SOPHOS

Intercept X

The World's Best Endpoint Protection

Sophos Intercept X stops the widest range of attacks with a unique combination of deep learning malware detection, exploit prevention, anti-ransomware, and more.

Highlights

- The #1 rated malware detection engine, driven by deep learning
- Exploit prevention stops the techniques attackers use to control vulnerable software
- Active adversary mitigation prevents persistence on machine
- Root cause analysis lets you see what the malware did and where it came from
- Ransomware specific prevention technology
- Endpoint Detection and Response (EDR) that delivers powerful IT security operations hygiene and threat hunting for both IT admins and security analysts

Sophos Intercept X employs a comprehensive defense-in-depth approach to endpoint protection, rather than simply relying on one primary security technique. This is the "the power of the plus" – a combination of leading foundational and modern techniques.

Modern techniques include deep learning malware detection, exploit prevention, and anti-ransomware specific features. Foundational techniques include signature-based malware detection, behavior analysis, malicious traffic detection, device control, application control, web filtering, data loss prevention, and more.

Deep Learning Malware Detection

The artificial intelligence built into Intercept X is a deep learning neural network, an advanced form of machine learning that detects both known and unknown malware without relying on signatures.

Powered by deep learning, Intercept X has the industry's best malware detection engine, as validated by third party testing authorities. This allows Intercept X to detect malware that slips by other endpoint security tools.

Stop the Exploit, Stop the Attack

Vulnerabilities show up at an alarming rate in software and need to be constantly patched by vendors. New exploit techniques on the other hand are much rarer, and are used over and over again by attackers with each vulnerability discovered. Exploit prevention denies attackers by blocking the exploit tools and techniques used to distribute malware, steal credentials, and escape detection. This allows Sophos to ward off evasive hackers and zero-day attacks in your network.

Proven Ransomware Protection

Intercept X utilizes behavioral analysis to stop never-before-seen ransomware and boot-record attacks, making it the most advanced anti-ransomware technology available. 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.

Endpoint Detection and Response (EDR)

Sophos Intercept X Advanced is the first EDR solution designed for IT administrators and security analysts to solve IT operations and threat hunting use cases. It allows you to ask any question about what has happened in the past, and what is happening now on your endpoints. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely respond with precision.

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.

Managed Threat Response (MTR)

24/7 threat hunting, detection and response delivered by a team of Sophos experts as a fully managed service. Utilizing the intelligent EDR found in Intercept X Advanced with EDR, Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

Technical Specifications

Sophos Intercept X supports Windows 7 and above, 32 and 64 bit. 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 (Hardware Assisted)	✓
	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 include CryptoGuard, Malicious Traffic Detection,Synchronized Security Heartbeat, Root Cause Analysis

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

2020-05-11 DS (PS)

SOPHOS

SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

Endpoint Detection and Response built for threat hunting and IT operations
Sophos Intercept X Advanced with EDR consolidates powerful endpoint detection and response (EDR) with unmatched endpoint protection. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely, respond with precision.

Highlights

- EDR combined with the strongest endpoint protection
- Designed for security analysts and IT administrators
- Proactively maintain IT hygiene and hunt threats before damage occurs
- Ask any question about what has happened in the past, and what is happening now
- Out-of-the-box, fully customizable SQL queries
- Up to 90 days fast access to current and historical on-disk data
- Remotely respond with precision using a command line tool
- Detect, investigate, and prioritize incidents with the aid of machine learning
- Speed up investigations and reduce attacker dwell time
- Available for Windows, MacOS*, and Linux

EDR starts with the strongest protection

To stop breaches before they start, prevention is crucial. Intercept X consolidates the world's best endpoint protection and EDR into a single solution. This means that most threats are stopped before they can ever cause damage. Intercept X Advanced with EDR provides additional cybersecurity assurance with the ability to detect, investigate, and respond to potential security threats.

The inclusion of EDR into a consistently top-rated endpoint protection suite enables Intercept X to significantly lighten the EDR workload. As more threats are prevented, less noise is created, which prevents analysts from wasting time chasing false positives and an overwhelming volume of alerts.

Add expertise, not headcount

Automatically detect, prioritize, and investigate threats using artificial intelligence: Intercept X Advanced with EDR leverages machine learning to automatically detect and prioritize potential threats. If a potentially malicious file is discovered, users can leverage deep learning malware analysis to automatically analyze malware in extreme detail, breaking down file attributes and code and comparing them to millions of other files.

Out-of-the-box queries designed for practitioners, by practitioners: Security analysts and IT administrators can start using Sophos EDR on day one thanks to out-of-the box SQL queries categorized by use case. Queries can easily be edited for custom searches, built from scratch, or sourced from our community.

Answer the tough questions by replicating the roles of hard-to-find analysts: Intercept X Advanced with EDR replicates the tasks normally performed by skilled analysts, so organizations can add expertise without having to add staff.

Built for threat hunting and IT operations

Sophos Intercept X Advanced is the first EDR solution designed for IT administrators and security analysts. It allows you to ask any question about what has happened in the past, and what is happening now on your endpoints. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely, respond with precision. This is achieved by leveraging two key features: Live Discover and Live Response.

**Coming soon*

Live Discover: Ask any question to stay ahead Live Discover gives security analysts and IT admins the ability to ask, and answer, almost any question they can think of across their endpoints and servers. Quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity. Live Discover uses powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include:

IT operations

- Why is a machine running slowly? Is it pending a reboot?
- Which devices have known vulnerabilities, unknown services, or unauthorized browser extensions?
- Are there programs running that should be removed?
- Is remote sharing enabled? Are unencrypted SSH keys on the device? Are guest accounts enabled?
- Does the device have a copy of a particular file?

Threat hunting

- What processes are trying to make a network connection on non-standard ports?
- List detected IoCs mapped to the MITRE ATT&CK framework
- Show processes that have recently modified files or registry keys
- Search details about PowerShell executions
- Identify processes disguised as services.exe

Live Response: Remotely respond with precision When issues are discovered, Live Response provides users command line access to endpoints and servers across their organization's estate. Remotely access devices to perform further investigation or remediate any issues. Administers can reboot devices, terminate active processes, run scripts, edit configuration file, install/uninstall software, run forensic tools, and more.

Managed detection and response

The Sophos Managed Threat Response (MTR) service provides 24/7 threat hunting, detection, and response delivered by a team of Sophos experts as a fully managed service. While other managed detection and response (MDR) services simply notify you of attacks or suspicious events, with Sophos MTR, your organization is backed by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats. Customers who choose to leverage Sophos MTR also receive Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
Foundational techniques	✓	✓	✓
Deep learning	✓	✓	
Anti-exploit	✓	✓	
CryptoGuard anti-ransomware	✓	✓	
Endpoint detection and response (EDR)	✓		

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

20-05-12 DS-NA (MP)

SOPHOS