs from container-based products. Our approach does not require the overhead of containerization but still tracks all running-code process relationships and convicts connected processes that have exceed a threshold considered normal. SentinelOne therefore provides protection with less overhead.

4.1.1.4.7 Provide the ability to restrict execution of high-risk applications and computer processing activities to an isolated environment

N/A

SentinelOne's architecture differs from container-based products. Our approach does not require the overhead of containerization but still tracks all running-code process relationships and convicts connected processes that have exceed a threshold considered normal. SentinelOne therefore provides protection with less overhead.

4.1.1.4.8 Automatically eliminate and report all isolation containers artifacts of compromise and intrusion remnants

N/A

SentinelOne's approach to protection enables systems to run in a reduced overhead way.

4.1.1.4.9 Provide continual verification of the integrity of the isolation container to ensure there is no unauthorized/malociousaccess or persistent modification

N/A

SentinelOne's approach to protection enables systems to run in a reduced overhead way.

4.1.1.4.10 Automatically report potentially malicious events detected within the isolation container and provide actionable information

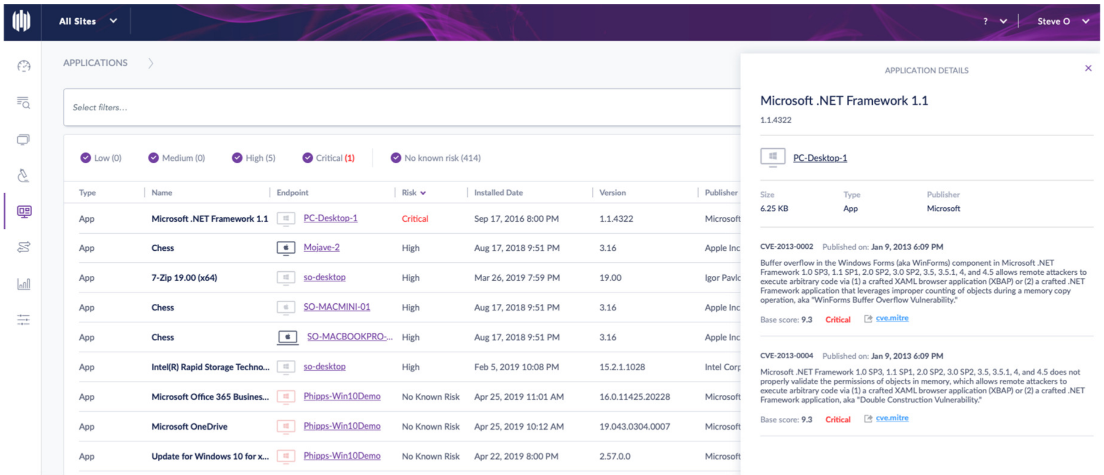
N/A

SentinelOne's approach to protection enables systems to run in a reduced overhead way.

4.1.1.4.11 *Be capable of containing operating system kernel-level vulnerability information*

Yes

SentinelOne agent takes a realtime inventory of all software installed including their versions. This data is correlated against MITRE's CVE database to provide insight into a system's risk level to the environment and show which applications pose the most risk on those endpoints.



Type	Name	Endpoint	Risk	Installed Date	Version	Publisher
App	Microsoft .NET Framework 1.1	PC-Desktop-1	Critical	Sep 17, 2016 8:00 PM	1.1.4322	Microsoft
App	Chess	Mojave-2	High	Aug 17, 2018 9:51 PM	3.16	Apple Inc
App	7-Zip 19.00 (x64)	so-desktop	High	Mar 26, 2019 7:59 PM	19.00	Igor Pavlc
App	Chess	SO-MACMINI-01	High	Aug 17, 2018 9:51 PM	3.16	Apple Inc
App	Chess	SO-MACBOOKPRO-...	High	Aug 17, 2018 9:51 PM	3.16	Apple Inc
App	Intel(R) Rapid Storage Techno...	so-desktop	High	Feb 5, 2019 10:08 PM	15.2.1.1028	Intel Corp
App	Microsoft Office 365 Busines...	Phipps-Win10Demo	No Known Risk	Apr 25, 2019 11:01 AM	16.0.11425.20228	Microsoft
App	Microsoft OneDrive	Phipps-Win10Demo	No Known Risk	Apr 25, 2019 10:12 AM	19.043.0304.0007	Microsoft
App	Update for Windows 10 for x...	Phipps-Win10Demo	No Known Risk	Apr 22, 2019 8:00 PM	2.57.0.0	Microsoft

APPLICATION DETAILS

Microsoft .NET Framework 1.1

1.1.4322

PC-Desktop-1

Size	Type	Publisher
6.25 KB	App	Microsoft

CVE-2013-0002 Published on: Jan 9, 2013 6:09 PM

Buffer overflow in the Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application that leverages improper counting of objects during a memory copy operation, aka "WinForms Buffer Overflow Vulnerability."

Base score: 9.3 Critical cve.mitre

CVE-2013-0004 Published on: Jan 9, 2013 6:09 PM

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 does not properly validate the permissions of objects in memory, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application, aka "Double Construction Vulnerability."

Base score: 9.3 Critical cve.mitre

4.1.1.4.12 *Provide options for configurable automated or manual remediation actions in response to detected potentially malicious events*

Yes

SentinelOne has a variety of automated and/or manual Response capabilities to control and remediate detected file-based and fileless attacks:

Alert

Isolate host from network. Only the console can interact with the device.

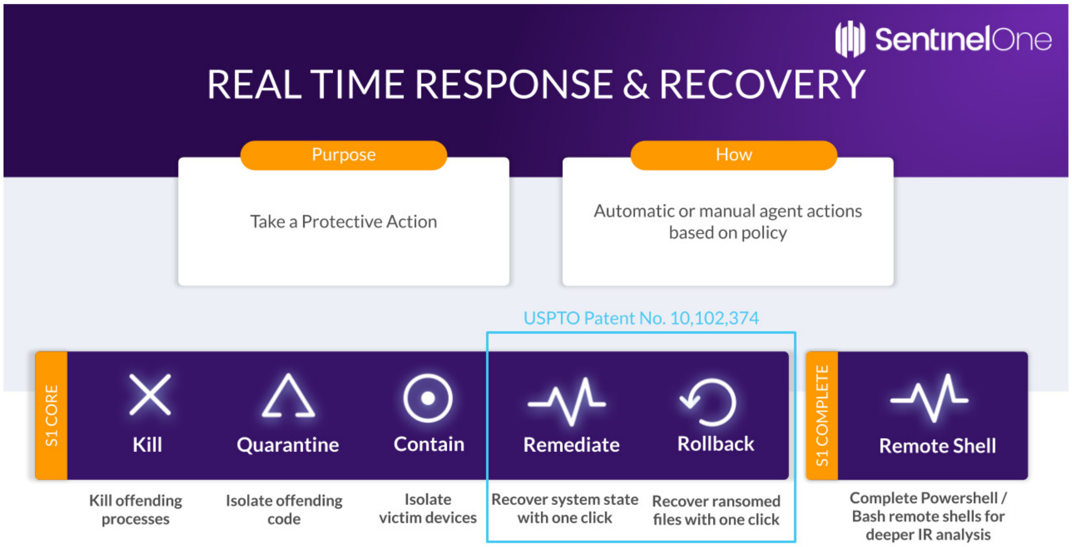
Kill offending process or processes

Quarantine malicious code

One-click Remediate (reverse unwanted system changes related to an incident, including artifact removal, droppers removed, registry keys restored, and scheduled tasks restored.

One-click Windows Rollback (restore affected data from Windows vss snapshot)

Remote Shell for Incident Responders



SentinelOne
REAL TIME RESPONSE & RECOVERY
Purpose
Take a Protective Action
How
Automatic or manual agent actions based on policy
USPTO Patent No. 10,102,374
S1 CORE
Kill
Quarantine
Contain
Remediate
Rollback
S1 COMPLETE
Remote Shell
Kill offending processes
Isolate offending code
Isolate victim devices
Recover system state with one click
Recover ransomed files with one click
Complete Powershell / Bash remote shells for deeper IR analysis

Administrators have the ability to execute system commands remotely via the console or the API. These are examples of remote commands:

Get configuration

Configure firewall logging

Decommission

Disconnect from network / reconnect to network

Fetch logs

File fetch (any file)

Initiate scan / abort scan

Move to another site

Reboot

Remote shell

Search on Deep Visibility

Send message to agent OS UI

Show applications

Show agent passphrase

Shut down

Uninstall

Update software

View threats

4.1.1.5 Reporting and Monitoring

4.1.1.6 The vendor must provide a software or service that shall interoperate with event monitoring and correlation systems to facilitate aggregated situational awareness

Yes

SentinelOne easily integrates with data analytics tools such as SIEMs either through syslog feeds or via our API. Feeds and pushes can be encrypted. We support a variety of syslog message formats including: CEF, CEF2, STIX, IOC and RFC-5424 (rSyslog)

We offer several SIEM integration apps including Splunk, QRadar, and LogRhythm.

We support Splunk as a syslog receiver and also offer a Splunk app that enables customers to control the SentinelOne platform within the Splunk app that leverages our API. The app is listed on Splunkbase: https://splunkbase.splunk.com/app/3677/

4.1.1.7 The software shall support open standards for automated threat information sharing

Yes

Threat Intelligence Current Capabilities

SentinelOne operates our own threat intel cloud that is comprised of data from Reversing Labs, Recorded Future, VirusTotal, and our own curated cloud data. Integration with 3rd party threat intelligence sources is comprised of live links to Recorded Future and VirusTotal directly within the console. SentinelOne uses threat intelligence as an IoC supplement to our machine-learning based StaticAI and ActiveEDR behavioral mechanisms that focus on accurate identification of the previously unknown malicious code.

SentinelOne can send syslog feeds in these formats: STIX, CEF, CEF2, IOC, rSyslog.

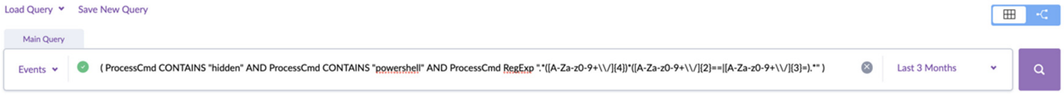
4.1.1.8 The software shall provide integrated and customizable search with, at minimum, the ability to search data from all systems for information relevant to an incident investigation or risk analysis

Yes

ActiveEDR Advanced Threat Hunting is part of the "SentinelOne Complete" offering. It provides integrated and customizable search for threat hunters and incident responders. Searches can be performed on a history of 90 days (to be expanded in 2019). All benign, suspicious, and malicious activity is monitored and logged by the SentinelOne agent. With ActiveEDR Advanced capabilities, benign activity that occurs on an endpoint is also sent up to the console for both manual and automated Threat Hunting. All data can either be viewed in a more raw format or can be visualized in a storyline (shown below).

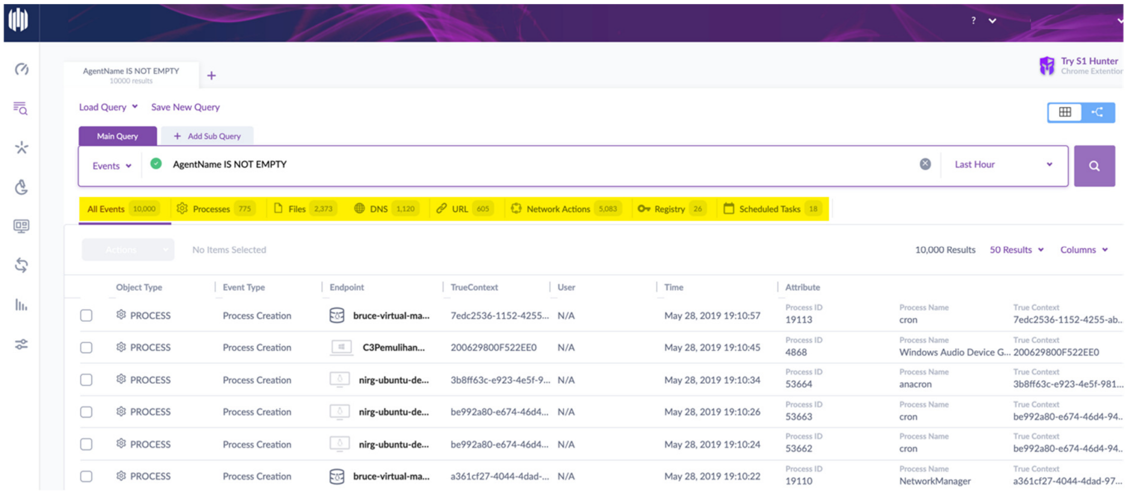
SentinelOne automatically links all related events and activity together in a storyline with a TrueContext ID. This allows security teams to pivot and see the full context of what occurred within seconds rather than needing to spend hours, days, or weeks correlating logs and linking events manually.

Queries can be built using compound expressions (joined by AND / OR), contain regex strings, utilize sub queries to refine previous search results, be displayed as a graphical PID tree, saved for automatic scheduled use, and more.



```
( ProcessCmd CONTAINS "hidden" AND ProcessCmd CONTAINS "powershell" AND ProcessCmd RegExp ".*([A-Za-z0-9+\\/]{4})*([A-Za-z0-9+\\/]{2}==|[A-Za-z0-9+\\/]{3}=).*" )
```

The following Visibility page screenshot is an examples of the provided benign data tracking. Our agent collects forensics related to Processes, Files, DNS, URL, Network Actions, Registry changes, and scheduled tasks. More data types are being added throughout 2019.

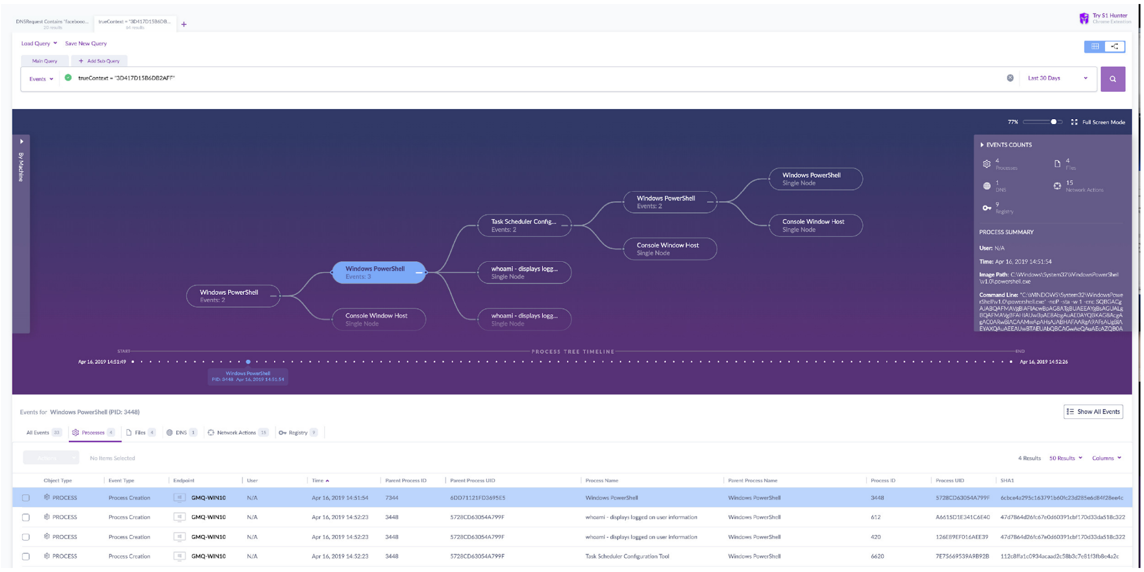


AgentName IS NOT EMPTY

All Events 10,000 | Processes 775 | Files 2,373 | DNS 1,120 | URL 605 | Network Actions 5,083 | Registry 26 | Scheduled Tasks 18

10,000 Results · 50 Results · Columns

	Object Type	Event Type	Endpoint	TrueContext	User	Time	Attribute		
☐	PROCESS	Process Creation	bruce-virtual-ma...	7edc2536-1152-4255...	N/A	May 28, 2019 19:10:57	Process ID 19113	Process Name cron	True Context 7edc2536-1152-4255-ab...
☐	PROCESS	Process Creation	C3Pemulihan...	200629800F522EE0	N/A	May 28, 2019 19:10:45	Process ID 4868	Process Name Windows Audio Device G...	True Context 200629800F522EE0
☐	PROCESS	Process Creation	nirg-ubuntu-de...	3b8ff63c-e923-4e5f-9...	N/A	May 28, 2019 19:10:34	Process ID 53664	Process Name anacron	True Context 3b8ff63c-e923-4e5f-981...
☐	PROCESS	Process Creation	nirg-ubuntu-de...	be992a80-e674-46d4...	N/A	May 28, 2019 19:10:26	Process ID 53663	Process Name cron	True Context be992a80-e674-46d4-94...
☐	PROCESS	Process Creation	nirg-ubuntu-de...	be992a80-e674-46d4...	N/A	May 28, 2019 19:10:24	Process ID 53662	Process Name cron	True Context be992a80-e674-46d4-94...
☐	PROCESS	Process Creation	bruce-virtual-ma...	a361cf27-4044-4dad-...	N/A	May 28, 2019 19:10:22	Process ID 19110	Process Name NetworkManager	True Context a361cf27-4044-4dad-97...



trueContext = "3D417D15B6DB2AFF"

PROCESS SUMMARY

User: N/A

Time: Apr 16, 2019 14:51:54

Image Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Command Line: "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBIAFIAcwBpAG8ATgBUAEEAYgBsAGUALgBQAFMAVgBFAHIAUwBpAE8AbgAuAE0AYQBKAG8AcgAgAC0ARwBlACAAMwApAHsAJABHAFAARgA9AFsAUgBIAEYAXQAuAEEAUwBTAEUAbQBCAGwAeQAuAEcAZQB0A

Events for Windows PowerShell (PID: 3448)

Object Type	Event Type	Endpoint	User	Time	Parent Process ID	Parent Process UID	Process Name	Parent Process Name	Process ID	Process UID	SHA1
PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:51:54	7344	6DD71121FD3695E5	Windows PowerShell	Windows PowerShell	3448	5728CD63054A799F	6cbce4a295c163791b60fc23d285e6d84f28ee4c
PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	612	A6615D1E341C6E40	47d7864d26fc67e0d60391cbf170d33da518c322
PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	420	126E89EF016AEE39	47d7864d26fc67e0d60391cbf170d33da518c322
PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	Task Scheduler Configuration Tool	Windows PowerShell	6620	7E75669539A9B92B	112c8ffa1c0934acaad2c58b3c7e81f3fb8e4a2c

4.1.1.9 The software shall have the ability to execute manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources

Yes

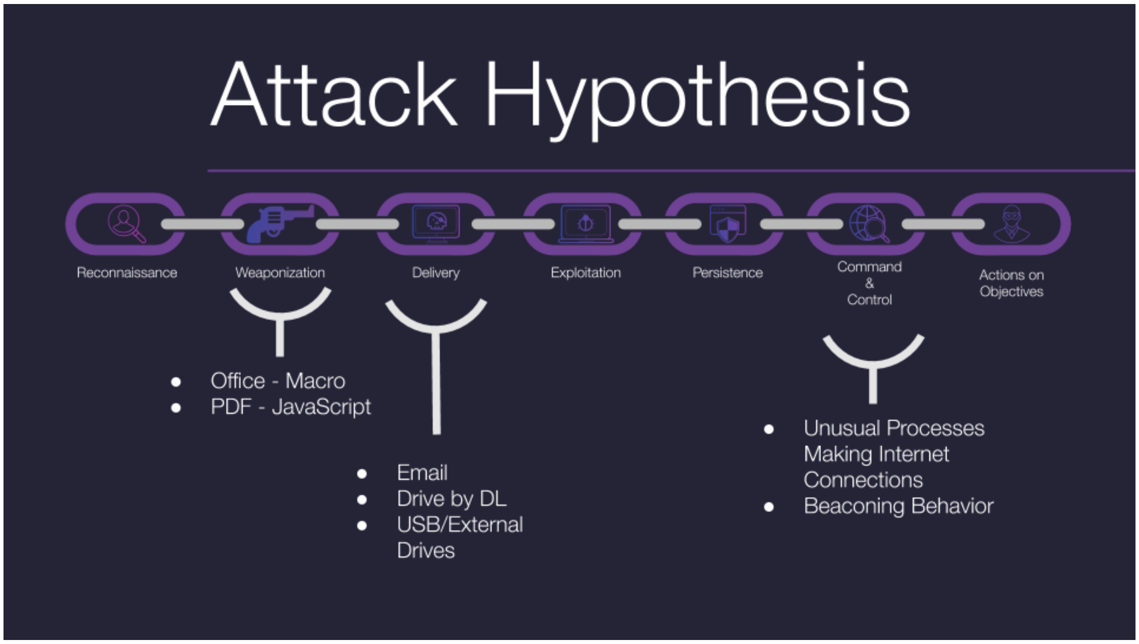
Full disk scan upon installation is optional. Subsequent full disk scans, if desired, can be triggered within the console or via API or at installation. Please note that continual, scheduled disk scans are not necessary because our architecture scans new and changed files as they arrive at the device. The SentinelOne solution does not rely on scanning techniques to maintain efficacy in detecting malicious files or activity thus keeping customer systems continuously clean. Such scanning techniques are generally relevant for legacy anti-malware systems. Similarly, SentinelOne does not rely on reputation data in order to remain effective against threats. Reputation data is consulted in situations where the endpoint happens to be connected to the cloud. The core of the product uses pre-execution static AI and on-execution ActiveEDR behavioral AI as pro-active engines that continuously detect and protect against even the most advanced forms of threats without relying on "scanning" the hard-drive because these engines operate in real-time and continuously monitor all running processes.

4.1.1.10 The software shall provide integrated analytics(including visualization) and support the creation of custom analytics, in order to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis

Yes

As described in previous sections, SentinelOne provides a multitude of incident-related raw data and visualizations to support an analysts understanding of an attack's origins.

Additionally, our product enables ad hoc benign data searching (by default a 90 day historical windows with more history available as an option). This searching can be manual or performed automatically on a defined periodic basis as a watchlist. These tools support Incident Responders as they form Attack Hypotheses.



Attack Hypothesis

- Office - Macro
- PDF - JavaScript

- Email
- Drive by DL
- USB/External Drives

- Unusual Processes Making Internet Connections
- Beaconing Behavior

4.1.1.11 The software shall provide administrative functions to be delegated to users based on roles/permissions and or grouping of endpoints they are responsible for managing

Yes

SentinelOne currently offers several administrative console roles with more roles. General users do not need to access the administrative console.

Global Administrator RW and Viewer for customer with a dedicated cluster or onebox

Account Administrator is the Global Administrator equivalent for shared tenant environments

Site Administrator RW and Viewer

SentinelOne plans to introduce additional levels of RBAC in November 2019.

4.1.1.12 The software shall support delegation(i.e user specified) of who can access/view collected endpoint data

Yes

See answer for 4.1.1.11 above.

4.1.1.13 The software shall have the capability to be tuned/configured to reduce alerts resulting from false positives

Yes

The SentinelOne solution does provide an "Exclusion" function that addresses false positive alerts as well as potential application compatibility issues. Though SentinelOne cannot predict every interoperability issue that might arise, we do document known interop issues with major software providers. Furthermore, SentinelOne provides a robust exclusion function that can be easily configured to enable compatibility with other products. SentinelOne encourages deployment strategies in order to preempt such potential interoperability. All guidelines and knowledge base articles can be access via the online customer portal. Exclusions may be needed for other products (on the box) that inject into memory (legacy AV products, privilege escalation control software, VPN software) or for software that is poorly written but acts powerfully. Other examples include server apps that are highly I/O intensive such as Microsoft applications. Microsoft itself recommends certain exclusion types for most security vendors, including SentinelOne.

Microsoft SQL Servers

Microsoft Domain Controllers

Backup servers

Exchange servers

SentinelOne's robust exclusion function is easily configured to enable compatibility and remedy interoperability false positives. Exclusions can be applied at the global level, site level and group level for granular control. Blacklisting or whitelisting specific applications is not a requirement in order for the SentinelOne solution to operate. However, it is considered best practices to ensure that no other endpoint security solutions may be conflicting with SentinelOne and thus cause interoperability issues. In such cases, it is advised that customers consider the use of exclusions to deal with 3rd part interoperability conflicts. SentinelOne is happy to discuss mass deployment strategies that include testing for potential interoperability issues and proactively handling them. SentinelOne agent exclusion mechanisms include:

hash value

path, path + subfolders, specific executable

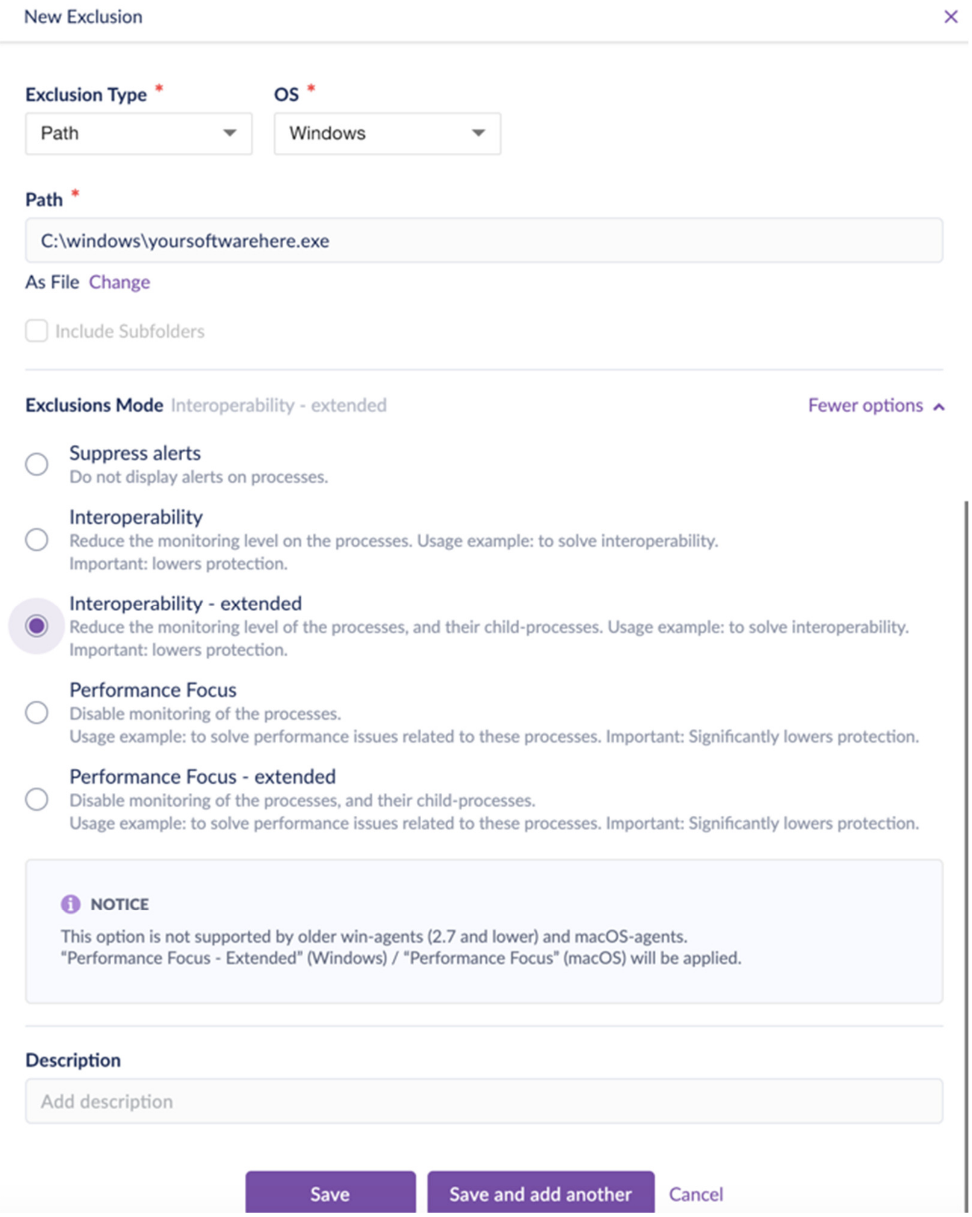
signer certificate identity

file type

browser type

The ability to not monitor certain executables as well as the option to use cascading exclusions. The latter is typically used by shops building code that use known-good compilers.

We also have multiple exclusion modes for highly specific (surgical) exclusions. Ability to turn on and off functionality for consideration of different deployment scenarios, including throttling of deployment. All guidelines and knowledge base articles can be access via the online customer portal.



New Exclusion ×

Exclusion Type * Path

OS * Windows

Path * C:\windows\yoursoftwarehere.exe

As File Change

□ Include Subfolders

Exclusions Mode Interoperability - extended

Fewer options

○ Suppress alerts
Do not display alerts on processes.

○ Interoperability
Reduce the monitoring level on the processes. Usage example: to solve interoperability.
Important: lowers protection.

● Interoperability - extended
Reduce the monitoring level of the processes, and their child-processes. Usage example: to solve interoperability.
Important: lowers protection.

○ Performance Focus
Disable monitoring of the processes.
Usage example: to solve performance issues related to these processes. Important: Significantly lowers protection.

○ Performance Focus - extended
Disable monitoring of the processes, and their child-processes.
Usage example: to solve performance issues related to these processes. Important: Significantly lowers protection.

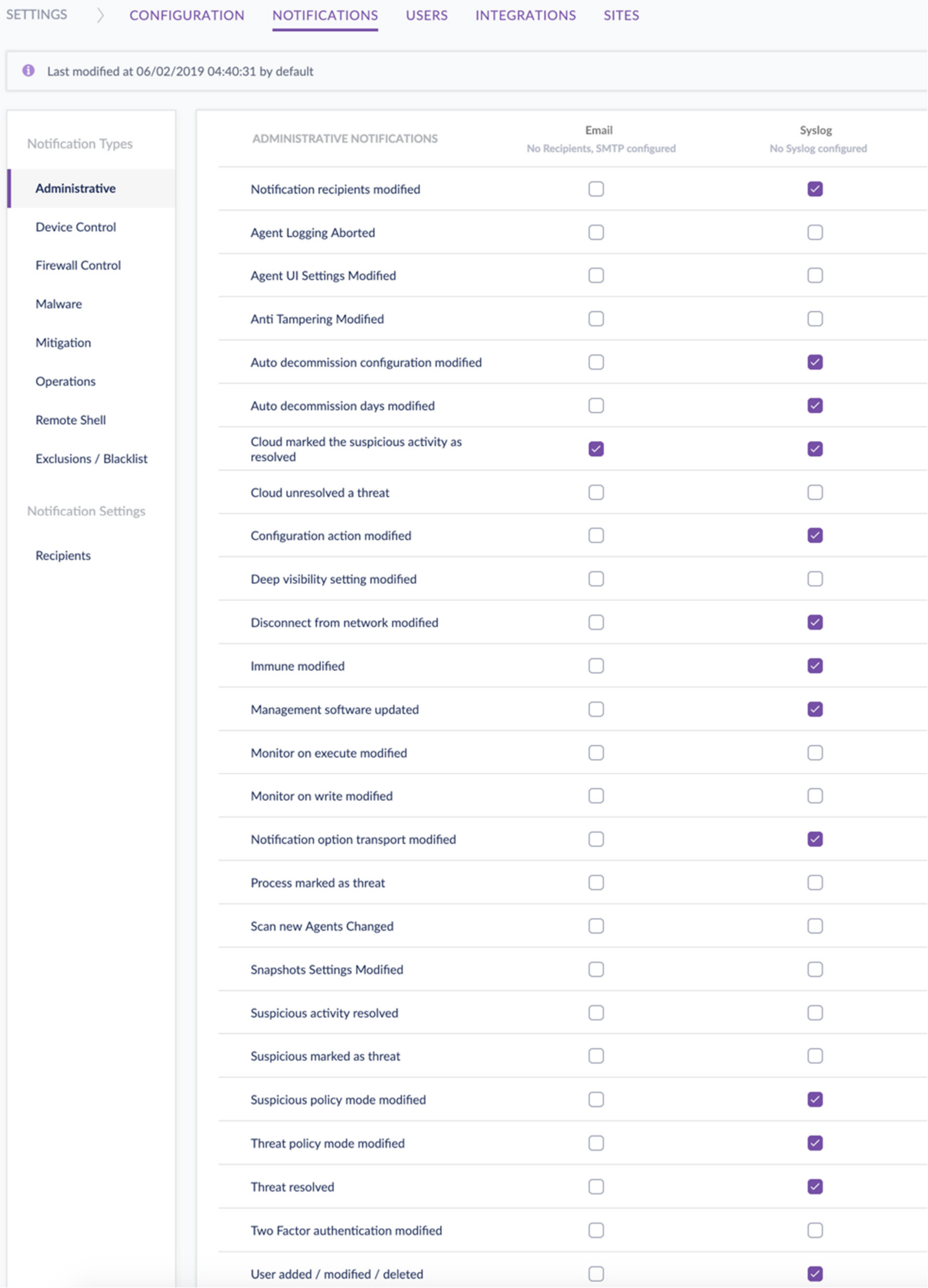
NOTICE
This option is not supported by older win-agents (2.7 and lower) and macOS-agents.
"Performance Focus - Extended" (Windows) / "Performance Focus" (macOS) will be applied.

Description
Add description

4.1.1.14 The software shall provide configurable alerting based upon administrator defined criteria

Yes

Alerts are generated for a wide variety of system, administrative, and agent incident events. Alerts can also be generated for matches on benign data conditions of interest (aka watchlists). These alerts appear in the console. They may also be dispatched to configured SIEMs, can be pulled via API, and/or emailed. The following screenshot depicts some of the audit log settings available to administrators via syslog and/or email. More information is available on request.



Last modified at 06/02/2019 04:40:31 by default

ADMINISTRATIVE NOTIFICATIONS	Email No Recipients, SMTP configured	Syslog No Syslog configured
Notification recipients modified	☐	☑
Agent Logging Aborted	☐	☐
Agent UI Settings Modified	☐	☐
Anti Tampering Modified	☐	☐
Auto decommission configuration modified	☐	☑
Auto decommission days modified	☐	☑
Cloud marked the suspicious activity as resolved	☑	☑
Cloud unresolved a threat	☐	☐
Configuration action modified	☐	☑
Deep visibility setting modified	☐	☐
Disconnect from network modified	☐	☑
Immune modified	☐	☑
Management software updated	☐	☑
Monitor on execute modified	☐	☐
Monitor on write modified	☐	☐
Notification option transport modified	☐	☑
Process marked as threat	☐	☐
Scan new Agents Changed	☐	☐
Snapshots Settings Modified	☐	☐
Suspicious activity resolved	☐	☐
Suspicious marked as threat	☐	☐
Suspicious policy mode modified	☐	☑
Threat policy mode modified	☐	☑
Threat resolved	☐	☑
Two Factor authentication modified	☐	☐
User added / modified / deleted	☐	☑

4.1.1.15 The software shall send alerts at administrator-definable intervals

Yes

SentinelOne's ActiveEDR feature provides a mechanism to create "watchlists" that can be configured to send alerts based on intervals set by the administrator. Once specified, a specific query configured by the administrator will run at the designated interval and will notify the administrator via email once a query returns results during the set interval.

4.1.1.16 The software shall provide the ability to automatically discover and alert on previously unknown external and/or internal hardware/peripheral devices (such as storage) connected to endpoints for the purpose of retrospective/post-event analysis

Yes

SentinelOne has Device Control which allows our agent to control all USB device types for Windows and Mac as well as support for Bluetooth radio control. These functions are built natively into the agent and do not leverage 3rd party add-ons. We also plan to add USB Read Only/Read-Write control in August 2019.

USB Details

Policy can be set to permit or deny USB by Vendor ID, Class (24 Class types - for example, Audio, Printer, Mass Storage, Personal Healthcare, others), Serial ID, and/or Product ID.

Bluetooth Details

Policy can be set to permit or deny Bluetooth using Hardware Class Identifiers (Computer, Phone, Wearable, others) and Minor Class Identifiers (within Wearables, for example, Wristwatch, Pager, Jacket, Helmet, Glasses). Policy can be set to permit or deny Bluetooth Version to eliminate device connectivity with vulnerabilities.

Once Device Control is enabled. All USB and bluetooth device activity will be logged on the SentinelOne management console.

4.1.1.17 The software shall generate reports based on pre-saved user-defined formats and datasets to facilitate rapid analysis, decision making, and follow-up actions following events

Yes

SentinelOne offers a variety of information to help track what is happening in the customers environment. Alerts are generated for agent incident events or matches on benign data conditions of interest (aka watchlists). These alerts appear in the console. They are also dispatched to configured SIEMs, can be pulled via API, and/or emailed.

Reporting is part of the product as well:

Several threat, application and Executive reports are available out of the box. The current list of default reports are:

Vigilance Insights

Threat Insights

Mitigation and Response Insights

Executive Insights

Executive Insights by Groups

Application Insights

New report types can be created for customers at their request and loaded into their console.

Incident data is downloadable in CSV and JSON format.

SentinelOne also provides an Excel plugin which utilizes existing API calls to retrieves all relevant data points that can then be sorted and displayed with the full features of Excel.

SentinelOne is continually adding new ways to access the data in your console for use in other tools. Please check back with our Team to learn what is most current.

Customized reports can be built using the SentinelOne built Excel plugin which utilizes existing API calls to retrieves all relevant data points that can then be sorted and displayed with the full features of Excel. Default reports can be scheduled either weekly or for the first of every month. Reports can be distributed either via PDF or HTML.

4.1.1.18 The software shall provide time stamping of all collected data and events based on a single time standard(e.g., coordinated universal time

Yes

All event alerts and benign data captured will be time-stamped with UTC. Such data when viewed on the management console will then have the time be translated to the respective time per the browser/system being used to access the alert and EDR data.

4.1.1.19 The software shall have the ability to pull locally stored data from specified endpoints in near real time to support high priority hunt and forensic operations

Yes

With SentinelOne CORE (our base offering) or higher, administrators can file fetch malware samples alerted by the agent (quarantined or not). With SentinelOne COMPLETE (our premium offering), administrators can additionally fetch any file on the system. All operations described here can be accomplished within the console or via API.

SentinelOne has a data graded data retention policy. Benign data is deleted 90 days after collection. Data that contains indicators of malicious content is kept for 1 year. Data regarding configuration and audit logs are kept for traceability and audit purposes as lifetime records. The SentinelOne “filefetch” feature used to grab malicious binary objects from endpoints for analysis, keeps the fetched data for 72 hours and then the data is irretrievably deleted. Upon termination of service, all of a customer's data is irretrievably deleted from SentinelOne storage.

4.1.1.20 The software shall provide automated analysis and visualization of an attack; including production of an event timeline and initial assessment of severity/impact

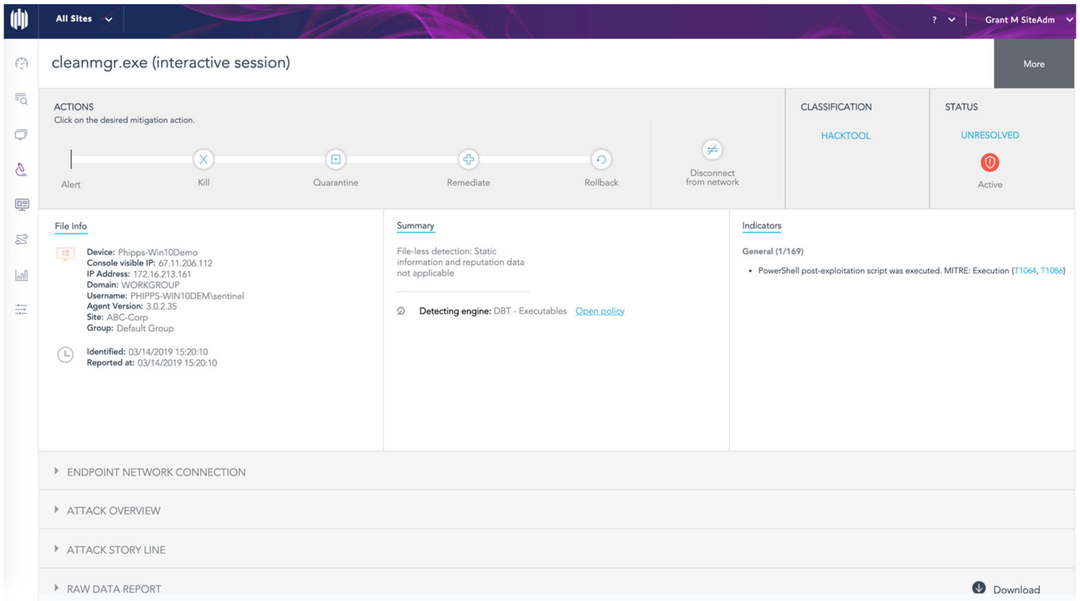
Yes

The local agent has prevention, detection, response, and threat hunting engines. If an incident occurs and the agent is not cloud connected, the agent can still take protective action. Events and forensics are queued until the agent is cloud connected whereupon the queued artifacts are streamed to the console.

The SentinelOne console has many attractive features for the administrator including visualizations and detailed forensics.

Analysis & Actions Summary

The following Analyze page screenshot is an examples of the provided forensic data. All incident forensic data is available as a CSV or JSON download.



cleanmgr.exe (interactive session)

ACTIONS
Click on the desired mitigation action.

CLASSIFICATION
HACKTOOL

STATUS
UNRESOLVED
Active

File Info

Device: Phipps-Win10Demo
Console visible IP: 67.11.206.112
IP Address: 172.16.213.161
Domain: WORKGROUP
Username: PHIPPS-WIN10DEM\sentinel
Agent Version: 3.0.2.35
Site: ABC-Corp
Group: Default Group

Identified: 03/14/2019 15:20:10
Reported at: 03/14/2019 15:20:10

Summary

File-less detection: Static information and reputation data not applicable

Detecting engine: DBT - Executables Open policy

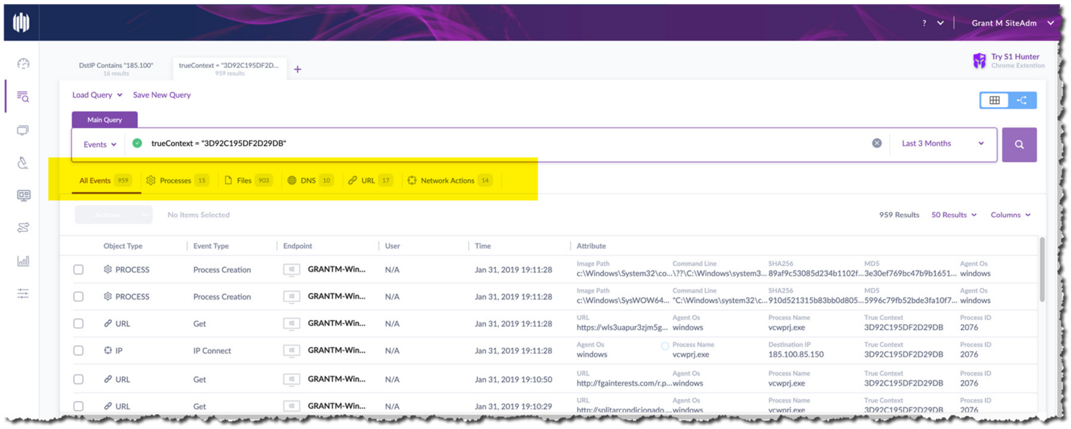
Indicators

General (1/169)

- PowerShell post-exploitation script was executed. MITRE: Execution {T1064, T1086}

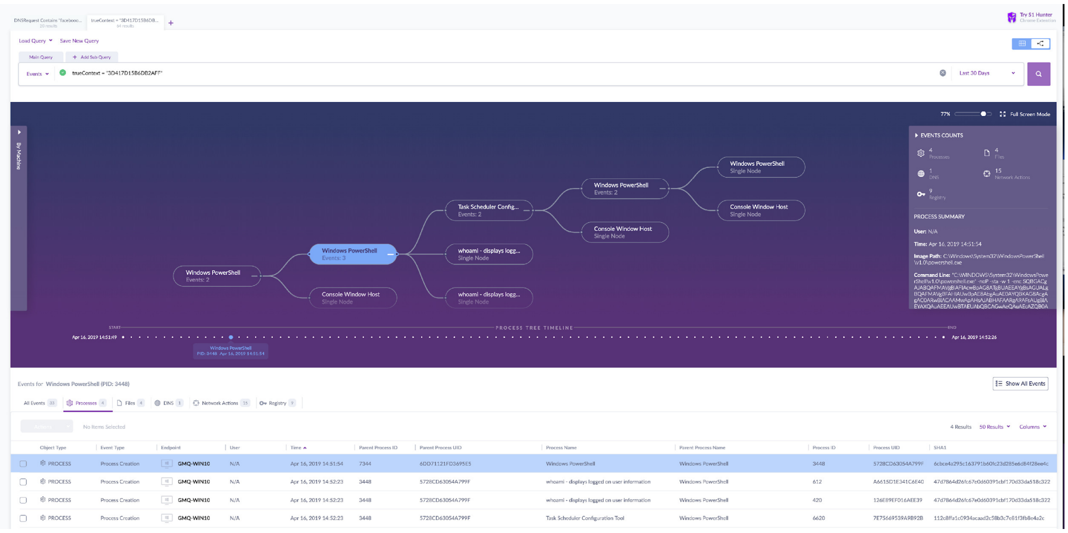
ActiveEDR Advanced Threat Hunting

The following Visibility page screenshot is an examples of the provided benign data tracking. Our agent collects forensics related to Processes, Files, DNS, URL, Network Actions, Registry changes, and scheduled tasks. More data types are being added throughout 2019.



trueContext = "3D92C195DF2D29DB"

	Object Type	Event Type	Endpoint	User	Time	Attribute
□	PROCESS	Process Creation	GRANTM-Win...	N/A	Jan 31, 2019 19:11:28	Image Path c:\Windows\System32\co... Command Line \??\C:\Windows\system3... SHA256 89af9c53085d234b1102f... MD5 3e30ef769bc47b9b1651... Agent Os windows
□	PROCESS	Process Creation	GRANTM-Win...	N/A	Jan 31, 2019 19:11:28	Image Path c:\Windows\SysWOW64... Command Line "C:\Windows\system32\c... SHA256 910d521315b83bb0d805... MD5 5996c79fb52bde3fa10f7... Agent Os windows
□	URL	Get	GRANTM-Win...	N/A	Jan 31, 2019 19:11:28	URL https://wls3uapur3zjm5g... Agent Os windows Process Name vcwprj.exe True Context 3D92C195DF2D29DB Process ID 2076
□	IP	IP Connect	GRANTM-Win...	N/A	Jan 31, 2019 19:11:28	Agent Os windows Process Name vcwprj.exe Destination IP 185.100.85.150 True Context 3D92C195DF2D29DB Process ID 2076
□	URL	Get	GRANTM-Win...	N/A	Jan 31, 2019 19:10:50	URL http://fgainterests.com/r.p... Agent Os windows Process Name vcwprj.exe True Context 3D92C195DF2D29DB Process ID 2076
□	URL	Get	GRANTM-Win...	N/A	Jan 31, 2019 19:10:29	URL http://splitarcondicionado.... Agent Os windows Process Name vcwprj.exe True Context 3D92C195DF2D29DB Process ID 2076



trueContext = "3D417D15B6DB2AFF"

EVENTS COUNTS

4 Processes	4 Files
1 DNS	15 Network Actions
9 Registry	

PROCESS SUMMARY

User: N/A

Time: Apr 16, 2019 14:51:54

Image Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Command Line: "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBIAFIAcwBpAG8ATgBUAEEAYgBsAGUALgBQAFMAVgBFAHIAUwBpAE8AbgAuAE0AYQBKAG8AcgAgAC0ARwBIACAAMwApAHsAJABHAFAARgA9AFsAUgBIAEYAXQAuAEEAUwBTAEUAbQBCAGwAeQAuAEcAZQB0A

Events for Windows PowerShell (PID: 3448)

	Object Type	Event Type	Endpoint	User	Time ▲	Parent Process ID	Parent Process UID	Process Name	Parent Process Name	Process ID	Process UID	SHA1
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:51:54	7344	6DD71121FD3695E5	Windows PowerShell	Windows PowerShell	3448	5728CD63054A799F	6cbce4a295c163791b60fc23d285e6d84f28ee4c
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	612	A6615D1E341C6E40	47d7864d26fc67e0d60391cbf170d33da518c322
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	whoami - displays logged on user information	Windows PowerShell	420	126E89EF016AEE39	47d7864d26fc67e0d60391cbf170d33da518c322
□	PROCESS	Process Creation	GMQ-WIN10	N/A	Apr 16, 2019 14:52:23	3448	5728CD63054A799F	Task Scheduler Configuration Tool	Windows PowerShell	6620	7E75669539A9B92B	112c8ffa1c0934acaad2c58b3c7c81f3fb8c4a2c

4.1.2 Technical Details

4.1.2.1 The vendor must provide the minimum supported platforms including: Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, Hyper-V

Yes

SentinelOne supports a wide variety of Windows, Mac and Linux distributions as well as virtualization OSes. Common software exceptions are documented in our support portal.

Windows Modern

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

Editions: Home, Pro, Pro for Workstations, Enterprise, Education, Pro Education, Enterprise LTSC

Supported without Agent UI: Embedded, Windows 10 IoT Enterprise

Not supported: Mobile, Windows 10 IoT Core

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

macOS 10.14 (Mojave), 10.13 (High Sierra), 10.12 (Sierra)

OS X 10.11.6 (El Capitan)

Linux (v2.x Agent)

Debian 8 (Jessie), 9 (Stretch)

Fedora 23-28

Amazon Linux (AMI) 2016.01+, 2017.01+, 2018.03

Amazon 2 64-bit

CentOS 5.5 - 5.11, 6.1 - 6.10, 7.0 - 7.6

Oracle Linux (formerly known as Oracle Enterprise Linux or OEL) 5.8 - 5.11, 6.5 - 6.9, 7.0+

Red Hat Enterprise Linux (RHEL) 5.5 - 5.11, 6.0 - 6.10, 7.0 - 7.6

SUSE Linux Enterprise Server 12.0+ (SP1+)

openSUSE 42.0+

Ubuntu 12.04, 14.04, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10

Virtuozzo 6.8, 7

HP ThinPro 6.2

Linux (v3.x Agent / New Architecture / GA expected Summer 2019)

CentOS 7.x

RHEL 7.x, 8.x

Ubuntu 14.04, 16.04, 18.04

Amazon Linux 2

Debian 8,9

Oracle 6.9, 7.x

Other distros to come

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)

4.1.2.2 The software shall not impair authorized system operations nor shall degrade managed system performance in any way, which may adversely impact a systems primary business/mission functions.The following authorize system operations include but not limited to:

4.1.2.2.1 Patching, Scanning,Business software usage

Yes

SentinelOne is always striving for great agent efficiency and to provide more functions within our single agent architecture while keeping performance within a set of reasonable bounds. Here are some examples:

Anecdotally speaking, our customers that migrate off of legacy AV tell us that our agent provides both better protection while decreasing endpoint load.

Specifically speaking, some of these customers are now able to use a full endpoint solution within their VDI infrastructure. VDI is notorious for being performance (I/O, RAM, disk size) sensitive; SentinelOne is light enough to be installed onto each persistent or non-persistent guest OS, something that is often not possible with legacy AV.

SentinelOne recently made efficiency improvements to its Windows installer and reduced its size from ~80 MB down to ~60MB, a 25% reduction.

SentinelOne monitors the agent performance in our labs and performance is part of our regression testing to ensure we are staying within our performance envelope.

SentinelOne has a demonstrated ability to work well in large distributed environments with 100,000 or more nodes. When rolling out the agent we suggest some due diligence on the target systems so that proper exclusions, if they are needed at all, can be put into place before the agent push. Doing so helps to minimize disruption to the user environment. Customers learn these techniques during POC and once you become a customer, our Vigilance Team can help further with our optional deployment services.

Our performance claims are proved in third-party performance testing by Passmark (www.passmark.com) that indicates faster browse times, faster file copies, moves and deletes, and faster network throughput than seven well-known competitors. See https://www.sentinelone.com/wp-content/uploads/2017/06/PassMark-Software-Performance-Benchmark-Test-Aug-17-2.pdf for more information.

4.1.2.2.2 The following Information Assurance Tools/Initiatives include but not limited to:

4.1.2.2.2.1 Secure host baseline, and assured compliance assessment software.

Yes

4.1.2.3 The software shall allow for patching and update of containerized applications through means of automated verification(i.e integration with automated patch management infrastructure/processes)

Yes

4.1.2.4 All software components shall have the ability to be automatically deployed and configured based on pre-defined configurations

Yes

The solution's components have the ability to be configured based on predefined configurations based on flags selected.

These flags include things like:

Silent installation (no UI, no user interaction, no reboot).

Sets the address of the Management Server to which the agent connects.

Sets a proxy server between the Agent and its Management Server

Sets credentials to authenticate with the Management proxy.

Sets a proxy server between the Agent and the Deep Visibility EDR data server.

Sets the username and password to authenticate with the Deep Visibility proxy.

Prevents fallback to direct communication if the proxy is not available.

Installs the Agent with the UI disabled (no tray icon or notifications).

Disables Agent logging.

Disables the Safe Boot Protection feature.

Install on Virtual Desktop Infrastructure or VMs with a Golden (Master) Image.

4.1.2.5 The software shall securely store and transmit data that insures confidentiality, integrity, availability, and source authenticity of the data

Yes

The SentinelOne solution provides end-to-end authentication and authorization for various communication types in order to ensure application confidentiality and integrity:

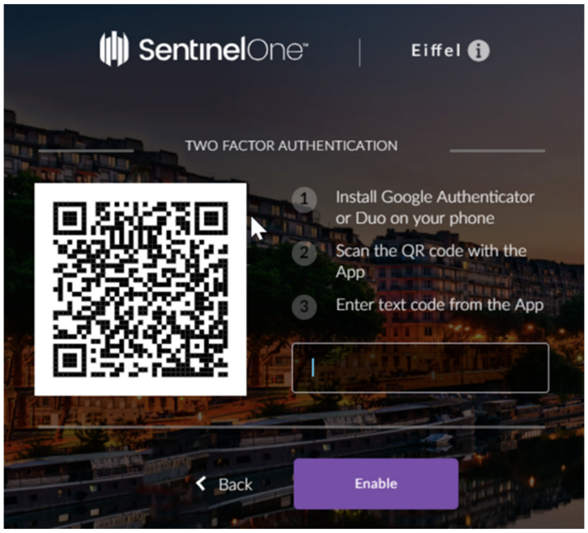
Management Console and API Administrative Access

Customer administrators log in through the web interface for the SentinelOne management console. Customers can also create API tokens for each administrative user if using the API for special purposes like 3rd party tool integration. Initially, an admin user is created for the customer and tied to the main administrator's email address. Once logged in, administrators can enable more advanced authentication mechanisms, such as SSO via SAML 2.0 (multi factor authentication) using a compatible application or built-in MFA. End users are not expected to log into the management console for any reason. A read-only user roles are provided if administrators would like to allow non-administrative users to access the console and view data.

Administrative users of the SentinelOne console can be authenticated in a variety of ways. The console offers a configurable authentication timeout setting. Attackers attempting a brute force attack will experience a slow down in console response after multiple unsuccessful attempts.

When using local username/password authentication, SentinelOne requires complex passwords comprised of 1) 10 to 25 characters; 2) Three or more of these character types: Upper-case letters, lower-case letters, numbers, special characters; 3) no whitespace. The SentinelOne management console does not enforce password expiration, password history, or require the initial password to be changed for accounts. These features can be enforced through an SSO/SAML and/or multi-factor authentication integration.

Customers can increase their security with SentinelOne's built-in Two-Factor Authentication (2FA, Multi-Factor Authentication, MFA), which adds a second authentication method. For example, Google Authenticator and Duo Security send a code through a phone app. When SSO using SAML is configured on the Management console, MFA becomes the responsibility of the IDP.



1 Install Google Authenticator or Duo on your phone

2 Scan the QR code with the App

3 Enter text code from the App

The management console offers the ability to integrate with SSO via SAML 2.0. Identity as a Service (IDaaS) and Identity Provider (IdP) services like Okta, Ping, and Azure AD, can be configured to provide authentication services using elaborate access policies as supported by the IdP like unsuccessful login attempts lockout, time of day access, and permitted source IP. We validate the assertion that the IDP has signed using the IDP provided certificate. The certificate is provided by the IDP admin and uploaded to the Management Console. As such, the certificate is subject to the lifecycle settings that the IDP admin has defined. SentinelOne utilizes LDAPS (LDAP over SSL). The LDAP protocol is transmitted over port 636 and communications are encrypted utilizing TLS and no passwords are stored as part of the LDAP authentication. We support extraction of the following attributes from the SAML assertion:

Name Id attribute (already contains the user id in email format)

Full name (Displayable)

Role - viewer or admin

Agent to Management Network Communication

SentinelOne supports secure communications via TLS 1.2 for modern OSes such as Windows 7 and newer, Windows Server 2008R2 and newer, OS X, macOS, and many Linux version. We also support the legacy OSes Windows XP, Windows Server 2003 / 2003R2, and Windows Server 2008. These older OSes are permitted to communicate via 3DES but these communications do not terminate directly onto the SaaS service. Instead, their weaker communications are proxied through application load balancers that receive the weak ciphers and convert them to TLS. We do this proxy function only to support the maximum capabilities of older OSes.

Authorization to Backend Data via the UI

The SentinelOne back end servers generate a unique "authToken" that resides on the back end. It governs a user's access to the data. The Javascript GUI interacts with the authToken indirectly via an isolated cookie. All application API calls use this authToken at the back end.

4.1.2.6 The software shall encrypyt all data in transit or data atvrest with FIPS 140-2 compliant cryptographic modules

Yes

Please note that SentinelOne's Information Security Management System is ISO/IEC 27001:2013 compliant as of September 2018. This means that we have developed, implemented, and follow security best practices and that the security program has been audited and approved by a third party. Customer may access our ISO certificate here: https://www.schellman.com/certificate-directory.

Summarized encryption practices

In our corporate environment, all passwords are encrypted, all endpoints are encrypted. All data transfers are encrypted as well using VPN utilizing 256-bit encryption. Multi-factor authentication is required.

In our production environment, all data transfers are encrypted, passwords are encrypted. All access into the customer environment is encrypted as well using VPN utilizing 256-bit encryption. Multi-factor authentication is required.

Our shared tenant data at rest is encrypted

Our dedicated OneBox tenants data at rest can be encrypted upon request

Physical Datacenter Security

Physical security controls address physical data theft. Customer Production Data resides physically within several AWS global data centers. Customers choose the region where they want data hosted. AWS is SOC2 compliant and has highly stringent rules for persons accessing their facilities thus controlling who has physical access to that data.

Encryption at Rest & Key Management

The SentinelOne product does not directly process customer data; SentinelOne processes customer metadata (data about the data) which is an abstraction of the statuses related to attacks, incidents, and core OS interactions all of which are used to respond to incidents or are used to research incidents related to a cyber investigation. Customers are most commonly deployed onto shared tenant hardware infrastructure (aka "shared clusters”) which are teams of computers working to provide the SaaS service. Shared clusters commingle customer data within the AWS RDS system. In some cases the customer environment may be deployed onto dedicated hardware infrastructure due to the customer's size or because of a compliance requirement. The first and most common type of dedicated infrastructure is a "OneBox" where all SaaS components reside on a single computer. The second type is a dedicated cluster (typically for very large customers). In both cases, OneBox and dedicated cluster, only that customer's data resides on those systems. The mechanisms described below are valid regardless of whether the infrastructure is shared or dedicated.

Encryption at rest is another form of physical security. By default, SentinelOne encrypts certain data stores by default to ameliorate risk of exposure to highly structured data sets.

For all cluster environments, customer production data at rest is encrypted at the volume level using hardware assisted cryptographic mechanisms. Customer data resides within the Amazon Relational Database Service (RDS) that run on these encrypted volumes. The encryption process utilizes industry standard AES-256 algorithms. Keys to encrypted data are managed within the AWS Key Management Service (KMS). Access to the keys is governed by the AWS Identity and Access Management (IAM) service that controls access based on personnel role. If physical data volumes are stolen or misappropriated, they are not mountable somewhere else because the keys are not stored in the same place as the encrypted data.

For OneBox environments, by default customer production data is not encrypted at rest using the techniques described above. However, at customers request, encryption can be enabled.

Encryption in Transit and Ensuring Proper Agent Communication

For Agent to Tenant communications these are some of the controls SentinelOne employs:

Communications between the agent and management are encrypted with TLS for OSes that support TLS. Older OSes that only support down-level cryptography have their communications proxied through a dedicated gateway so that the core SaaS system can maintain TLS 1.2 or better support.

Agent uses a management token unique to each customer site. Management token connects the agent to the correct site. Agent identifies itself with a unique UUID. No credentials are stored on the agent but instead in protected management space in our cloud. Agent communications to the SaaS using the token and the UUID and the management brokers the communication with the core database system on the agent's behalf.

If the token were to be stolen, it cannot be used to directly access data stored within the system.

The permissions assigned to the agent via this process tag and process data correctly to that customer and not another customer.

Logical Product Security for Shared & Dedicated Tenants

Logical security controls are in place to prevent the leakage of one customer's data to another. For Administrators accessing the management UI, these are some of the controls SentinelOne employs:

Communications are encrypted with TLS and must use a modern browser

Administrators are authenticated with username/password, username/password + 2-factor authentication, or SSO. More details are available on this topic.

Administrators are authorized to sites based on their assigned role in the customer environment.

No direct credentials are stored locally. Instead, the SentinelOne back end servers generate a unique "authToken" that resides on the back end. It governs an administrator's access to the data. The local browser Javascript GUI interacts with the authToken indirectly via an isolated cookie. All application API calls use this authToken at the back end.

The permissions assigned to the administrator govern the data they see in the console so that they see their customer data and not other customer data.

for dedicated infrastructure, these mechanisms still apply but only that customer's data resides on those systems.

Appendix

SENTINELONE TERMS OF SERVICE

These SentinelOne Terms of Service ("**Terms**") are between Sentinel Labs, Inc. or one of its Affiliates (together, "**SentinelOne,**" "**Our,**" "**We**," "**Us**" or similar terms) and the customer ("**Customer**," "**You**," "**Your**" or similar terms) who accepts these Terms, or accesses and/or uses the SentinelOne Solutions (as defined below). These Terms govern Customer's subscription to the SentinelOne Solutions, and constitutes a binding contract in connection with any paid or Evaluation use of the SentinelOne Solutions.

This is a legal, enforceable contract between You and SentinelOne, and by accepting these Terms, clicking the "Log In" button to access the Solutions, otherwise indicating Your consent to the Terms electronically or through access or use of the SentinelOne Solutions, or signing these Term (and such time "Effective Date"), You agree to be bound by these Terms. If You are entering these Terms on behalf of another entity or person, You hereby represent to SentinelOne that You have the authority to bind Customer and its affiliates to these Terms. If You do not have such authority, or if You do not agree to these Terms, You may not subscribe to or use the SentinelOne Solutions.

Capitalized terms will have the meaning assigned to such terms where defined throughout these Terms. Each of SentinelOne or Customer is sometimes described in these Terms as a "**Party**" and together, "**Parties**," which Parties agree as follows:

1. **License**.

1.1. Purchase Order. A "**Purchase Order**" means an online form completed by You directly through the SentinelOne website, or a written document such as a SentinelOne quote with corresponding purchase order, service order or a similar document agreed to in writing and executed among the Parties, or agreed to among You and a SentinelOne approved partner (such as a reseller and collectively, "**Partner**") and referencing a quote from SentinelOne ("**Quote**"), in each case covering Your subscription to Solutions or Evaluation offering. For a Purchase Order to be valid, it must be executed by both the Customer and SentinelOne, by a Partner and Customer, or by a Partner if the executed Purchase Order references and accepts a corresponding SentinelOne Quote. Unless otherwise expressly specified in the Purchase Order executed by SentinelOne, the terms of these Terms shall supersede any conflicting terms in a Purchase Order.

1.2. Scope of Agreement. These Terms govern Your purchase of a subscription to SentinelOne's malware protection, detection and remediation solutions directly or through a Partner, together with the software underlying such products and services and any updates, patches, bug fixes and versions ("**Enhancements**" to the "**SentinelOne Software**", and collectively, the "**SentinelOne's Solutions**" or "**Solution(s)**"). You agree to accept all Enhancements necessary for the proper function of the Solutions as released by SentinelOne from time to time, and further agree that SentinelOne shall not be responsible for the proper performance of the Solutions or security issues encountered with the Solutions related to Your failure to accept Enhancements in a timely manner.

1.3. Related Services and Products. As an active Customer subscribing to the Solutions in accordance with these Terms, during the Subscription Term You may receive and/or subscribe to other related services from SentinelOne, such as support services (“**SentinelOne Support**”), Technical Account Management (“**TAM**”), SentinelOne’s Vigilance Service or other services (collectively “**SentinelOne Services**”); and/or You may procure a license to certain SentinelOne products such as Our Nexus SDK (“**SDK**” and together with SentinelOne Services, “**Other SentinelOne Services and Products)**; in each of the foregoing, as detailed in a relevant Purchase Order listing any such Other SentinelOne Services and Products**.** Your subscription to such Other SentinelOne Services and Products is subject in each case to applicable terms and conditions of these Terms as well as the specific terms for each such Other SentinelOne Services and Products detailed here: https://www.sentinelone.com/legal/.

1.4. Documentation. All use of the Solutions shall be in accordance with Our then**-**current written or electronic communication such as reports or other documents, images, recordings and/or videos specifying the functionalities of the Solutions and made available by Us to all licensees through the SentinelOne website (“**Site**,” at www.sentinelone.com) or otherwise, as updated by Us from time-to-time in the normal course of business (“**Documentation**”).

1.5. License
Grant.

1.5.1. Subject to Your compliance with the terms and conditions of these Terms, We hereby grant You (directly or through a Partner, as applicable) a worldwide, non-transferable, non-exclusive license during the Subscription Term or any Evaluation Period to install, store, access, use, execute and display the Solutions (including Enhancements) solely in support of Your (and Your Affiliate(s)) internal business security and operation, in accordance with the Documentation describing the permissible use of the Solutions (“**License**”). The License granted herein is limited to the number of physical or virtual computing devices that can process data (“**Endpoints**”) or the number of SDK copies licensed to You, where the SentinelOne Software and/or SDK is installed and for which license has been acquired pursuant to a valid Purchase Order. We will make the SentinelOne Software and/or SDK available to You via download from Our website or other means determined by Us.

1.5.2. “**Affiliate(s)**” means any entity that directly, or indirectly through intermediaries, controls, is controlled by, or is under common control with a Party. The license granted to You herein includes the right to connect Your Affiliates’ Endpoints to the Solutions so as to provide the Solutions to such Affiliates’ Endpoints, provided that You agree to remain fully responsible and liable under these Terms for Your Affiliates use of the Solutions.

1.6. Other Services. If You decide to enable, access or use third Party products, applications, services, software, networks or other systems, and/or information which the Solutions link to (collectively, “**Other Services**”), including integrating such Other Services directly to Your instance of the Solutions, be advised that Your access and use of such Other Services is governed solely by the terms and conditions of such Other Services, and We do not endorse, are not responsible or liable for, and make no representations as to any aspect of such Other Services, including, without limitation, their content or the manner in which they handle data or any interaction between You and the provider of such Other Services, or any damage or loss caused or alleged to be caused by or in connection with Your enablement, access or use of any such

Other Services. You may be required to register for or log into such Other Services on their respective websites. By enabling any Other Services, You are expressly permitting Us to disclose Your Login as well as Your Data to such Other Services as necessary to facilitate Your enablement and use of such Other Services.

1.7. Third Party Service. If You enter into an agreement with a third party to manage the installation, onboarding and/or operation of the Solutions on Your behalf ("**Third Party Service**") then You may allow such Third Party Service to use the Solutions provided that (i) as between the Parties, You remain responsible for all its obligations under the terms of these Terms; (ii) such Third Party Service only uses the Solutions for Your internal purposes and not for the benefit of any third party or the Third Party Service, and agrees to the terms of these Terms in providing services to You; and (iii) You remain liable to Us for the Third Party Service's service on Your behalf.

2. **Evaluations; Early Adoption and Beta Use.**

2.1. Evaluation Offering**.** If You receive the Solutions for evaluation purposes, then You may use the Solutions for Your own internal evaluation purposes ("**Evaluation**") for a period of up to thirty (30) days from the start date of the Evaluation (the "**Evaluation Period**"), unless otherwise agreed to in the valid Purchase Order and/or Quote covering the Evaluation.

2.2. Evaluation License and Restrictions. In addition to the license scope detailed elsewhere in these Terms, during Evaluation You: (i) may install and use, solely during the Evaluation Period, one (1) copy of the Solutions malware protection software for network services ("**Server Software**") and up to fifty (50) copies of Endpoints (unless the Parties mutually agree on a different Evaluation Period, or a different number of copies in a Purchase Order executed by both Parties and referencing these Terms); (ii) may install an evaluation framework comprising of malware and exploit samples, to the extent applicable, only on a single computer, in a controlled environment, which is not connected to a

production network, with access to only the Your management server, all in accordance with documentation and materials furnished by Licensor; (iii) shall comply with the use restrictions in Section 3; and (iv) shall uninstall any portion of the Solutions residing on Your computers or servers after the Evaluation Period, return all Documentation in its possession to Us, and confirm to Us in writing (email accepted) of such deletion and uninstallation. If the Evaluation offering is a subscription, You understand that We may disable access to the subscription automatically at the end of the Evaluation period, without notice to Customer. During and following the Evaluation Period, the Parties shall discuss Evaluation results in good faith.

2.3. Early Adoption or Beta Use. If You are invited to and agree to participate in SentinelOne's Early Adoption Program or Beta Program, You acknowledge that Early Adoption or Beta versions of the Solutions are prerelease versions of the Solutions and as such may contain errors, bugs or other defects. Accordingly, Your use and testing of the Early Adoption and/or Beta versions of the Solutions is subject to the disclaimers stated in Section 2.4 below. Additionally, Your use of Early Adoption and/or Beta versions of the Solutions is subject to SentinelOne's sole discretion as to length and scope of use, updates and support of such Early Adoption or Beta versions of the Solutions.

2.4. DISCLAIMER OF WARRANTIES AND LIABILITY. DURING EVALUATION, OR EARLY ADOPTION OR BETA USE OF THE SOLUTIONS, THE SENTINELONE SOLUTIONS ARE OFFERED ON AN “AS IS” BASIS, WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NON-INFRINGEMENT, OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE, OR COURSE OF DEALING. YOU ASSUME ALL RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOLUTIONS AND ACKNOWLEDGES THAT THE USE OF THE SOLUTIONS, TO THE EXTENT APPLICABLE, MUST BE MADE IN STRICT CONFORMANCE WITH SENTINELONE'S INSTRUCTIONS. WITHOUT DEROGATING FROM THE FOREGOING, IT IS UNDERSTOOD AND AGREED THAT SENTINELONE WILL NOT BE LIABLE FOR ANY NETWORK DOWNTIME, SOLUTIONS DOWNTIME, AND/OR IDENTIFYING AREAS OF WEAKNESS IN THE SOLUTIONS. FOR ALL EVALUATIONS, OR EARLY ADOPTION OR BETA USE OF THE SOLUTIONS, WE SHALL HAVE NO LIABILITY TO YOU OR ANY OTHER PERSON OR ENTITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR PROFIT, LOST OR DAMAGED DATA, LOSS OF PROGRAMS OR INFORMATION OR OTHER INTANGIBLE LOSS ARISING OUT OF THE USE OF OR THE INABILITY TO USE THE SOLUTIONS, OR INFORMATION, OR ANY PERMANENT OR TEMPORARY CESSATION OF THE SOLUTIONS OR ACCESS TO INFORMATION, OR THE DELETION OR CORRUPTION OF ANY CONTENT OR INFORMATION, OR THE FAILURE TO STORE ANY CONTENT OR INFORMATION OR OTHER COMMERCIAL OR ECONOMIC LOSS, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE), EVEN IF SENTINELONE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR THAT THEY ARE FORESEEABLE. SENTINELONE IS ALSO NOT RESPONSIBLE FOR CLAIMS BY ANY THIRD PARTY. WHILE THE SOLUTIONS ARE PROVIDED FREE OF CHARGE FOR EVALUATION, EARLY ADOPTION OR BETA PURPOSES ONLY, SENTINELONE’S MAXIMUM AGGREGATE LIABILITY TO YOU SHALL NOT EXCEED US $100. IN JURISDICTIONS WHERE THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES IS NOT ALLOWED THE LIABILITY OF SENTINELONE SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY LAW. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO THE PARTIES OBLIGATIONS UNDER SECTION 7 HEREIN.

3. **Restrictions**. Except as expressly authorized by these Terms, You may not do any of the following: (i) modify, disclose, alter, translate or create derivative works of the SentinelOne Solutions (or any components thereof) or any accompanying Documentation; (ii) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Solutions (or any components thereof) or any Documentation; (iii) use the Solutions other than for their intended uses as directly related to Your internal business operations and described in the Documentation, and not otherwise use the Solutions for any other commercial or business use, including without limitation offering any portion of the Solutions as benefits or services to third parties; (iv) disassemble, decompile or reverse engineer the Solutions (except to the extent and for the express purposes authorized by any and all applicable federal or state laws or regulations); (v) use the Solutions to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party privacy rights; (vi) use the Solutions to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, to disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (vii) probe, scan or test the vulnerability of the

Solutions, or take any action in an effort to circumvent the Solutions; (viii) copy, frame or mirror any part or content of the Solutions; (ix) access the Solutions to build a competitive product or service, or copy any features or functions of the Solutions; (x) interfere with or disrupt the integrity or performance of the Solutions; (xi) attempt to gain unauthorized access to the Solutions or their related systems or networks; (xii) disclose to any third party or publish in any media any performance information or analysis relating to the Solutions; (xiii) fail to maintain all copyright, trademark and proprietary notices on the Solutions and any permitted copy thereof; or (xiv) cause or permit any Solutions user or third party to do any of the foregoing.

4. **Ownership and Reservation of Rights**.

4.1 Customer. As between the Parties, You reserve all right, title and interest in and to Your Data and all Intellectual Property Rights embodied in the foregoing (collectively, the "**Customer IP**").

4.2 SentinelOne. As between the Parties, We reserve all right, title and interest in and to the Solutions (and any and all modifications to or derivative works of the Solutions) and any and all Intellectual Property Rights embodied in the SentinelOne Solution (collectively, the "**SentinelOne IP**").

4.3 Reservation of Rights. Each Party reserves all rights not expressly granted in these Terms, and no licenses are granted by one Party to the other Party under these Terms, whether by implication, estoppel or otherwise, except as expressly set forth in these Terms. For the purpose of these Terms, "**Intellectual Property Rights**" means all patents, copyrights, moral rights, trademarks, trade secrets and any other form of intellectual property rights recognized in any jurisdiction, including applications and registrations for any of the foregoing.

5. **Billing, Plan Modifications and Payments**.

5.1. Fees. The fees for the Solutions and SentinelOne Support are collectively set forth in an applicable Quote or valid Purchase Order (the "**Service Fees**" and "**Support Fees,**" collectively, "**Fees"**). All Fees are due payable directly to Us, or to the applicable Partner, within the timeframe detailed in the applicable valid Purchase Order (and absent such valid Purchase Order, within thirty (30) days of Customer's first use of the Solutions). If You fail to pay Your Fees or charges for other services indicated in a valid Purchase Order or Quote within five (5) days of Our notice to You that payment is past due or delinquent, or if You do not update payment information upon Our (or a Partner's) request, in addition to Our other remedies We may suspend or terminate Your access to the Solutions. Where Fees are paid directly to Us, all payments due under these Terms will be made in U.S. Dollars by check, bank wire transfer or credit card, in immediately available funds to the applicable account designated by Us. No refunds or credits for paid Fees will be issued to Customer unless Customer terminates these Terms pursuant to Section 11.2 or We terminate these Terms pursuant to Section 9.1.

5.2. Plan Modifications. If You choose to increase the number of Endpoints You subscribe to under an applicable Purchase Order or Quote during Your then-effective Subscription Term (a "**Subscription Upgrade**"), We shall invoice You (or Your Partner) for the incremental Fees associated with such Subscription Upgrade on a *pro rata* basis at the price per Endpoint specified in the corresponding Quote or valid Purchase Order over the remaining period of such Subscription Term, which Fees shall be due and payable upon implementation of such Subscription Upgrade. In any future Subscription Term, Your updated Fees will reflect any such Subscription Upgrades; and provided that no Fee refund or credit shall be granted where Customer elects to not use the Solutions on previously subscribed Endpoints.

5.3. Interest and Taxes. Interest on any late payments for undisputed amounts owed will accrue at the rate of 1.5% per month, or the highest rate permitted by law, whichever is lower, from the date such amount is due until the date such amount is paid in full. You will be responsible for and pay all sales and similar taxes and all license fees and similar fees levied upon the provision of the Solutions provided under these Terms excluding only taxes based solely on Our net income. You will indemnify and hold Us harmless from and against any and all such taxes and related amounts levied upon the provision of the Solutions and any costs associated with the collection or withholding thereof, including

penalties and interest. The foregoing shall apply with applicable changes to Purchase Orders among You and a Partner specifying different terms for late payments, tax liability, or indemnification obligations relating to such tax liability.

6. **Privacy and Security**.

6.1. Processing Limitations and Security Obligation**.** In providing You the Solutions and Other SentinelOne Services and Products, We will (i) store, process and access Your Data only to the extent reasonably necessary to provide you the Solutions and/or Other SentinelOne Services and Products, and to improve the Solutions and Other SentinelOne Services and Products; and (ii) implement and maintain commercially reasonable technical, physical and organizational measures to protect the security, confidentiality and integrity of Your Data hosted by Us or Our authorized third parties from unauthorized access, use, alteration or disclosure. "**Your Data**" means all data and information associated with You which is uploaded to, processed by and/or stored within the Solutions by You or in providing the Solutions to You.

6.2. Data Privacy. In these Terms, "**Personal Information**" shall have the meaning ascribed to such term in SentinelOne's Privacy Policy available at https://www.sentinelone.com/privacy-policy/**.** SentinelOne will handle Your Personal Information in accordance with its Privacy Policy and these Terms. Furthermore, to the extent You provide to SentinelOne Personal Information of individuals residing in the European Economic Area ("**EEA**"), You and SentinelOne hereby agree that You shall be deemed the data controller and SentinelOne shall be deemed the data processor of such Personal Information, as those terms are defined under the applicable data protection laws of the EEA (including (i) prior to May 25, 2018, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, (ii) on and after May 25, 2018, the EU General Data Protection Regulation 2016/679 ("**GDPR**," and any applicable national laws made under it), and (iii) where You are established in Switzerland, the Swiss Federal Act of 19 June 1992 on Data Protection, as may be amended or superseded). In its capacity as processor of Personal Information, SentinelOne shall process such Personal Information only for the purpose of providing the Solutions subject to these Terms, and as otherwise instructed by the controller of such Personal Information.

6.3. Hosting Location. Unless otherwise specifically agreed among the Parties, Your Data may be hosted by SentinelOne or its authorized third-party service providers in the United States, the EEA or other locations around the world.

6.4. Anonymized Data. Notwithstanding anything to the contrary in these Terms, We may monitor, collect, use and store anonymous and aggregate statistics and/or data regarding use of the Solutions solely for Our business purposes (including, but not limited to, improving the Solutions and creating new features) and such anonymized and aggregate data shall not be considered Your Data.

7. **Confidentiality.**

7.1. Definition. "**Confidential Information**" means all information disclosed (whether in oral, written, or other tangible or intangible form) by one Party (the "**Disclosing Party**") to the other Party (the "**Receiving Party**") concerning or related to these Terms or the Disclosing Party that is marked as confidential or proprietary, or that the Receiving Party knows or reasonably should know, given the facts and circumstances surrounding the disclosure of the information by the Disclosing Party, is confidential information of the Disclosing Party. Confidential Information includes, but is not limited to, the terms and conditions of these Terms, as well as all proprietary and/or non-public technical, business, commercial, financial and/or legal information, such as, without limitation, business plans, product information, pricing, financial plans, know how, Customer information, strategies, and other similar information.

7.2. Obligations. The Receiving Party will maintain in confidence, during the term of these Terms and for three (3) years following the effective date of termination of these Terms, the Confidential Information, and will not use such Confidential Information except as expressly permitted in these Terms. The Receiving Party will use the same degree of care in protecting the Confidential Information as the Receiving Party uses to protect its own confidential and proprietary information from unauthorized use or disclosure, but in no event less than reasonable care. Confidential Information will be used by the Receiving Party solely for the purpose of carrying out the Receiving Party's obligations under these Terms, and the Receiving Party will only disclose Confidential Information to its directors, officers, employees and/or contractors who have a need to know such Confidential Information in order to perform their duties under these Terms, and if such directors, officers, employees and/or contractors have executed a non-disclosure agreement with the Receiving Party with terms no less restrictive than the non-disclosure obligations contained in this Section 7.2. Provided, however, that each Party may disclose the terms and conditions of these Terms: (i) to legal counsel of such Party; (ii) to such Party's accountants, banks, financing sources and their advisors; (iii) in connection with the enforcement of these Terms or rights under these Terms; or (iv) in connection with an actual or proposed merger, acquisition, or similar transaction. Our compliance with the provisions of Section 6.1 (Security) with respect to Your Data shall be deemed as compliance with its obligations under this Section 7 with respect to Your Data.

7.3. Exceptions. Confidential Information will not include information that: (i) is in or enters the public domain without breach of these Terms through no fault of the Receiving Party; (ii) the Receiving Party can reasonably demonstrate was in its possession prior to first receiving it from the Disclosing Party; (iii) the Receiving Party can demonstrate was developed by the Receiving Party independently, and without use of or reference to, the Confidential Information; or (iv) the Receiving Party receives from a third party without restriction on disclosure and without breach of a nondisclosure obligation. In addition, the Receiving Party may disclose Confidential Information that is required to disclose by law, or by a subpoena or order issued by a court of competent jurisdiction (each, an "**Order**"), and where such Order is shown the Receiving Party shall: (a) give the Disclosing Party written notice of the Order within 24 hours after receiving it; and (b) cooperate fully with the Disclosing Party before disclosure to provide the Disclosing Party with the opportunity to interpose any objections it may have to disclosure of the information required by the Order and seek a protective order or other appropriate relief. In the event of any dispute between the Parties as to whether specific information is within one or more of the exceptions set forth in this Section 7.3, Receiving Party will bear the burden of proof, by clear and convincing evidence, that such information is within the claimed exception(s).

7.4. Remedies. The Receiving Party acknowledges that any unauthorized disclosure of Confidential Information will result in irreparable injury to the Disclosing Party, which injury could not be adequately compensated by the payment of money damages. In addition to any other legal and equitable remedies that may be available, the Disclosing Party will be entitled to seek and obtain injunctive relief against any breach or threatened breach by the Receiving Party of the confidentiality obligations hereunder, from any court of competent jurisdiction, without being required to show any actual damage or irreparable harm, prove the inadequacy of its legal remedies, or post any bond or other security.

8. **Representations, Warranties and Remedies**.

8.1. General Representations and Warranties. Each Party represents and warrants the following: (i) it is validly existing and in good standing under the laws of the place of its establishment or incorporation; (ii) it has full corporate power and authority to execute, deliver and perform its obligations under these Terms; (iii) the person signing these Terms on its behalf has been duly authorized and empowered to enter into these Terms; (iv) these Terms are valid, binding and enforceable against it in accordance with its terms; and (v) it will perform its obligations under these Terms in accordance with applicable federal or state laws or regulations.

8.2. Conformity with Documentation. We warrant that at any point in time during Your Subscription Term, the most recent release of the Solutions ("**Current Release**") will substantially conform in all material respects with the Documentation. SentinelOne's sole obligation for material non-conformity with this warranty shall be, in SentinelOne's sole discretion, to use commercially reasonable efforts (i) to provide You with an error-correction or workaround which corrects the reported non-conformity; (ii) to replace the non-conforming portions of the Solutions with conforming items; or (iii) if SentinelOne reasonably determines such remedies to be impracticable within a reasonable period of time, to terminate these Terms and refund the Fees paid for the Solutions. The above warranty will not apply: (a) if the Solutions are not used in compliance with the Documentation; (b) if any unauthorized modifications are made to the Solutions by You or any third party; (c) to use of early releases of the Solutions which are not the Current Release or the Solutions release immediately preceding the Current Release; (d) to defects due to accident, abuse or improper use by You; or (e) to Evaluation or Early Adoption use of the Solutions.

8.3. Disclaimer. EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES SET FORTH IN THIS SECTION 8, EACH PARTY DISCLAIMS ANY AND ALL REPRESENTATIONS OR WARRANTIES (EXPRESS OR IMPLIED, ORAL OR WRITTEN) WITH RESPECT TO THESE TERMS AND THE SENTINELONE SOLUTIONS, WHETHER ALLEGED TO ARISE BY OPERATION OF LAW, STATUTE, CUSTOM OR USAGE

IN THE TRADE, BY COURSE OF DEALING OR OTHERWISE, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE (WHETHER OR NOT SUCH PARTY KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE AWARE OF ANY SUCH PURPOSE), ACCURACY, NON-INFRINGEMENT, CONDITION OF TITLE. THIS DISCLAIMER AND EXCLUSION WILL APPLY EVEN IF ANY EXPRESS WARRANTY HEREIN FAILS OF ITS ESSENTIAL PURPOSE.

9. **Indemnification Obligations**.

9.1. Infringement Indemnity. SentinelOne will indemnify You and Your directors, officers, employees, contractors, agents, or other authorized representatives ("**Customer Indemnitees**") from and against any and all third party claims, suits, actions or proceedings (each a "**Claim**") alleging that Your use of the Solutions infringes or misappropriates a third party's valid Intellectual Property Right. SentinelOne, at its expense, will defend any such Claim by reason of Your use of the Solutions as permitted hereunder, and pay damages, payments, deficiencies, fines, judgments, settlements, liabilities, losses, costs and expenses (including, but not limited to, reasonable attorneys' fees, costs, penalties, interest and disbursements) finally awarded by a court of competent jurisdiction or included in a settlement approved by SentinelOne. In the event of a Claim pursuant to this Section 9.1, SentinelOne may, at SentinelOne's option and at SentinelOne's expense: (i) obtain for Customer the right to continue to exercise the license granted to Customer under these Terms; (ii) substitute the allegedly infringing component for an equivalent non-infringing component; or (iii) modify the Solutions to make them non-infringing. If (i), (ii), or (iii) is not obtainable on commercially reasonable terms, SentinelOne may terminate these Terms, after providing Customer a reasonable time (no less than 30 days) to transition to an alternative solution, unless SentinelOne determines in its reasonable discretion that such use of the Solutions will likely result in infringement and in such case may terminate these Terms effective immediately with concurrent written notice to Customer. In the event of a termination of these Terms pursuant to this Section 9.1, all rights and licenses with respect to the Solutions will immediately cease and SentinelOne will refund to Customer all prepaid Fees for the Solutions attributable to the Subscription Term (as outlined in the applicable Purchase Order) following the termination of these Terms. SentinelOne's indemnification obligations do not extend to Claims arising from or relating to: (a) any negligent or willful misconduct of any Customer Indemnitees; (b) any combination of the Solutions (or any portion thereof) by any Customer Indemnitees or any third party with any equipment, software, data or any other materials where the infringement would not have occurred but for such combination, unless such combination is the customary, ordinary, and intended use of the Solutions; (c) any modification to the Solutions by any Customer Indemnitees or any third party where the infringement would not have occurred but for such modification; (d) the use of the Solutions by any Customer Indemnitees or any third party in a manner contrary to the terms of these Terms where the infringement would not have occurred but for such use; or (e) the continued use of the Solutions after SentinelOne has provided a substantially equivalent non-infringing software or service.

9.2. Customer Indemnity. Customer, at its sole expense, will indemnify SentinelOne and its directors, officers, employees and agents or other authorized representatives ("**SentinelOne Indemnitees**") from and against any Claim, and be liable for any related damages, payments, deficiencies, fines, judgments, settlements, liabilities, losses, costs and expenses (including, but not limited to, reasonable attorneys' fees, costs, penalties, interest and disbursements) arising out of, based on either Customer's business operations (including, but not limited to, any Customer IP) or any breach or alleged breach of Customer's obligations under Sections 1.7 (Other Services), 1.8 (Third Party Service) or 3 (Restrictions) herein, or the failure of Your administrators of Your account to maintain the confidentiality of their login information to such account.

9.3. Procedures. The indemnifying Party's indemnification obligations under this Section 9 are conditioned upon the indemnified Party: (i) giving prompt written notice of the Claim to the indemnifying Party once the indemnified Party becomes aware of the Claim (provided that failure to provide prompt written notice to the indemnifying Party will not alleviate an indemnifying Party's obligations under this Section 9 to the extent any associated delay does not materially prejudice or impair the defense of the related Claims); (ii) granting the indemnifying Party the option to take sole control of the defense (including granting the indemnifying Party the right to select and use counsel of its own choosing) and settlement of the Claim (except that the indemnified Party's prior written approval will be required for any settlement that reasonably can be expected to require an affirmative obligation of the indemnified Party); and (iii) providing reasonable cooperation to the indemnifying Party and, at the indemnifying Party's request and expense, assistance in the defense or settlement of the Claim.

10. **Limitation of Liability**. EXCEPT FOR BREACHES OF SECTION 3 (RESTRICTIONS), 7 (CONFIDENTIALITY) OR EACH PARTY'S INDEMNIFICATION OBLIGATIONS, IN NO EVENT WILL EITHER PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THESE TERMS EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER TO SENTINELONE (OR ITS RESELLER) FOR 6 MONTHS SUBSCRIPTION FEES AT THE TIME OF THE EVENT OR EVENTS LEADING TO THE ALLEGED DAMAGES, AND IN THE CASE OF A BREACH OF SECTION 6 (PRIVACY AND SECURITY), NO MORE THAN 12 MONTHS SUBSCRIPTION FEES AT THE TIME OF THE EVENT OR EVENTS LEADING TO THE ALLEGED DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, ANY INTERRUPTION OF BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF, OR IN CONNECTION WITH THESE TERMS, WHETHER IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED OR IS OTHERWISE AWARE OF THE POSSIBILITY OF SUCH DAMAGES. MULTIPLE CLAIMS WILL NOT EXPAND THIS LIMITATION. THIS SECTION 10 WILL BE GIVEN FULL EFFECT EVEN IF ANY REMEDY SPECIFIED IN THESE TERMS IS DEEMED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

11. **Term, Termination and Effect of Termination**.

11.1. Term. Unless otherwise agreed to in writing among Parties or in a valid Purchase Order among You and a Partner, the term of these Terms will begin on the Effective Date and continue for twelve (12) months (the "**Initial Subscription Terms**"), and thereafter these Terms shall renew for additional successive periods identical in length to the Initial Subscription Term ("**Renewal Subscription Term**" and collectively, "**Subscription Term**"). Any Subscription Term may also terminate if (i) terminated in accordance with Section 11.2 below; (ii) either Party notifies the other in writing no less than thirty (30) days prior to the close of the then-current Initial or Renewal Subscription Term of its intention not to renew; or (iii) terminated by Us in accordance with Section 9.1.

11.2. Termination. In addition to Our right to terminate these Terms pursuant to Section 9.1, either Party may terminate these Terms, for cause, if the other Party: (i) materially breaches these Terms and does not cure such breach within thirty (30) days after its receipt of written notice of such breach; or (ii) becomes insolvent, makes an assignment for the benefit of creditors, or becomes subject to direct control of a trustee, receiver or similar authority. Additionally, We may terminate these Terms immediately for cause by providing concurrent notice to You if We believe that You are using the Solutions in any unauthorized manner likely to cause harm to SentinelOne, the Solutions or a third party.

11.3. Effect of Termination. Upon any termination of these Terms: (i) all rights and licenses granted to Customer under these Terms will immediately terminate; (ii) all of Our obligations under these Terms (including, Our performance of the SentinelOne Support) will immediately cease; (iii) there will be no refund for any pre-paid and unused Fees as of the termination date, and You will immediately pay Us any Fees due and payable under these Terms as of the termination date, except where You terminate these Terms due to SentinelOne's material breach or where SentinelOne terminates these Terms under Section 9.1 herein; and (iv) upon receiving a written request from the Disclosing Party, the Receiving Party will promptly return to the Disclosing Party all Confidential Information of the Delivering Party then in its possession or destroy all copies of such Confidential Information, at the Delivering Party's sole discretion and direction. Customer will immediately confirm, in writing, that it has complied with this Section 11.3(iv) at Our request. Notwithstanding any terms to the contrary in these Terms, Sections 3, 4, 5, 7, 8.2, 9, 10, 11.3 and 12 will survive any termination of these Terms.

12. **General Provisions**.

12.1. Entire Agreement. These Terms, together with all exhibits attached thereto (all of which are incorporated herein by reference), set forth the entire agreement and understanding of the Parties relating to Your subscription to the Solutions, and supersede all prior or contemporaneous conflicting terms in agreements proposals, negotiations, conversations, discussions and understandings, written or oral, with respect to such subject matter and all past dealing

or industry custom (including without limitation any nondisclosure agreement, any Quote or Purchase Order and/or another agreement among the Parties in connection with Your consideration and/or evaluation of the Solutions), excluding only a written agreement executed by SentinelOne, expressly referencing these Terms and only to the extent expressly superceding specific terms in these Terms.

12.2. Independent Contractors. Neither Party will, for any purpose, be deemed to be an agent, franchisor, franchise, employee, representative, owner or partner of the other Party, and the relationship between the Parties will only be that of independent contractors. Neither Party will have any right or authority to assume or create any obligations or to make any representations or warranties on behalf of any other Party, whether express or implied, or to bind the other Party in any respect whatsoever.

12.3. Governing Law and Venue. These Terms will be governed by and construed in accordance with the laws of the State of California, without regard to conflict of law principles. The state or federal court in Santa Clara County, California will be the jurisdiction in which any suits should be filed if they relate to these Terms. Prior to the filing or initiation of any action or proceeding relating to these Terms, the Parties must participate in good faith mediation in Santa Clara County, California (except an action or proceeding required to protect or enforce a Party's Intellectual Property Rights). If a Party initiates any proceeding regarding these Terms, the prevailing Party to such proceeding is entitled to reasonable attorneys' fees and costs for claims arising out of these Terms.

12.4. Publicity. You agree that We may reference and use Your name and trademarks in SentinelOne marketing and promotional materials, including, but not limited to, the SentinelOne website, solely for purposes of identifying You as Our customer. Otherwise, neither Party may use the trade names, trademarks, service marks, or logos of the other Party without the express written consent of the other Party.

12.5. Assignment. Neither these Terms nor any right or duty under these Terms may be transferred, assigned or delegated by a Party, by operation of law or otherwise, without the prior written consent of the other Party and such consent shall not be unreasonably delayed or withheld. Any attempted transfer, assignment or delegation without such consent will be void and without effect. Notwithstanding the foregoing, each Party may assign these Terms to a successor of substantially all of its business or assets, whether by merger, sale of assets, sale of stock, reorganization or otherwise, with written notice to the other Party, provided that such successor in interest agrees in writing to assume all of the assigning Party's obligations under these Terms. Subject to the foregoing, these Terms will be binding upon and will inure to the benefit of the Parties and their respective representatives, heirs, administrators, successors and permitted assigns.

12.6. Export Compliance. The Solutions, and SentinelOne Software or other components of the Solutions which We may provide or make available to You for use by Your users are subject to U.S. export control and economic sanctions laws. You agree to comply with all such laws and regulations as they relate to Your access to and use of the Solutions. You shall not access or use the Solutions if You are located in any jurisdiction in which the provision of the Solutions is prohibited under U.S. or other applicable laws or regulations (a "**Prohibited Jurisdiction**") and You agree not to grant access to the Solutions to any government, entity or individual located in any Prohibited Jurisdiction. You represent, warrant and covenant that (i) You are not named on any U.S. government list of persons or entities prohibited from receiving U.S. exports, or transacting with any U.S. person; (ii) You are not a national of, or a company registered in, any Prohibited Jurisdiction; (iii) You shall not permit users to access or use the Solutions in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (iv) You shall comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which You and users are located.

12.7. Amendments and Waivers. No modification, addition or deletion, or waiver of any rights under these Terms will be binding on a Party unless made in a written agreement executed by a duly authorized representative of each Party. No failure or delay (in whole or in part) on the part of a Party to exercise any right or remedy hereunder will operate as a waiver thereof or effect any other right or remedy, and no waiver of one breach or default or any delay in exercising any rights will not constitute a waiver of any subsequent breach or default. All rights and remedies hereunder are cumulative and are not exclusive of any other rights or remedies provided hereunder or by law.

12.8. Notices. Any legal notice (whether these Terms expressly state "written notice" or "notice") or communication required or permitted to be given hereunder must be in writing, signed or authorized by the Party giving notice, and may be delivered by hand, deposited with an overnight courier, sent by confirmed email, confirmed facsimile, or mailed by registered or certified mail, return receipt requested, postage prepaid, in each case to the address of the receiving Party as identified in the signature box below, on a valid Purchase Order, in the case of SentinelOne to legal.notices@sentinelone.com, or at such other address as may hereafter be furnished in writing by either Party to the other Party. Such notice will be deemed to have been given as of the date it is delivered. Notice is effective on the earlier of 5 days from being deposited for delivery or the date on the confirmed facsimile, confirmed email or courier receipt.

12.9. Severability. If any provision of these Terms is deemed invalid, illegal, or incapable of being enforced by any rule of law or public policy, all other provisions of these Terms will nonetheless remain in full force and effect so long as the economic and legal substance of the transactions contemplated by these Terms is not affected in any manner adverse to any Party. Upon such determination that any provision is invalid, illegal, or incapable of being enforced, the Parties will negotiate in good faith to modify these Terms so as to affect the original intent of the Parties as closely as possible in an acceptable manner to the end that the transactions contemplated hereby are fulfilled.

12.10. Force Majeure. Except for payments due under these Terms, neither Party will be responsible for any failure to perform or delay attributable in whole or in part to any cause beyond its reasonable control, including but not limited to acts of God (fire, storm, floods, earthquakes, etc.), civil disturbances, disruption of telecommunications, disruption of power or other essential services, interruption or termination of service provided by any service providers being used by Us, labor disturbances, vandalism, cable cut, computer viruses or other similar occurrences, or any malicious or unlawful acts of any third Party(a "**Force Majeure Event**").

12.11. Counterparts. These Terms may be executed: (i) in two or more counterparts, each of which will be deemed an original and all of which will together constitute the same instrument; and (ii) by the Parties by exchange of signature pages by mail, facsimile or email (if email, signatures in Adobe PDF or similar format).

IN WITNESS WHEREOF, the Parties authorized representatives have executed these SentinelOne Terms of Service as of the Effective Date.

CUSTOMER: Sentinel Labs, Inc.

By: By:

Nam
e:

Nam
e:

Title:

Title:

Date: Date:

Address: Address: 605 Fairchild Drive,
Mountain View, CA 94043 USA

Email: Email: legal.notices@sentinelone.com

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 655561

Doc Description: Addendum 2-EndPoint Detection and Response Software - OT1912

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-12-09	2019-12-16 13:30:00	CRFQ 0210 ISC2000000010	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

Sentinel One
703-608-6223

605 Fairchild Dr
Mountain View CA
94093

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature X **FEIN #** **DATE** 12/16/19

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

Addendum

Addendum No.02 is being issued to extend the bid opening date one wee to give the agency enough time to address all technical questions received.

New date and time is: 12/16/2019 at 1:30 PM (EST). .

****

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish an open-end contract for an End Point Detection and Response Software to support endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats. The open-end contract resulting from this solicitation will provide licensing for this platform, as needed per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	CNTRCT ITEM: Containment Remediation Reporting & Monitoring	2000.00000	EA	16.00	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	SentinelOne	Complete Subscription	cmp-2K1

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Opt Renew Y2 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	16.00	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	Sentinel One	Complete Supscription	CMP-ZK1

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Opt Renew Y3 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$16.00	$32,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	Sentinel One	Complete Subscription	cmp-ZK1

Extended Description :

4.1.1 Contract Item: Containment, Remediation, Reporting & Monitoring

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Opt Renew Y4 - Cntrct Item: Contain Remediate Report Monitor	2000.00000	EA	$20.00	$40,000.00

Comm Code	Manufacturer	Specification	Model #
43233204	Sentinel One	Complete Supscripton	cmp-zk1

Extended Description :

4.1.1.1 The Vendor must provide a cloud-based software as a service solution that is capable of supporting endpoints throughout the State of West Virginia. The endpoint licenses must be billed on an annual basis.

4.1.1.2 The Vendor must provide a cloud-based software as a service solution that can be centrally managed by a West Virginia Office of Technology Administrator.

For further details see attached specifications.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Question Deadline 9:00 AM	2019-12-02

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions