SOLUTION BROCHURE

Sophos Endpoint

Powered by Intercept X

SOPHOS

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

Sophos Endpoint, powered by Intercept X technology, delivers unparalleled protection, stopping advanced attacks before they impact your systems. Powerful endpoint and extended detection and response (EDR/XDR) tools let your organization hunt for, investigate, and respond to suspicious activity and indicators of an attack.

A prevention-first approach to security

Sophos Endpoint takes a comprehensive, prevention-first approach to security, blocking threats without relying on any single technique. Multiple deep learning AI models secure against known and never-before-seen attacks. Web, application and peripheral controls reduce your threat surface and block common attack vectors. Behavioral analysis, anti-ransomware, anti-exploitation, and other advanced technologies stop threats fast before they escalate, so resource-stretched IT teams have fewer incidents to investigate and resolve.

Airtight ransomware protection

Sophos Endpoint is the industry's most robust zero-touch endpoint defense against advanced ransomware. CryptoGuard technology stops malicious encryption in real-time and automatically rolls back any affected files to their original state, minimizing business impact.

Adaptive defenses

Industry-first dynamic defenses adapt in response to active adversaries and hands-on-keyboard attacks. This removes the attacker's ability to operate, disrupting and containing the attack while buying valuable additional time to respond.

Easy to set up and manage

Sophos Central is a powerful, cloud-based cybersecurity management platform that unifies all Sophos next-gen security solutions. Recommended technologies and features are enabled by default, ensuring you immediately have the strongest protection with no tuning required.

A trusted industry leader in endpoint security

Sophos Endpoint consistently earns top recognition from customers, analysts, and independent testing organizations. Sophos is a 16-time Leader in the Gartner® Magic Quadrant™ for Endpoint Protection Platforms and the #1 Endpoint Detection and Response solution in the Spring 2025 G2 Grid® Reports.

Highlights

- Multiple deep learning AI models protect against known and never-before-seen attacks.
- Reduce your threat surface and block common attack vectors with web, application and peripheral controls.
- Stop threats fast before they escalate with behavioral analysis, anti-ransomware, anti-exploitation, and other advanced technologies.
- 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.
- Hunt for, investigate and respond to suspicious activity with powerful EDR and XDR tools.

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

Blocks outbound browser traffic to malicious websites, stopping threats at the delivery stage and preventing phishing or malware sites.

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

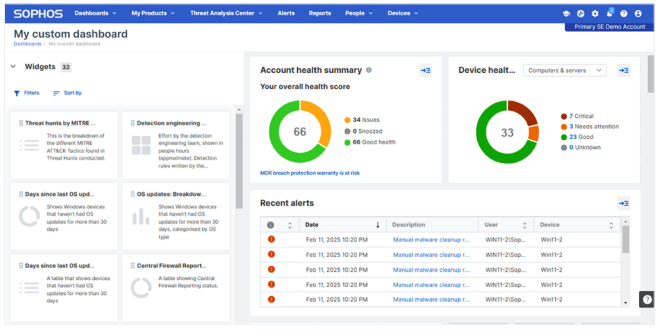
Blocks vulnerable or unsuitable applications with pre-defined categories, eliminating the need to block apps individually by hash.

Peripheral (device) control

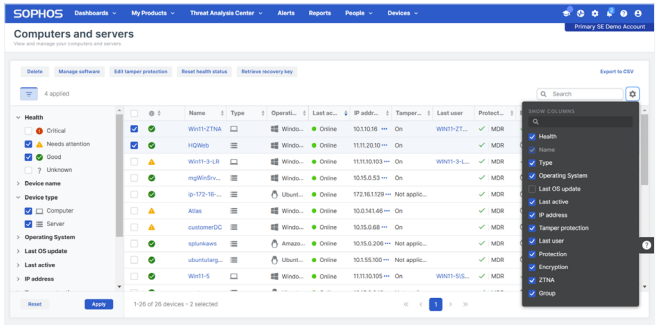
Monitors and blocks access to removable media, bluetooth, and mobile devices to prevent certain hardware from connecting to your network.

Data loss prevention

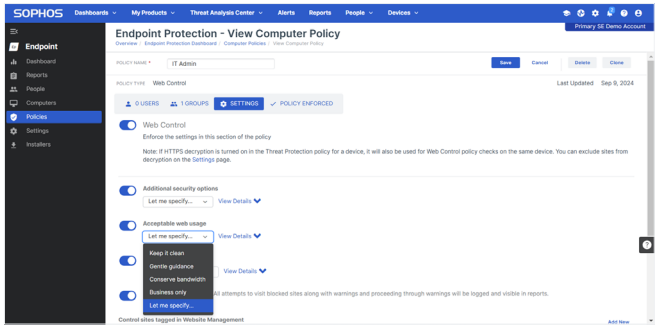
Monitor or restrict the transfer of files containing sensitive data. For example, prevent a user from sending a confidential file using web-based email.



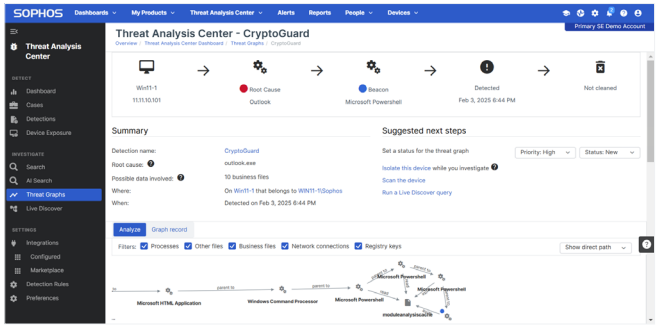
Create custom dashboards to meet your needs.



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.

AI-powered deep learning malware prevention

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

Anti-exploitation

Protects process integrity with memory hardening and 60+ anti-exploitation techniques, requiring no tuning and surpassing native Windows capabilities and other security solutions.

Behavioral protection

Monitors process, file, and registry events to detect and stop malicious activity. It scans memory, inspects running processes for hidden threats, and detects attackers injecting malicious code to evade detection.

Synchronized security

Sophos Endpoint shares status and health information with Sophos Firewall, 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 strong on-device protection with real-time lookups to SophosLabs' global threat intelligence for additional file context, decision verification, false positive suppression, and file reputation.

Application lockdown

Prevents browser and application misuse by blocking actions not commonly associated with those processes.

Antimalware Scan Interface (AMSI)

The Windows Antimalware Scan Interface (AMSI) blocks fileless attacks where malware is loaded directly from memory. Sophos Endpoint also includes a proprietary mitigation against evasion of AMSI detection.

Malicious traffic detection

Detects devices communicating with command and control (C2) servers by intercepting and analyzing non-browser traffic for malicious destinations.

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. Sophos Endpoint blocks actions that may not be inherently malicious in an everyday context but are dangerous in the context of the attack. This functionality dynamically responds to and disrupts active attacks where attackers may have gained a foothold without raising red Flags or using 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

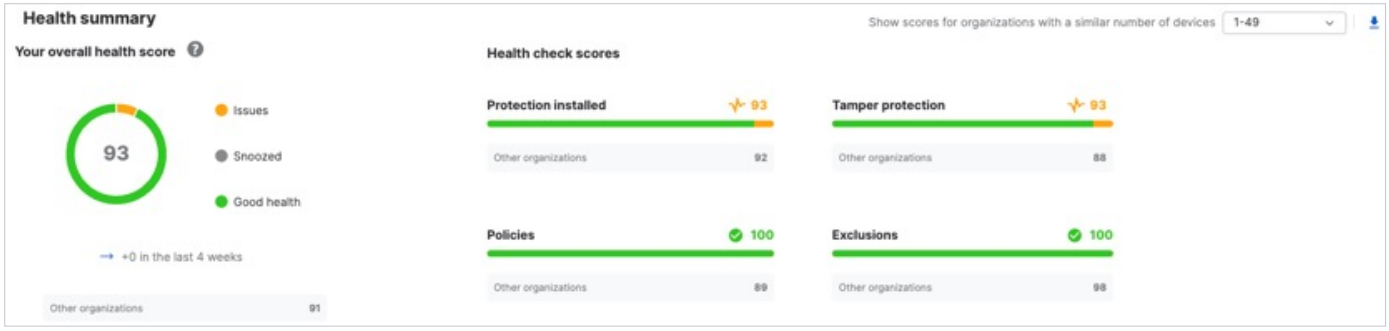
Notifies admins of serious adversarial in progress across multiple endpoints, based on organization-wide threat detections.

	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

Identify drifts in security posture

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 one click.



Account health check

Additional protection layers (add-ons)

Sophos ZTNA

Securely connect your users to your applications with the ultimate VPN replacement. Sophos ZTNA is the only zero-trust network access solution tightly integrated with next-gen endpoint protection.

Device encryption

With devices lost or stolen daily, full disk encryption is essential. Device encryption integrated with Sophos Endpoint provides effective management of BitLocker (Windows) and FileVault (macOS).

Accelerate detection, investigation, and response

Sophos Endpoint automatically blocks most threats upfront, reducing the number of events that need to be investigated. For suspicious activity and threats that require human-led analysis, Sophos provides powerful solutions to quickly detect, investigate, and respond across all key attack vectors.

Sophos XDR

Sophos Extended Detection and Response (XDR) enables you to hunt for, investigate, and respond to suspicious activity and multi-stage attacks across your full security environment. Designed by security analysts for users of all skill levels, our powerful GenAI-powered tools enable everyone — from IT generalists to top-tier SOC analysts — to quickly investigate threats and neutralize adversaries.

Sophos XDR provides turnkey integrations with an extensive ecosystem of endpoint, Firewall, network, email, identity, productivity, cloud, and backup solutions, enabling you to get more ROI from your existing security tools.

Learn more at Sophos.com/XDR

Sophos MDR

For organizations without the resources to manage threat detection and response in-house, Sophos Managed Detection and Response (MDR) is a 24/7 service delivered by an elite team of experienced security analysts, threat hunters, and incident responders. Sophos MDR leverages telemetry from both Sophos and third-party security technologies to detect and neutralize even the most sophisticated threats.

Sophos MDR meets you where you are, with multiple service tiers and response modes to suit your organization's needs, and compatibility with your existing tools and technologies.

Learn more at Sophos.com/MDR

	Sophos Endpoint	Sophos XDR	Sophos MDR
Next-gen threat protection AI-powered deep learning anti-malware, web protection	✓	✓	✓
Malicious activity blocking Anti-ransomware, anti-exploitation, adaptive defenses	✓	✓	✓
Threat exposure reduction DLP, web, peripheral, and application control features	✓	✓	✓
Detection and response Powerful threat investigation and response tools		✓	✓
Visibility across key attack surfaces Sophos and third-party technology integrations		✓	✓
Managed detection and response 24/7 expert-led threat monitoring and incident response			✓

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.

G2 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

2025-07-16 BR-EN (NP)

SOPHOS