SOLUTION BROCHURE

Sophos Endpoint and EDR

Complete endpoint protection, detection, and response

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

Sophos Endpoint delivers unparalleled defense against advanced cyberattacks with a prevention-first approach and best-in-class endpoint security. Sophos Endpoint Detection and Response (EDR) is a comprehensive protection, detection, and response solution that includes Sophos Endpoint and is designed for security analysts and IT administrators. Protect and monitor your endpoints and servers for suspicious activity, whether they are in the office, remote, or in the cloud.

A prevention-first approach to security

Sophos Endpoint takes a comprehensive, prevention-first approach to security, automatically blocking threats without relying on any single technique. Deep learning AI models protect against known and novel attacks. Controls reduce your threat surface, while behavioral analysis, anti-ransomware, anti-exploitation, and other advanced technologies stop threats fast before they escalate.

Adaptive defenses

When Sophos Endpoint detects a hands-on-keyboard attack, it dynamically enables additional defenses with a "shields up" approach to stop adversaries in their tracks. This industry-first capability, unique to Sophos, minimizes the attack surface and disrupts and contains the attack, restricting cybercriminals from taking further actions and buying your team valuable time to respond.

Gain insights into evasive threats

Sophos EDR provides AI-prioritized threat detections that highlight suspicious activity requiring immediate attention. Analyze activity in real-time with access to rich on-device data and telemetry in the Sophos data lake, including historical activity, even when devices are offline.

Accelerate and empower your team

Sophos EDR is designed for IT generalists and security analysts. Powerful tools enable your team to quickly and easily conduct extensive IT operational tasks with a direct, secure connection to your devices. Outcome-focused AI tools streamline investigation and response, enabling your team to investigate and neutralize suspicious activity and evasive threats targeting your endpoints and servers with speed and precision.

Highlights

- A prevention-first approach that reduces your attack surface and stops threats fast
- Safeguard data from local and remote ransomware attacks with best-in-class protection.
- Benefit from industry-first dynamic defenses that automatically adapt in response to active adversaries and hands-on-keyboard attacks.
- AI-prioritized detections highlight where your team should focus.
- Outcome-focused AI tools streamline investigation and response to suspicious activity and evasive threats.
- Powerful tools for IT generalists and security analysts.

A prevention-first approach reduces your attack surface

Stopping attacks early is less resource-intensive than monitoring and remediating them later in the attack chain. Sophos Endpoint includes sophisticated protection technologies that block the broadest ranges of attacks. Web, application and peripheral controls reduce your attack surface and block common attack vectors, reducing the opportunities for attackers to penetrate your environment.

Web protection

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

Web control

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

Download reputation

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

Application control

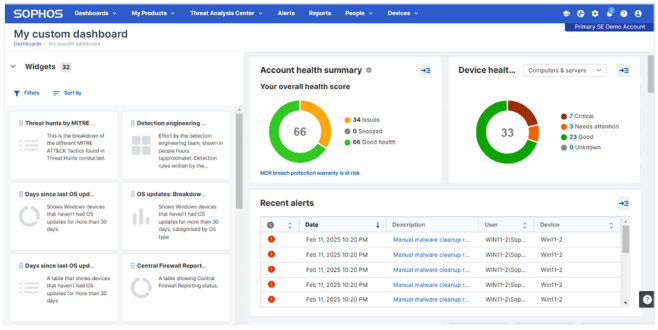
Block applications that may be vulnerable, unsuitable for your environment, or that could be used for nefarious purposes. Sophos provides pre-defined categories to block or monitor apps, removing the burden of blocking individual applications by hash.

Peripheral (device) control

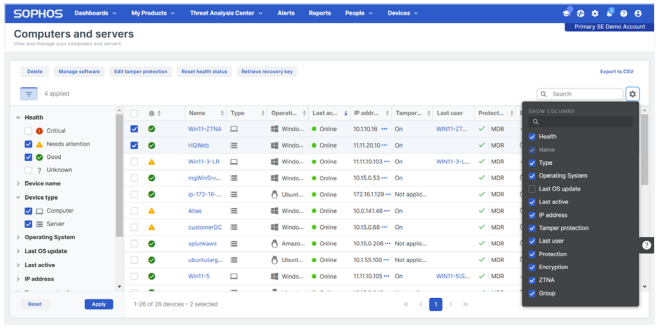
Monitors and blocks access to removable media, Bluetooth, and mobile devices to prevent certain hardware from connecting to your network.

Data loss prevention

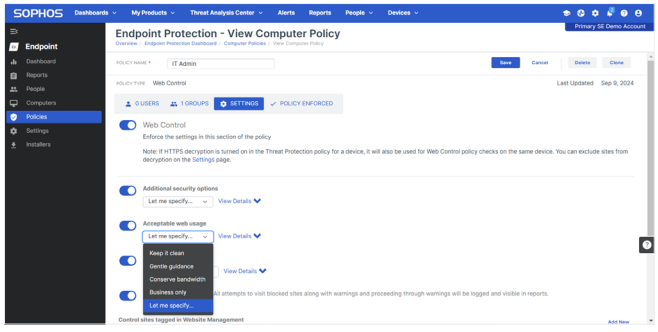
Monitor or restrict the transfer of files containing sensitive data. For example, prevent a user from sending a confidential file using web-based email.



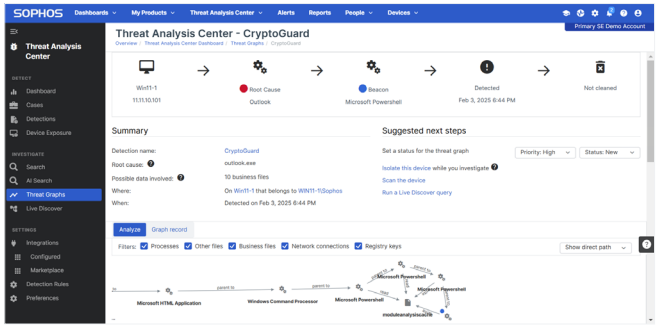
Create custom dashboards to meet your needs.



Endpoint security that's easy and setup and manage.



Configurable policies with recommended settings enabled by default.



Analyze threats to establish their root cause.

A prevention-first approach stops threats quickly

Detecting and remediating threats as early as possible reduces risk. Sophos Endpoint stops threats quickly before they escalate, so resource-stretched IT teams have fewer incidents to investigate and resolve. Sophos delivers strong threat prevention capabilities, validated through consistent top scores in independent security tests.

Airtight ransomware protection

According to Microsoft's 2024 Digital Defense Report, remote encryption is now seen in 70% of successful attacks, with 92% originating from unmanaged devices in the network. Sophos Endpoint provides the strongest zero-touch endpoint defense against both local and remote ransomware, leveraging advanced CryptoGuard technology to detect encryption attempts, regardless of the source.

- Blocks new and novel ransomware variants.
- Inspects file changes in real-time to detect malicious encryption.
- Prevents remote ransomware from encrypting files remotely over the network.
- Automatically rolls back any encrypted files to their original unencrypted state – using proprietary technology that doesn't rely on the Windows Shadow Copy Service.
- Protects all file types and sizes with minimal performance impact.
- Safeguards the Master Boot Record (MBR) from advanced attacks targeting the hard disk.

Deep learning (AI-powered) malware prevention

Detects and blocks both known and unknown malware by analyzing file attributes and using predictive reasoning to identify threats.

Anti-exploitation

Guards process integrity by hardening application memory and applying runtime code execution guardrails. Sophos Endpoint includes over 60 anti-exploitation techniques that are enabled by default, requiring no training or tuning. These techniques offer protections that significantly surpass those provided by Windows and most other endpoint security solutions.

Behavioral protection

Monitors process, file, and registry events over time to detect and stop malicious behaviors and processes. It also performs memory scanning, inspects running processes to detect malicious code only revealed during process execution, and detects attackers implanting malicious code in the memory of a running process to evade detection.

Synchronized security

Sophos Endpoint shares status and health information with Sophos Firewall, Sophos Wireless, Sophos Zero Trust Network Access (ZTNA), and other Sophos products to provide additional visibility into threats and application usage and isolate compromised devices automatically.

Live protection

Extends comprehensive on-device protection with real-time lookups to SophosLabs' latest global threat intelligence for additional file context, decision verification, false positive suppression, and file reputation. Our Tier 1 threat research provides additional live intelligence from Sophos' expansive product portfolio and global customer base.

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.

Antimalware Scan Interface (AMSI)

The Windows Antimalware Scan Interface (AMSI) determines whether scripts (e.g., PowerShell or Office macros) are safe, including if they are obfuscated or generated at runtime, blocking fileless attacks where malware is loaded directly from memory. Sophos also has a proprietary mitigation against malware that attempts to evade AMSI detection.

Malicious traffic detection

Detects devices attempting to communicate with a command and control (C2) server by intercepting traffic from non-browser processes and analyzing whether it is destined for a malicious address.

Adaptive defenses

Sophos Endpoint leverages industry-first dynamic defenses that automate protection by adapting in real-time to battle active adversaries and hands-on-keyboard attacks. The adaptive defenses block actions that might not seem malicious in a typical context but can be harmful during an attack. They dynamically respond to and disrupt active attacks, even when attackers have established a foothold, all without raising alarms or relying on malicious code.

Adaptive attack protection

Dynamically enables heightened defenses on an endpoint when a hands-on-keyboard attack is detected, disrupting the adversary and giving you more time to respond.

Critical attack warning

Notifies admins of serious adversarial in progress across multiple endpoints, based on organization-wide threat detections.

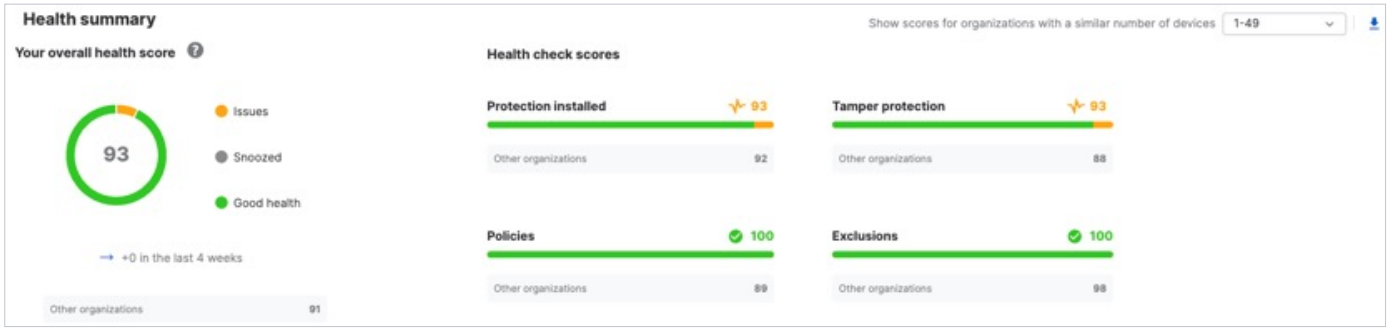
	BEHAVIORAL PROTECTION	ADAPTIVE ATTACK PROTECTION	CRITICAL ATTACK WARNING
SCOPE	INDIVIDUAL DEVICE	INDIVIDUAL DEVICE	ENTIRE ESTATE
BENEFITS	Behavioral engine stops early stages of active adversary attacks	Elevates protection sensitivity to prevent attacks	Alerts you to an attack requiring immediate incident 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

Strong default policies and identifying drifts in security posture

By default, Sophos Endpoint comes with our recommended protection technologies enabled, immediately providing you with the strongest protection settings. 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.



Account health check

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
Next-Gen Endpoint Protection Deep learning (AI-powered) malware prevention, anti-ransomware, behavioral analysis, anti-exploitation, 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 data 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 Incident Response (IR) Services Retainer An elite team of experts on standby in the event of a breach	Optional add-on	Optional add-on

Sophos XDR

Sophos Extended Detection and Response (XDR) provides visibility beyond your endpoints and servers. It provides powerful tools and threat intelligence that enable you to detect, investigate, and neutralize threats across your entire IT ecosystem, delivered through Sophos' adaptive AI-native, open platform.

Our open, extensible 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

No matter where you are in your security journey, our Sophos' Managed Detection and Response (MDR) services keep you one step ahead of adversaries. We combine easy-to-use, AI-driven technology with world-class security experts who monitor, prevent, detect, and respond to threats 24/7.

Choose from a range of service tiers and threat response modes to meet your needs. Sophos MDR integrates threat information from your existing and future security investments.

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 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for 16 consecutive reports.

SE Labs

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

Leader

Sophos is the only vendor named a Leader across the G2 Spring 2025 Overall Grid® Reports for Endpoint Protection Suites, EDR, XDR, Firewall Software, and MDR.

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 2025

Sophos is a Gartner® Peer Insights™ "Customers' Choice" vendor in the 2025 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

2025-09-17 BR-EN (NP)

SOPHOS