

Sophos Endpoint Tech Specs

[Free trial](#)[Online demo →](#)[Download solution brief →](#)

Strongest protection. Simple licensing.

[Sophos Endpoint Detection and Response \(EDR\)](#) elevates your endpoint defenses by enabling you to identify, investigate, and neutralize evasive threats.

[Sophos Extended Detection and Response \(XDR\)](#) extends EDR to provide visibility across your entire attack surface.

Organizations with limited in-house resources can engage [Sophos' Managed Detection and Response \(MDR\)](#) services, delivered by a team of global cybersecurity experts that monitor your environment for threats 24/7.

Sophos Endpoint System Requirements:

 [Windows >](#)  [Windows Server >](#)

 [macOS >](#)  [Linux >](#)

Protect your iOS and Android devices with [Sophos Mobile](#).

Windows Server and Linux devices require a subscription to [Sophos Workload Protection](#).

[Sophos Endpoint for Legacy Platforms](#) add-on available for critical systems running older operating systems.

Endpoint protection and control

	Sophos Endpoint Endpoint protection and control	Sophos EDR Complete endpoint protection, detection and response Learn more	Sophos XDR Comprehensive detection and response across the environment Learn more	Sophos MDR 24/7 expert-led threat monitoring and response service Learn more	Available on
THREAT SURFACE REDUCTION					
Web Protection	✓	✓	✓	✓	 
Web Control	✓	✓	✓	✓	 
Download Reputation	✓	✓	✓	✓	
Application Control	✓	✓	✓	✓	 
Peripheral Control	✓	✓	✓	✓	 
Data Loss Prevention	✓	✓	✓	✓	
Unauthorized File Protection (Windows Server)	✓	✓	✓	✓	
Full Disk Encryption	Add-on	Add-on	Add-on	Add-on	 
THREAT PREVENTION					
Ransomware file protection (CryptoGuard)	✓	✓	✓	✓	 
Remote ransomware protection (CryptoGuard) Watch video	✓	✓	✓	✓	
Ransomware Master Boot Record (MBR) protection	✓	✓	✓	✓	
Context-sensitive Defense: Adaptive Attack Protection Watch video	✓	✓	✓	✓	
Context-sensitive Defense: Estate-wide Critical Attack Warnings	✓	✓	✓	✓	
Deep Learning AI-powered malware prevention	✓	✓	✓	✓	 
Anti-malware file scanning	✓	✓	✓	✓	  

Potentially Unwanted App (PUA) blocking	✓	✓	✓	✓	  
Live Protection cloud-lookups	✓	✓	✓	✓	  
Behavioral Analysis	✓	✓	✓	✓	 
Anti-Exploitation (60+ mitigations)	✓	✓	✓	✓	
Application Lockdown	✓	✓	✓	✓	
Anti-malware Scan Interface (AMSI)	✓	✓	✓	✓	
Malicious Traffic Detection	✓	✓	✓	✓	 
Intrusion Prevention System (IPS)	✓	✓	✓	✓	
File Integrity Monitoring (Servers)	✓	✓	✓	✓	
Integrated ZTNA agent	✓	✓	✓	✓	 
Workspace Protection (Protected browser, ZTNA, DNS Protection and Email Monitoring System)	Add-on	Add-on	Add-on	Add-on	  

Detection, investigation and response

	Sophos Endpoint Endpoint protection and control	Sophos EDR Complete endpoint protection, detection and response Learn more	Sophos XDR Comprehensive detection and response across the environment Learn more	Sophos MDR 24/7 expert-led threat monitoring and response service Learn more	Available on
DETECTION 					
Rich on-device data for real-time insights	—	✓	✓	✓	
Suspicious event detections	—	✓	✓	✓	
AI-powered prioritization of detections	—	✓	✓	✓	 
Automatic MITRE Framework mapping	—	✓	✓	✓	 
Linux container behavioral and exploit detections	—	✓	✓	✓	
Device Exposure	—	✓	✓	✓	
Generate detections on integrated third-party data	—	—	✓	✓	
Cross-product event correlation and analysis	—	—	✓	✓	
INVESTIGATION 					
RCA threat graphs	✓	✓	✓	✓	 
Automatic and manual case creation	—	✓	✓	✓	 
On-demand Sophos X-Ops threat intelligence	—	✓	✓	✓	
AI Case Summary	—	✓	✓	✓	
AI Command Analysis	—	✓	✓	✓	
AI Search	—	✓	✓	✓	
AI Assistant	—	—	✓	✓	
Forensic data export	—	—	✓	✓	
RESPONSE 					
Automatic malware cleanup	✓	✓	✓	✓	  
Automatic ransomware file encryption roll-back	✓	✓	✓	✓	 
Automatic process termination	✓	✓	✓	✓	 
Synchronized Security: Automatic device isolation via Sophos Firewall	✓	✓	✓	✓	 
On-demand Adaptive Attack Protection	—	✓	✓	✓	
On-demand device isolation	—	✓	✓	✓	 

Live Response remote terminal access	—	—	✓	✓	✓	  
Microsoft 365 response actions	—	—	—	✓	✓	

DATA INGESTION 						
Extensive data on-device and in the cloud (Sophos Products)	✓	✓	✓	✓		
Cloud data retention	—	30 days	90 days	90 days	  	
Additional cloud storage retention	—	1 Year (Add-on)	1 Year (Add-on)	1 Year (Add-on)	  	
Ingest and correlate data from your existing (non-Sophos) technology investments	—	—	✓	✓		

	Sophos Endpoint Endpoint protection and control	Sophos EDR Complete endpoint protection, detection and response Learn more	Sophos XDR Comprehensive detection and response across the environment Learn more	Sophos MDR 24/7 expert-led threat monitoring and response service Learn more
24/7 MANAGED DETECTION AND RESPONSE SERVICE 				
24/7 threat monitoring and response	—	—	—	✓
Weekly and monthly reporting	—	—	—	✓
Health Check	—	—	—	✓
Expert-led threat hunting	—	—	—	✓
Threat containment	—	—	—	✓
Direct call-in support during active incidents	—	—	—	✓
Full-scale incident response: threats are fully eliminated	—	—	—	✓
Root cause analysis	—	—	—	✓
Dedicated Incident Response Lead	—	—	—	✓
\$1M Breach Protection Warranty	—	—	—	✓
Guided threat insights from Sophos X-Ops	—	—	—	✓

	Sophos Endpoint Endpoint protection and control	Sophos EDR Complete endpoint protection, detection and response Learn more	Sophos XDR Comprehensive detection and response across the environment Learn more	Sophos MDR 24/7 expert-led threat monitoring and response service Learn more
OPTIONAL ADD-ONS 				
Sophos Endpoint for Legacy Platforms	Optional	Optional	Optional	Optional
Sophos Device Encryption	Optional	Optional	Optional	Optional
Sophos Workspace Protection	Optional	Optional	Optional	Optional
Sophos Advisory Services	Optional	Optional	Optional	Optional
Sophos Incident Response (IR) Services Retainer	Optional	Optional	Optional	Optional
Additional cloud storage retention	—	Optional	Optional	Optional
Sophos Identity Threat Detection and Response (ITDR)	—	—	Optional	Optional
Sophos Network Detection and Response (NDR)	—	—	Optional	Optional
Sophos Managed Risk powered by Tenable	—	—	—	Optional



Finder

INFORMATIČKE TEHNOLOGIJE I USLUGE
Božidarevićeva 13,
10000 Zagreb, Republika Hrvatska

tel. (01) 2337 731
e-mail: prodaja@finder.hr
www.finder.hr