Sophos Managed Detection and Response

Expert-Led Threat Response

Sophos Managed Detection and Response (MDR) provides 24/7 threat hunting, detection, and response delivered by an expert team as a fully managed service.

Threat Notification Isn't the Solution – It's the Starting Point

Most organizations lack the in-house tools, people and processes to defend against cyber threats and manage their security program. Sophos MDR delivers round-the-clock threat detection and response. We neutralize sophisticated threats 24/7/365.

Sophos MDR is delivered by threat hunters and response experts who:

- Proactively hunt for and validate potential threats and incidents.
- Use all available information to determine the scope and severity of threats.
- Provide insights into a threat's context and potential impact.
- Take action to remotely disrupt, contain, and neutralize threats.
- Provide guidance for addressing the root cause of recurring incidents.

Machine-Accelerated Human Response

Built on our Sophos XDR, Sophos MDR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision. This fusion of Sophos' consistently top-rated endpoint protection and intelligent XDR, with a world-class team of security experts results in what we call "machine-accelerated human response."

Complete Transparency and Control

With Sophos MDR, you control how and when potential incidents are escalated, what response actions are taken, and who is included in incident communications. Sophos MDR features three response modes, giving you the flexibility to choose the best way for you to work with our MDR team during incidents.

Notify: We notify you about a potential incident, provide you with details about it, and help you prioritize it and respond accordingly.

Collaborate: We work with your internal team or external point(s) of contact to respond.

Authorize: We contain and neutralize the incident and let you know what action(s) we've taken.

Highlights

- Advanced threat hunting, detection, and response delivered as a fully managed service
- 24/7/365 response team remotely contains and neutralizes threats
- You control what actions the MDR team takes on your behalf and how incidents are managed
- Access top-rated machine learning technology and a highly trained team of experts
- Two tiers of service (Standard and Advanced) provide a comprehensive set of capabilities for organizations of all maturity levels

SOPHOS

Sophos MDR Service Tiers

Sophos MDR features two service tiers (Standard and Advanced) to provide a comprehensive set of capabilities for organizations of all sizes and maturity levels. Regardless of service tier, organizations can use any of the three response modes (notify, collaborate, or authorize).

Sophos MDR: Standard

24/7 Lead-Driven Threat Hunting

Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated. This frees up threat hunters to perform lead-driven hunts, which involve investigating and analyzing causal and adjacent events (weak signals) to discover new indicators of attack (IOAs) and indicators of compromise (IOCs).

Security Health Check

Our proactive examinations keep you up to date on your operating conditions and configurations. We also provide recommendations you can use to keep Sophos XDR and other Sophos Central products performing at peak levels.

Activity Reporting

We summarize case activities so you know what threats we found and what response actions were taken within different reporting periods.

Adversarial Detections

We use advanced investigation techniques to differentiate legitimate behaviors from cybercriminal tactics, techniques, and procedures (TTPs).

Sophos MDR: Advanced Includes All Standard Features, Along with:

24/7 Leadless Threat Hunting

We use data science and threat intelligence to anticipate cyberattacks and identify IOAs.

Enhanced Telemetry

We supplement our threat investigations with telemetry from Sophos Central products beyond the endpoint to provide a full picture of your security posture.

Proactive Posture Improvement

We provide prescriptive guidance to help you optimize your security posture.

Dedicated Threat Response Lead

We provide you with a dedicated threat 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..

Direct Call-In Support

Your team has direct call-in access to our security operations center (SOC). Our MDR Operations Team is available 24/7/365 and backed by support teams spanning 26 locations worldwide.

Asset Discovery

We provide insights into your managed and unmanaged assets and how to secure them.

Onboarding Plus Package for MDR Customers

Our Onboarding Plus offering is a remote-guided onboarding service for customers that have purchased Sophos MDR. This service includes a dedicated contact within Sophos' Professional Services organization for onboarding and scheduling, assistance with deployment and training, and a health check to ensure that you are get the most value out of our best practice recommendations. 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 a security operations center (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.

If you have any questions, please reach out to our Professional Services team.

Americas: ProfessionalServices@sophos.com

APJ: ProfessionalServicesAU@Sophos.com.au

Europe: ProfessionalServicesEmea@Sophos.com

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

SOPHOS