SOLUTION BROCHURE

Sophos MDR

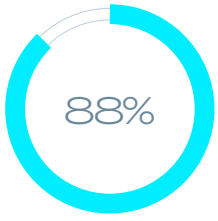
Detection and response that keeps you ahead of adversaries while solving your security challenges

No matter where you are in your security journey, Sophos Managed Detection and Response (MDR) services provide comprehensive MDR options that reduce your risk, simplify your security approach, maximize your technology investments, and fortify your defenses.

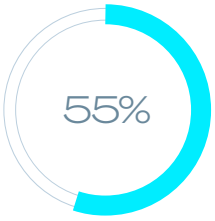
Seeking the answer to today's security problems

You face plenty of challenges staying ahead of the threats targeting your business. The threat landscape continues evolving at a dizzying pace, with new attacker tactics and ransomware types appearing all the time. Organizations constantly try to hire, train, and retain in-house security personnel amidst high turnover and burnout rates. The resources you do have struggle to manage the output from various security tools that produce too much noise, do not integrate together, and leave gaps in coverage.

The numbers don't lie

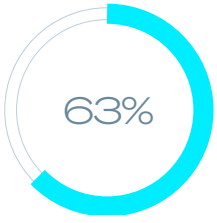


Percentage of ransomware attacks that occur outside normal business hours[1]

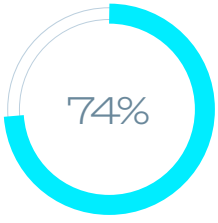


Percentage of ransomware attacks that use legitimate credentials or exploit an unknown vulnerability[2]

The gap in the global cybersecurity workforce[3]



Percentage of ransomware victims that lacked people or skills to stop the attack[4]



Percentage of IT/security professionals that experienced cybersecurity fatigue or burnout in the last year[5]

Sophos MDR services

No matter your company's size, industry, budget, or security maturity, Sophos has an MDR service that fits your needs today — with additional options as your business needs evolve. Our MDR services are built on the combination of easy-to-use, AI-driven technology with world-class security experts who monitor, prevent, detect, and respond to threats 24/7.

Benefits

- **Reduce your risk:** Protection driven by the latest insights into attacker trends and techniques, discoveries from world-class threat researchers, and findings from security testing and threat hunting engagements.
- **Consolidate your security approach:** Consolidate outputs from disparate security products into one platform for correlation, assessment, and decision making.
- **Maximize your technology investments:** Integrate hundreds of leading security products into one service, from endpoint to cloud, identity to network, backup to email – odds are we integrate with your next product purchase, too.
- **Fortify your defenses:** Enable detailed investigation into suspicious activity, rapid response to confirmed threats, and around-the-clock access to security analysts and cross-discipline experts.

What Sophos MDR delivers

Instant AI-accelerated security operations center (SOC).

Our team of global cybersecurity experts monitors your environment for threats 24/7.

Industry-leading threat researchers constantly discover new threat groups and attack techniques.

Proactive threat hunting to find stealthy threats that allude detection by security tools.

Full-scale incident response to fully eliminate adversaries. No caps or extra fees.

Constant updates to threat detection rules and technology integrations ensure you stay protected.

Defer high log storage costs with options for data retention.

Choose from a range of service tiers and threat response modes to meet your needs.

Rapid access to cross-discipline cybersecurity expertise.

Reduce your risk exposure

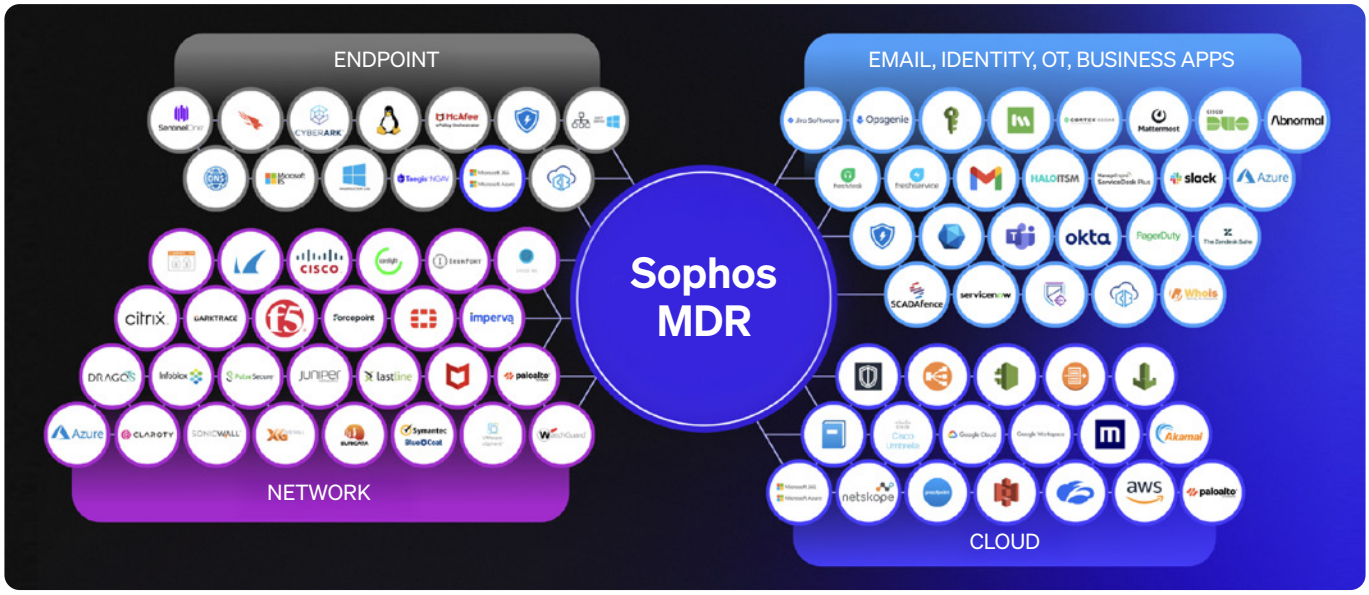
Attack surfaces are expanding and you are challenged with securing a broadening technology landscape. Sophos MDR harnesses the power of automation and an AI-native platform – combined with deep threat intelligence, research, and insights from threat hunting and security testing engagements – to weed out real threats from the mountains of noise your environment generates. This allows us to rapidly prioritize the most serious threats to your business.

Protect your technology investments

Safeguard your cybersecurity product investments and avoid rip-and-replace with Sophos MDR. With 350+ technology integrations, we can ingest telemetry from leading third-party products to accelerate threat detection and response, and give you more flexibility if your product footprint changes in the future.

Service features

- 24/7 threat monitoring, detection, investigation, and response.
- Vast integrations at no extra cost across endpoint, network, cloud, identity, email, OT, and more.
- Rapid access to cross-discipline security experts.
- Expert-led threat hunting.
- Root cause analysis.
- Breach protection warranty.



The above is a representative sample of our 350+ technology integrations.

Surround yourself with security experts

Finding skilled security resources is difficult. Keeping them is an even bigger challenge. Sophos MDR alleviates this burden by surrounding you with vast cross-discipline security expertise at every part of your cybersecurity journey:

Security Analysts: Serving as your first line of defense: highly skilled, experienced analysts delivering 24/7 threat monitoring, investigation, and incident response.

Threat Researchers: Proactively researching threat actors, adversary activity, and emerging tactics, techniques, and procedures.

Threat Hunters: Performing lead-based and hypothesis-driven hunting of threat actor activity to discover hidden threats.

Incident Responders: Driving threat mitigation activities, containment, and remediation of complex cyber incidents to fully eliminate adversaries and understand root causes.

Detection Engineers: Continuously developing and deploying new detections informed by threat research, incident response, threat hunting, and security testing activities.

Security Automation Engineers: Optimizing and scaling operations to reduce noise and accelerate response to real threats.

Customer Success: Serving as your advocate and first point of contact to manage your Sophos experience.

To learn more, visit
sophos.com/mdr

1 – Sophos, Active Adversary Report, April 2025
2 – Sophos, The State of Ransomware 2025
3 – ISC2, 2024 Cybersecurity Workforce Study
4 – Sophos, The State of Ransomware 2025
5 – The Human Cost of Vigilance: Addressing Cybersecurity Burnout in 2025

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

2025-09-19 BR-EN (DD)

SOPHOS