

# 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, backups, 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 managed detection and response (MDR) capabilities that provide complete security coverage wherever your data reside, Sophos MDR can:

- **Detect more cyberthreats than security tools can 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-winning portfolio, or our analysts can leverage your existing cybersecurity technologies to detect and respond to threats.

Sophos' open, AI-native platform is compatible with a wide range of identity, network, firewall, email, cloud, productivity, backup, and endpoint security solutions - with Microsoft and Google Workspace integrations included at no additional cost.

## 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

## 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 seven 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, network, identity, email, backup and recovery, and other technologies.

#### 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. With a Sophos MDR Complete license, you benefit from unlimited full-scale incident response, with no caps and no extra fees.

#### Reports and service insights

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

#### Endpoint and workload protection included

Sophos MDR analysts can use telemetry from your existing endpoint protection solution to detect and respond to threats targeting your computers and servers. Alternatively, switch to Sophos Endpoint for superior protection — included at no additional cost.

#### 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 MDR 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

Weekly Sophos MDR "ThreatBrief" bulletins and monthly live "ThreatCast" webinars — exclusive to Sophos MDR customers — provide insights into the latest threat intelligence and security best practices.

#### Breach protection warranty

Included with all Sophos MDR Complete annual (one to five years) and monthly licenses, the warranty covers up to \$1 million in response expenses. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

#### Backed by Sophos X-Ops

Sophos X-Ops brings together deep expertise across the attack environment. Our elite teams provide unparalleled threat intelligence and continuously build and deploy new detection rules on your behalf, to protect against active adversaries as they evolve their tactics.

## Integrations included

Security data from the following sources can be integrated for use by the Sophos MDR operations team at no additional cost. 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 Endpoint**

Block advanced threats and detect malicious behaviors across your endpoints

Product included in Sophos MDR pricing

### **Workload Protection**

Advanced protection and threat detection for Windows and Linux servers and containers

Product included in Sophos MDR pricing

### **Sophos Mobile**

Keep your iOS and Android devices and data secure from the latest mobile threats

Product sold separately; integrated at no additional charge

### **Sophos Firewall**

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

Product sold separately; Xstream Protection subscription required; integrated at no additional charge

### **Sophos Email**

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

Product sold separately; integrated at no additional charge

### **Sophos Cloud Optix**

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and GCP

Product sold separately; integrated at no additional charge

### **Sophos ZTNA**

Replace remote access VPN with least-privileged access to securely connect your users to your networked applications

Product sold separately; integrated at no additional charge

### **Third-party endpoint protection**

Integrations include:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Compatible with other endpoint protection solutions with the Sophos 'XDR Sensor' agent

### **Microsoft security tools**

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

### **90-days data retention**

Retains detection data in the Sophos data lake for 90 days as standard

### **Microsoft Office 365 Management Activity**









Provides information on user, admin, system, and policy actions and events ingested via the Office 365 Management Activity API

### **Google Workspace**


Ingests security telemetry from the Google Workspace Alert Center API

## 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.

 <b>Sophos NDR</b> <p>Continuously monitor activity inside your network to detect suspicious actions occurring between devices that are otherwise unseen</p> <p>Compatible with any network via SPAN port mirroring</p>	 <b>Firewall</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Barracuda</li><li>• Check Point</li><li>• Cisco Firepower</li><li>• Cisco Meraki</li><li>• Fortinet</li><li>• F5</li><li>• Forcepoint</li><li>• Palo Alto Networks</li><li>• SonicWall</li><li>• Ubiquiti</li><li>• WatchGuard</li></ul>	 <b>Network</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Cisco Umbrella</li><li>• Darktrace</li><li>• Secutec</li><li>• Skyhigh Security</li><li>• Thinkst Canary</li><li>• Vectra</li><li>• Zscaler</li></ul>
 <b>Identity</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Auth0</li><li>• Cisco ISE</li><li>• Duo</li><li>• ManageEngine</li><li>• Okta</li></ul> <p>Microsoft integration included at no additional charge</p>	 <b>Email</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Mimecast</li><li>• Proofpoint</li><li>• Trend Micro</li></ul> <p>Microsoft 365 and Google Workspace integrations included at no additional charge</p>	 <b>Cloud</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Orca Security</li></ul> <p>AWS, Azure and GCP integrations included with Sophos Cloud Optix product, sold separately.</p>
 <b>Backup and Recovery</b> <p>Integrations include:</p> <ul style="list-style-type: none"><li>• Acronis</li><li>• Rubrik</li><li>• Veeam</li></ul>	 <b>1-year data retention</b> <p>Retains detection data in the Sophos data lake for 1 year</p>	

## Add-on service

 <b>Sophos Managed Risk, Powered by Tenable</b> <p>Reduce cybersecurity risk with proactive attack surface vulnerability management, delivered as a service. Sophos Managed Risk identifies high-priority vulnerabilities so action can be taken to prevent attacks before they disrupt your business. Available as an add-on for Sophos MDR.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Sophos MDR service tiers

	Sophos MDR Essentials	Sophos MDR Complete
24/7 expert-led threat monitoring and response	✓	✓
Sophos Endpoint and Sophos Workload Protection included	✓	✓
Compatible with non-Sophos security products	✓	✓
Service insights and reporting	✓	✓
Sophos threat intelligence briefings	✓	✓
Sophos account health check	✓	✓
Expert-led threat hunting	✓	✓
Threat containment: attacks are interrupted, preventing spread Use the full Sophos XDR agent or the Sophos 'XDR Sensor' agent	✓	✓
Direct call-in support during active incidents	✓	✓
Full-scale incident response: threats are fully eliminated Requires the full Sophos XDR agent	IR service add-on*	✓
Dedicated incident response lead	IR service add-on*	✓
Root cause analysis	IR service add-on*	✓
Breach protection warranty		✓
Microsoft and Google Workspace integrations included	✓	✓
Integrations with non-Sophos firewall, network, email, cloud, identity, and backup solutions	Add-on	Add-on
Sophos Network Detection and Response (NDR)	Add-on	Add-on
Sophos Managed Risk, powered by Tenable	Add-on	Add-on

\*An annual subscription to a Sophos IR Services Retainer provides discounted pricing on incident response services. Benefit from an elite team of incident response experts on standby to get you back to business quickly in the event of a breach.

## Guided onboarding (option)

Sophos MDR Guided Onboarding is available for remote onboarding assistance, as an optional additional purchase. The service provides hands-on support for a smooth and efficient deployment, ensures best practice configurations, and delivers training to maximize the value of your MDR service investment. You are provided a dedicated contact from the Sophos Professional Services organization who will be with you through your first 90 days to make sure your implementation is a success. Sophos MDR Guided Onboarding includes:

### Day 1 – Implementation

- Project kickoff
- Configure Sophos Central and review of features
- Build and test deployment process
- Configure MDR integrations
- Configure Sophos NDR sensor(s)
- Enterprise-wide deployment

### Day 30 - MDR training

- Learn to think and act like a SOC
- Understand how to hunt for indicators of compromise
- Gain an understanding of using our MDR platform for administrative tasks
- Learn to construct queries for future investigations

### Day 90 - Security posture assessment

- Review current policies for best practice recommendations
- Discuss features that are not in use that could provide additional protection
- Security assessment following NIST framework
- Receive summary report with recommendations from our review

## See why customers choose Sophos MDR

Sophos is an established leader in managed detection and response, with industry recognition to back it up.



*A Leader in the 2024 IDC MarketScape for Worldwide Managed Detection and Response Services*



*A Customers' Choice in the 2024 Gartner® Voice of the Customer report for Managed Detection and Response*



*Rated overall Leader by customers in the Winter 2025 G2 Grid® Report for Managed Detection and Response*



*A Leader in the 2024 Frost Radar report for Global Managed Detection and Response*



*A strong performer in MITRE ATT&CK Evaluations for Managed Services*

To learn more, visit

[sophos.com/mdr](https://sophos.com/mdr)

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)