

Intercept X & Central Endpoint Protection Overview

Managed by Sophos Central

		SKU	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓	✓	
		Download Reputation	✓	✓	✓	
		Web Control / Category-based URL Blocking	✓	✓	✓	
		Peripheral Control [e.g. USB]	✓	✓	✓	
		Application Control	✓	✓	✓	
	BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection			✓	✓
		Anti-Malware File Scanning	✓	✓	✓	
		Live Protection	✓	✓	✓	
		Pre-execution Behavior Analysis (HIPS)	✓	✓	✓	
		Potentially Unwanted Application (PUA) Blocking	✓	✓	✓	
		Intrusion Prevention System (IPS, coming 2020)	✓	✓	✓	
	STOP RUNNING THREAT	Data Loss Prevention	✓	✓	✓	
		Runtime Behavior Analysis (HIPS)	✓	✓	✓	
		Antimalware Scan Interface (AMSI)	✓	✓	✓	
		Malicious Traffic Detection (MTD)	✓	✓	✓	
		Exploit Prevention (details on page 2)		✓	✓	
		Active Adversary Mitigations (details on page 2)		✓	✓	
		Ransomware File Protection (CryptoGuard)		✓	✓	
		Disk and Boot Record Protection (WipeGuard)		✓	✓	
		Man-in-the-Browser Protection (Safe Browsing)		✓	✓	
		Enhanced Application Lockdown		✓	✓	
	DETECT AND INVESTIGATE	DETECT	Cross Estate Threat Searching (inc. files, scripts)			✓
			Suspicious Events Detection and Prioritization			✓
		INVESTIGATE	Threat Cases (Root Cause Analysis)		✓	✓
			Deep Learning Malware Analysis			✓
			Advanced On-demand SophosLabs Threat Intelligence			✓
			Forensic Data Export			✓
	RESPOND	REMEDiate	Automated Malware Removal	✓	✓	✓
Synchronized Security Heartbeat			✓	✓	✓	
Sophos Clean				✓	✓	
On-demand Endpoint Isolation					✓	
Single-click "Clean and Block"					✓	

Sophos Intercept X Features

Details of features included in Intercept X. Intercept X Advanced also includes features from Sophos Central Endpoint Protection.

	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	✓
Dynamic Shellcode Protection	✓	
EFS Guard	✓	
CTF Guard	✓	
ApiSetGuard	✓	
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 PROTECTION	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications [PUA] Blocking	✓
	False Positive Suppression	✓
RESPOND INVESTIGATE REMOVE	Threat Cases [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, 8, 8.1, 10	✓
	macOS*	✓

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

Sophos Central Endpoint Protection Features

		OPERATING SYSTEMS	
		Windows	macOS
ATTACK SURFACE REDUCTION	Web Security	✓	✓
	Download Reputation	✓	
	Web Control / URL Category Blocking	✓	✓
	Peripheral Control (e.g. USB)	✓	✓
	Application Control	✓	✓
PRE-EXECUTION PREVENT	Anti-Malware File Scanning	✓	✓
	Live Protection	✓	✓
	Pre-execution Behavior Analysis (HIPS)	✓	
	Potentially Unwanted Application (PUA) Blocking	✓	✓
	Data Loss Prevention	✓	
STOP RUNNING THREAT	Runtime Behavior Analysis (HIPS)	✓	
	Malicious Traffic Detection (MTD)	✓	✓
REMEDiate	Automated Malware Removal	✓	✓
	Synchronized Security Heartbeat	✓	✓

Server Operating Systems are not covered by Central Endpoint of Central Intercept X. Visit [Sophos.com/server](https://www.sophos.com/server) for more detail.