Intercept X & Endpoint Protection

SOPHOS
Security made simple.

			ENDPOINT PROTECTION					INTERCEPT X
		SKU	ENDPOINT PROTECTION STANDARD	ENDPOINT PROTECTION ADVANCED	ENDPOINT EXPLOIT PREVENTION	CENTRAL ENDPOINT STANDARD	CENTRAL ENDPOINT ADVANCED	CENTRAL INTERCEPT X
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓		✓	✓	
		Download Reputation	✓	✓		✓	✓	
		Web Control / Category-based URL Blocking	✓	✓			✓	
		Peripheral Control (e.g. USB)	✓	✓			✓	
		Application Control	✓	✓			✓	
		Client Firewall	✓	✓				
	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	✓	✓		✓	✓	
		Patch Assessment		✓				
		Data Loss Prevention		✓			✓	
		Exploit Prevention			✓			✓
DETECT	STOP RUNNING THREAT	Runtime Behavior Analysis (HIPS)	✓	✓		✓	✓	
		Malicious Traffic Detection (MTD)		✓			✓	✓
		Active Adversary Mitigations						✓
		Ransomware File Protection (CryptoGuard)			✓			✓
		Disk and Boot Record Protection (WipeGuard)						✓
		Man-in-the-Browser Protection (Safe Browsing)			✓			✓
RESPOND	INVESTIGATE AND REMOVE	Automated Malware Removal	✓	✓		✓	✓	✓
		Synchronized Security Heartbeat					✓	✓
		Root Cause Analysis						✓
		Sophos Clean			✓			✓

Intercept X managed by Sophos Central

SOPHOS
Security made simple.

	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

Endpoint Protection managed by Enterprise Console

SOPHOS
Security made simple.

			ENDPOINT PROTECTION			OPERATING SYSTEMS			
		SKU	ENDPOINT PROTECTION STANDARD	ENDPOINT PROTECTION ADVANCED	ENDPOINT EXPLOIT PREVENTION	Windows	Windows Server*	macOS	Linux*
			EPS	EPA	EXP				
		Pricing	Per User	Per User	Per User add-on to EPS/EPA				
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓		✓	✓	✓	
		Download Reputation	✓	✓		✓	✓		
		Web Control / Category-based URL Blocking	✓	✓		✓	✓		
		Peripheral Control (e.g. USB)	✓	✓		✓	✓		
		Application Control	✓	✓		✓	✓	✓	
		Client Firewall	✓	✓		✓			
	BEFORE IT RUNS ON DEVICE	Anti-Malware File Scanning	✓	✓		✓	✓	✓	✓
		Live Protection	✓	✓		✓	✓	✓	✓
		Pre-execution Behavior Analysis (HIPS)	✓	✓		✓	✓		
		Potentially Unwanted Application (PUA) Blocking	✓	✓		✓	✓	✓	
		Patch Assessment		✓		✓	✓		
		Data Loss Prevention		✓		✓	✓		
		Exploit Prevention			✓	✓			
DETECT	STOP RUNNING THREAT	Runtime Behavior Analysis (HIPS)	✓	✓		✓	✓		
		Malicious Traffic Detection (MTD)		✓		✓			
		Ransomware File Protection (CryptoGuard)			✓	✓	✓		
		Man-in-the-Browser Protection (Safe Browsing)			✓	✓			
RESPOND	INVESTIGATE AND REMOVE	Automated Malware Removal	✓	✓		✓	✓	✓	
		Synchronized Security Heartbeat							
		Sophos Clean			✓	✓	✓		

* Recommend server-specific SVRWLV and SAVSVR licenses that include the full agent offering and Sophos for Virtual Environments (centralized scanning, light agent) offering for Windows servers.

Endpoint Protection managed by Sophos Central

SOPHOS
Security made simple.

			ENDPOINT PROTECTION		OPERATING SYSTEMS	
		SKU	CENTRAL ENDPOINT STANDARD	CENTRAL ENDPOINT ADVANCED	Windows	macOS
			CES	CEA		
		Pricing	Per User	Per User		
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓	✓	✓
		Download Reputation	✓	✓	✓	
		Web Control / URL Category Blocking		✓	✓	✓
		Peripheral Control (e.g. USB)		✓	✓	✓
		Application Control		✓	✓	✓
	BEFORE IT RUNS ON DEVICE	Anti-Malware File Scanning	✓	✓	✓	✓
		Live Protection	✓	✓	✓	✓
		Pre-execution Behavior Analysis (HIPS)	✓	✓	✓	
		Potentially Unwanted Application (PUA) Blocking	✓	✓	✓	✓
		Data Loss Prevention		✓	✓	
DETECT	STOP RUNNING THREAT	Runtime Behavior Analysis (HIPS)	✓	✓	✓	
		Malicious Traffic Detection (MTD)		✓	✓	
RESPOND	INVESTIGATE AND REMOVE	Automated Malware Removal	✓	✓	✓	✓
		Synchronized Security Heartbeat		✓	✓	✓

Server Operating Systems are not covered by Central Endpoint or Central Intercept X.

© Copyright 2017. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.