SOPHOS
Security made simple.

SOPHOS
INTERCEPT X
A completely new approach to endpoint security.

Sophos Intercept X

Stopping Active Adversaries

An explanation of features included in Sophos Intercept X

Last updated 22th June 2017 v1.0

Contents

SOPHOS

Introduction

Sophos Intercept X is a next-generation endpoint protection product that addresses modern endpoint threats by targeting the tactics techniques and procedures used by active adversaries. The product can be deployed alongside existing antivirus products or as a single, integrated agent when deployed with Sophos Central Endpoint Advanced. Intercept X contains a number of key features that address threats differently than most other endpoint protection products, but it has the same objective, preventing compromise of your critical systems and data. The key features in the product include:

Intercept X

- **Comprehensive Anti-Exploit –** Detecting and stopping over 20 exploit methods used to compromise vulnerable applications (see our whitepaper on Exploits Explained).
- **CryptoGuard –** Detecting and rolling back malicious file encryption (ransomware).
- **Application Lockdown –** Preventing malicious behaviors of applications, like a macro in a Word document that installs another application and runs it.
- **Safe Browsing –** Intercept X includes policy options to monitor a web browser's crypt, presentation, and network interfaces to detect man-in-the-browser attacks that are common in many banking Trojans.
- **Root Cause Analysis –** Providing an explanation of what happened and how when malicious activity is detected.
- **Clean –** This provides a robust malware removal capability that will restore tampered Windows OS files and registries.
- **Compatibility with other vendor Anti-Virus –** Sophos Intercept X is designed to work alongside competitive antivirus products or to be deployed as a single, integrated agent with Sophos Endpoint Advanced.
- **Synchronized Security –** Collaboration with other Sophos Synchronized Security-enabled products to share contextual threat information and to respond automatically to detected threats.

The design objective of Sophos Intercept X is to build a pure, next-generation protection agent that leverages our understanding of the methods used by advanced adversaries to attack organizations, devices, and users. With several hundred thousand new variants of malware created each day, the intent is to detect the methods used by the adversary instead of the millions of individual samples that have been collected. We understand that not all attacks will use malware or that if malware is used it will not always come in a convenient file or executable that can be analyzed. Modern attacks are often leveraging legitimate system components or residing purely in the memory space of a compromised process. To provide comprehensive protection, a new approach was needed. Intercept X provides that new approach.

Some common questions

What is the performance impact? Intercept X, when deployed with all features enabled, consumes <1% CPU utilization on a typical system. This can spike when malicious activity is detected and files are being restored, a root cause analysis is being performed, and Sophos Clean is triggered to remove the attacking software. In those scenarios, CPU usage can spike to 1 core for several seconds.

What is the memory utilization? The full Intercept X product consumes about 150MB of runtime memory.

Comprehensive Anti-Exploit

Unlike other endpoint protection products, Intercept X addresses exploit detection with a comprehensive approach. While almost all other vendors can claim some degree of exploit prevention, they are often only targeting a small subset of the exploit methods available to adversaries. Sophos comprehensive exploit prevention addresses all exploit methods available. With over 20 exploit detection and prevention techniques included, Intercept X provides the most robust exploit prevention product on the market today. See our Exploits Explained whitepaper for a description of each technique and a vendor comparison chart.

How does Intercept X prevent vulnerabilities being exploited

Intercept X monitors classes of applications at the kernel level. This injection into the process allows close and continuous monitoring of activity in the process, including memory access, disk, network access, DLLs loaded, and other process interactions.

As part of Intercept X the agent will classify applications based on how they are registered in the system to understand what types of protection should be applied. Applications that interact with the end user or the internet are automatically classified as such and exploit protection is provided. Applications are classified into the following profiles.

- **Web Browsers:** Works with all commercial web browsers.
- **Browser Plugins:** These are toolbar helpers and other applications that directly integrate into the browser.
- **Java Applications:** Java-based applications are identified and protected.
- **Media Applications:** This classification includes image readers, editors, audio players, and other media players.
- **Office Applications:** These constitute your document creation and reader applications like Word, Excel, Adobe, and the variety of PDF readers and editors.

What happens when an attack is detected

When exploit activity is detected the exploited application will be terminated, the user notified of the detected activity, a clean scan will be triggered, and an RCA will be requested.

What should an admin do

Exploit activity can be from a drive-by attack where the browser is interrogated by an adversary site and compromised. In this case, the browser is shut down and the adversary never successfully breached the system. In other cases, the adversary may have gained access to the device and launched the attack from another process. In this situation, the device penetrated by the adversary and other non-exploit actions could have been performed by the adversary. The administrator should review the incident report, RCA visualization, and artefact list to get an understanding of the root cause of the exploit. Understanding how the adversary penetrated the device is important. Often it will be found that the user downloaded or authorized an application that granted the adversary access and training will be advised for safe browsing.

Some common questions

False Positive Suppression: If anti-exploit detection happens for a desired application the administrator has three options to suppress the detection. It is important to focus the exclusion to the specific detection and application first. If this fails broader exclusion options are available.

Fine-grained exclusion controls: The recommended action is to suppress the specific exploit method detected and to continue to monitor the process for other exploit activity. The admin can check the user/device policy and examine the Scanning Exclusions, exclusion type 'Detected Exploits.' From here the administrator will see a list of exploit detections for users and devices and can add suppression for the specific exploit detection and application.

Course grained exclusion controls: Intercept X also has a broader exclusion capability where an identified application will be exempt from all exploit protection. This control is available in the global settings, exploit mitigation exclusions. The administrator will be provided a list of all detected applications that have been monitored to date by the Intercept X agent and can identify the application that should have all exploit detections suppressed.

Disable Exploit Policy: Administrators can turn off exploit notifications for entire application profiles like web browsers, plug-ins, java applications, media applications, and Office applications. Disabling exploit notifications for the application profile is a broad exemption and not recommended but available for when administrators require it.

CryptoGuard

Ransomware protection is a tough problem to solve, and most vendors currently detect ransomware attacks by the same old methods, detecting the specific malware variants that perform the attack. Given how easy it is to create new software that encrypts or otherwise renders unusable valuable documents, it is not surprising that these types of attacks have flourished. With CryptoGuard, Intercept X is monitoring the file data for rapid change and when that is detected CryptoGuard suspends the offending process and evaluates if it is a legitimate tool like Sophos SafeGuard, a file and folder based encryption product. If it is not a legitimate business tool performing the encryption the process will be terminated and the just-encrypted files will be restored.

By observing the behavior performed by ransomware attacks instead of trying to detect the infinite variety of software that can be written to perform these attacks, CryptoGuard has been able to detect over 99% of the new ransomware variants unleashed on businesses and consumer users without having to change the behavior-monitoring model. For those rare variants we miss with behavior monitoring we often prevent the attack with the other security layers, like exploit prevention. We recognize that no protection is perfect, so we continue to advance the technology and add additional base behavior model updates for better/faster detection of existing variants and more complete protection from adversaries that have bypassed our initial technology.

Some of the technical questions we frequently receive on CryptoGuard are answered below, but please refer to our FAQ on CryptoGuard if your questions are not answered.

How does Intercept X stop ransomware

Intercept X monitors over 70 file types that are often targeted in a ransomware attack. These files are what the adversaries have determined individuals and organizations are likely to pay to recover and are primarily focused on productivity documents, images, audio files, etc. Most ransomware attacks are careful to not encrypt the operating system's core components. They want the device to still function so that they can easily provide instructions to the end user and can eventually decrypt files when a ransom payment is made.

CryptoGuard monitors process activity that interacts with the designated file types and will take a copy of a file prior to any modification. These files are cached on the device using a Sophos-designated recovery folder, and when the files are encrypted the process performing the activity is suspended and examined.

What happens when an attack is detected

The process is examined to determine if it is a legitimate business application like a file/folder encryption product. If the process is not a legitimate business application, the process is terminated and the files are recovered to their pre-modification state. The end user will be notified of the detection and a root cause analysis and an incident report will be generated and made available for the admin to understand the origin of the attack so they can determine if additional actions should be taken.

The detection event will also trigger a Sophos Clean scan to identify any other latent malware on the device.

On termination of the ransomware process, the device is restored to a Green health state. The attack has been mitigated.

What should an admin do

The attack was detected at runtime so the adversary was able to interact with the device. Administrators should review the root cause analysis data and confirm that no other actions are required.

Depending on how the ransomware process was deployed and if other activity associated to activity, it may be appropriate to remove the device from the network and perform a more thorough investigation.

Some common questions

Is there a size limit to the files protected? For performance reasons we currently only take a copy of files under roughly 75MB. It is our experience that most files targeted by ransomware are significantly smaller than this limit and as we are able to detect a ransomware attack after observing just a handful of file changes we will almost always detect and terminate the attack before larger files have been impacted.

Is there a difference in what files are protected for a Windows desktop, server, or Mac? CryptoGuard for Windows desktop and servers works the same. In addition, CryptoGuard for Mac will be available in mid-2017. On Mac devices. different productivity document types are protected to conform to the available Mac applications.

How long does it take to recover files? File recovery is fairly straight forward, as the cached file has not been encrypted so all CryptoGuard has to do is move it back to where it was prior to the attack. Typically, ransomware attacks are detected after only a handful of files have been modified and so recover takes less than a second.

What happens to files put in the Sophos cache location? Files arrive in the cache automatically as part of CryptoGuard protection and are removed once a process is determined to be non-ransomware or when the automatic restore has completed.

How much disk space does the CryptoGuard file recover space use? We do not set a size limit on how much space CryptoGuard can consume when protecting against ransomware. It is our experience that the file space used to cache files stays under 100MB, but this could vary depending on the number of processes being monitored and the rate of file changes.

Application Lockdown

Application Lockdown stops attacks that do not typically rely on software bugs in applications, but instead abuse legitimate capabilities to perform the attack or deploy malware.

How does Intercept X protect applications

The agent will classify applications based on how they are registered in the system to understand what types of protection should be applied. Applications that interact with the end user or the internet are automatically classified as such and exploit protection is provided. Applications are classified into the following profiles.

- **Web Browsers:** Works with all commercial web browsers.
- **Browser Plugins:** These are toolbar helpers and other applications that directly integrate into the browser.
- **Java Applications:** Java-based applications are identified and protected.
- **Media Applications:** This classification includes image readers, editors, audio players, and other media players.
- **Office Applications:** These constitute your document creation and reader applications like Word, Excel, Adobe, and a variety of PDF readers and editors.

Application Lockdown monitors an application's activity. It automatically terminates the application under lockdown when it attempts to run new code introduced by the application.

For example: Macros in documents are potentially dangerous, as they are created in the Visual Basic for Applications (VBA) programming language, which includes the ability to download and run binaries from the web and also allows the use of PowerShell and other trusted applications. This unexpected feature (or logic-flaw exploit) offers attackers an obvious advantage as they do not need to exploit a software bug or find a way to bypass code and memory defenses to infect computers. They simply abuse standard functionality offered by a widely-used trusted application and only need to use social engineering to persuade the victim to open the specially-crafted document.

What happens when an attack is detected

Sophos Intercept X with Application Lockdown will automatically terminate a protected application based on its behavior. For example: when an office application is leveraged to launch PowerShell, run a macro to install arbitrary code, or manipulate critical system areas, Sophos Intercept X will block the malicious action – even when the attack doesn't spawn a child process.

Upon detection the user is notified, Sophos Clean is triggered to detect potential other malware components, and a root cause analysis incident report is requested and made available to the administrator.

What should an admin do

The attack was detected at runtime as a prohibited behavior. Often what was detected was an activity being controlled by a document, webpage, or media file. The incident report and root cause analysis data should identify the file or activity that is the root cause of the attack. Administrators should review the RCA data and confirm that no other actions are required.

Some common questions

What behaviors are prohibited by lockdown? The primary behaviors prohibited involve an application is attempting to download and install other software or modify auto-start registry and folder locations.

Can I configurable the prohibited behavior controls? Prohibited behaviors are controlled by Sophos and are not available for customization by the administrator.

Folder Restrictions vs. Application Lockdown? Some next-gen solutions employ a list of folders that applications can use to run code from (trusted/whitelisted folders). Many solutions, for example, block the temp folder from being used by attackers, whereas Application Lockdown monitors the activity of applications and automatically blocks attacks without IT administrators having to maintain allow or deny lists.

Attackers can easily bypass folder restrictions by using a folder not listed in the blacklist. Due to the behavior-based nature of Application Lockdown, Sophos Intercept X offers a more robust and automated approach to preventing attackers from abusing legitimate applications for a malicious purpose.

Prevent Child Process vs. Application Lockdown? Some next-gen solutions require IT administrators to specify which applications should not spawn child processes. They need to chart the workings of each and every application, typically 500 or more, in use by the organization.

But in today's threat landscape, attackers inject and run arbitrary code from within trusted applications without spawning new child processes. So, unlike other solutions, Sophos Intercept X's behavior-based Application Lockdown monitors an application's activity. When the protected application runs code that was already present on the system, these new processes inherit the lockdown features of the parent process.

Also unlike any other solution, a lockdown is not limited to the protected application. Lockdown is system-wide, meaning attackers cannot leverage the Windows Registry, Windows Command Prompt or other trusted applications to run the new code either.

Protect critical functions in web browsers

This protection is intended to warn when a browser is compromised by a man-in-the-browser attack (MITB) and was developed to defend users from banking Trojans by informing them when their browser may be compromised.

How does Intercept X protect the browser

Detects when the browser's presentation to the user may not match what is posted by detecting when critical browser functions get hooked by malicious code, and monitors for presentation, networking and cryptographic functions of the browser. This protection is provided to all applications that register as a browser, including commercial browsers and some homegrown ones.

What happens when an attack is detected

Intercept X will notify the user that they should close the browser session, as it appears compromised. Upon detection, a Sophos Clean scan is run, and an incident report generated with root cause analysis information for the administrator to review.

What should an admin do

Given that a potential MITB attack was detected, the administrator is advised to utilize the incident report to identify the IP/URL connection that was associated with the attack and determine if that is a location that should be added to a blacklist in the corporate firewall. Because the attack reached this point before it was detected, if web protection was enabled the site is not currently classified as malicious and blocked earlier in the attack.

If the user was providing authentication passwords as part of the session, they should be advised to change their passwords. And if they were in fact trying to connect to their financial institution they are advised to notify the institution to confirm no abnormal activity on the account has occurred.

Root Cause Analysis

When malicious activity is detected on a device it is critical that the administrator has more information so that they can understand the nature of the incident, how did it happen, what lead to the detection and what actions that should be taken to prevent similar incidents in the future. This ability to perform forensics on an attack has been the work of security operations centers armed with SIEM and device forensic tools. Unfortunately, the volume of malicious activity detections in a typical organization can easily overwhelm understaffed IT security administrators. To address this challenge, Sophos Intercept X includes automatic root cause attribution with recommended next steps.

RCA core components

Sophos data recorder – Intercept X includes a data recorder that tracks activity on the device. Information collected on process, memory, network, disk, and registry changes are recorded locally on the device and made available for RCA generation when an incident is detected. Activity over the last 30 days on the device is stored and consumes about 100MB of disk space.

Root cause attribution – Detection of malicious activity, including malware, exploits, ransomware detections, and blocking activity will trigger the RCA algorithm to examine the contents of the data recorder. The objective of the algorithm is take an identified malicious action, called a beacon event, and then track events associated with the beacon back to an origin or root cause. The root cause can be things like opening an email attachment, inserting a USB drive, browsing to website, and other activity. Once we have traced back to the root cause, the algorithm then moves forward from that event and identifies associated activity. This collection of actions is automatic and will screen out all other activity on the device that was not associated to the beacon or root cause event. By automatically tracking to the root cause and collecting associated data, we are able to perform much of the work that a manual forensic examination would need to do. This dramatically reduces the time required to understand the origin of malicious activity, and by discarding non-associated activity on the device we are able to present the most critical information to the administrator. This is provided in an incident report that is automatically made available at the administration console.

In addition to collecting the associated cause and effect information for each malicious activity, the algorithm also makes an initial determination of the severity of the incident. This will automatically set the priority as low for events that are simple block actions and raise the priority for incidents that may have interacted with multiple user-generated files, or involved multiple processes that may themselves be suspect.

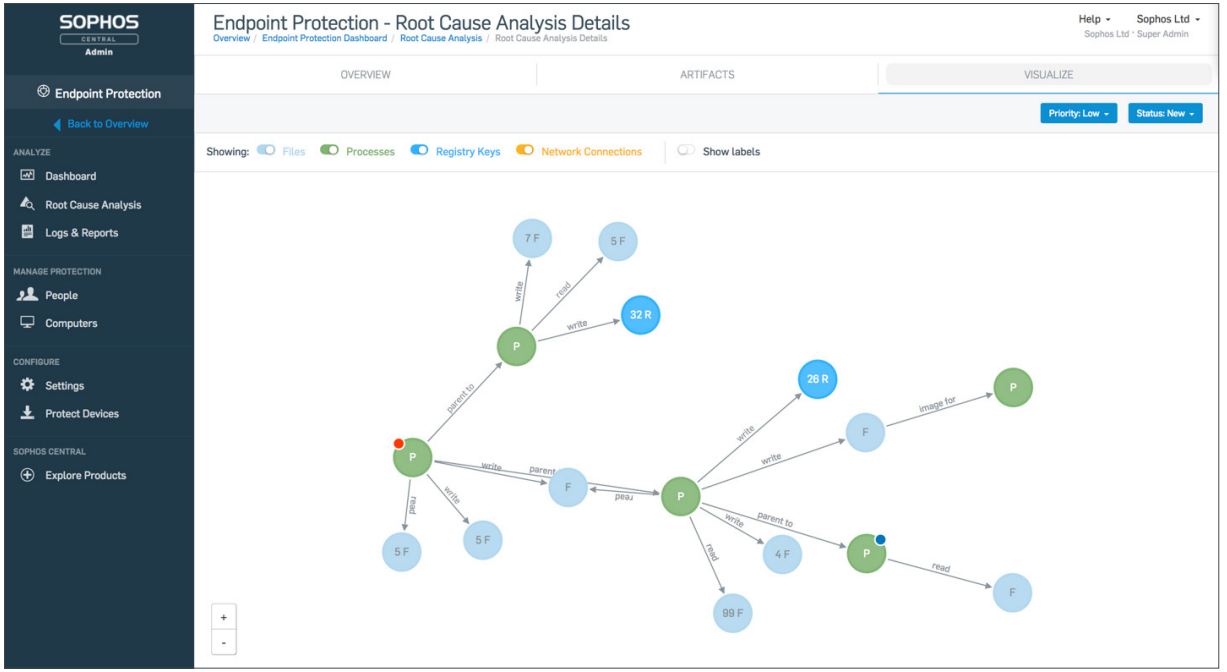
Artefact list information – Artefacts collected during RCA determination are further evaluated to determine additional information about the individual artefact. How long was the process running, what is the reputation of the artefact, is this just a Windows-protected resource being used or is this an unknown or low-reputation executable, what is the SHA256 hash identity of the process involved, was that network connection to a known classified website or not.

Visualization of attack – To facilitate understanding the attack, a visualization graph is available to the administrator that shows how each process in the activity chain interacted with the file system, registry hive, network, and other processes. Administrators can select each node of the graph and receive additional information to further clarify the activity.

Recommended Actions – As part of the incident report we include recommended actions for the administrator. These can be as simple as recommending the administrator evaluate the visualization to as specific as a recommendation to confirm device control features are enabled to prevent unauthorized USB media from being connected to the machine.

Additional Forensics

Given the insights provided by the incident response report, administrators often want to understand if particular artefacts, such as the low-reputation file called droper.exe are elsewhere in the environment and to take action on suspect processes or network connections – for example, to block access to a particular IP/URL believed to be the origin of the threat. These types of search and respond activities will soon be available form Sophos with our Security Analytics product. Security analytics enable administrators to search for artefacts across all devices in their Sophos ecosystem, generate an on-demand RCA report for any artefacts found, and to take action to block specific applications, executables, and network activity. Security analytics will also include the ability to isolate a device for deeper investigation. Look for more information on Security analytics coming in early 2018.



Top RCA questions

- **What is the performance impact of running the data recorder?** The Sophos data recorder consumes less than .5% of a typical machines CPU.
- **What will trigger an RCA?** A detection event through Intercept X or Sophos Endpoint Protection will trigger a request to generate RCA data.
- **Will I get an incident report for third-party detections?** When deployed alongside a competitive antivirus product, Sophos Intercept X will not be notified to generate the RCA data for detection events from the third-party software. If the third-party software fails to detect the threat and Intercept X intervenes, an RCA will be requested.
- **Can this integrate with my SIEM?** API information on all detection events are available for integration with third-party SIEM products.
- **Why don't all Sophos-detected malicious activities generate an RCA?** When malicious activity is detected, the RCA generation process will start. There are instances where the RCA generation algorithm is unable to track to a definitive root cause. In these instances, no RCA will be available.

SOPHOS

Sophos Clean

Sophos Clean is a component that is called upon whenever malware is detected. Its objective is to collect the detected file, confirm it is not in fact a critical system file that is being abused, and to collect associated elements to the file, like it's registry keys, links, and other files installed with it. For most malware files, the collection is quite small, but for potentially unwanted applications the collection of files, registry settings, and other components can be extensive. Once collected, the components are removed from the device.

Sophos Clean requires an active internet connection to enable the product to evaluate files, registry, and other remnants of malware as they are collected and to confirm if the component is malicious or not.

When Sophos Clean encounters a tampered Windows resource-protected file it will restore the file to correct version and remove the malicious one. This ability to restore resource-protected files on the device allows clean to successfully take a machine with multiple infections and recover it to a fully working and safe state.

Sophos clean can detect and remove malware files, cookies, unwanted applications, and registry-based malware and provides detailed results in a log file. When run alone, Sophos Clean provides a detailed report on what was found and the actions taken during the removal and restore process.

Top Clean questions

See our Sophos Clean FAQ for more info. https://community.sophos.com/kb/en-us/124101)

- **What triggers a clean scan?** Sophos Clean is triggered when malware has been detected and can be run standalone by the end user on the device. An admin-requested scan will perform scanning of software, run-time memory, and registry components to detect and remove malware. This scan operation is separate from Sophos Clean and leverages file heuristics, Sophos live lookup, and malware definition files to perform the detection and removal of the scanned artefacts. Sophos Clean can also have a scheduled scan setup from inside the desktop application.
- **Can a Sophos Clean scan be triggered by an admin or end user?** If the admin or user want to trigger a standalone Clean evaluation, they can do so from the endpoint by running the SophosClean.exe application from C:\Program Files\Sophos\Clean. When run directly the Clean results are presented to the user and also available in the log file in C:/ProgramData/Sophos/Clean/Logs.
- **Is Clean different than Scan?** Yes, Sophos Clean is triggered upon detection of malware and can be run directly by the user from the endpoint. Scanning is the operation that can be scheduled or initiated from the administration console.
- **What performance impact does a Clean scan have?** Sophos Clean typically completes in just a few minutes. While running a Clean evaluation the endpoint is still fully responsive to user activity and applications that are already running on the device continue to operate correctly.
- **Where are the Clean logs/reports stored?** Results from Sophos Clean evaluation are available in C:\ProgramData\Sophos\Clean\Logs.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Last updated 22th June 2017 v1.0

SOPHOS