SentinelOne Technical Brief

SentinelOne unifies prevention, detection and response in a fundamentally new approach to endpoint protection, driven by machine learning and intelligent automation.

By rethinking the entire approach to detecting malware, exploits and other cyber attacks, SentinelOne has developed a product that can effectively protect against sophisticated modern threats in real time. SentinelOne's patent pending dynamic behavior tracking (DBT) engine keeps organizations and individuals safe, even from the most advanced cyber attacks. It runs continuously on the endpoint, without using emulation, or sandboxing techniques.

SENTINELONE REAL-TIME UNIFIED ENDPOINT PROTECTION

SentinelOne's advanced threat protection agent is a lightweight, small footprint module that is installed on devices both at the kernel level and in user space. This agent can be deployed using a standard MSI/PKG package.

Monitoring

The agent "taps" every process and thread on the system, and extracts all relevant operations data, including system calls, network, IO, registry (on Windows) and more, so it can monitor the behavior of every process that executes on the system.

Traditional antivirus, and other preventive solutions that leverage inline processes, use static signatures or other reputation methods to evaluate executing binaries to determine whether it's malicious or not. By contrast, the SentinelOne approach doesn't require being inline – the agent automatically "taps" and obtains operation data, and allows the process to continue while monitoring everything the process does during and after execution.

Pre-processing

The monitoring module asynchronously sends the operation data to the preprocessing module, which analyzes the operation data and builds a full context around every process. This stage translates the raw monitored operations data log into a much more structured, abstract operation language.

Analysis

The analyzing module is constantly working in the background and runs sophisticated pattern matching algorithms to detect malicious behaviors in full context process operations, looking system-wide at the operations, as well as historical information.

The "patterns" – malware behaviors and techniques – are researched in SentinelOne's labs by reverse engineering thousands of malware samples daily, clustering them, and deducing behaviors to research and score.

The analyzing module scores every malicious and suspicious pattern detected during process execution, and once the aggregate score exceeds a threshold, the process is considered malicious.

Suspicious patterns of execution are typically different techniques or interactions with the operating system that malware is employing throughout its execution lifecycle. This lifecycle can include (although cases will vary) the following stages: exploitation, obfuscation, persistence, collection, and exfiltration.

Mitigation

When a process is considered malicious, the mitigation module takes action, and there are different settings to either configure as a policy or manually perform including: kill the process, quarantine malicious binaries or delete them and all associated remnants. The module can and also includes the ability to restore deleted or modified files to their state prior to malware execution effectively rolling back almost everything the process has changed on the system.

Immunization

Each time a new, unknown malicious binary has been found through our behavioral pattern detection – we instantly sign it and notify other SentinelOne agents on the network – making the whole network immune to this unknown attack, by preventing it from running on other machines, and further spreading on the network.

Prevention

To block existing, known threats SentinelOne provides a layer of preemptive protection by leveraging leading cloud reputation services.

With the Cloud intelligence setting, SentinelOne sends hashes from executed binaries that exhibit suspicious behavior and uses multiple, leading scan engines to check the reputation. Binaries identified as malicious are proactively blocked while benign ones are added to the whitelist to minimize false positives.

Performance

SentinelOne's approach enables the agent to be very lightweight. The minimal overhead incurred with monitored operations is 4 micro seconds, which-- per an average machine usage of over 24 hours-- amounts to a total delay of only one second.

SentinelOne's process runs in low priority on the system, and takes between 0%-4% CPU usage. The memory footprint is about 20MB and the agent takes about 200MB on disk on an average machine usage simulated to run for over a year.

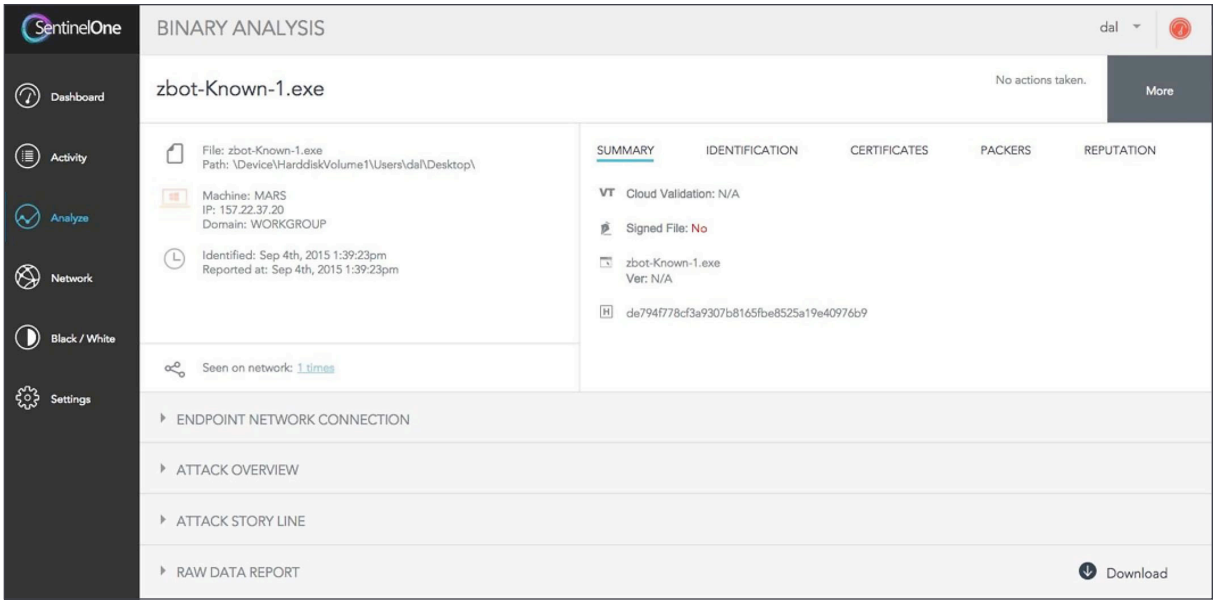
Endpoint Forensics

All the relevant data collected on the endpoint is offloaded to a centralized, unified, management console to allow admins to view and analyze binaries and threats, and conduct forensic investigation across their entire network of endpoints. The management console also provides retrospective search capabilities and endpoint remote control features. See the Real-time Endpoint Forensics section for complete details.

Real-time Endpoint Forensics

Constant monitoring of all processes at the endpoint enables SentinelOne to provide real-time forensics and a 360° view of attacks through a single management console, accessible from any device, anywhere. Security or Incident Response analysts can quickly access forensic data, and investigate to determine the root cause and accelerate incident response activities.

All the data monitored and collected from the agent is sent back to the management console over an encrypted SSL link, and stored on the management server in encrypted file systems (for details on types of data collected, refer to Appendix). SentinelOne uses this data to compile real-time forensic information to identify where attacks originated and trace the malicious actions. In addition, this data can be easily offloaded to popular SIEM systems, including Splunk, LogRhythm, for further investigation or sent to network security devices for proactively blocking threats at the gateway.

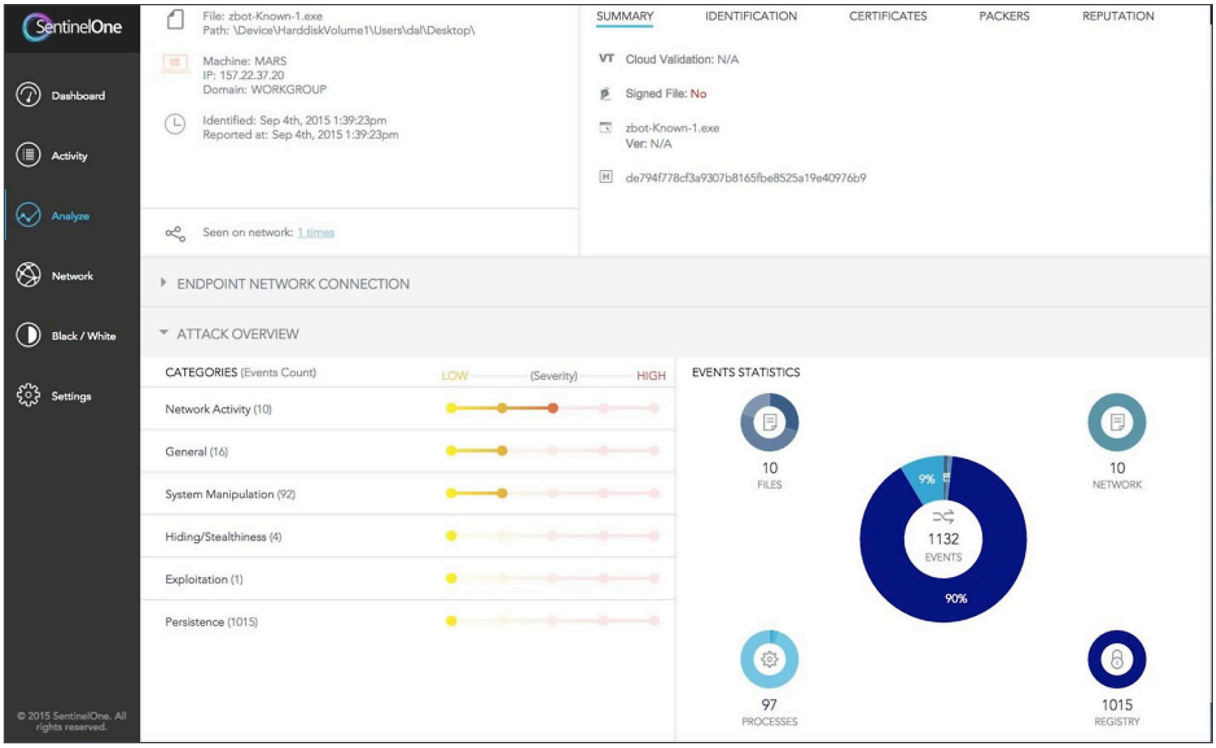


360° view of attacks

SentinelOne provides a 360° view of attacks including:

SUMMARY INFORMATION	ATTACK OVERVIEW	ATTACK STORY LINE	RAW DATA
provides indicators the solution used to determine if a process was malicious, including capturing attack statistics and dwell time. This analysis content includes, file information, path, machine name, IP, domain also where else across the network it has been seen. In addition, any cloud reputation validation, certificate information (file signed or not), and advanced attack details such as listing known packers that were used.	detailed information about the indicators the solution used to determine if a process was malicious, including capturing attack statistics and dwell time. See the table below for complete explanation of the different event categories.	a graphical way of identifying how malware propagated during execution including what other processes it created, terminated or tainted, what kind of low level calls (kernel) and api calls (user space and wmi) were called, what files it dropped, altered, deleted and created, which registry keys it changed, created or deleted (and their values), and finally, which network connections - inbound and outbound were made and to where during malware execution.	a comprehensive line-by-line detailed technical view of changes made to the system, files, processes, and registry settings

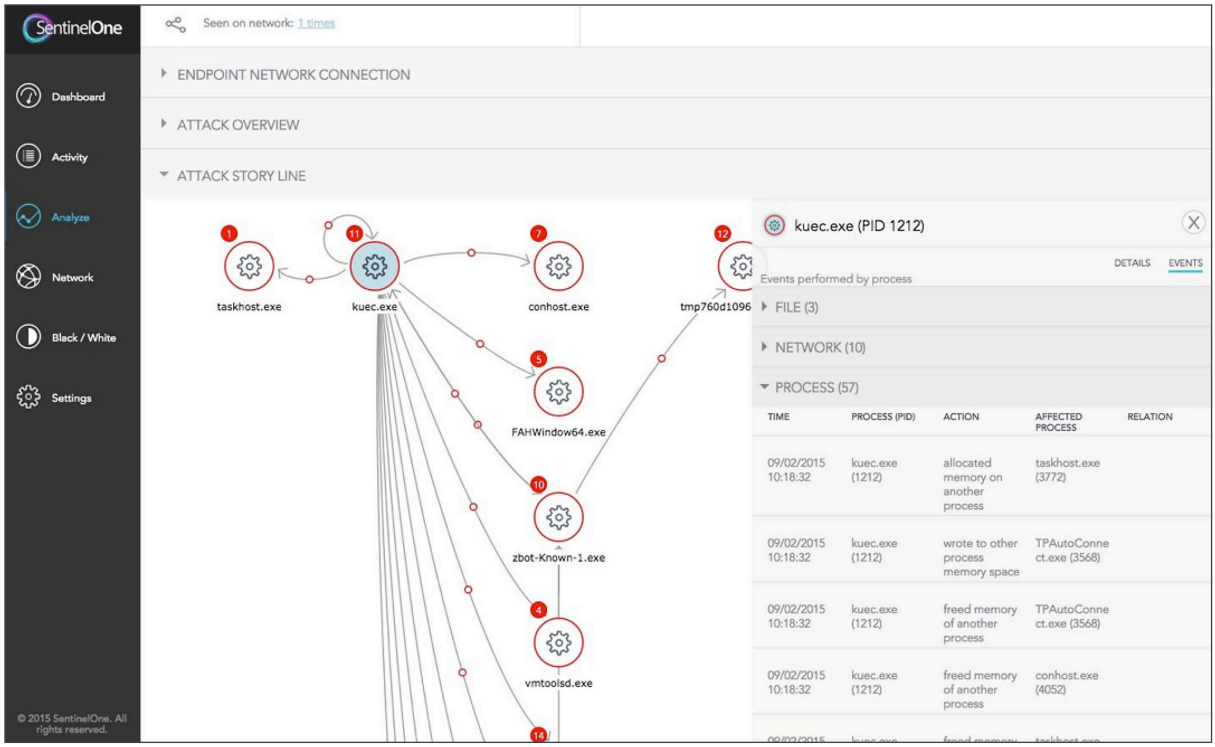
The forensic reports are accessed through the management console and provide rich, visual details in real time that simplify collection and analysis of security incident data to accelerate investigative efforts. This information enables analysts to easily determine if other machines on the network were also compromised.



Attack Overview

The Attack Overview provides a quick breakdown of the different malicious behaviors that were detected and their associated risk levels. In addition, it reports key activities performed by the malicious file, dwell time, and the number of network calls made. This report provides an overview of the activity that was monitored and used to identify the file as malicious.

CATEGORIES	AGENT MONITORS MALWARE ATTEMPTS TO:
HIDING/STEALTHINESS	Hide operation from traditional antivirus solutions, as well as from the user. Common methods include: modifying registry keys or file attributes, using obscure file names and code obfuscation. Other techniques the agent monitors are: sophisticated code injections, in memory encryption/ decryption, and the use of commercial or custom/modified packers.
PROCESS OPERATIONS	Manipulate process operations by performing remote code injections to other processes, hiding processes and services, as well as elevating or manipulating processes.
SPYING	Track user behavior (e.g., log keystrokes, take screenshots) through API, sys, or IO calls.
ANTI-DETECTION	Evade detection from standard anti-virus solutions through obfuscation techniques such as deleting its own files or leveraging packers.
GENERAL	Perform behaviors that may not be strictly malicious in isolation, but provides additional context to help determine whether the process is part of an attack flow or not.
EXPLOITATION	Take advantage of vulnerabilities through memory manipulations, privileged function calls, or buffer overflows.
SYSTEM MANIPULATION	Manipulate operating system files that typically do not change often (e.g., registry settings, task scheduler, etc). This enables malware to take advantage of the system to avoid detection, persist, collect data, and mitigation.
NETWORK ACTIVITY	Connect to command and control servers. The purpose is to allow malware to download additional components or exfiltrate data.
PRIVILEGE ESCALATION	Elevate user privilege levels to gain access to system resources. This would allow malware to perform unauthorized actions including modifying files and settings or access to system resources.
PERSISTENCE	Persist on the system using a number of approaches such as, loading itself after a system reset through operating system manipulation (e.g., task scheduler, registry settings, launch agents, etc), injecting into existing system libraries, and modifying the master boot record.

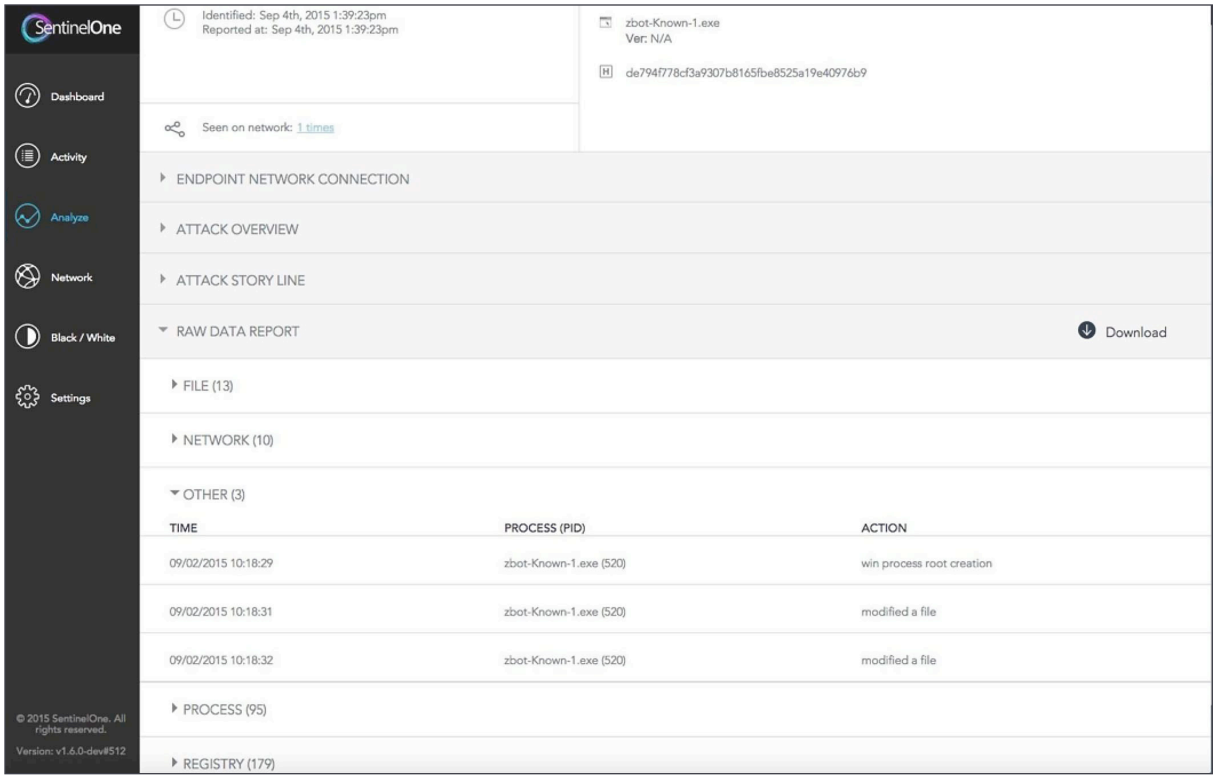


Attack Story Line

The Attack Story Line report provides a detailed view of the threat execution flow including the sequence of events, malicious behaviors, and affected system components. The unique visual format of the report graphically correlates chain related events of attacked systems which helps analysts minimize the effort needed to investigate security incidents and plan further actions.

Specific details provided by this view include the names of the malicious processes (e.g., identifying the initial process), the actions taken (e.g., creating, modifying, or deleting other system files, including registry settings or processes), and the sequence of the execution flow.

In addition, users can select a specific process on the attack storyline and view network, file, process, data actions that were specifically taken.



Raw Data Report

For a deeper dive of all the events associated with security incidents, the Raw Data report provides comprehensive attack related technical details including activity for files, network, processes, and registry (Windows only). The Raw Data report is also available for download for easier analysis. This Raw Data report provides detailed data based on the behavior executed by the malware. Although there are other indicators that the solution provides details about, the information represented here is based on the behavior of the Zeus malware.

FILE	PROCESS	NETWORK	REGISTR
The File section provides further details about files involved in an attack including the timestamp, file names, file actions executed, and the file location.	The Process section contains details for processes involved in an attack including the timestamp, process name/ID, process actions executed, the names of impacted processes, and the relationship of those processes.	The Network section includes details about the connections a process attempted to make including the protocol used, the source and destination addresses, and when the attempts took place.	The Registry section provides specific information about the registry key associated with the attack as well as the action performed, when the action took place, and the registry key location.

SYSTEM REQUIREMENTS

CLIENTS	
OPERATING SYSTEMS	• Windows 7, 8, 8.1 • Windows Server 2008 R2, 2012 R2 • .NET 4.5 • OS X 10.9.x, 10.10.x • Virtual environments: vSphere, Microsoft Hyper-V, Citrix Xen Server, Xen Desktop, Xen App
HARDWARE	• 1 GHz Dual-core CPU or better • 1 GB RAM or higher if required by OS (recommended 2 GB) • 1 GB free disk space

MANAGEMENT SERVER *(ON PREMISE)*	
OPERATING SYSTEM	• Linux Ubuntu 14.04 LTS Server
HARDWARE	• Dual core CPU, 2GHz and above • 8 GB RAM • 32 GB free disk space

APPENDIX - DATA COLLECTION

The following sections list the types of data collected by the SentinelOne agent.

HARDWARE DATA	• CPU data (ID, architecture, # of cores, clock speed) • RAM size • Disk size • Hardware device info • Device type (Desktop/Server/Mobile)
USER DATA	• User name • Machine name • Workgroup/domain
VERSION DATA	• Installed OS version • Installed SentinelOne EDR agent version
PROCESS ACTIVITY	• Time of machine activity • Running processes (name, ID, CPU usage, memory) • Low level System calls • User space API calls • For each process the SentinelOne EDR agent collects: - File access, metadata only (full path, file type, type of access, time of access etc.) - Network access, metadata only (IP, protocol used, time of access etc.) - Memory access, metadata only (memory addresses, permissions, sources, targets) - Registry access [Windows only] (keys created, altered, deleted, values) - Registry modified content [Windows only] (values of new or modified keys)
NETWORK	• Internal network IP address, domain name, DNS server • Public IP address (if running cloud-based management) • URLs accessed • Inbound/Outbound connections, metadata only (source, target, and application)