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