SOLUTION BROCHURE

Sophos Endpoint and EDR

AI-Era attacks stop here.

The industry's most sophisticated AI-powered endpoint security solution

Sophos Endpoint is a unified Endpoint Protection and EDR solution built to defeat AI attacks. It blocks the techniques at the heart of attacks, stopping threats launched by either humans or Agentic AI tools. Powerful anti-ransomware, behavioral threat detection, exploit prevention, adaptive defenses, and threat surface reduction capabilities stop attacks before they occur. Sophos EDR adds AI-accelerated detection and response capabilities, designed for IT generalists and security analysts.

Prevent more, by default

AI gives attackers speed and scale, but exploitation still depends on a finite set of techniques. Sophos Endpoint blocks those techniques, with 60+ exploit mitigations enabled by default on every process, stopping threats before they execute, including AI-generated zero-days.

Stop attackers in their tracks

Agentic AI compresses the path from initial access to impact. Adaptive Attack Protection raises defenses on endpoints under active attack, and active adversary mitigations disrupt the techniques attackers rely on to escalate, blocking credential theft and lateral movement.

Hunt, investigate, and respond

When attackers move at machine speed, your investigation needs to as well. Built-in EDR capabilities turn endpoint telemetry into answers, with AI capabilities that triage alerts and accelerate response in seconds across endpoints and servers.

Manage less. Trust more

Strong defaults and a single lightweight agent mean less time managing security and more time on the rest of IT. Sophos Fusion manages every endpoint from one console, with built-in controls that surface shadow AI use and govern generative AI access.

Sophos Fusion

Sophos Endpoint is part of Sophos Fusion, the industry's most complete cyber defense system, engineered for a world where threats move at AI speed. Sophos Endpoint is your strongest first line of defense, blocking AI- and human-led attacks and feeding real-time telemetry to Sophos Fusion so every layer can respond as one.

Highlights

- 60+ proprietary exploit mitigations enabled by default on every process.
- CryptoGuard ransomware detection and automatic rollback, no signatures required.
- Adaptive defenses respond automatically to active adversaries and hands-on-keyboard attacks.
- AI-accelerated detection, investigation, and response in Sophos EDR.
- Shadow AI visibility and generative AI access controls.
- One lightweight agent for Windows, macOS, and Linux endpoints and servers.

Prevention-first approach at the speed of AI

Agentic AI has collapsed attack timelines to seconds, and detection-first defenses are exposed when the payload is already running before the alert fires. Sophos Endpoint matches the attack velocity, automatically blocking exploits, ransomware, and attacker techniques by default with zero tuning. Threats are stopped at every stage of the attack: before a payload runs, while it is running, and before it can complete its objective.

Anti-exploitation capabilities engineered for what's next, proven against what's now

AI accelerates vulnerability discovery and exploit chaining, but the techniques attackers must use to turn a vulnerability into a compromise remain a finite, slow-moving set. Sophos Endpoint blocks those techniques with 60+ proprietary mitigations, enabled by default on every protected process with no per-application configuration. They run in real time on the endpoint, with no dependence on cloud lookups or signature updates, and they fire whether the underlying vulnerability is known, unknown, or AI-generated five minutes ago.

- 60+ proprietary mitigations enabled by default on every protected process.
- Memory corruption defenses block stack pivoting, heap spraying, and ROP chains.
- Application hardening protects browsers, plug-ins, document readers, and Office.
- Post-exploitation mitigations disrupt credential theft, privilege escalation, and persistence.

Deep learning AI prevention

Multiple AI models identify known and never-seen malware before execution, including AI-generated and AI-mutated variants. Pre-execution scanning blocks payloads at the point of execution.

Behavioral protection

Blocks access to undesirable and inappropriate content. Enforce acceptable web usage across your organization and protect against data loss.

AMSI Protection

The Windows Antimalware Scan Interface inspects scripts (PowerShell, Office macros), including those obfuscated or generated at runtime, blocking fileless attacks loaded directly from memory. Sophos also mitigates malware that attempts to evade AMSI detection.

Application lockdown

Prevents browser and application misuse by blocking actions not commonly associated with those processes. For example, a web browser or Office application attempting to launch PowerShell.

Airtight ransomware protection

CryptoGuard monitors file contents for malicious encryption and rolls back affected files automatically, whether the attack runs locally or remotely against a network share. Master Boot Record protection safeguards drives from ransomware designed to leave computers unbootable.

Tamper Protection

EDR killers using bring-your-own-vulnerable-driver techniques are a common pre-ransomware step. Kernel-level self-defense blocks interference with the Sophos agent, catching defense evasions before a malicious driver can act.

Malicious traffic detection

Detects devices attempting to communicate with command and control servers by intercepting traffic from non-browser processes and analyzing whether it is destined for a malicious address.

Live protection

Extends on-device protection with real-time lookups to SophosLabs latest global threat intelligence for additional file context, decision verification, and false positive suppression, drawing on telemetry from 600,000+ customers.

Reduce your attack surface

The fewer paths attackers have into the endpoint, the fewer threats your team must investigate later. Sophos Endpoint blocks malicious web traffic, controls which applications and peripherals can run, and surfaces shadow AI use, on and off the corporate network. Each control reduces your attack surface using the same lightweight agent.

Web protection

Intercepts outbound browser connections and blocks traffic destined for malicious or suspicious websites. Stops threats at the delivery stage by preventing users from being diverted to malware delivery or phishing sites.

Web control

Enforces acceptable-use policies on user web activity, including Generative AI usage. Restricts access to inappropriate content or unsanctioned AI tools, with allow, warn, or block actions per website category.

Download reputation

Analyzes downloaded files using SophosLabs global threat intelligence and provides a verdict based on prevalence, age, and source, prompting users to block files with low or unknown reputation.

Application control

Blocks vulnerable, unauthorized, or risky applications by category. Pre-defined categories, including Generative AI tools, remove the burden of managing individual applications by hash. Restrict AI tool usage to reduce shadow AI risks.

Peripheral (device) control

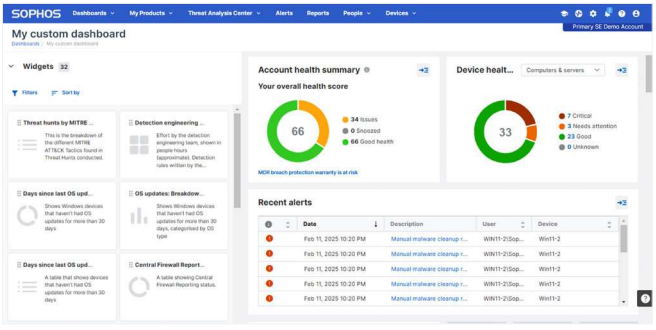
Monitors and blocks access to removable media, Bluetooth, and mobile devices to prevent unauthorized hardware from connecting to your network.

Data loss prevention

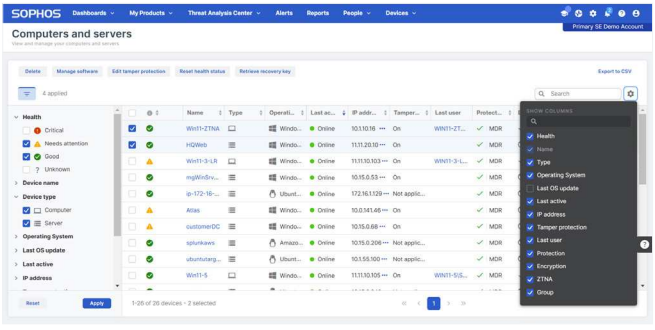
Monitors or restricts the transfer of files containing sensitive data. For example, prevents a user from sending a confidential file using web-based email.

Govern your AI adoption journey

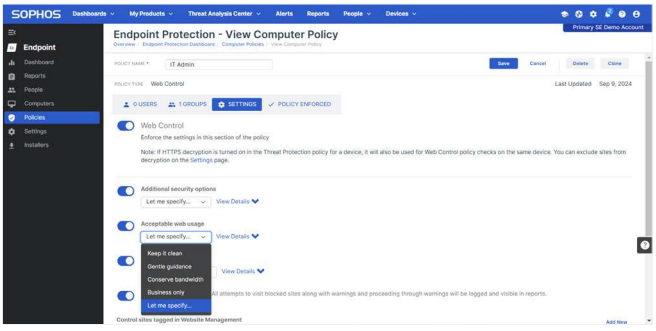
Employees are adopting AI tools faster than security teams can govern them. Sophos Endpoint surfaces shadow AI use and controls access to generative AI services through Web Control and Application Control categories, giving security teams the visibility and control they need to support AI adoption confidently, without slowing the business down.



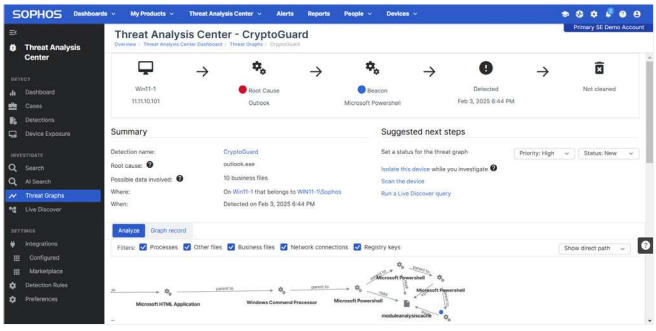
Create custom dashboards to meet your needs.



Endpoint security that's easy and setup and manage.



Configurable policies with recommended settings enabled by default.



Analyze threats to establish their root cause.

Adaptive defenses

Sophos Endpoint's adaptive defenses respond to hands-on-keyboard attacks at machine velocity, automatically tightening protection the moment an attack is detected and warning of more widespread attacks across your environment. They trigger on attacker behaviors and techniques and known attack toolkit usage, with the trigger logic continuously sharpened by the compounding intelligence from Sophos X-Ops.

Adaptive Attack Protection

Dynamically enables heightened defenses on an endpoint when a hands-on-keyboard attack is detected, disrupting the adversary and giving your team more time to respond. Triggers on behavior combinations and known attack toolkit usage, not file hashes, making it effective against zero-day AI attacks and novel variants.

Critical Attack Warning

Notifies administrators of serious adversary activity in progress across multiple endpoints, based on organization-wide threat detections. Compresses an estate-wide signal into a single, actionable alert so your team knows when to escalate.

	BEHAVIORAL PROTECTION	ADAPTIVE ATTACK PROTECTION	CRITICAL ATTACK WARNING
SCOPE	INDIVIDUAL DEVICE	INDIVIDUAL DEVICE	ENTIRE ESTATE
BENEFITS	Behavioral engine stops early stages of active adversary attacks	Elevates protection sensitivity to prevent attacks	Alerts you to an attack requiring immediate incident response
TRIGGER	Behavioral rules	Hacking toolsets detected	High-impact active adversary indicators, including org-level correlations and thresholds
ANALOGY	"SHIELDS ON!"	"SHIELDS UP!"	"RED ALERT!"

Adaptive defenses in Sophos Endpoint

Synchronized Security™

Sophos Endpoint does not defend alone. It is part of Sophos Fusion, the Sophos AI-Native Cybersecurity Defense System. Synchronized Security™ turns a detection at the endpoint into a coordinated response at the other control points, so containment happens in seconds rather than after someone notices.

Between Sophos control points, the Security Heartbeat™ carries device health status directly. When Sophos Endpoint finds a threat, it sets that device's status to Red. Sophos Firewall, Sophos Wireless, Sophos Switches, and Sophos Workspace Protection restrict its network access. Healthy endpoints reject its connection requests. Once the threat is remediated, the status returns to Green, and access is restored automatically.

Strong default policies and identifying drifts in security posture

By default, Sophos Endpoint comes with our recommended protection technologies enabled, immediately providing the strongest protection settings with zero tuning, stopping threats launched by either humans or Agentic AI tools from the moment of installation. There's no need for complicated configuration or tuning. However, if you need it, you also have the option for more granular control.

Poorly configured policy settings, exclusions, and other factors can compromise your security posture. The Account Health Check feature identifies security posture drift and high-risk misconfigurations, and enables you to remediate issues with a single click from Sophos Fusion.

Accelerate detection, investigation, and response

Sophos EDR is a comprehensive protection, detection, and response solution designed for IT generalists and security analysts. Sophos EDR reduces your security risk by enabling you to respond to evasive threats and reducing the potential impact on your business. Sophos Endpoint is included and natively integrated with Sophos EDR.



AI-prioritized detections

Easily identify suspicious activity that needs immediate attention. Sophos EDR automatically prioritizes detections based on risk, providing full context.



Automated responses

Automated actions like process termination, ransomware rollback, network isolation, and adaptive attack protection, contain threats rapidly and save your team valuable time.



Security analyst responses

Your team can isolate an endpoint, manually engage adaptive attack protection while they investigate suspicious activity, and more.



AI Search

Uses natural language to accelerate day-to-day tasks and lower the technology barrier to security operations.



AI Case Summary

Provides an easy-to-understand overview of detections and recommended next steps, helping you make smart decisions fast.



AI Command Analysis

Analyzes complex command line arguments to uncover their intent and impact, with explanations in plain language.

Live Response

Sophos EDR enables IT generalists and security analysts to perform IT operational tasks and remediate threats with speed and precision. A direct, secure, and audited connection to your endpoints and servers to investigate and remediate possible issues directly from your Sophos console.



Remotely access devices to

- Install and uninstall software
- Run scripts and programs
- Edit configuration files
- Shutdown / reboot
- Run third-party forensic tools
- And more

Device Exposure

Quickly identify risky, out-of-date, and vulnerable devices in your environment. Device exposure provides you with information on what devices are most vulnerable to threats and enables you to act on devices that haven't performed operating system updates in some time.

What's included in Sophos Endpoint and Sophos EDR

	Sophos Endpoint	Sophos EDR
Protection built for the AI-era Deep learning (AI-powered) malware prevention, anti-exploitation, anti-ransomware, behavioral analysis, and more.	✓	✓
Adaptive Defenses Adaptive attack protection, critical attack warning	✓	✓
Endpoint threat exposure reduction Web protection, web control, peripheral control, app control, and data loss prevention	✓	✓
Endpoint detection and response (EDR) Detect, investigate, and respond to attacks targeting endpoints and servers		✓
Live response and device exposure Powerful tools for IT generalists and security analysts		✓
Detection data retained in the Sophos unified context lake 30 days as standard		✓ (Upgradeable to 1-year)
Sophos Endpoint for Legacy Platforms Comprehensive security for legacy and out-of-support Windows and Linux operating systems	Optional add-on	Optional add-on
Sophos Device Encryption Centralized management of native disk encryption on Windows and macOS devices	Optional add-on	Optional add-on
Sophos Security Services Retainer Services to help organizations uncover weaknesses, respond to cyberattacks, and strengthen security maturity.	Optional add-on	Optional add-on

Sophos XDR

Sophos Extended Detection and Response (XDR) provides visibility beyond your endpoints and servers. It provides powerful AI Assistants and threat intelligence that enable your team to detect, investigate, and neutralize threats across your entire IT ecosystem, delivered through Sophos' AI-Native Cybersecurity Defense System.

Our open, vendor agnostic architecture provides visibility across the entire attack surface by integrating threat information from your existing and future security investments. Sophos XDR includes turnkey integrations with an extensive ecosystem of endpoint, firewall, network, email, identity, backup, cloud security, and productivity solutions.

Learn more at Sophos.com/XDR

Sophos MDR

Sophos Managed Detection and Response is a fully managed, 24/7 detection and response service for the agentic era. AI handles speed and scale. Humans provide judgment and accountability. Sophos MDR is the world's largest Agentic SOC: AI investigates and responds in seconds, analysts own the outcomes.

Choose from a range of service tiers and threat response modes to meet your needs. Sophos MDR operates with specialist-level depth across diverse architectures and vendor environments, including the most complete Microsoft security integration on the market, ensuring strong outcomes regardless of your technology stack.

Learn more at Sophos.com/MDR

See why customers choose Sophos Endpoint

Sophos is an established leader in endpoint security, with industry recognition to back it up.

Gartner

Sophos named a Leader in the 2026 Gartner® Magic Quadrant™ for Endpoint Protection for 17 consecutive reports

SE Labs

Sophos consistently achieves industry-leading protection results in independent endpoint security tests.

Leader

Rated the #1 Overall solution in EPP, MDR, XDR, EDR, and Firewall in the G2 Summer 2026 Reports.

IDC

Sophos named a Leader in the 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.

Gartner Peer Insights Customers' Choice 2026

Sophos has been recognized as a Customers' Choice vendor in the 2026 Voice of the Customer report for Endpoint Protection Platforms.

Try it now for free

Register for a free 30-day evaluation at sophos.com/endpoint

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. 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.

2026-08-26 BR-EN (MP)

SOPHOS