Sophos Central Intercept X Adv EDR

Sophos Central Intercept X Advanced with EDR Instruction Manual

Brand: Sophos | **Model:** Central Intercept X Adv EDR

Product Overview

Sophos Central Intercept X Advanced with EDR is a comprehensive cybersecurity solution designed to provide advanced endpoint protection. It combines next-generation anti-exploit, anti-ransomware, and root cause analysis capabilities to defend against a wide range of modern cyber threats. This manual provides essential information for setting up, operating, maintaining, and troubleshooting your Sophos Intercept X Advanced with EDR license.

Image: Sophos Intercept X Advanced with EDR product packaging, illustrating the software license box.

Setup and Installation

This product is a 1-year license for Sophos Central Intercept X Advanced with EDR for 1 user. Installation typically involves activating the license through the Sophos Central platform and deploying the endpoint agent to your device.

1. **License Acquisition:** Ensure you have received your digital license key or activation instructions. This is typically provided via email or a physical card within the product packaging.
2. **Access Sophos Central:** Navigate to the Sophos Central administration console. If you do not have an account, you will need to create one using the provided instructions.
3. **Activate License:** Within Sophos Central, locate the section for license activation or subscription management. Enter your license key as prompted.
4. **Download Endpoint Agent:** After successful license activation, download the appropriate Sophos Intercept X endpoint agent for your operating system (e.g., Windows, macOS).
5. **Install Agent:** Run the downloaded installer on the device you wish to protect. Follow the on-screen prompts to complete the installation. An internet connection is required during installation.
6. **Verify Installation:** Once installed, the endpoint agent will connect to Sophos Central. Verify that the device

appears in your Sophos Central dashboard and is reporting its status correctly.

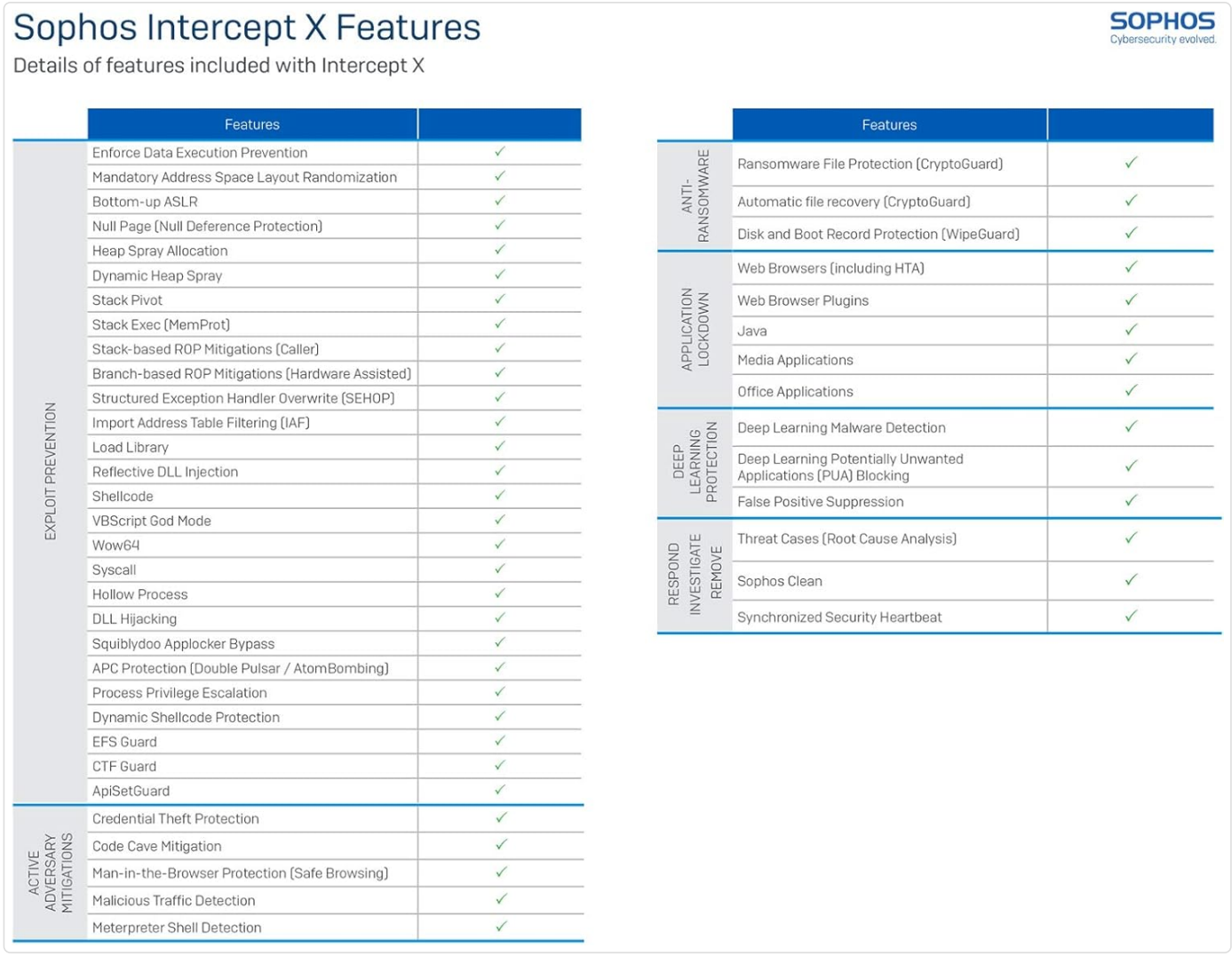
Image: Sophos Intercept X product box, highlighting the "Activation Key" component, which is essential for setup.

Operating the Software

Sophos Central Intercept X Advanced with EDR operates primarily in the background, providing continuous protection. Management and configuration are performed through the Sophos Central cloud-based console.

Key Features and Capabilities

Sophos Intercept X Advanced with EDR offers a robust set of features for endpoint security, including exploit prevention, anti-ransomware, deep learning malware detection, and extended detection and response (EDR) capabilities.



Sophos Intercept X Features

Details of features included with Intercept X

SOPHOS
Cybersecurity evolved.

	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	✓

Image: Detailed table outlining Sophos Intercept X features, categorized by Exploit Prevention, Application Lockdown, Anti-Ransomware, Deep Learning Protection, and Respond/Investigate/Remediate capabilities.

- **Exploit Prevention:** Protects against exploit techniques used in malware attacks, including memory protection, code injection prevention, and API call protection.
- **Anti-Ransomware (CryptoGuard):** Detects and blocks ransomware attacks by monitoring file encryption behavior and automatically recovering affected files.
- **Deep Learning Malware Detection:** Utilizes artificial intelligence to identify both known and unknown malware without relying on signatures.
- **Application Lockdown:** Controls which applications can run and how they interact with system resources.
- **Root Cause Analysis:** Provides detailed insights into security incidents, showing the attack chain and helping to understand how threats entered and spread.

Intercept X, EDR, and MTR Overview

The Sophos Central platform provides a unified management interface for various security features, including those found in Intercept X Advanced with EDR. The following tables illustrate the comprehensive coverage provided by this solution across different stages of threat protection.

Intercept X, EDR, and MTR Overview

SOPHOS
Cybersecurity evolved

Managed by Sophos Central

		FEATURES	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	INTERCEPT X ADVANCED WITH MTR STANDARD	INTERCEPT X ADVANCED WITH MTR ADVANCED
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓	✓	✓
		Download Reputation	✓	✓	✓	✓
		Web Control / Category-based URL blocking	✓	✓	✓	✓
		Peripheral Control	✓	✓	✓	✓
		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)	✓	✓	✓	✓
	STOP RUNNING THREAT	Data Loss Prevention	✓	✓	✓	✓
		Runtime Behavior Analysis (HIPS)	✓	✓	✓	✓
		Antimalware Scan Interface (AMSI)	✓	✓	✓	✓
		Malicious Traffic Detection (MTD)	✓	✓	✓	✓
		Exploit Prevention (details on page 5)	✓	✓	✓	✓
		Active Adversary Mitigations (details on page 5)	✓	✓	✓	✓
		Ransomware File Protection (CryptoGuard)	✓	✓	✓	✓
		Disk and Boot Record Protection (WipeGuard)	✓	✓	✓	✓
		Man-in-the-Browser Protection (Safe Browsing)	✓	✓	✓	✓
		Enhanced Application Lockdown	✓	✓	✓	✓

Image: Part 1 of a comparative table detailing features across Intercept X Advanced, Intercept X Advanced with EDR, and MTR versions, covering Attack Surface Reduction, Before It Runs On Device, Prevent, and Stop Running Threat categories.

Intercept X, EDR, and MTR Overview

SOPHOS
Cybersecurity evolved.

Managed by Sophos Central (continued)

		FEATURES	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	INTERCEPT X ADVANCED WITH MTR STANDARD	INTERCEPT X ADVANCED WITH MTR ADVANCED
DETECT AND INVESTIGATE	DETECT	Live Discover (Cross estate SQL querying for threat hunting and IT security operations hygiene)		✓	✓	✓
		SQL Query Library (pre-written, fully customizable queries)		✓	✓	✓
		Suspicious Events Detection and Prioritization		✓	✓	✓
		Fast Access, On-disk Data Storage (up to 90 days)		✓	✓	✓
	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	✓	✓	✓	✓
		Remote Terminal Access (remotely investigate and take action)		✓	✓	✓
		On-demand Endpoint Isolation		✓	✓	✓
		Single-click "Clean and Block"		✓	✓	✓
MANAGED SERVICE	HUMAN-LED THREAT HUNTING AND RESPONSE	24/7 Lead-driven Threat Hunting			✓	✓
		Security Health Checks			✓	✓
		Data Retention			✓	✓
		Activity Reporting			✓	✓
		Adversarial Detections			✓	✓
		Threat Neutralization & Remediation			✓	✓
		24/7 Lead-less Threat Hunting				✓
		Threat Response Team Lead				✓
		Direct Call-in Support				✓
		Proactive Security Posture Improvement				✓

Image: Part 2 of a comparative table detailing features across Intercept X Advanced, Intercept X Advanced with EDR, and MTR versions, covering Detect and Investigate, Respond/Remediate, and Managed Service categories.

- **Attack Surface Reduction:** Includes web security, download reputation, web control, peripheral control, and application control.
- **Pre-execution Prevention:** Features like deep learning malware detection, anti-malware scanning, live protection, and intrusion prevention systems.
- **Runtime Threat Stopping:** Incorporates data loss prevention, runtime behavior analysis, anti-malware scan interface (AMSI), malicious traffic detection, and exploit prevention.
- **Detection and Investigation (EDR):** Provides live discover capabilities for threat hunting, suspicious events detection, threat cases (root cause analysis), deep learning malware analysis, and forensic data export.
- **Response and Remediation:** Offers automated malware removal, synchronized security heartbeat, Sophos Clean, remote terminal access, on-demand endpoint isolation, and single-click "Clean and Block" actions.

Why Choose Intercept X

Sophos Intercept X is designed to address modern cybersecurity challenges with its comprehensive approach to endpoint protection.

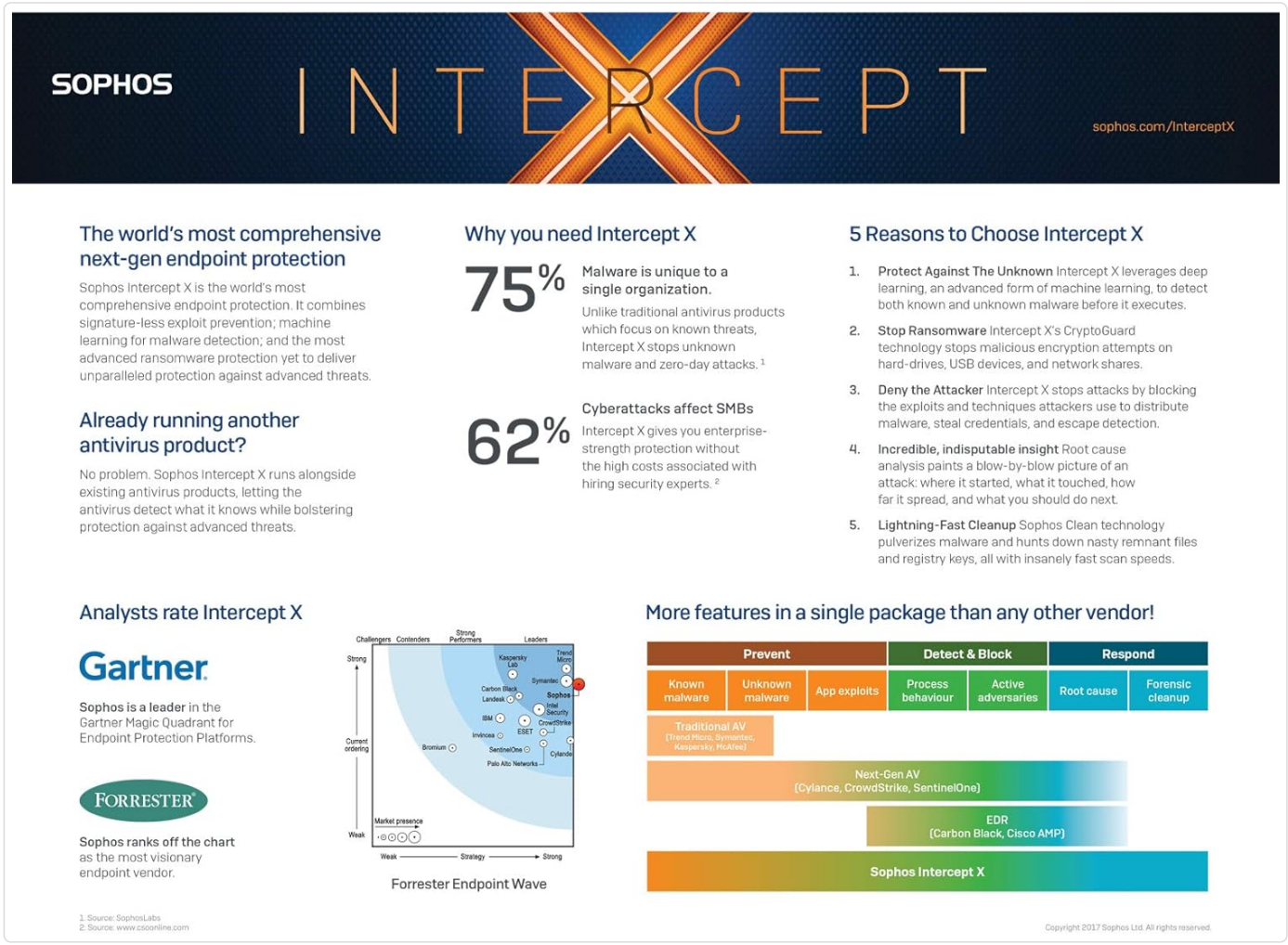


Image: An overview slide highlighting the benefits and reasons to choose Sophos Intercept X, including its comprehensive nature, unique malware detection, and robust protection against cyberattacks.

- **Next-Gen Endpoint Protection:** Combines signature-less exploit prevention, machine learning for malware detection, and advanced ransomware protection.
- **Unique Malware Detection:** Intercept X stops unknown malware and zero-day attacks, unlike traditional antivirus.
- **Anti-Ransomware:** CryptoGuard technology stops malicious encryption attempts on hard drives, USB devices, and network shares.
- **Defense Against Attackers:** Blocks exploits and techniques attackers use to distribute malware, steal credentials, and escape detection.

- **Indisputable Root Cause Analysis:** Provides a visual attack chain, showing how threats entered and what actions were taken.
- **Fast Cleanup:** Sophos Clean pulverizes malware and hunts down nasty remnant files and registry keys.

Maintenance

Regular maintenance ensures optimal performance and protection from your Sophos Intercept X Advanced with EDR software.

- **Automatic Updates:** Ensure that automatic updates are enabled within Sophos Central. This ensures your endpoint agent always has the latest threat definitions and software enhancements.
- **Regular Scans:** While real-time protection is active, consider scheduling full system scans periodically to catch any dormant or deeply embedded threats.
- **Monitor Alerts:** Regularly check the Sophos Central dashboard for any alerts, warnings, or detected threats. Address any reported issues promptly.
- **System Requirements:** Ensure your operating system and hardware continue to meet the minimum system requirements for the Sophos endpoint agent.

Troubleshooting

If you encounter issues with your Sophos Intercept X Advanced with EDR, consider the following troubleshooting steps:

- **Connectivity Issues:** If the endpoint agent is not reporting to Sophos Central, check your internet connection and firewall settings to ensure Sophos communication is not blocked.
- **Performance Degradation:** If your system experiences slowdowns, ensure your device meets the recommended system requirements. You can also temporarily disable specific Sophos features (e.g., deep learning) for testing, but re-enable them promptly.
- **False Positives:** If legitimate applications or files are being blocked, you can add them to exclusions within the Sophos Central policy. Exercise caution when creating exclusions.
- **Installation Failures:** Ensure no other antivirus software is installed on the system, as this can cause conflicts. Restart your computer and try the installation again.
- **License Expiry:** If your license is nearing expiry or has expired, you will receive notifications. Renew your license through Sophos or your reseller to maintain protection.
- **Contact Support:** For persistent or complex issues, refer to the Sophos support resources or contact Sophos technical support directly.

Specifications

Feature	Detail
Product Name	Sophos Central Intercept X Advanced with EDR
Model Number	Central Intercept X Adv EDR
License Duration	1 Year
User Count	1 User
Included Components	1-year license for Sophos Central Intercept X Advanced with EDR for 1 user
Recommended Use	Security for Laptops and Endpoints
Key Features	Anti-Exploit, Anti-Ransomware, Deep Learning Malware Detection, EDR (Endpoint Detection and Response), Root Cause Analysis

Warranty and Support

This product is a software license. The terms of service and support are governed by Sophos's end-user license agreement (EULA) and support policies.

- **License Validity:** The license is valid for 1 year from the date of activation. Ensure timely renewal to maintain continuous protection.
- **Technical Support:** For technical assistance, product inquiries, or to report issues, please visit the official Sophos support website or contact their customer service. Support options may vary based on your license agreement.
- **Online Resources:** Sophos provides extensive online documentation, knowledge bases, and community forums that can assist with common questions and advanced configurations.

For the most up-to-date information on warranty, support, and terms of service, please refer to the official Sophos website: www.sophos.com