SOPHOS

Security made simple.

Intercept X

Deep Learning Malware Detection, Exploit Prevention, Anti-Ransomware, Root Cause Analysis, and Sophos Clean

Sophos Intercept X uses the right technique at the right time to stop unknown threats and deny the attacker. Layer on top of your antivirus or run with Sophos Endpoint Protection for full stack, next generation protection.

Highlights

- Trained deep learning models detect unseen malware
- Exploit Prevention stops the techniques attackers use to control vulnerable software
- Active Adversary Mitigation prevent persistence on machine
- Root cause analysis lets you see what the malware did and where it came from
- Sophos Clean removes the malware and the remains it left behind
- Augments your existing antivirus investment

Build Your Next-Gen Endpoint Security

The days of straightforward file scanning are long gone. Your goal is now to prevent threats from reaching your devices, stop them before they run, detect them if they have bypassed preventative methods, and not just clean up malware, but analyze and undo everything it does.

Sophos Intercept X uses multiple layers of technology that co-exist with your antivirus to provide full stack next-generation protection.

Deep Learning Malware Detection

Trained in SophosLabs using deep learning neural networks, Intercept X will detect new and unseen malware files with high accuracy, without signatures. Alternate methods of machine learning often demand data scientists identify attributes to look for. The resulting model is then limited by the effectiveness of the attribute selection and training data. Deep learning used in Intercept X identifies the important attributes to distinguish between malware and benign files for itself. This, coupled with an extensive training data set provided by SophosLabs, ensures an accurate and effective decision boundary is created between benign and malicious files. This trained model is smaller than 20mb in size and needs infrequent updates. Back in the cloud, SophosLabs is continuously training the model and monitoring the effectiveness of the decision boundary using new and previously unseen malware samples.

Protect Vulnerable Software

Vulnerabilities show up at an alarming rate. they represent flaws in software and need to be patched by vendors. new exploit techniques on the other hand show up on average only twice a year and are used over and over again by attackers with each vulnerability discovered. Exploit Prevention stops the techniques, stopping the attacker exploit the vulnerability before it can be patched.

Effective Ransomware Detection

CryptoGuard technology detects spontaneous malicious data encryption to stop ransomware in its tracks. Even if trusted files or processes are abused or hijacked, CryptoGuard will stop and revert them without any interaction from users or IT support personnel. CryptoGuard works silently at the file system level, keeping track of remote computers and local processes that attempt to modify your documents and other files.

Root Cause Analysis

Identifying malware and isolating and removing it solves the immediate problem. But do you really know what the malware did before it was removed, or how it was introduced in the first place? Root cause analysis shows you all the events that led up to a detection. You'll be able to understand what files, processes, and registry keys were touched by the malware and activate your advanced system clean to rewind time.

Simplify Management and Deployment

Managing your security from Sophos Central means you no longer have to install or deploy servers to secure your endpoints. Sophos Central provides default policies and recommended configurations to ensure that you get the most effective protection from day one.

Four Steps to Protection

1. Visit sophos.com/intercept-x to start your trial.
2. Create a Sophos Central admin account.
3. Download and install the Intercept X agent.
4. Manage your protection via Sophos Central.

Technical Specifications

Sophos Intercept X supports Windows 7 and above, 32 and 64 bit. It can run alongside Sophos Endpoint Protection Standard or Advanced when managed by Sophos Central. It can also run alongside third party endpoint and antivirus products to add deep learning malware detection, anti-exploit, anti-ransomware, and root cause analysis, and Sophos Clean.

	Features	
EXPLOIT PREVENTION	Enforce Data Execution Prevention	✓
	Mandatory Address Space Layout Randomization	✓
	Bottom-up ASLR	✓
	Null Page (Null Deference Protection)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Stack-based ROP Mitigations (Caller)	✓
	Branch-based ROP Mitigations	✓
	Structured Exception Handler Overwrite (SEHOP)	✓
	Import Address Table Filtering (IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	APC Protection (Double Pulsar / AtomBombing)	✓
	Process Privilege Escalation	✓
ACTIVE ADVERSARY MITIGATIONS	Credential Theft Protection	✓
	Code Cave Mitigation	✓
	Man-in-the-Browser Protection (Safe Browsing)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection	✓

	Features	
ANTI-RANSOMWARE	Ransomware File Protection (CryptoGuard)	✓
	Automatic File Recovery (CryptoGuard)	✓
	Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN	Web Browsers (including HTA)	✓
	Web Browser Plugins	✓
	Java	✓
	Media Applications	✓
	Office Applications	✓
DEEP LEARNING	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
	False Positive Suppression	✓
	Live Protection	✓
RESPOND INVESTIGATE REMOVE	Root Cause Analysis	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DEPLOYMENT	Can run as standalone agent	✓
	Can run alongside existing antivirus	✓
	Can run as component of existing Sophos Endpoint agent	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* features supported CryptoGuard, Malicious Traffic Detection,Synchronized Security Heartbeat, Root Cause Analysis

Already using Sophos Endpoint Protection with Enterprise Console for management? You can manage your endpoints using Sophos Central and enable Intercept X for automatic deployment.

Try it now for free

Register for a free 30-day evaluation at 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

SOPHOS