betechsecure
cyber security consultants

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 MOR 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 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.

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 aligibility with 24/7 monitoring and endpoint detection and response (EDR) capabilities

- ⊘ Free up your internal IT and security staff to focus on business enablement

Cybersecurity Delivered as a Service

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, Rapid?, Amazon Web Services (AWS), Google, Okta, Barktrace, and many others. Telemetry is automatically consolidated correlated, and prioritized with insights from the **Sophos Adaptive Cybersecurity Ecosystem (ACE) and Sophos X-Ups** threat intelligence unit

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 MOR 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.

☑ 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.

☑ 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,

☑ 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

☑ 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

☑ 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.

☑ 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 MOR operations team can also use third-party vendor telemetry to conduct threat hunts and identify attackar behaviors that evaded detection from deployed toolsets

☑ 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 teama and enables them to rapidly execute remediation actions

☑ Intelligence Briefings: "Sophos MDR ThreatCast"

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

☑ Breach Protection Warranty

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

betechsecure
cyber security consultants

Sophos MDR Included Integrations

Security data from the following sources can be integrated for use by the Sophos MOR 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

Workload Protection
Advanced protection and threat detection for Windows and Linux servers and containers
Product included in Sophos MDR pricing

Sophos Mobile
Keep your IDS and Android devides 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; 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
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
Compatible with:
- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)
  + compatible with other solutions with the Sophos 'XDR Sensor' agent

Microsoft Security Tools
- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

90-Days Data Retention
Retains data from Sophos products and third-party [non-Sophos] solutions in the Sophos Data Lake
Extendable to 1 year as an optional add-on

Microsoft Audit Logs
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.

Sophos NDR
Continuously monitor activity inside your network to detect suspicious actions occurring between devices that are otherwise unseen
Compatible with any network via SPAN port mirroring

Firewall
Compatible with:
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- Palo Alto Networks SonicWall
- WatchGuard

Network
Compatible with:
- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary

Identity
Compatible with:
- Autho
- Duo
- ManageEngine
- Okta
Microsoft integration included at no additional charge

Email
Compatible with:
- Proofpoint
- Mimecast
Microsoft 365 and Google Workspace integrations included at no additional charge

Public Cloud
Compatible with:
- AWS Security Hub
- AWS CloudTrail
- Orca Security
Integrate additional AWS, Azure and GCP data via Sophos Cloud product, sold separately

Backup and Recovery
Compatible with:
- Veeam

1-Year Data Retention
Retains data from Sophos products and third-party (non-Sophos) solutions in the Sophos Data Lake

Sophos Service Tiers

	Sophos MDR Essentials	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 MDR agent (protection, detection, and response) or Sophos MDR Sensor (detection and response)	✓	✓
Direct call-in support during active incidents	✓	✓
Full-scale incident response: threats are fully eliminated	✓	✓
Dedicated Incident Response Lead	IR Retainer Add-on	✓
Root cause analysis		✓
Dedicated Incident Response Lead		✓
Breach Protection Warranty Covers up to $1 million in response expenses		✓

Sophos MDR Guided Onboarding

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.

Gartner — Representative Vendor in the Gartner Market Guide for Managed Detection and Response Services

Gartner peerinsights — A Gartner Peer Insights Customers' Choice for Managed Detection and Response

G2 Leader — Rated the Number 1 MDR solution by customers in the G2 Winter 2024 Grid Reports

FROST & SULLIVAN — A Leader in the 2024 Frost Radar report for Global Managed Detection and Response

MITRE ATT&CK — Exceptional results in the first-ever MITRE Engenuity ATT&CK Evaluation of Security Service Providers