SOPHOS

SOPHOS ENDPOINT

AI-Era attacks stop here.

A unified Endpoint Protection and EDR solution built to defeat AI attacks.

Sophos Endpoint 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.

32%
of ransomware attacks start with an exploited vulnerability[1]

41%
of exploited vulnerabilities used in ransomware attacks are on a user's device[2]

$1.53M
the average cost to recover from a ransomware attack in 2025[1]

WHAT SOPHOS ENDPOINT DELIVERS

Four outcomes. One endpoint agent.

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. Threats are stopped before they execute, including AI-generated zero-days that have never been seen before.

- AI, ML and deep learning detect known and never-seen threats
- 60+ proprietary exploit mitigations enabled by default
- CryptoGuard ransomware detection and rollback

Stop attackers in their tracks.

Agentic AI compresses the path from initial access to impact. Adaptive Attack Protection automatically 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 by humans or AI agents.

- Active adversary mitigations disrupt post-exploitation
- Credential theft protection blocks lateral movement
- Container and Linux workload hardening

Hunt, investigate, 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. Correlate signals across endpoints and servers to expose attacks that move too fast to follow.

- AI search enables rapid threat hunting
- AI capabilities accelerate investigation and response
- Direct response: isolate, terminate, remediate

Manage less. Trust more.

AI-generated threats evolve faster than most security teams can tune their tools. Strong defaults and a single lightweight agent mean less time managing security and more time on the rest of IT. Sophos Central manages every endpoint from one console, with built-in controls that surface shadow AI use and govern generative AI access so teams can support AI adoption confidently.

- Lightweight agent protects Windows, macOS, Linux
- Discover shadow AI use and govern generative AI access
- Synchronized Security with firewall, identity, and email

SOPHOS ENDPOINT AT A GLANCE

- 60+ exploit mitigations, on by default protect every process
- CryptoGuard ransomware rollback, no signatures required
- AI-accelerated EDR capabilities for threat hunting and response
- One lightweight agent: Windows, macOS, Linux for endpoints and servers

WHO SOPHOS ENDPOINT IS FOR

- Orgs facing AI-discovered exploits, AI-generated phishing, deepfake-assisted social engineering, and automated commodity malware
- Security Teams that need AI-driven protection to operate autonomously, with minimal tuning or alert triage overhead
- MSPs delivering comprehensive endpoint protection at scale

YOUR EDGE IN THE AGENTIC THREAT ERA

Engineered for what's next, proven against what's now.

Prevention-first at the speed of AI.

Agentic AI has collapsed attack timelines to seconds. Sophos Endpoint matches the attack velocity, automatically blocking exploits, ransomware, and attacker techniques by default with zero tuning.

Blocks AI-discovered exploits and vulnerabilities.

AI accelerates vulnerability discovery, exploit chaining and attacks, but exploit techniques remain finite. Sophos Endpoint blocks those techniques by default, neutralizing known and undiscovered exploits.

One system, every control point.

Sophos Endpoint shares real-time threat and health telemetry with the Sophos ecosystem, so a detection at any control triggers a coordinated response that contains attacks faster.

INDUSTRY RECOGNITION

Validated by the analysts, labs, and customers that matter most.

GARTNER MAGIC QUADRANT

16x Leader for Endpoint Protection Platforms

G2 SPRING 2026

#1 in Endpoint, EDR & XDR

GARTNER PEER INSIGHTS

"Customers' Choice" for Endpoint

SE LABS 2025

AAA enterprise & SMB endpoint

IDC MARKETSCAPE 2024

Leader in Modern Endpoint Security

MITRE ATT&CK EVALS

100% detection coverage

START HERE

See Sophos Endpoint in action.

Start a free trial or speak with an expert about replacing your current endpoint protection.

sophos.com/endpoint

[1] Sophos State of Ransomware Report 2025
[2] Sophos research

SOPHOS