SOPHOS
Cybersecurity delivered.

Top Five Reasons to Use MDR Services

A Sophos Whitepaper. September 2022

Introduction

As cyber threats increase in volume, complexity, and impact, organizations are increasingly turning to managed detection and response (MDR) services to detect and neutralize advanced attacks that technology solutions alone cannot prevent. In fact, Gartner anticipates that by 2025, 50% of companies will be using MDR for threat monitoring, detection, and response[1].

However, the proliferation of defense solutions on the market can make it difficult to understand what exactly MDR is, how MDR fits within your wider cybersecurity ecosystem, and the benefits of using an MDR service. This guide answers these questions and offers practical guidance on what to consider when choosing an MDR service.

Sophos MDR

Sophos MDR is the world's most trusted MDR service, securing over 11,000[2] organizations against the most advanced threats, including ransomware. With the highest rating on Gartner Peer Insights™[3] and the Top Vendor recognition in the 2022 G2 Grid® for MDR services serving the midmarket[4], with Sophos MDR your cyber defenses are in good hands.

MDR Defined

To understand the benefits of MDR and what's behind the growing demand for MDR services, it's important to understand what MDR is — and what it's not.

Managed detection and response (MDR) is a fully managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent.

MDR should not be confused with EDR (endpoint detection and response) and XDR (extended detection and response). While MDR, EDR, and XDR all support and enable threat hunting, EDR and XDR are tools that enable analysts to hunt for and investigate potential compromise; with MDR, a security vendor's analysts hunt for, investigate, and neutralize threats on your behalf.

As their names suggest, EDR tools work with data points from endpoint protection technology, while XDR tools extend their data sources across a wide IT stack (including firewall, email, cloud, and mobile security solutions) to provide greater visibility and insights. At Sophos we used our industry-leading EDR and XDR solutions when delivering our MDR service.

What MDR doesn't do is day-to-day cybersecurity management, such as deploying your security technologies, updating policies, applying patches, or installing updates. Managed service providers (MSPs) deliver IT security management services to organizations looking for support in this area.

Who Uses MDR Services

All types of organizations across all sectors use MDR services, from small companies with limited IT resources to large enterprises with an in-house SOC group. The question is really: how do organizations work with MDR services? There are three main MDR response models:

- MDR team completely manages threat response on behalf of the customer
- MDR team works with the in-house team, co-managing threat response
- MDR team alerts the in-house team and provides remediation guidance

At Sophos we support all three approaches, adapting to individual customer requirements as needed.

[1] Gartner Market Guide for MDR 2021
[2] As of August 2022.
[3] Reviews from the last 12 months as of August 1, 2022. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.
[4] Sophos is rated the Top Vendor in the 2022 G2 Grid® for MDR Services serving the midmarket.

The Need for Human-Led Threat Detection and Response

The reality is that technology solutions alone cannot prevent every cyberattack. To avoid detection by cybersecurity solutions, malicious actors increasingly use legitimate IT tools, exploit stolen credentials and access permissions, and leverage unpatched vulnerabilities in their attacks. By emulating authorized users and taking advantage of weaknesses in an organization's defenses, malicious actors can avoid triggering automated detection technologies.

The image below details the top artifacts (tools) used by attackers in each stage of the MITRE ATT&CK chain, as seen by Sophos' frontline threat hunters in 2021. As you can see, tools used regularly by IT teams such as PowerShell, PsExec and RDP are frequently abused by adversaries. Automated technologies struggle to differentiate between legitimate IT staff using these tools and attackers exploiting them using stolen credentials.

Stopping these advanced 'living-off-the-land' attacks requires a combination of technology and human expertise. Every time an attacker takes an action, it creates a signal. By combining human expertise with powerful protection technologies and advanced AI-powered machine learning models, security analysts can detect, investigate, and neutralize even the most advanced human-led attacks to prevent data breaches.

While threat hunting, investigation, and response can be performed solely in house using EDR and XDR tools, there are extensive benefits to using an MDR service either alongside your in-house team or as a fully outsourced service.

Stages of MITRE Attack

Artifacts

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Services	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Network Browsing	Cobalt Strike	Rclone	Data Encrypted
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

Top artifacts used in each stage of Mitre attack chain. Active Adversary Playbook 2022, Sophos

Protection Technologies Continue to Play a Vital Role in Today's Defenses

While human-led managed detection and response is an essential layer of cyber defense, high-quality protection technologies remain critical. Endpoint, network, email, and cloud security technologies continue to play a vital role in today's defenses — and the right solutions can increase the effectiveness and impact of an MDR service:

- Automated protection technologies enable defenders to stay ahead of the ever-increasing volume of attacks, as adversaries take advantage of automation, AI, and malware-as-a-service offerings to proliferate their threats. Sophos Endpoint Protection blocks 99.98% of threats automatically before they can impact an organization.
- One of the biggest practical challenges facing threat hunters is noise: with a high volume of signals, it can be hard to see the wood from the trees. Superior prevention technologies reduce the number of alerts that human analysts need to investigate. By enabling threat hunters to focus on fewer, more accurate detections, high-quality prevention technologies accelerate human-led threat response.
- Human analysts use detections and signals from prevention technologies to identify and investigate suspicious activities. The higher the quality of the detections and the greater the contextual insights, the faster and better the investigation and response.

With that in mind, let's now look at the top five benefits reported by organizations that use MDR services.

1. Elevate Your Cyber Defenses

One of the major advantages of using an MDR provider over in-house only security operations programs is elevated protection against ransomware and other advanced cyber threats.

With MDR you benefit from the breadth and depth of experience of the provider's analysts. An MDR vendor will experience a far greater volume and variety of attacks than any individual organization, giving them a level of expertise that is almost impossible to replicate in house.

MDR teams also investigate and respond to incidents every day, giving them much greater fluency in using threat hunting tools. This enables them to respond more quickly and accurately at all stages of the process — from identifying the signals that matter to investigating potential incidents and neutralizing malicious activities.

Working as part of a large team also enables analysts to share their knowledge and insights, further accelerating response. The Sophos MDR team collates runbooks for each threat or unique actor that we come across. Once an adversary is identified in the course of an investigation, rather than needing to carry out widespread research at the time of an attack, our team can reference the runbook and then leap straight into action.

The runbooks are continually updated, and analysts record salient information with every engagement, such as:

- TTPs (tactics, techniques, and procedures) common or specific to a particular attack or threat actor(s).
- Relevant IOCs (indicators of compromise).
- Known proof of concepts for exploits tied to open vulnerabilities.
- Useful threat hunting queries when dealing with a particular attack or threat actor.

A further advantage of an MDR service is that it can apply intel from one customer to others that match the same target profile, enabling them to proactively prevent similar attacks in that community. Examples of scenarios when the Sophos MDR team proactively investigates customers' estates include:

- A customer in a specific vertical has been targeted in a particular way.
- Sophos X-Ops provides intel on a significant attack targeting a certain industry or organization profile.
- A significant event has occurred within the security landscape, and we want to ascertain if any customers are affected.

Should our analysts detect any suspicious signals, they are able to swiftly investigate and remediate the situation, creating community immunity for the targeted group.

The greater breadth and depth of experience and ability to apply learnings across our customers' environments enables the Sophos MDR team to elevate organizations' defenses above and beyond what they could achieve on their own.

"Tangible returns from Sophos MDR include 90% reduction in time to detect high-risk threats that require investigation, 95% reduction in time to identifying the source of attack and type of threats, and improved accuracy of detections."

Chitale Dairy, India

"The pen testers were shocked they couldn't find a way in. That was the point we knew we could absolutely trust the Sophos service."

University of South Queensland, Australia

"With Sophos MDR, we have reduced our threat response time dramatically."

Tata BlueScope Steel, India

"We receive notification of any threats in real time."

Bardiani Valvole, Italy

2. Free-Up IT Capacity

Threat hunting is time consuming and unpredictable. For IT professionals juggling multiple tasks and priorities, it can be hard to keep up with the challenge: 79% of IT teams admit they are not completely on top of reviewing logs to identify suspicious signals or activities[5].

Given the potential impact of an attack on the organization, when something suspicious is detected, you need to drop everything so the threat can be investigated and acted on immediately. The urgent nature of the work can prevent teams from focusing on more strategic — and often more interesting — challenges.

Working with an MDR service enables you to free up IT capacity to support business-focused initiatives. Organizations using Sophos MDR consistently report considerable IT efficiency gains from using our service, which in turn enables them to better support their organization's goals.

79%
of small and mid-sized organizations admit they are not completely on top of reviewing logs to identify suspicious signals or activities.

"Since implementing Sophos, we've managed to free up significant operational hours that have allowed our teams to focus on initiatives that have increased our student satisfaction."
London South Bank University, UK

"Sophos MDR's ability to remediate or remove threats in a swift manner and bring them to our attention frees us up to focus on high-value tasks."
Tomago Aluminium, Australia

"Because Sophos MDR is there, we can prop up and mature other areas of the organization like vulnerability management, patching, and security awareness."
The Fresh Market, U.S.

"Sophos keeps on top of the latest activity and threats, so we can focus on delivering a secure, world-class service for customers and artists"
CD Baby, U.S.

[5] Independent survey of 5,600 IT professionals , January-February 2022. Commissioned by Sophos and conducted by Vanson Bourne.

3. Get 24/7 Peace of Mind

With malicious actors located around the globe, an attack can come at any time. Adversaries are most active at the times when your IT team is least likely to be online, such as evenings, weekends, and holiday periods. Consequently, threat detection and response is a round-the-clock task; if you only do it during office hours, you leave your organization exposed.

By providing 24/7 coverage, MDR services provide considerable reassurance and peace of mind. For IT teams this means — literally — being able to sleep better at night. They can relax knowing that the buck stops with the MDR provider — not them — and regain their personal time.

For senior leaders and customers, 24/7 expert coverage and a high level of cyber readiness at all times provides powerful reassurance that their data and the organization itself are well protected.

"Having the Sophos MDR team behind me helps me sleep at night because I know that we are being protected 24/7."
Vancouver Canucks, Canada

"The Sophos team acts as our goalkeepers, sitting behind us with their skillsets and giving us reassurance that they have our back."
Inspire Education Group, UK

"We now have improved confidence in the reliability, robustness, and comprehensive nature of our security setup."
Aligned Automation, India

"The business has become much more resilient with Sophos MDR."
McKenzie Aged Care Group, Australia

4. Add Expertise, Not Headcount

Threat hunting is a highly complex operation. Individuals in this space need to possess a specific and niche set of skills, and the typical traits required of a threat hunter include:

- **Creative and Curious** – Looking for threats can be akin to looking for a needle in a haystack, and threat hunters can often spend days looking for threats, using numerous methods to unearth them.
- **Experience in Cybersecurity** – Threat hunting is one of the most advanced operations within cybersecurity, so prior experience in the field and foundational knowledge are a must.
- **Threat Landscape Knowledge** – Understanding the latest threat trends is essential when seeking out and neutralizing unknown entities.
- **Adversarial Mindset** – The ability to think like a hacker is critical in combating today's human-led approaches.
- **Technical Writing Ability** – Threat hunters are required to log their findings as part of the investigation process. Therefore, the ability to communicate such complex information is critical in seeing the hunt through to its conclusion.
- **Operating System (OS) and Networking Knowledge** – Advanced working knowledge of both is essential.
- **Coding/Scripting Experience** – This is required to help threat hunters build programs, automate tasks, parse logs, and carry out data analysis tasks to aid and progress their investigations.

This list represents a rare combination of competencies, exacerbated by a notable skills shortage in the IT sector, which makes recruiting threat hunting expertise an uphill — if not impossible — task for many organizations.

MDR services provide the expertise for you. At Sophos, we have hundreds of expert analysts that provide continuous MDR services to customers across the globe. Sophos MDR enables customers to expand their security operations capabilities without expanding their headcount.

"We now have an extension of our existing security practice without needing to build our own in-house capability."

Hammondcare, Australia

"Sophos MDR helped us keep up with the growing volume and sophistication of cyber threats without ramping up our security operations team."

Tourism Finance Corporation of India Limited, India

"Sophos saves us the expense of recruiting up to five new employees to take on this work."

AG Barr, UK

5. Improve Your Cybersecurity ROI

Maintaining a 24/7 threat hunting team is expensive. To provide round-the-clock coverage, you need a minimum of five or six cybersecurity staff members working separate shifts.By leveraging economies of scale, MDR services provide a cost-effective way to secure your organization and stretch your cybersecurity budget further.

Plus, by elevating your protection, MDR services also greatly reduce the risk of experiencing a costly data breach and avoid the financial pain of dealing with a major incident. With the average cost of remediating a ransomware attack in mid-sized organizations coming in at $1.4 million in 2021[6], investing in prevention is a wise financial decision.

If you use an MDR vendor that also offers endpoint – and other – cybersecurity offerings you can enjoy considerable TCO advantages from consolidating with a single provider as well as streamlining your vendor management efforts.

Finally, by choosing a vendor that integrates with your current security technologies you can increase return on existing investments. At Sophos, we have a vendor-agnostic approach to MDR that enables you to leverage your existing products for threat detection, investigation and response, enhancing your RoI. With Sophos MDR you can use our world-class tools, non-Sophos tools, or a combination of the two.

"Sophos provides the equivalent coverage and workload of six full-time staff for the cost of less than one."

Detmold Group, Australia

"Bringing all of our security products under one roof has allowed us to save money and drive efficiency as well."

Independent Parliamentary Standards Authority, UK

"Sophos MDR pays for itself in spades. If it stops one major incident a year, it's paid for itself ten times over, if not more."

Hammondcare, Australia

"We've saved 15 hours per week and seen 2.6X uptick in productivity."

Tourism Finance Corporation of India Limited, India

[6] The State of Ransomware 2022, Sophos. Independent survey of 5,600 IT professionals across 31 countries

What to Consider When Selecting an MDR Service

MDR services differ from provider to provider. There are many things to consider when evaluating services — be sure to explore the four areas below.

1. **Levels of Support and Interaction Offered**

   Do you want an MDR vendor to completely manage your threat response, co-manage threat response with your team, or alert your team so it can take action? Identify your preferred level of support and interaction and see how vendors stack up.

   At Sophos, we act as an extension of our customers' IT teams in whichever capacity they need us. From fully managed 24/7 support to quarterbacking an in-house team, we meet you where you are.

2. **Breadth and Depth of Threat Experience**

   Broader, deeper experience responding to cyber threats leads to better defenses. Understand the scale of experience that vendor MDR analysts can access and how they apply collective learnings across their customers' estates.

   Also, explore the depth of security expertise behind a vendor's MDR team and the quality of contextual insights provided to help analysts prioritize and investigate alerts.

   Sophos MDR secures over 11,000 organizations across the globe, working across sectors such as healthcare, education, manufacturing, retail, technology, finance, government, services, and many others. This breadth and depth of experience enables us to deliver unparalleled protection to our customers.

   Behind Sophos MDR is the Sophos X-Ops team. With over 30-years' malware expertise and world-leading AI capabilities, Sophos X-Ops provides deep insights and analysis to help MDR agents quickly identify and neutralize attacks.

3. **Day-to-Day Customer Experience**

   An effective MDR vendor becomes an extension of your own team — make sure it is a vendor you want to work with once the contract is signed. Speak to existing customers to understand their experiences and check out independent review sites for customer feedback.

   Sophos MDR is the most reviewed and highest rated MDR provider on Gartner Peer Insights as of August 1, 2022, with an average rating of 4.8/5*. Read independent customer testimony here.

4. **Breadth and Depth of Telemetry**

   Adversaries don't follow a single technology path — neither should your MDR vendor's threat hunting. The greater the analyst visibility across your environment, the better analysts can detect and respond to malicious activities. Ask vendors about their security integrations and how broadly they can integrate signals from across your IT environment.

   Sophos MDR provides extensive integrations across the full IT stack, including both native and third party integrations with endpoint, network, cloud, email, and Microsoft 365 technologies. Our vendor-agnostic approach enables analysts to have broad visibility across the entire customer environment, which in turn elevates threat detection, investigation and response.

Summary

As cyber threats continue to evolve, MDR is rapidly becoming a must-have protection for organizations of all sizes. Working with a trusted, proven MDR vendor offers multiple benefits — whether you want to fully outsource your threat hunting or complement and enhance your in-house services:

1. Elevate your cyber defenses.
2. Free-up IT capacity.
3. Get 24/7 peace of mind.
4. Add expertise, not headcount.
5. Improve your cybersecurity ROI.

For more information about Sophos MDR, speak with your Sophos partner or visit www.sophos.com/mdr

www.sophos.com/mdr

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

SOPHOS