SOPHOS

SOPHOS MANAGED DETECTION AND RESPONSE

AI speed. Human judgment.

Fully managed, 24/7 detection and response 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.

52%
of cases resolved end-to-end by AI

89sec
from alert to automated response

500+
integrations with security and IT tools

Attackers are using AI to move faster, target more systems, and evade traditional defenses. Sophos MDR combines agentic AI and elite human expertise to detect, investigate, and stop advanced attacks across your environment, 24/7, with no caps and no gaps.

Whether you're building your first line of expert defense or strengthening an existing SOC, Sophos MDR delivers measurable outcomes: reduced risk, faster response, stronger resilience, and trusted protection that continuously improves over time.

OUTCOMES THAT MATTER

- **Reduced cyber risk** with protection powered by world-class threat research and intelligence that compounds from more than 625K defended organizations.
- **Faster detection, investigation, and response** using agentic AI, autonomous investigation agents, and expert analysts that act with speed, depth, and accountability.
- **Better return on security investments** by maximizing the value of existing tools. Integrate hundreds of leading security products into one service.
- **A trusted edge in the AI era.** Partner with an MDR provider that combines agentic AI and expert human judgment at scale.
- **Protection against after-hours attacks,** addressing the reality that most ransomware incidents occur outside standard business hours.
- **Detection of sophisticated, multi-stage threats** designed to evade automated defenses and standalone tools.
- **Lower operational burden and burnout** for internal IT and security teams.
- **Improved insurance and compliance posture,** helping secure better terms and meet regulatory requirements.
- **Greater confidence** with boards, insurers, regulators, and stakeholders.

THE CHALLENGE

AI has changed the game



Faster attacks



Expanded attack surface



Disconnected tools



Skills gap



Alert overload

Adversaries are using AI and automation to move faster across endpoints, networks, cloud workloads, identity, email, and business applications, often using legitimate credentials and trusted tools to evade traditional defenses. AI hasn't just increased attack volume; it has compressed the window to detect, investigate, and respond.

AI has also expanded the attack surface. Sensitive business data now flows through email, files, SaaS applications, collaboration tools, and AI services, making it easier to reach, misuse, and exfiltrate.

At the same time, organizations face mounting operational pressure:

- **AI-enabled attacks** that move faster than human defenders can respond alone.
- **Persistent skills shortages** and burnout across IT and security teams.
- **Alert overload from disconnected tools** and incomplete context.
- **Attacks that span multiple layers,** making them harder to detect, investigate, and stop.
- **Growing pressure** from boards, insurers, and regulators to prove resilience.

Effective defense now requires more than standalone tools. It requires AI-accelerated operations, always-on expertise, deep threat intelligence, and decisive response, delivered by an MDR partner built to harness AI as attackers weaponize it.

THE SOLUTION

Sophos MDR Agentic SOC

Sophos MDR is a fully managed cybersecurity service that detects, hunts, investigates, and remediates advanced threats that standalone tools cannot stop. It's the world's largest Agentic SOC — AI investigates and responds in seconds. Analysts own the outcomes.

The service is powered by **Sophos Fusion**, the Sophos AI-Native Cybersecurity Defense System. It's the industry's most complete defense system where endpoint, network, email, cloud, identity, SIEM, threat intelligence, and managed detection and response share a common data fabric, unified AI layer, and single operational workflow. This enables Sophos to apply agentic AI across threat hunting, investigation, and response, detecting attacker behavior earlier, prioritizing threats faster, and acting with precision across your entire environment.

AGENTIC SOC

The architecture that makes it possible

Human in the loop

TRADITIONAL AI-POWERED SOC

A human must approve every action before it executes.

AI assists but never acts alone.

- Every alert routes to a human analyst for review and approval.
- Throughput is capped at human reaction time. The bottleneck cannot move.
- Every alert competes for the same finite pool of analyst attention.
- AI acts only as a suggestion engine. The human is always in the critical path.
- Cannot match the speed or scale of modern AI-driven adversaries.

VS.

Human on the loop

SOPHOS MDR AGENTIC SOC

AI is authorized to act inside well-defined boundaries.

Humans supervise the system, calibrate trust, and step in when needed.

- 52% of cases resolved end-to-end by AI with no human intervention required.
- 89-second average detection-to-automated-response time. Humans are not in the critical path.
- Analysts supervise the system, calibrate its trust envelope, and own outcomes.
- When stakes are high or context is novel, a human is already there with full context.
- Accountability lives with people, not models. Judgment is a feature, not an afterthought.

THE SOPHOS APPROACH

AI handles speed and scale. Humans own the outcome.

Sophos operates both human-on-the-loop and human-in-the-loop models within our Agentic SOC: human-on-the-loop for the high-volume, well-bounded work where speed matters, and human-in-the-loop for high-stakes decisions where context, business impact, or novel adversary behavior require an analyst's judgment before action is taken.

What Sophos MDR delivers

An instant, AI-accelerated SOC

88% of ransomware attacks occur outside normal business hours.[1] Sophos MDR gives you access to a global team of security experts operating across nine regional hubs to provide 24/7/365, follow-the-sun coverage. Our analysts, AI assistants, and autonomous agents work together to monitor your environment, investigate suspicious activity, hunt for hidden threats, and respond to confirmed attacks across all time zones.

Agentic AI and expert-led outcomes

Sophos MDR brings agentic AI and human expertise together in a new SOC operating model. Autonomous agents reduce noise, investigate threats, and accelerate response, while Sophos experts guide decisions, govern actions, and own outcomes when it matters most.

Unmatched threat intelligence, built in

Sophos MDR combines intelligence from over 625,000 defended organizations and advanced threat actor tracking from Sophos X-Ops, giving our AI models, agents, and analysts the context to identify emerging adversary behaviors earlier, to help you stay ahead.

Detect what your tools miss

Advanced threat detectors, autonomous threat hunting agents, and expert analysts work together across endpoint, identity, email, network, and cloud to uncover human-led and AI-driven attacks designed to bypass standalone security controls.

Respond in seconds. Humans in command

When AI can act alone, it does. When judgment is needed, a human is already there. The right response, from the right responder, every time. AI or human, decided in seconds. Sophos MDR acts on your behalf to disrupt, contain, and eliminate the adversary.

Continuous, autonomous, and intelligence-led threat hunting

Always-on threat hunting powered by agentic AI and informed by the latest intelligence from Sophos X-Ops. Autonomous agents turn new threat intelligence into explainable hunts. Positive findings trigger deeper investigation and response by Sophos experts.

Reduce risk. Reduce claims. Reduce cost.

Security spend is easier to defend when it pays for itself. Sophos MDR reduces the three costs that matter to your leadership team: your risk of a breach, insurance costs, and the wasted spend in your existing stack.

$1.53M

Reduced risk of an average ransomware bill.[2]

97.5%

Lower insurance claims for MDR-protected organizations.[3]

ROI+

Maximize ROI on your existing stack with 500+ integrations included.

INTEGRATION ECOSYSTEM

Vendor-agnostic. Bring your stack or use ours.

Most organizations operate a mix of security tools from different vendors. AI-enabled attacks cross layers, so your defense must too. Sophos MDR is vendor-agnostic by design, integrating with hundreds of leading IT and security technologies across endpoint, network, cloud, identity, email, and business applications, at no extra cost.

This means you can:

- Defend against attacks that move across systems, without replacing your tools.
- Preserve flexibility as your security environment evolves over time.
- Gain unified visibility across endpoint, network, identity, and cloud.
- Maximize the return on your existing security tooling investments.

A representative sample of Sophos MDR integrations

Visit sophos.com/marketplace for more.



Third-party trademarks belong to their respective owners.

90%+

of successful cyberattacks start with a phishing email[4]

Expose hidden email threats

The Sophos Email Monitoring System (EMS), included with Sophos MDR, gives analysts deep visibility to uncover and take action on advanced threats other tools miss. It adds an additional layer of defense across your existing email security without impacting mail flow.

MICROSOFT SECURITY INTEGRATION

Sophos MDR analysts operate with specialist-level depth across diverse architectures and vendor environments, including **the most complete Microsoft security integration on the market**.

Sophos MDR is a **Microsoft-verified** Small and Medium Business (SMB) Solution through the Microsoft Intelligent Security Association (MISA), validating deep integration with Microsoft Defender for Endpoint and Defender for Business to deliver stronger, faster protection across Microsoft environments.

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified SMB Solution

Protection-first. Stop more threats early.

Attacks frequently enter through email and execute or spread on the endpoint. Sophos MDR takes a protection-first approach, stopping more threats upfront so analysts can focus on more sophisticated attacks that evade automated tools.

Endpoint protection included as standard

Sophos Endpoint ships with Sophos MDR — delivering AI-driven threat prevention and behavioral detection, plus high-fidelity telemetry that gives analysts deeper context for faster, more confident response.

AI speed. Human judgment. Real-word expertise.

52%
of Sophos MDR cases resolved end-to-end by AI.

89 sec
from alert to automated response.

9
regional SOC teams for global coverage.

Sophos MDR combines agentic AI and human expertise — operating as one — to provide continuous support from a broad, cross-discipline security team:



Security Analysts
24/7 monitoring, investigation, and response, with AI-accelerated analysis and prioritization.



AI and Automation Engineers
Designing agentic AI and autonomous workflows to accelerate detection and response at scale.



Threat Hunters
Continuous, intelligence-led threat hunting. Agentic AI at scale, guided by human expertise.



Threat Researchers
Tracking adversary groups, campaigns, and emerging tactics.



Incident Responders
The right response, from the right responder, every time. Hands-on containment, remediation, and recovery support.



Detection Engineers
Designing and evolving detections for today's threats, including AI-enabled techniques.



Customer Success Experts
Serving as your advocate and first point of contact.

WORKS THE WAY YOU DO

Flexible service tiers to suit your organization

Sophos MDR is available in two service tiers, each designed to deliver comprehensive protection while adapting to your operational needs:

SOPHOS MDR

- 24/7 threat monitoring, detection, investigation, and response.
- Continuous, intelligence-led threat hunting, powered by agentic AI.
- Unlimited threat response — no hourly caps or extra fees.
- Seamless integration with your existing IT and security tools. Includes the Sophos Email Monitoring System (EMS) and hundreds of turnkey integrations.
- Sophos Endpoint included, with the flexibility to use non-Sophos endpoint protection if preferred.

SOPHOS MDR PLUS

- Includes everything in Sophos MDR, plus enhanced protection with Sophos Endpoint deployed across your environment.
- **Plus:** Access to the Incident Response team, including a named Incident Response Advisor, investigation of scope, impact, and techniques, full threat neutralization, remediation guidance, and a post-incident summary.
- **Plus:** A $1M Sophos-underwritten breach protection warranty for qualifying customers.

FLEXIBLE ENGAGEMENT MODELS

Run a world-class SOC without building one

Partner with the world's largest MDR operation, staffed for the agentic era with security analysts, threat hunters, incident responders, and specialists who govern every autonomous action.

Sophos MDR is designed to work the way you do, with customizable engagement models to match your needs:

- **Fully outsourced detection and response** for organizations without an in-house security team or SOC.
- **Co-managed models** for organizations with mature SOCs seeking AI-accelerated triage and investigation, with full human accountability.
- **24/7 coverage** for lean security teams.
- **A scalable service** for MSP and MSSP managed security practices.

From small and mid-sized organizations to complex enterprises, Sophos MDR adapts to your operational reality rather than forcing you into a rigid model.

Your partner in the agentic era

01

Secure the AI you depend on

Copilots, agents, and LLM-powered workflows expand your attack surface. Sophos protects them — and the data they touch — against AI-targeted attacks.

02

A trusted edge in the AI era

Partner with an MDR provider that combines agentic AI and expert human oversight at scale. We own the response, so your team can focus on the AI transformation in front of them.

03

Intelligence that compounds

Every threat across 625,000+ defended organizations makes the next defense stronger. The system doesn't just scale, it learns — increasing the value of your Sophos partnership.

WHY SOPHOS MDR

The Sophos MDR advantage



Global scale and proven protection

Sophos MDR protects organizations across every vertical, every size, and every region. We see and stop more threats than anyone else, so you're better protected.



Compounding intelligence

Every threat across 625,000+ defended organizations makes the next defense stronger. The system doesn't just get bigger, it gets smarter. Every customer benefits from the collective intelligence of the entire community.



AI-accelerated, human-led operations

Agentic AI delivers the speed and scale modern attacks demand. Human experts deliver the judgment, accountability, and decisive action that drives outcomes.



Vendor-agnostic by design

Sophos MDR meets you where you are, integrating with your existing technology stack to defend across every layer, protecting your investments and preserving flexibility as your environment evolves.



Full-scale threat response

When threats are confirmed, Sophos MDR doesn't just contain the problem, we eradicate it. No hourly caps, no extra fees, no compromises.

INDUSTRY RECOGNITION

Validated by the analysts and organizations that matter most

GARTNER 2026

A "Customers' Choice" for MDR Services

G2 SUMMER 2026

#1 in Endpoint, EDR, XDR, MDR & Firewall

KUPPINGERCOLE 2026

Leader, Managed Detection and Response

MITRE ATT&CK EVALS

100% detection coverage

FROST & SULLIVAN 2025

Leader, Frost Radar for MDR

GARTNER PEER INSIGHTS

4.8 / 5.0 rated by MDR customers

SPEAK WITH AN EXPERT

Sophos MDR: Fully managed, 24/7 detection and response for the agentic era.

Request a custom service proposal for Sophos MDR.

sophos.com/MDR →

[1] The State of Ransomware 2025 — Sophos.

[2, 3] Sophos research; Quantifying ROI: Understanding the impact of cybersecurity products and services on cyber insurance claims.

[4] Cybersecurity & Infrastructure Security Agency (CISA).

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, PEER INSIGHTS is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

Gartner®, Peer Insights™ Voice of the Customer for Managed Detection and Response, Peer Contributors, 31 March 2026.

2026-07-09 BR (MC)

SOPHOS