SOPHOS

Managed Detection and Response (MDR) Services Buyers Guide

Few organizations have the right tools, people, and processes in-house to effectively manage their security program around-the-clock while proactively defending against new and emerging threats. As a result, organizations are increasingly looking towards managed detection and response (MDR) services to run their security operations program.

According to Gartner[1], by 2025, 50% of organizations will be using MDR services (this is up from less than 5% in 2019).

However, the security services marketplace is relatively new to many, and can be filled with false claims and confusing technical jargon. Making an educated decision for your organization is increasingly difficult. This guide provides clarity by walking you through the key considerations when choosing an MDR service. It also enables you to see how MDR providers stack up against one another, helping you make an informed choice.

Security operations requires skilled professionals

The cybersecurity industry is experiencing a massive gap in talent and experience. As a result, organizations are struggling to build effective security operations (SecOps) programs to detect, investigate, and respond to threats before damage occurs.

While tools, such as EDR, are built to hunt for threats and respond to incidents, they still require a skilled operator to benefit from all their capabilities. In a 2019 survey of 2,300 IT and security professionals[2], 54% of respondents claimed they were "unable to take full advantage of their EDR solution" due to a lack of experienced talent.

This problem is so widespread among organizations that according to analyst research firm ESG[3], "34% say their biggest challenge is that they lack skilled resources to investigate a cybersecurity incident involving an endpoint to determine root cause and the attack chain."

With security threats growing in both volume and sophistication how are organizations expected to keep up without aggressively ramping up their security operations team? This dilemma has given way to a new alternative: managed security services. Specifically, managed detection and response (MDR) services.

Managed Detection and Response (MDR) service definition

Managed detection and response (MDR) services are outsourced security operations delivered by a team of specialists. MDR services act as an extension of the customer's security team, combining human-led investigations, threat hunting, real-time monitoring, and incident response with a technology stack to gather and analyze intelligence.

MDR providers often use a combination of host and network-layer technologies as well as advanced analytics, threat intelligence, forensic data, and human expertise to rapidly identify and neutralize threats. The goal of MDR is to detect and respond to threats in customer environments that have circumvented preventative security controls. These preventive controls—such as firewalls, antivirus, and content filtering—are effective at stopping known commodity threats but can fail to successfully defend against new and sophisticated cyberattacks. MDR providers have risen to fill the threat detection and response gap left by these tools.

Reasons organizations choose an MDR service

Some of the primary drivers for employing an MDR service include:

- **Limited security operations capabilities in-house:** Many organizations struggle to go beyond a prevention focused security strategy and do not have the ability to stand up and maintain their own security operations program.
- **Struggling to get full value out of EDR tools:** Some organizations have purchased EDR solutions, either as a reactive technology in case of an incident, or with the hopes of utilizing it for proactive threat hunting and response. However, they are not able to fully develop their own security operations program and need to leverage outside experts.
- **Augmenting an existing security operations team:** Even organizations that have a team of skilled security analyst have gaps in coverage (i.e. nights, weekends, holidays) and specialized roles (i.e. malware analyst, incident response specialist). Similarly, some security teams need additional coverage from an outsourced SOC so they can focus on more general IT and security tasks that they struggle to keep up with.
- **Ensuring your team is not missing anything:** Even mature security operation centers often want a second set of eyes monitoring their environment to ensure nothing slips through the cracks.

Benefits of MDR services

24/7/365 team of experts

MDR services should also have the required expertise to detect and respond to any type of attack. Not only are they staffed with professionals who are notoriously hard to hire, train, and retain, a properly staffed MDR service should also offer continuous coverage. This means that they're constantly monitoring your environment and can respond to any potential threat at any time. This includes weekends, holidays, and the middle of the night. It's like having a large security operations team that never takes vacation, never takes sick leave, and never sleeps.

Services are an enabler

Most organizations already struggle to conduct their own threat hunting, incident response, and security health checks. By outsourcing detection and response operations, security services allow team members to focus on the tasks that match their skill set. For more advanced organizations the addition of MDR also allows teams to prioritize "hero moments" while offloading much of the day-to-day security operations tasks.

Cost savings

Organizations that look to build their own security operations program will quickly realize the difficulty and cost of building a true security operation center (SOC) in house. Even a mid-sized organization would need at least four cybersecurity analysts to maintain 24/7/365 coverage. Larger organizations would need several more highly paid team members. Organizations still need to factor in the cost for team managers and engineers to customize and maintain the team's tools. And this is just the cost of hiring team members; the budget would still need to allow for the tools the team will need, such as endpoint protection, network protection, endpoint detection and response (EDR), SIEM, workflow processing (SOAR), intelligence feeds, and more.

Peace of mind

With a proper MDR service, you and your organization can sleep well knowing that that there is a team of skilled experts constantly monitoring your organization, hunting threats, investigating suspicious activity, and responding to potential incidents. With the ever-growing cyber security threat landscape, there is peace of mind when you are working with a team whose entire focus is cybersecurity.

Evaluating MDR providers: Top questions to ask

General criteria

How many customers does the MDR service have?

Part of what separates MDR providers is the experience they have detecting and responding to incidents. The current customer count will not only give you an idea of how many other organizations trust the service provider, but how well versed they are at responding to a wide variety of suspicious activity. Additionally, ensure that the provider has experience working with organizations with a similar profile (size, vertical, security challenges) as yours.

What is the scope of the service? Is threat response included?

Not all MDR services are designed the same. One increasingly important customer requirement of MDR services—and one that still very few vendors provide—is the ability to take targeted actions to neutralize threats on the customer's behalf versus simply notifying them of potential or imminent threats. Despite the "R" of MDR, the majority of vendors focus primarily or exclusively on threat identification and notification, leaving it up to the customer to manage all response and remediation efforts. Effective MDR services require analysts to conduct methodical investigations to determine the validity and scope of potential threats, minimize false positives, neutralize confirmed threats, and provide additional context and recommendations for improving the organization's overall security posture.

Is the service 24/7/365? If an issue arises at 2AM on a Sunday who will respond?

Ensure the MDR service truly monitors your environment and is able to respond any time of day or night.

Which technologies does the service utilize? Are they included in the price?

When evaluating an MDR service, it is important to understand if the technology used by the operators is included in the price of the service. Some will require you to purchase your own tools (such as endpoint protection and EDR) separately. Others will offer the full technology stack in addition to the services component.

Is the service being provided proactive or reactive?

MDR is an inherently proactive discipline. Unlike retainer-based digital forensics (DF) and incident response (IR) services which are typically offered to help clients deal with a crisis that has already occurred (such as a security incident or breach), MDR offers a proactive, around-the-clock service that monitors customer environments for adversarial activity and, as threats emerge, guides, assists, or performs threat neutralization in real time.

How will you interact with the MDR team?

It is important to understand what the process is to communicate with you service provider. Is there direct call in support? Will you be able to communicate via email? Will you be able to speak directly with SOC analysts or is communication managed through an intermediary (e.g. client success manager)? In some cases, the difference between MDR providers can be as stark as communicating with a person versus communicating with a portal. Regardless of how communication occurs, MDR providers should always include summaries of case activities to ensure your team knows what threats were detected and what follow-ups need to occur.

Methodology and efficacy criteria

What is the security operations threat detection and response (TDR) methodology?

It is important for MDR providers to have a well-defined TDR methodology. If they don't then they will likely struggle to scale as their business grows and will be more likely to miss important indicators of suspicious activity.

How fast is the service?

In security, seconds matter. MDR providers should be able to estimate the following:

- Average time to detect
- Average time to respond
- Average time to resolve

What types of remediation actions can the MDR operators take? Can they take active response for you?

MDR providers should be able to explain what happens when the service detects suspicious activity. As noted earlier, many will simply monitor and notify you that something suspicious has occurred. The MDR operator should be able to take action on your behalf, providing proactive response by a person, not just an automated blocking of threats by a tool.

Is threat hunting lead-driven (responding to alerts), lead-less (looking for new indicators of attack without an alert), or both?

Not all threat hunting is the same. Although threat hunting is by definition a human-led activity, there are vendors who refer to automated alert generation as threat hunting (it's not). It is also important to understand if the MDR operators will proactively hunt to detect adversaries lurking in your environment regardless of whether a strong indicator of activity or compromise has been detected or not. Ask what type of activity would initiate a threat investigation.

What data sources are utilized to provide visibility? Is the service just "managed EDR"?

While endpoint data is absolutely critical for a security operation program, some MDR providers don't have any additional visibility beyond the endpoint. These are not true MDR providers and are more akin to a "managed EDR" solutions that have limited visibility to threats that may be present in your environment.

Does the MDR provider have access to threat intelligence and threat researchers?

MDR providers should have a level of expertise that goes beyond what most organizations can build on their own. This would of course include skilled security analysts. However, the provider should also have access to proprietary threat intelligence and collaborate with threat researchers when something novel is detected.

Vendor comparison

Managed Detection & Response (MDR) providers tend to fall into three categories:

- **Monitoring only:** Focused on prioritizing and notifying customers when an automated alert in the product is generated. They do not offer remediation options other than advice on what the customer needs to do. Additionally, they only leverage "automated" threat hunting, and don't proactively investigate or hunt for threats on the customer's behalf.
- **Limited response (lowercase "r"):** Includes lighter response actions, however they are limited to automated actions. Threat hunting is conducted but only when an alert triggers the investigation.
- **Full response (capital "R")**: Includes full response capabilities. Proactively takes action on the customer's behalf with a manual, human-led response. Threat hunting is not only lead-driven, but the MDR team will routinely hunt for threats even when an indicator of attack may not be visible.

Key Capabilities	Monitoring only	Limited response (lowercase "r")	Full response (capital "R")
24/7 Monitoring	✓	✓	✓
Notification and prioritization	✓	✓	✓
Remediation guidance	✓	✓	✓
Activity reporting	✓	✓	✓
"Automated" threat hunting	✓	✓	✓
Automated response		✓	✓
Lead-driven threat hunting		✓	✓
Lead-less threat hunting			✓
Human-led response			✓

Representative Vendors[4]		
Monitoring only	Limited response (lowercase "r")	Full response (capital "R")
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Sophos Managed Threat Response (MTR) service

Sophos Managed Threat Response (MTR) provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service. Going beyond simply notifying you of attacks or suspicious behaviors, the Sophos MTR team takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats.

The Sophos MTR team of threat hunters and response experts:

- Proactively hunt for and validate potential threats and incidents
- Use all available information to determine the scope and severity of threats
- Apply the appropriate business context for valid threats
- Initiate actions to remotely disrupt, contain, and neutralize threats
- Provide actionable advice for addressing the root cause of recurring incidents

Sophos MTR key capabilities

Sophos MTR: Standard

24/7 Lead-Driven Threat Hunting

Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct lead-driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

Security Health Check

Keep your Sophos Central products--beginning with Intercept X Advanced with EDR--operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.

Activity Reporting

Summaries of case activities enable prioritization and communication, so your team knows what threats were detected and what response actions were taken within each reporting period.

Adversarial Detections

Most successful attacks rely on the execution of a process that can appear legitimate to monitoring tools. Using proprietary investigation techniques, our team determines the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

Sophos MTR: Advanced

24/7 Leadless Threat Hunting

Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high-value assets, and high-risk users to anticipate attacker behavior and identify new Indicators of Attack (IoA).

Enhanced Telemetry

Threat investigations are supplemented with telemetry from other Sophos Central products, extending beyond the endpoint to provide a full picture of adversary activities.

Proactive Posture Improvement

Proactively improve your security posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities.

Dedicated Threat Response Lead

When an incident is confirmed, a dedicated threat response lead is provided to directly collaborate with your on-premises resources (internal team or external partner) until the active threat is neutralized.

Direct Call-In Support

Your team has direct call-in access to our security operations center (SOC). Our MTR Operations Team is available around-the-clock and backed by support teams spanning 26 locations worldwide.

Asset Discovery

From asset information covering OS versions, applications, and vulnerabilities to identifying managed and unmanaged assets, we provide valuable insights during impact assessments, threat hunts, and as part of proactive posture improvement recommendations.

Sophos Managed Threat Response (MTR): Protection, EDR, and MDR			
Key Capabilities	Sophos Intercept X Advanced with EDR (technology only)	Sophos MTR Standard (technology + managed service)	Sophos MTR Advanced (technology + managed service)
Endpoint protection	✓	✓	✓
Endpoint Detection and Response (EDR) for IT operations	✓	✓	✓
Endpoint Detection and Response (EDR) for threat hunting	✓	✓	✓
Managed Service: 24/7 Monitoring and Response		✓	✓
Managed Service: Proactive, manual response		✓	✓
Managed Service: Lead-driven threat hunting		✓	✓
Managed Service: Advanced lead-less threat hunting			✓
Managed Service: Dedicated response lead			✓

Sophos MTR key differentiators

Sophos takes action on your behalf: Unlike Sophos MTR, other services just monitor and notify when suspicious activity is detected. The Sophos MTR team takes action. We remotely initiate actions to disrupt, contain, and neutralize even the most sophisticated threats.

Elite expertise: With over 2,000 customers, Sophos has seen it all and stopped it all. Our highly-trained team of threat hunters, engineers, and ethical hackers has your back 24/7, investigating anomalous behavior and taking action against threats.

Robust threat hunting: Sophos conducts lead-driven and lead-less threat hunts to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

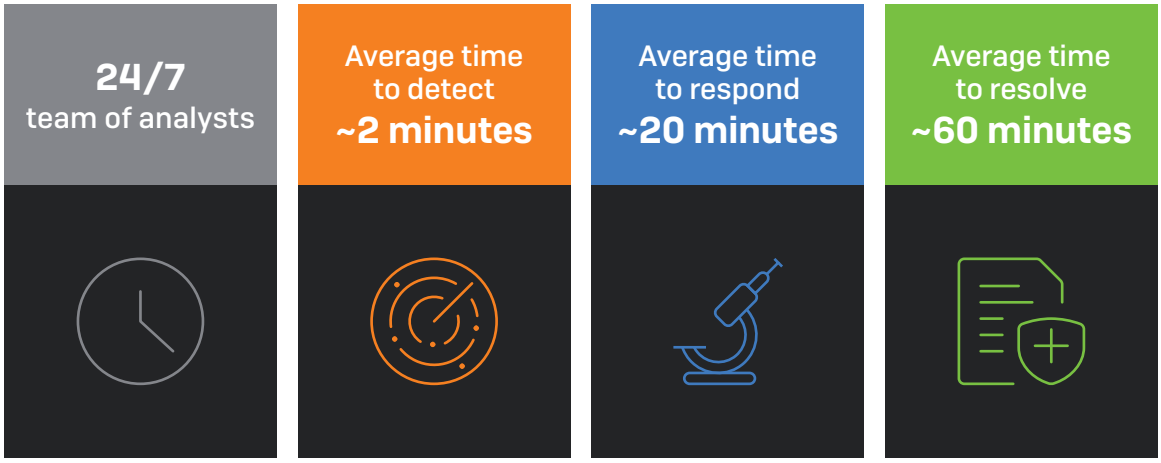
High-fidelity detections: Going beyond traditional detections, Sophos combines deterministic and machine learning models to spot suspicious behaviors and the tactics, techniques and procedures used by the most advanced adversaries.

Focused human response: The Sophos MTR service includes Intercept X Advanced with EDR – the world's beset endpoint protection. This means it automatically stops threats that others let through. Because the service includes better, proactive prevention, the team can focus on detecting, responding to, and taking action on the most challenging incidents.

Transparency and control: With Sophos you own the decisions and control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications. Organizations can take advantage of any of the three response modes - Notify, Collaborate, or Authorize - to fit their unique needs.

Outcome-Focused Security™: Every hunt, investigation, and response action results in decision-driving data that is meant to enhance configurations and automated detection capabilities.

Sophos MTR key stats



Sophos Rapid Response service

Sophos Rapid Response provides lightning-fast assistance with identification and neutralization of active threats against an organization, delivered by an expert team of incident responders. The Rapid Response service is geared for organizations who are currently under attack. Sophos MTR customers would not need the Rapid Response service as incident response is part of the Sophos MTR service.

The Rapid Response service provides immediate action for active incidents. On-boarding starts within hours, and most customers are triaged in 48 hours.

The Sophos Rapid Response 24/7 team of remote incident responders, threat analysts, and threat hunters:

- Quickly take action to triage, contain, and neutralize active threats
- Eject adversaries from your estate to prevent further damage to your assets
- Perform ongoing 24/7 monitoring and response to enhance your protection
- Recommend real-time preventative actions to address the root cause
- Provide a detailed post-incident threat summary that describes our investigation

The Sophos Rapid Response service is available for both existing Sophos customers as well as non-Sophos customers.

For more information on the Sophos Managed Threat Response (MTR) service, visit our website or speak with a Sophos representative.

If you prefer to conduct your own threat hunts, Sophos EDR gives you the tools you need for advanced threat hunting and security operations hygiene. Start a 30-day no-obligation trial today.

Source:

1 Gartner, Market Guide for Managed Detection and Response Services, 26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

2 2019 survey of 3,100 IT managers https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

3 https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

4 This comparison and information document is based on the Sophos interpretation of publicly available data as of the date of preparing this comparison. This document has been prepared by Sophos and not the other vendors listed herein. The features or characteristics of the products under comparison, which may have direct impact on the accuracy and/or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own decision based on their requirements and should also research original sources of information and not rely only upon this comparison while selecting any product.

For more information about
Sophos Managed Threat Response (MTR)

visit sophos.com/mtr

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

2021-02-25 BG-EN (PC)

SOPHOS