Sophos Managed Detection and Response

24/7 Threat Detection and Response

Sophos MDR is a fully managed 24/7 service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

Ransomware and Breach Prevention Services

The need for always-on security operations has become an imperative. However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage detection and response on their own.

With Sophos MDR, our expert team stops advanced human-led attacks. We take action to neutralize threats before they can disrupt your business operations or compromise your sensitive data. Sophos MDR is customizable with different service tiers, and can be delivered via our proprietary technology or using your existing cybersecurity technology investments.

Cybersecurity Delivered as a Service

Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside, Sophos MDR can:

- **Detect more cyberthreats than security tools can identify on their own**
  Our tools automatically block 99.98% of threats, which enables our analysts to focus on hunting the most sophisticated attackers that can only be detected and stopped by a highly trained human.
- **Take action on your behalf to stop threats from disrupting your business**
  Our analysts detect, investigate, and respond to threats in minutes — whether you need full-scale incident response or help making accurate decisions.
- **Identify the root cause of threats to prevent future incidents**
  We proactively take actions and provide recommendations that reduce risk to your organization. Fewer incidents mean less disruption for your IT and security teams, your employees, and your customers.

Compatible with the Cybersecurity Tools You Already Have

We can provide the technology you need from our award-wining portfolio, or our analysts can leverage your existing cybersecurity technologies to detect and respond to threats.

Sophos MDR is compatible with security telemetry from vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others. Telemetry is automatically consolidated, correlated, and prioritized with insights from the Sophos Adaptive Cybersecurity Ecosystem (ACE) and Sophos X-Ops threat intelligence unit.

Highlights

- Stop ransomware and other advanced human-led attacks with a 24/7 team of threat response experts
- Maximize the ROI of your existing cybersecurity technologies
- Let Sophos MDR execute full-scale incident response, work with you to manage security incidents, or deliver detailed threat notifications and guidance
- Improve cyber insurance coverage eligibility with 24/7 monitoring and endpoint detection and response (EDR) capabilities
- Free up your internal IT and security staff to focus on business enablement

SOPHOS

MDR That Meets You Where You Are

Sophos MDR is customizable with different service tiers and threat response options. Let the Sophos MDR operations team execute full-scale incident response, work with you to manage cyberthreats, or notify your internal security operation teams any time threats are detected. Our team quickly learns the who, what, when, and how of an attack. We can respond to threats in minutes.

Key Capabilities

24/7 Threat Monitoring and Response

We detect and respond to threats before they can compromise your data or cause downtime. Backed by six global security operations centers (SOCs), Sophos MDR provides around-the-clock coverage.

Compatible with Non-Sophos Security Tools

Sophos MDR can integrate telemetry from third-party endpoint, firewall, identity, email, and other security technologies as part of Sophos ACE.

Full-Scale Incident Response

When we identify an active threat, the Sophos MDR operations team can execute an extensive set of response actions on your behalf to remotely disrupt, contain and fully-eliminate the adversary.

Weekly and Monthly Reporting

Sophos Central is your single dashboard for real-time alerts, reporting, and management. Weekly and monthly reports provide insights into security investigations, cyberthreats, and your security posture.

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE automatically prevents malicious activity and enables us to search for weak signals for threats that require human intervention to detect, investigate, and eliminate.

Expert-Led Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own. The Sophos MDR operations team can also use third-party vendor telemetry to conduct threat hunts and identify attacker behaviors that evaded detection from deployed toolsets.

Direct Call-in Support

Your team has direct call-in access to our Security Operations Center (SOC) to review potential threats and active incidents. The Sophos MDR operations team is available 24/7/365 and backed by support teams across 26 locations worldwide.

Dedicated Incident Response Lead

We provide you with a Dedicated Incident Response Lead who collaborates with your internal team and external partner(s) as soon as we identify an incident and works with you until the incident is resolved.

Root Cause Analysis

Along with providing proactive recommendations to improve your security posture, we perform root cause analysis to identify the underlying issues that led to an incident. We give you prescriptive guidance to address security weaknesses so they cannot be exploited in the future.

Sophos Account Health Check

We continuously review settings and configurations for endpoints managed by Sophos XDR and make sure they are running at peak levels.

Threat Containment

For organizations that choose not to have Sophos MDR perform full-scale incident response, the Sophos MDR operations team can execute threat containment actions, interrupting the threat and preventing spread. This reduces workload for internal security operations teams and enables them to rapidly execute remediation actions.

Intelligence Briefings: "Sophos MDR ThreatCast"

Delivered by the Sophos MDR operations team, the "Sophos MDR ThreatCast" is a monthly briefing available exclusively to Sophos MDR customers. It provides insights into the latest threat intelligence and security best practices.

Sophos Service Tiers

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓	✓
Compatible with non-Sophos security products	✓	✓	✓
Weekly and monthly reporting	✓	✓	✓
Monthly intelligence briefing: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Account Health Check		✓	✓
Expert-led threat hunting		✓	✓
Threat containment: attacks are interrupted, preventing spread Uses full Sophos XDR agent (protection, detection, and response) or Sophos XDR Sensor (detection and response)		✓	✓
Direct call-in support during active incidents		✓	✓
Full-scale incident response: threats are fully eliminated Requires full Sophos XDR agent (protection, detection, and response)			✓
Root cause analysis			✓
Dedicated Incident Response Lead			✓

Integrations Included Free of Charge

Security data from the following sources can be integrated for use by the Sophos MDR operations team free of charge. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations

Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint

Block advanced threats and detect malicious behaviors—including attackers mimicking legitimate users

Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions occurring between devices that otherwise are unseen

Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform

Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks

90-Days Data Retention

Sophos XDR and Sophos Endpoint Protection products are included with Sophos MDR service
Sophos Firewall, Sophos Cloud, Sophos Email, and Sophos NDR products must be purchased and deployed prior to integration with Sophos MDR service

Add-On Integrations

Security data from the following third-party sources can be integrated for use by the Sophos MDR operations team via the purchase of Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

Firewall

Compatible with...

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

Cloud

Compatible with...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identity

Compatible with...

- Okta
- Duo

Network Security

Compatible with...

- Darktrace
- Forcepoint
- McAfee (web gateway)

Email

Compatible with...

- Proofpoint
- Mimecast

1-Year Data Retention

Onboarding Plus Package for Sophos MDR

Our Onboarding Plus offering is a remotely guided onboarding service available to Sophos MDR customers. It gives you access to a dedicated contact within Sophos' Professional Services organization for onboarding and scheduling, deployment and training assistance, and a health check to ensure you can get the most value out of our best practices. Onboarding Plus includes:

Day 1 - Implementation Planning and Execution:

- Kick off project
- Configure Sophos Central
- Review Sophos Central features
- Build and test deployment process
- Deploy Sophos Central across your organization

Day 30 - XDR Training

- Learn how to think and act like an SOC
- Hunt for IOCs
- Construct queries for future investigations

Day 90 - XDR Training

- Review your current security policies and update them as needed
- Determine which features (if any) can be used to further enhance your cyber protection
- Receive written documentation with recommendations from our health check

To learn more, visit

sophos.com/mdr

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

22-11-01 DS-EN (DD)

SOPHOS