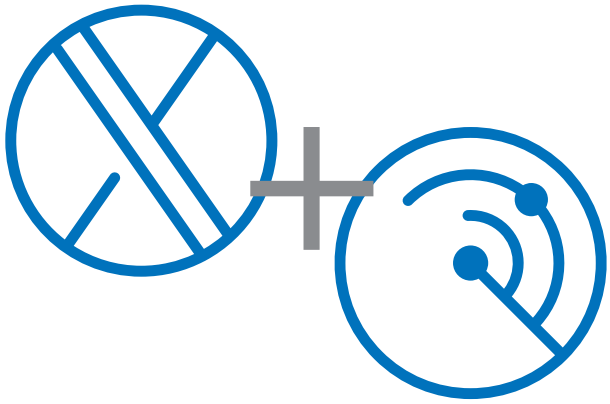
SOPHOS
Security made simple.



Solution Brief: Next Generation Endpoint Security

Evaluating endpoint security, particularly one marketed as next-gen, is not an easy task. Next-gen products often focus on one particular area of security, often just detection. Vendors are scrambling to tell you they are next-gen when what really matters is that you are protecting against and mitigating all threats to your endpoints, and that you can respond to the inevitable situation when an attack is detected.

This paper outlines the techniques applied by Sophos across its Endpoint Protection, Intercept X and Clean technology covering the three core areas of prevention, detection, and response. This is Sophos' definition of next-generation endpoint security.

Prevention: The core objective of prevention is to ensure that an adversary cannot gain access to or execute code on a protected device. The adversary's objective is unknown at this point. Endpoint security products that ignore the need to prevent the device from being attacked in the first place have already given up a valuable opportunity to protect an endpoint.

Detection: Nobody can promise 100% protection. Skilled attackers react and adopt new techniques to evade your defensive layers. But it's not only the actions of the attacker we need to be able to detect. All too often users themselves take actions that unknowingly put our endpoints at risk. We must be able to detect malicious activity occurring on the device, be it malware, data exfiltration, or lateral movement throughout your network. Detection is a must to identify and stop an attack in progress.

Response: If malicious activity has been detected, you need to take action to not only stop the attack but remove any malware already present and to inform the administrator about the details of the event. Administrators must able to quickly understand what was detected, the root cause of the event, what data was put at risk, what components of the system were involved, what should they do to prevent a future attack, and if the components of the malicious activity are on any other devices so they can provide an effective incident response.

Prevention

There are three categories of prevention that should be applied to stop malware from establishing a foothold on the endpoint device: exposure prevention, exploit prevention, and execution prevention. Within each category are multiple technologies.

Exposure prevention

Exposure prevention prevents the user's device from ever encountering an adversary or malware delivery mechanism.

Web Security and Web Control: Sophos Endpoint Protection uses intelligence from Sophos Labs to prevent devices from communicating with or browsing known bad websites or command and control hosts. Endpoint Protection also uses Live Protect to look up real time malicious URL information from Sophos Labs.

Malicious sites are constantly changing. Sophos Labs uses both proprietary techniques and industry feeds to curate its list of known bad locations. Beyond simply preventing the browser from navigating to a suspect site, Sophos will scan the content of sites accessed to look for malicious redirection code, or compromised components on the page like malicious flash objects or java scripts. Web Control features allow administrators to create a list of permitted or denied websites based upon site content category.

Device Control: Malware can easily be introduced through removable media. Plugging in an unknown USB could have devastating consequences. Device Control gives administrations policy controls to explicitly allow or deny the use of removable media when a new device is detected.

Patching: Patching is an often overlooked and simple protection method. Vendors produce patches to fix software vulnerabilities. Attackers look to exploit software vulnerabilities. f your up-to-date with patching, you reduce the attack surface for the adversary. Sophos Endpoint Protection provides patch assessment to help administrators understand which devices need to apply patches.

In addition to the exposure prevention techniques that can be executed on the endpoint other prevention methods include strong user authentication, email filtering, and the use of firewalls and UTM appliances. Detection and prevention of phishing attacks for malware delivery, blocking of access to blacklisted URLs and other methods all the way up to and including physical isolation of the device from access to the internet and pouring super glue into the USB port are all available to the security team. Sophos provides email and firewall products, to help customers deliver a layered security approach to limiting their exposure.

When evaluating any next generation endpoint security product it is important to understand what the vendor provides for exposure prevention. Many of the new entrants have ignored this aspect of next generation endpoint security all together and offer nothing here. Some go as far as saying it is OK to have your users click on everything. Others rely on a firewall to offer to offer protection, which is only applicable when the device is on the protected network.

Exploit Prevention: Exploits take advantage of weaknesses in legitimate software products like Adobe Flash and Microsoft Office to infect computers for criminal purposes.

It's common to find exploits used as part of cyber attacks: upwards of 90% of reported data breaches find that an exploit is used at one or more points in the attack chain. Including exploit prevention as part of a comprehensive lineup of security defenses is clearly valuable.

Exploits have been around for more than 30 years, so it should come as no surprise that almost every major security vendor can claim some level of exploit prevention. However, the breadth and depth of that protection varies significantly between vendors. For some, it's a box to tick; for others, it's a major focal point.

Sophos Intercept X anti-exploit technology protects against the techniques that attackers may use to exploit a software vulnerability. This entirely signatureless approach to security needs no knowledge of any malware. Intercepting attack techniques provides an incredibly efficient way to protect modern endpoints. Many of the techniques Sophos Intercept X protects against are listed in the included table.

Memory Mitigations	Code Mitigations
‣ Enforce Data Execution Prevention (DEP) – Prevents abuse of buffer overflows ‣ Mandatory Address Space Layout Randomization (ASLR) – Prevents predictable code locations ‣ Bottom Up ASLR – Improved code location randomization ‣ Null Page (Null Dereference Protection) – Stops exploits that jump via page 0 ‣ Heap Spray Allocation – Pre-allocated common memory areas to block example attacks ‣ Dynamic Heap Spray – Stops attacks that spray suspicious sequences on the heap	‣ Stack Pivot – Stops abuse of the stack pointer ‣ Stack Exec (MemProt) – Stops attacker' code on the stack ‣ Stack-based ROP Mitigations (Caller) – Stops standard Return-Oriented Programming attacks ‣ Branch-based ROP Mitigations (Hardware Augmented) – Stops advanced Return-Oriented Programming attacks ‣ Structured Exception Handler Overwrite Protection (SEHOP) – Stops abuse of the exception handler ‣ Import Address Table Filtering (IAF) (Hardware Augmented) – Stops attackers that lookup API addresses in the IAT ‣ Load Library – Prevents loading of libraries from UNC paths ‣ Reflective DLL Injection – Prevents loading of a library from memory into a host process ‣ VBScript God Mode – Prevents abuse of VBScript in IE to execute malicious code ‣ WoW64 – Stops attacks that address 64-bit function from WoW64 process ‣ Syscall – Stops attackers that attempt to bypass security hooks ‣ Hollow Process – Stops attacks that use legitimate processes to hide hostile code ‣ DLL Hijacking – Gives priority to system libraries for downloaded applications ‣ Application Lockdown – Stops logic-flaw attacks that bypass mitigations ‣ Java Lockdown – Prevents attacks that abuse Java to launch Windows executables ‣ Squiblydoo AppLocker Bypass – Prevents regsvr32 from running remote scripts and code ‣ CVE-2013-5331 & CVE-2014-4113 via Metasploit – In-memory payloads: Meterpreter & Mimikatz

Execution prevention

It is inevitable that an endpoint will be exposed to malware, so what technologies are in place to identify and block the malware before it is allowed to execute?

Execution prevention encompasses a number of interesting technologies and includes traditional signature matching of known malware, heuristic evaluation, emulation, sandboxing, file reputation scoring, application whitelisting and of course a variety of machine learning algorithms that use statistical mathematics to determine if a file is malicious or benign.

Pre-Execution Analysis: Heuristic evaluation can capture both known malware and new, never-before-seen malware. With the ability to capture zero-day and new variants of malware, heuristics models need to be adjusted and curated to prevent false positive detections. Sophos does not require the administrator to curate the rules and detection models. Right out of the box, the Sophos heuristic engine has been pre-tuned for optimal detection with minimal false positive detections, and as threats evolve, the Sophos Labs team will send out automatic model adjustments.

The Sophos heuristics engine examines any sample file to look for snippets of code that may indicate it will delete other files, make registry changes, install other files, use encrypted execution code, and the like. Heuristic-based detection is part of how Sophos detects malware and building the algorithms for heuristic malware detection involves a balance between the ability to detect malicious characteristics, while at the same time ensuring that non-malicious software that happens to possess characteristics similar to malware are not detected. This process of 'fitting' the algorithms is where the balance between detection and false positives begins to get interesting. If the heuristic rules are 'under fit' they will catch malware and non-malware alike. If they become 'over fit' they lose the ability to detect future variants. This challenge of false positives is an area where many of the newer endpoint security products simply do not compare, often requiring weeks of initial setup and continuous adjustment by the IT security administrators.

Sophos Endpoint Protection also includes an on-device emulator that detonates executables in a controlled environment. The emulator is primarily used to allow malware to uncloak and expose cyphered execution components, and to collect indicators of compromise like registry modifications and access to other files/ applications. Once uncloaked the Endpoint Protection can apply a deeper heuristic evaluation of the now exposed components.

Sandboxing: Sophos Labs has its own sandbox that is used to evaluate samples collected from industry feeds, our own honey pot network and from customer endpoints. Results from the sandbox guide the data scientists and threat analysts in the creation of the rules for both prevention models and more advanced behavior detection models. Updates go through a testing period to confirm efficacy, efficiency and false positive exclusion prior to being automatically published to all endpoints.

Download Reputation: With download reputation, Sophos Endpoint Protection has the ability to interact with the end user when a suspicious executable is downloaded to the device. When we observe the download of a highly suspicious file that has not already been classified as malicious or benign we can ask the user if they want to continue or

not. The level of suspicion for a downloaded executable is driven by a number of factors including the origin of the file, the frequency we have seen it, if it was produced by a known software publishing company, the crowd sourced results from what other users have done when asked if they want to continue downloading the file or not and multiple other attributes. In the first three months of deployment download reputation created risk scores for over 70 million executables; the list just keeps growing.

Application Whitelisting: Sophos provides an application whitelisting technology called lockdown. This technology looks to identify the allowed applications, services and processes for a server and will prevent anything new from being added. As a technology this is a great way to prevent unauthorized applications from installing. Like all technology whitelisting is not a single silver bullet and with the Sophos protected endpoint whitelisting is just a part of the overall next generation endpoint security story.

Machine Learning: This technique leverages Bayesian analytics, linear regression, random forests and other well understood machine learning algorithms to determine the probability that a file is malicious or not. The way these models work requires the algorithm to go through a training period where it is allowed to observe hundreds to thousands of detected attributes of known malicious files and given that observation the model will determine the probability that any given attribute or collection of attributes are indicators of maliciousness. Once the model is created and the weighting for each of the detection attributes set you can submit any file for evaluation and the algorithm will provide a decision on if it is malicious, benign or somewhere in between. The technique was first used extensively for anti-spam protection over a decade ago and has made its way into more general malware detection since then. At Sophos Labs a variety of machine learning algorithms are available to both detect malicious software and to adjust the rules and models of the multiple protection techniques included in the agent.

Signature Matching: It's widely acknowledged that signature matching alone is no longer good enough. By its very nature it can only detect what it already knows. Many infections are fileless, exploiting vulnerabilities; others use polymorphic malware, making it incredibly difficult for signature based systems to detect. On its own signature matching is not an effective solitary use of technology. But sometimes the old ways are still the best. Signature technology can be cheap and effective way to protect against what we already know about, providing a base line for security. Coupled with other techniques described in this document, signature technology continues to be an effective and efficient component or endpoint protection.

Detection

The malware may have been deployed by accident or purpose by a user, it may have exploited a process vulnerability and taken control of a legitimate business or operating system process, or equally troubling it may be leveraging existing authorized applications directly through a script, social engineering or by user accident or intent. This is a broad area for malicious activity detection that includes everything from insider threat detection, identity compromise and of course malware.

When looking at just malware detection we want to understand that we may not be dealing with a malware executable, it may be a script that leverages legitimate software or code that has been injected directly into a running process through an exploit. We will look at a few technologies that address detection of active malicious software, these include, network behavior, application/process behavior, data protection and exploit detection.

Network behavior: Network behavior monitoring has traditionally been a technique applied only at the firewall or through the aggregation of network data into a SIEM for analytics processing. By performing network behavior monitoring on the endpoint with Malicious Traffic Detection, Sophos Endpoint Protection and Intercept X can observe the process level communications to external devices and detect communications to suspect command and control or other malware delivery servers both when the endpoint is on the corporate network and when the device is roaming off the network. Sophos uses malicious traffic detection to trigger additional analysis of the process that generated the traffic to convict malware that has avoided other detection techniques.

Application behavior: The core objective is to determine when an application is performing a known threatening action. This includes everything from interaction between processes, the registry, and network, to specific methods used by a process for cyphering, memory access, buffers etc.

To detect threatening behaviors, a next generation endpoint security product must first ensure that runtime application activities can be detected and correlated. The observation of application activity can be done through kernel hooking, event monitoring, process injection or other means and needs to have knowledge of the current runtime as well as historic activity of the application.

Given that 'threatening' application behaviors are often legitimate actions for a business application (Word macros connecting to the internet) it becomes critical for the vendor to not only detect a threatening behavior but to understand if the behavior or combination of behaviors is sufficient to convict the application as malicious or not. Management of how the vendor determines what to notify administrators of and when to convict software as malicious can create significant challenges with behavior monitoring.

Unlike many of the other vendors offering application behavior monitoring Sophos Labs curates the models and rules required for accurate detection of malware so that our customers are not asked to perform complex training, configuration, and exemption settings to successfully deploy the product.

Anti-ransomware: The ability to detect malicious code and shut it down is undeniably valuable. But if your endpoint security only detects when ransomware runs, it may be too late. You may already have lost your files.

Sophos Intercept X uses our unique CryptoGuard technology to detect ransomware through its behaviors, stop it from encrypting your files, and then automatically roll back any files that were encrypted before detection. CryptoGuard keeps a proprietary rolling cache of the last few files accessed, allowing it to automatically restore files in the event of a crypto-ransomware attack. This avoids costly backup restore processes or having to pay the ransom. Your users just keep working.

Response

When looking at response we want to cover a few topics in more detail. Does the vendor's product provide malware removal, root cause analysis, compromised asset identification, suspect component identification, the ability to scan for the malware and suspect components across other devices and an actionable recommendation to improve overall security for detected malicious activity.

Malware removal: Be cautious of the endpoint antivirus that just wants to quarantine or delete any malware it finds. That may get rid of the immediate threat, but it doesn't typically undo any changes the malware made to the system. For example, if malware was detected, will you know if made any changes to the registry or created any other files? Did it leave any dormant code behind for use in a future attack? Sophos Clean technology performs a deep system inspection to identify any changes that malware may have made to a system and reverts them back. Sophos Clean is automatically invoked as a component of Sophos Intercept X when a detection is made. Sophos Clean can also be used as a standalone product to remove malware and any remnants from an infected system.

Root cause analysis: How do you effectively respond to an attack if you can't visualize exactly what happened? Root cause analysis provides an IT-friendly visualization of the full attack, how it started, and what it did. It also provides you with details on all the artifacts involved in the attack such as registry keys, processes, and network connections. It goes even further by automating your incident response, providing a recipe of clean up activities for the endpoint to undertake, restoring it back to original health.

Synchronized Security: By automating threat discovery, investigation, and response, Synchronized Security revolutionizes threat detection. Incident response times are reduced exponentially and tactical resources can be refocused on strategic analysis. Synchronized security allows next generation endpoint and network security solutions to continuously share meaningful information about suspicious and confirmed bad behaviour across an entire organization's extended IT ecosystem. Leveraging a direct and secure connection called the Sophos Security Heartbeat, endpoint and network protection act as one integrated system, enabling organizations to prevent, detect, investigate, and remediate threats in near real time, without adding any staff. As an example, when the Sophos next-gen firewall detects an advanced threat or an attempt to leak confidential data, it can automatically utilize the Sophos Security Heartbeat to take a series of actions across both the network and endpoint to mitigate risk and stop data loss instantly. Similarly, if a protected endpoint is discovered to

be compromised, synchronized security allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential information or sending data to a Command and Control server. This type of discovery and incident response, which could take weeks or months, has been reduced to seconds with synchronized security.

Summary

Many definitions of what a next generation endpoint security product is or does exist today. This makes selecting the right technology a complex task. With an ever increasing risk surface and complexity and volume of attacks, combined with small teams and very tight labor markets creates a very challenging world for IT security teams in small and midsized organizations.

Multiple point product approaches introduce more problems alongside the challenges they are trying to solve. We must implement new solutions that are simple, yet effective, automated and coordinated, in short synchronized via technology innovation such as the Sophos Security Heartbeat. The good news is that this capability is available today from Sophos and can be evaluated easily. To learn more and see how Sophos Intercept X and Endpoint Protection can better protect your business, visit sophos.com/intercept-x.

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

Oxford, UK

2016-12-21 SBD-NA (NP)