ESG
Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab First Look

Sophos Intercept X

Date: September 2016 **Author:** Tony Palmer, Senior Lab Analyst

Cybersecurity Challenges:[1, 2]

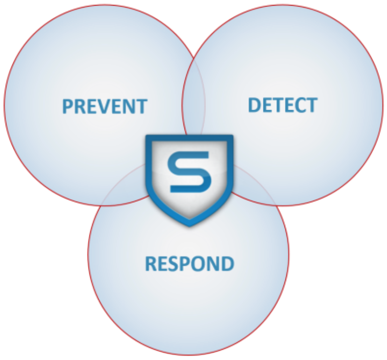
46% The percentage of surveyed IT professionals who believe ***they have a problematic shortage of cybersecurity skills***—the biggest skills gap of all types of IT skills.

37% The percentage of respondents who consider *cybersecurity* to be **an important IT priority** within their organization over the next 12 months.

In ESG's 2015 report, *The Endpoint Security Paradox*, 80% of security professionals agree that managing endpoint security processes and technologies had become increasingly difficult over the previous two years due to the increasingly dangerous threat landscape, the rise of targeted attacks, and the frequency of publicly disclosed data breaches.[3] What is needed to address these challenges is next-generation endpoint security coupled with simple, intuitive management and forensics to enable organizations of all sizes and cybersecurity skill levels to deploy advanced threat protection. While the term "endpoint security" is often equated with antivirus software, true endpoint security extends well beyond AV alone. Endpoint security is a lifecycle discipline that includes many components and disciplines. For the purposes of this report, "next-generation endpoint security" is defined as: endpoint security software controls designed to prevent, detect, and respond to previously unseen exploits and malware.

Sophos Intercept X

Sophos Intercept X is a next-generation endpoint detection and response platform for anti-exploit protection. Intercept X is designed to stop malicious threats and exploits, including zero-day attacks and ransomware. Key capabilities include advanced detection and remediation of next-generation threats using signatureless exploit detection; an end-to-end, forensic view of an attack that doesn't require a security expert to understand; and the ability to clean up both the malicious software and the effects of its activity.



Sophos Intercept X:

- Stops ransomware encryption attacks and automatically rolls back changes.
- Provides signatureless malicious traffic detection.
- Delivers root-cause analytics and advanced malware removal.

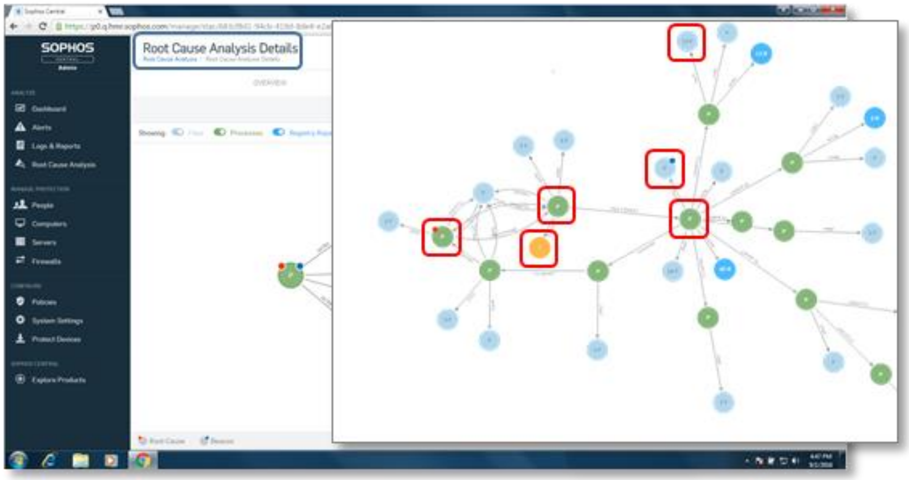
There are four features in Sophos Intercept X that work together to provide next-generation endpoint protection:

- **Signatureless threat and exploit detection**—is the anti-malware and anti-hacker defense feature designed to block zero-day, unknown, and memory-resident attacks and threat variants without the need for file scanning.
- **Anti Ransomware**—Sophos **CryptoGuard** identifies and stops unauthorized encryption activity within a few files to block ransomware before it can lock and cripple systems, and rolls encrypted files back to their pre-attack state.
- **Sophos Clean**—hunts for and removes any trace of spyware and deeply embedded, lingering malware. Designed for performance and efficiency, it can be silently installed across an entire organization and runs headless.
- **Root-cause analysis**—provides an interactive visual guide through an attack event that shows where the attack gained entry, what was affected, and where the attack stopped, and provides recommendations to prevent similar attacks in the future. This level of analysis can provide deep information and context to organizations, speeding incident response while potentially reducing the need for dedicated security analysts.

[1] Source: ESG Brief, *Cybersecurity Skills Shortage: A State of Emergency*, February 2016.
[2] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[3] Source: ESG Research Report, The Endpoint Security Paradox, January 2015.

This ESG Lab First Look was commissioned by Sophos and is distributed under license from ESG.

ESG Lab Demo Highlights



ESG Lab had the opportunity to get hands-on experience with Sophos Intercept X with a focus on how Intercept X detects and prevents advanced threats and exploits without signatures and enables rapid response through root-cause analysis.

- Sophos Intercept X detected and prevented a stack pivoting attack that used an exploit inside an Adobe PDF file. The attack was detected without using signatures or file scanning.
- An MS Word document containing real ransomware code was emailed to a user, disguised to look like it came from that user's manager with important internal data. This is a common social engineering technique used by malicious actors. When the document was opened, the ransomware code began encrypting and deleting files in the target directory, but within seconds Sophos Intercept X convicted the process, stopped the encryption, and rolled the files back to their unencrypted state. The entire event, from the double click on the attachment, through block, roll-back, and clean took less than 30 seconds.
- Finally, ESG Lab looked at root cause analysis by examining another event with Sophos Intercept X. On the ***Root Cause Analysis*** page of the Sophos Central Administration Console, we selected a case, and from the ***Root Cause Analysis Details*** page, clicked ***Visualize*** for a detailed diagram of the attack. The diagram showed the files, processes, registry keys, and network connections involved with or affected by the attack, color coded for easy identification. With a few clicks, ESG Lab was able to identify the root cause of the attack: A user had browsed to a website and downloaded a file, *free-report.exe*, which downloaded another file, *zipper.exe*. That file then read the contents of *My Documents*, zipped them up and wrote them to the root directory of the C drive before it communicated with a command and control site and attempted to upload the file, at which point it was caught by Sophos and stopped. Traditional tools would be able to detect the individual events in this incident, but would be challenged to provide the depth of context provided by Sophos Intercept X.

First Impressions

ESG believes that next-generation endpoint security should really include both advanced prevention technologies to offer superior efficacy for malware and exploit prevention when compared with traditional AV products, and advanced detection and response tools for efficient detection and remediation of malicious endpoint activities.

ESG Lab was impressed with the ability of Sophos Intercept X to provide advanced prevention, detection, and response capabilities focused on exploit techniques, and not merely the signatures of the tools used. ESG Lab found Sophos Intercept X to be simple enough for an IT generalist, while providing features and functionality advanced enough for the professional security analyst. Based on ESG Lab testing, Sophos Intercept X has made excellent progress closing many of the endpoint security gaps that still exist for organizations worldwide.