SOPHOS
Security made simple.

Intercept X: Reviewers Guide

About this guide

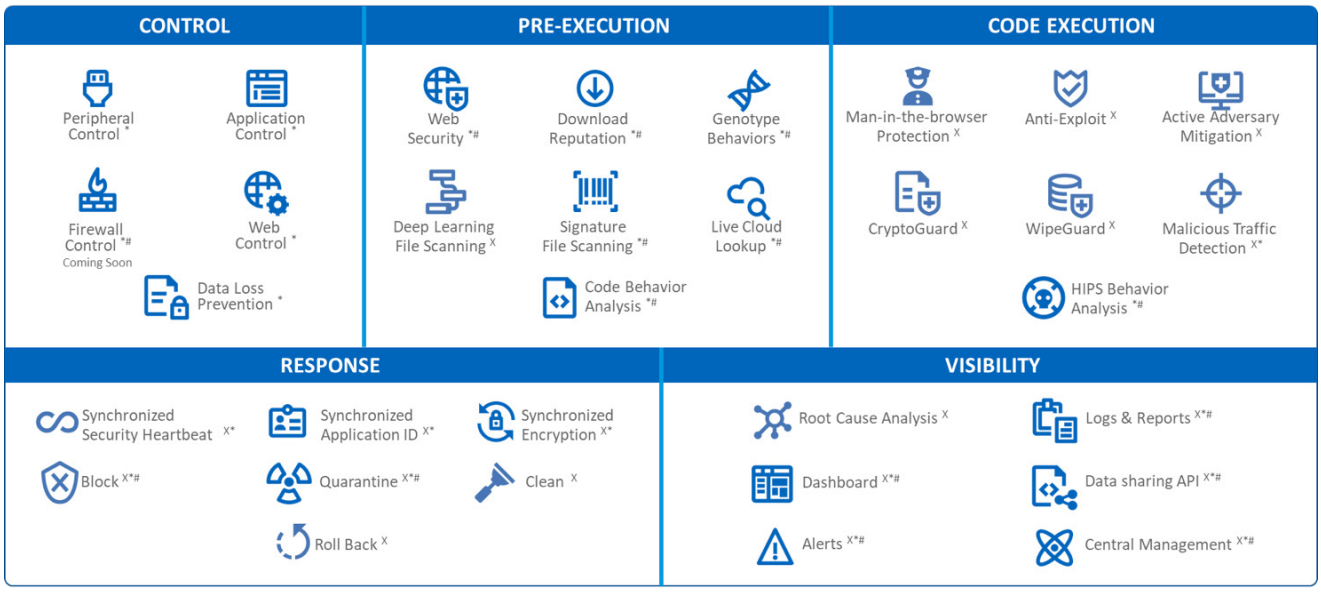
Sophos Intercept X is the world's most comprehensive endpoint protection solution. Built to stop the widest range of attacks, Intercept X has been proven to prevent even the most advanced ransomware and malware by leveraging a unique combination of next-generation techniques. This includes the ability to detect never-before-seen malware with deep learning, stop ransomware with Sophos anti-ransomware technology, and deny attacker tools with signatureless exploit prevention. Intercept X also includes root cause analysis to provide insight into threats, and instant malware removal to ensure no attack remnants remain.

This reviewer's guide is designed to help you quickly install and test Sophos Intercept X as part of a trial evaluation. It guides you through signup, downloading, installing, and testing protection.

Intercept X provides anti-ransomware, anti-exploit, active adversary mitigations, deep learning predictive malware detection, root cause analysis, and remediation. Many of these features are not provided by traditional antivirus products and, where available, may require the deployment of additional agents and management platforms, extensive configuration, and significant management overhead.

Intercept X seamlessly integrates with Sophos Endpoint Protection to deliver all of this functionality in a single agent with a single management interface. Intercept X can also be used to supplement protection alongside alternate vendor products, such as antivirus. Unlike antivirus products, Intercept X does not register itself in the Windows Security Center and can be installed when antivirus is already in place.

A Sophos Guide January 2018



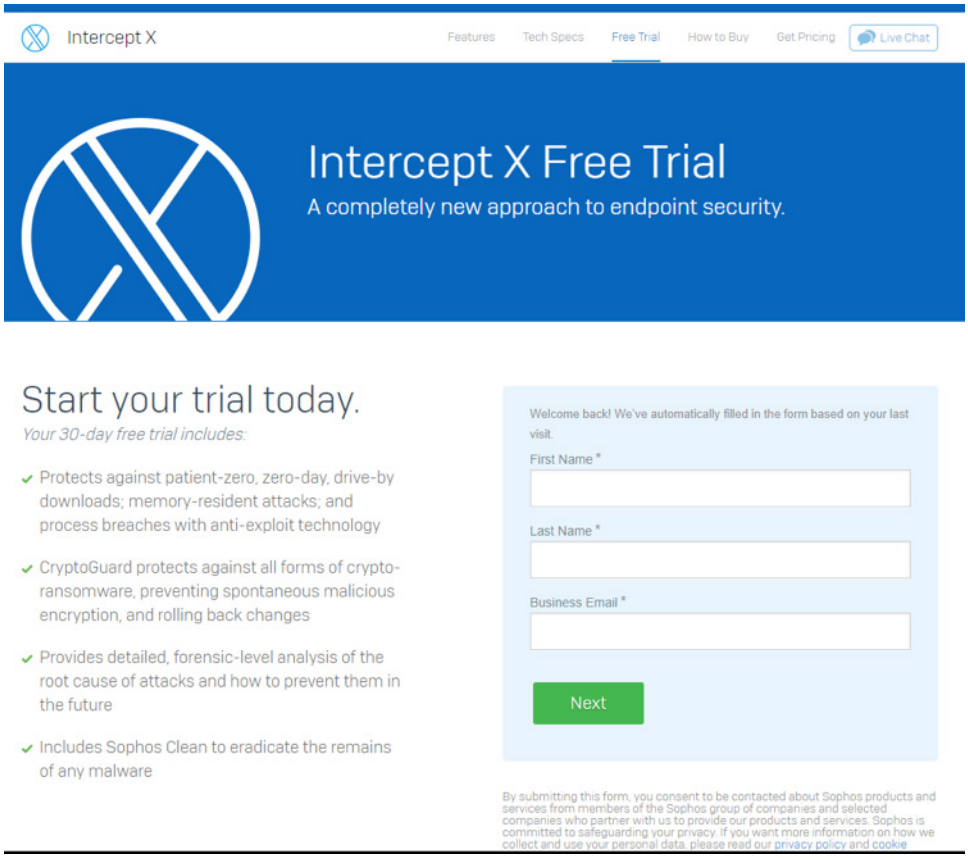
The guide covers two deployment scenarios:

1. Sophos Intercept X and Sophos Endpoint Protection Advanced running on Windows 10
2. Sophos Intercept X running on Windows 10 with an alternate vendors antivirus product that has been registered in the Windows Security Center

X Intercept X
* Endpoint Protection Advanced
# Endpoint Protection Standard

Getting Started

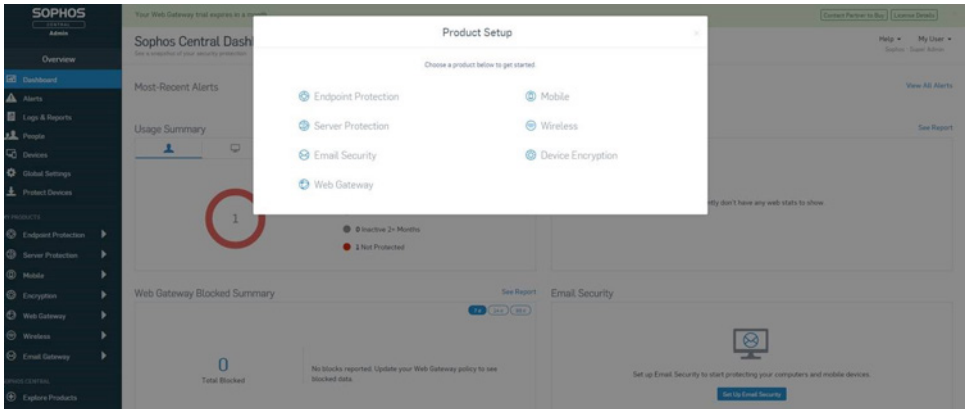
Start your free 30 day trial by registering at
https://secure2.sophos.com/en-us/products/intercept-x/free-trial.aspx



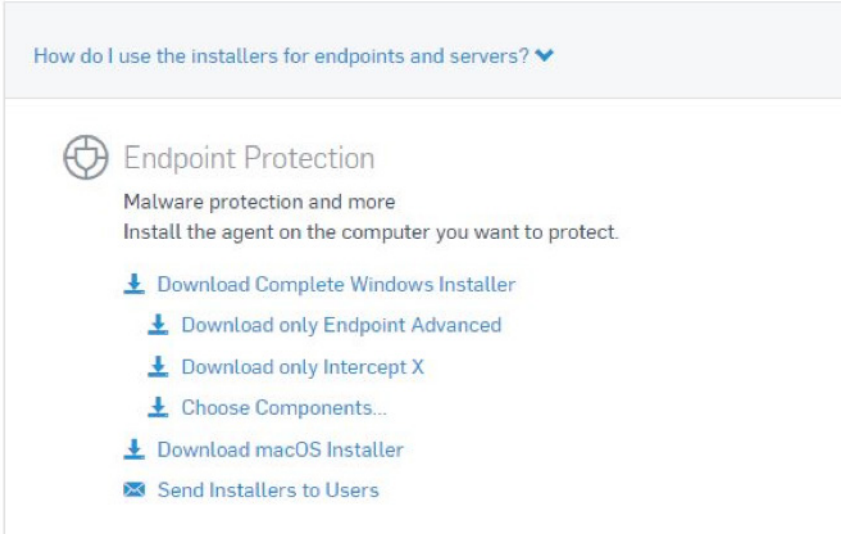
Once complete, in a few minutes you'll receive an email asking you to activate your account. You'll be guided through creating a password for Sophos Central.

Note: Sophos Central is the cloud-based administration platform used to configure and administer Sophos products.

One logged in to Sophos Central, you'll be asked to choose a product. For both deployment models, select **Endpoint Protection**.



Now we can download the agent.



Deployment mode 1 – Sophos Intercept X running on Windows 10 with an alternate vendors antivirus product registered in the Windows Security Center

Select "**Download Complete Windows Installer**"

This will download a combined installer for Sophos Intercept X and Sophos Endpoint Protection. Both products leverage the same core agent for communication with Sophos Central and will be configured with the default protection policies.

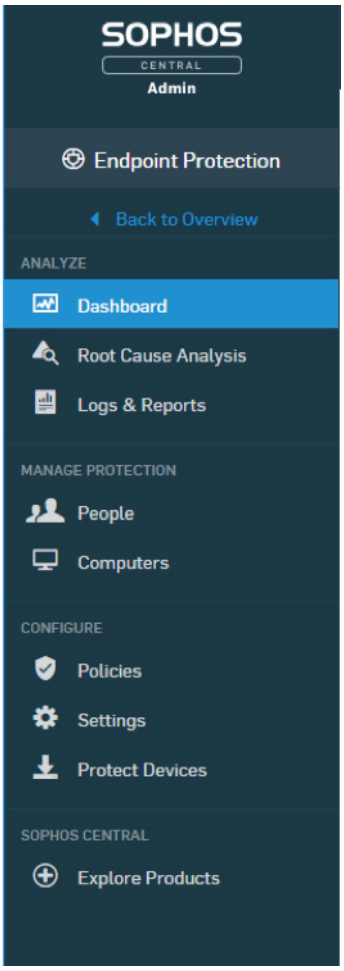
Deployment mode 2 - Sophos Intercept X and Sophos Endpoint Protection running on Windows 10

Select "**Download only Intercept X**"

This will download the Intercept X agent installer to your workstation. You can install Intercept X on any workstations you wish to use during your trial evaluation. Each workstation will register directly with Sophos Central and be configured with the default protection policies.

Copy the downloaded installer to your target workstation and execute it. The agent will register itself with Sophos Central, automatically downloading the required components and configuration. You may be prompted to restart your workstation following the installation.

You can review and adjust your policy configuration from within Sophos Central. Click **Endpoint Protection** in the **My Products** panel on the left-hand side to enter the Endpoint Protection Dashboard. From within here, you can review and amend policy settings.



Sophos Tester tool

To help demonstrate some of the capabilities of Intercept X, we have created a tool that will invoke some of the techniques an attacker may use. The tool does not contain malware or perform any malicious actions on the machine. The techniques it invokes will be detected by Intercept X to demonstrate its detection, alert, and response capability. The tool can be downloaded from https://community.sophos.com/cfs-file/__key/widgetcontainerfiles/3fc3f82483d14ec485ef92e206116d49-g-W81jjQdx00G94SmYNXfjPQ-page-1home/SophosTesterv3212.zip

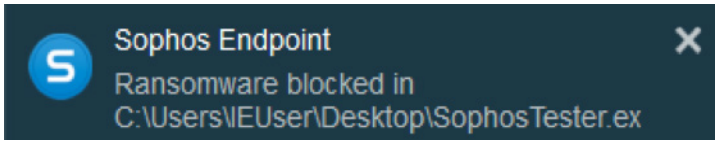
Testing anti-ransomware

Businesses large and small are under threat from increasingly aggressive and brutal ransomware attacks. Loss of access to critical files, followed by a demand for payment, can cause massive disruption to an organization's productivity.

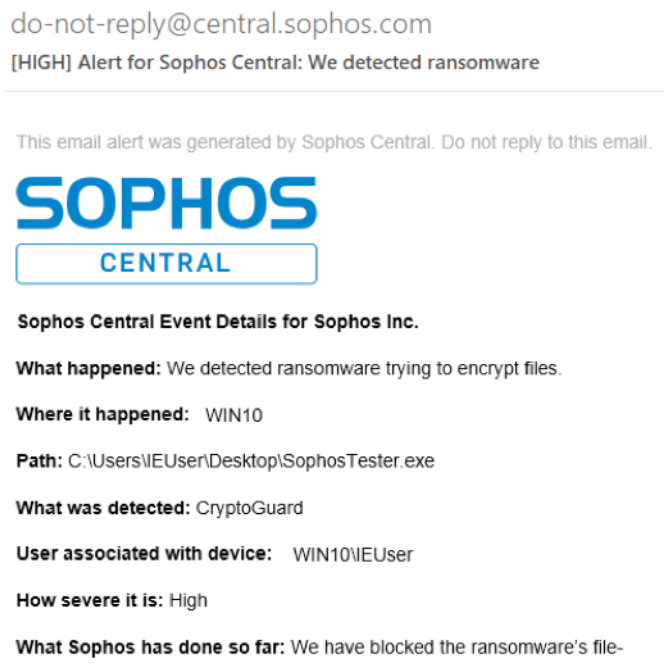
The proven CryptoGuard capabilities in Sophos Intercept X block ransomware – including Wanna and Petya variants – as soon as it attempts to encrypt your files, rolling back encrypted files to their original state.

To validate the CryptoGuard technology, open the Sophos Tester tool, select Dummy application target, Ransomware, Locky, and then Execute. This will simulate the behaviour of a variant of the Locky ransomware. The test tool will attempt to encrypt some sample RTF files. Intercept X CryptoGuard technology detects the threat and prevents any malicious impact of the ransomware.

On the users desktop a toast notification will appear, informing the user that ransomware has been blocked.



The administrator will receive an email to inform of the detection and block.


do-not-reply@central.sophos.com

[HIGH] Alert for Sophos Central: We detected ransomware

This email alert was generated by Sophos Central. Do not reply to this email.

SOPHOS CENTRAL

Sophos Central Event Details for Sophos Inc.

What happened: We detected ransomware trying to encrypt files.

Where it happened: WIN10

Path: C:\Users\IEUser\Desktop\SophosTester.exe

What was detected: CryptoGuard

User associated with device: WIN10\IEUser

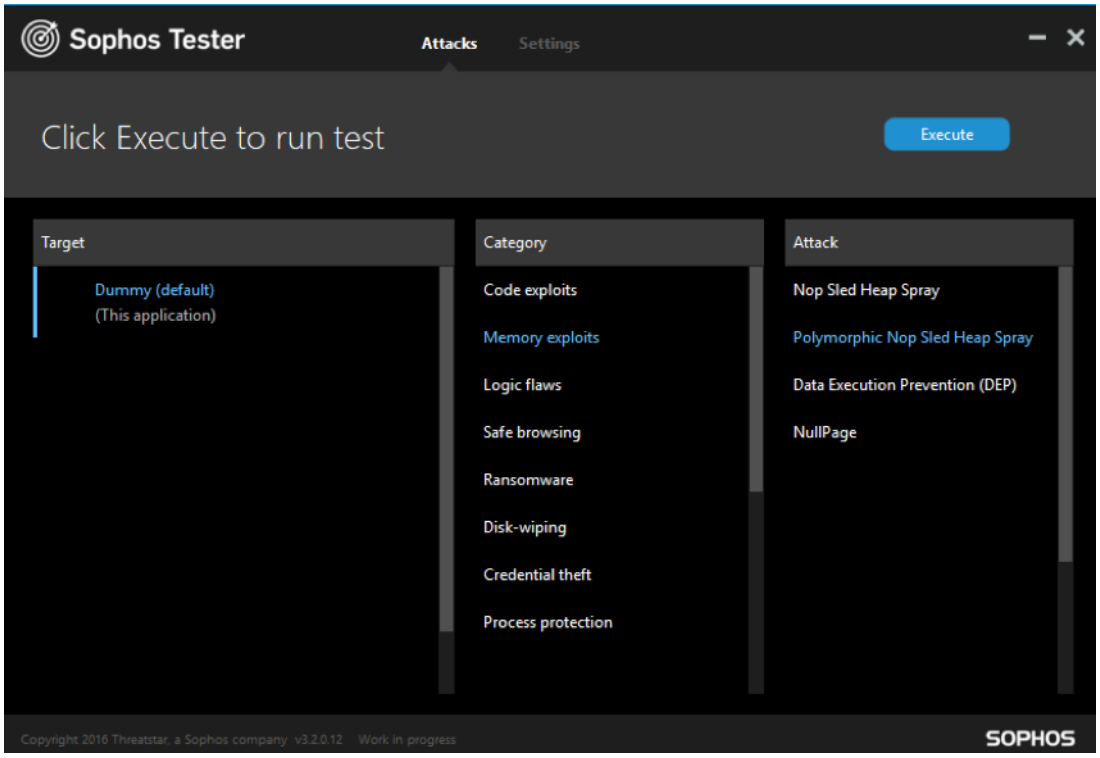
How severe it is: High

What Sophos has done so far: We have blocked the ransomware's file-

Testing anti-exploit & active adversary mitigations active adversary mitigations

Exploits are one of the main techniques used by cybercriminals to silently infect and spread malware. They take advantage of weaknesses in legitimate software products like Flash and Microsoft Office to infect computers for their criminal ends. A single exploit can be used by a myriad of malware, all with a different, nefarious purpose. Antivirus solutions focus on stopping the malware that uses the exploit as a delivery vehicle, rather stopping the exploits themselves. They go after the payloads that an attacker detonates, but not the underlying way they got inside the 'building'. While there are millions of different pieces of malware in existence, attackers only use tens of different techniques to exploit software vulnerabilities. By blocking these exploit techniques, you can stop an attack before it gets started.

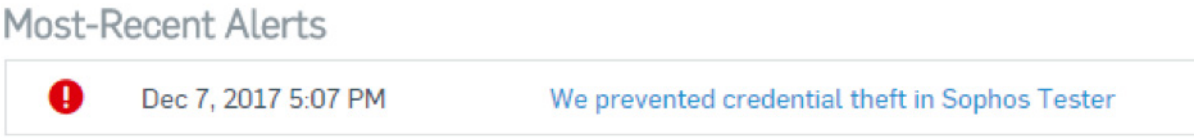
To test this, launch the Sophos tester tool. Select the Dummy application target, Memory exploits, and Polymorphic Nop Sled Heap Spray as shown. This is an example of a technique that may be used in an attack. Click **Execute**.



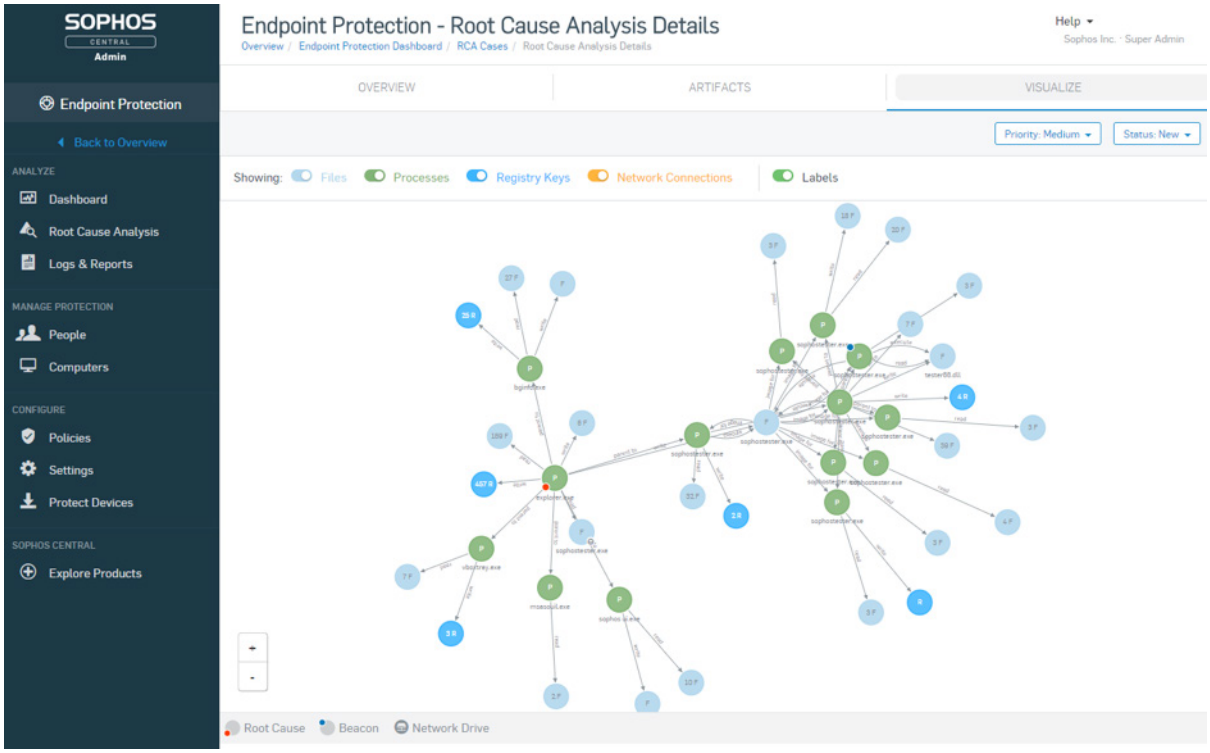
Intercept X will stop the technique and alert the user. Alert information will also be logged and sent to the Sophos Central console.

Root Caue Analysis

Sophos Central https://central.sophos.com is the unified console for managing your Sophos products. It gives you one place to manage your endpoint, mobile, encryption, web, email, server, and wireless security. It's also the place where you will find policy controls, alerts and root cause analysis.



From the left navigation menu select **Endpoint Protection**, **Root Cause Analysis**. Your most recent alerts with root cause analysis cases will be shown. From here you will be able to investigate security incidents, see the root cause, see what files and artefacts were involved and visualise the incident.



Concluding your trial

If you choose to purchase the software, you can continue to use the same Sophos Central account and will not need to redeploy any software. After your 30 day trail has concluded, your endpoints will no longer be protected.

Should you wish to trail any of the other product and services available through Sophos Central, you can activate a trial from within your existing account https://central.sophos.com/manage/central/products

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

21-12-17 RGNA (GH)