# Intercept X & Central Endpoint Protection Overview

SOPHOS
Cybersecurity made simple.

## Managed by Sophos Central

| | | SKU | CENTRAL ENDPOINT PROTECTION | INTERCEPT X | 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 | ✓ | | ✓ | ✓ |
| | STOP RUNNING THREAT | Data Loss Prevention | ✓ | | ✓ | ✓ |
| | | Exploit Prevention | | ✓ | ✓ | ✓ |
| | | 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) | | ✓ | ✓ | ✓ |
| | | Enhanced Application Lockdown | | ✓ | ✓ | ✓ |
| DETECT AND INVESTIGATE | DETECT | Cross Estate Threat Searching | | | | ✓ |
| | | Suspicious Events Detection and Prioritization *(coming in 2019)* | | | | ✓ |
| | 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

SOPHOS
Cybersecurity made simple.

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 | ✓ |
| 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 | ✓ |
| | Windows 8 | ✓ |
| | Windows 8.1 | ✓ |
| | Windows 10 | ✓ |
| | macOS* | ✓ |

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

# Sophos Central Endpoint Protection Features

SOPHOS
Cybersecurity made simple.

| | | 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 or Central Intercept X.
Central Intercept X Advanced also includes all Intercept X features.

# Endpoint Protection Managed by Enterprise Console

SOPHOS
Cybersecurity 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.