SOPHOS

Managed Detection and Response Buyer's Guide

As cyberthreats evolve, many organizations are turning to Managed Detection and Response (MDR) services to provide the 24/7 expert threat monitoring and response needed to stop today's sophisticated adversaries.

However, with a growing number of players in the MDR market space, a range of deployment options, and many unsubstantiated marketing claims, selecting the right MDR services partner for your organization can be challenging.

This guide provides clarity by walking you through what a best-in-class MDR service looks like and the superior security and business outcomes every MDR service should deliver. Armed with these insights, you'll be better equipped to make the right decision for your organization.

A Sophos Whitepaper. March 2024

The Growing Need for Security Operations

Recent changes in the threat landscape have increased the challenge for defenders and accelerated the need for dedicated security operations support for organizations of all sizes.

The Evolution of the Cybercriminal Economy

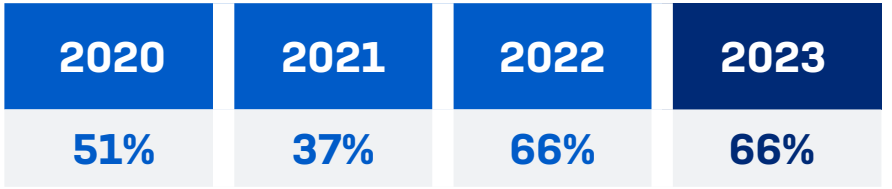
One of the most significant changes in the threat landscape in recent years has been the transformation of the cybercriminal economy into an industry with a network of supporting services and well-established, professional approaches to operations.

As technology companies have shifted to "as-a-service" offerings, the cybercrime ecosystem has done the same. This has lowered the barrier to entry for would-be cybercriminals and enabled threat actors to accelerate the volume, speed, and impact of their attacks. As a result, adversaries can now execute a wide range of sophisticated attacks at scale.

To learn more, read The State of Cybersecurity 2023: The Business Impact of Adversaries.

Ransomware Remains an Ongoing Threat

Two-thirds (66%) of organizations said they fell victim to a ransomware attack in the last year.



In the last year, has your organization been hit by ransomware?
Yes. n=3000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020)

While the rate of attack reported in 2023 remained level with the 2022 figure, data encryption from ransomware is at its highest level in four years, with adversaries succeeding in encrypting data in over three-quarters of attacks (76%).

Read our annual ransomware study, The State of Ransomware, to learn more, including the frequency, cost, and root cause of attacks.

Remote Ransomware is a fast-growing threat that can have a huge impact on victims. Used in around 60% of human-led ransomware attacks[1], Remote Ransomware is when a compromised device is used to maliciously encrypt data on other devices on the same network.

With remote ransomware, a single unmanaged or under-protected device can expose an organization's entire network to malicious remote encryption, even if all the other devices are running a next-gen antivirus or endpoint security solution.

Adversaries Don't Break In – They Log In

23%
of organizations experienced an attack involving an Active Adversary in the last year

30%
say Active Adversaries are one of their top cyberthreat concerns for 2023

Every organization has some investment in cyber-risk mitigation technology, but no matter the strength of that defense, a determined attacker will eventually defeat technology alone.

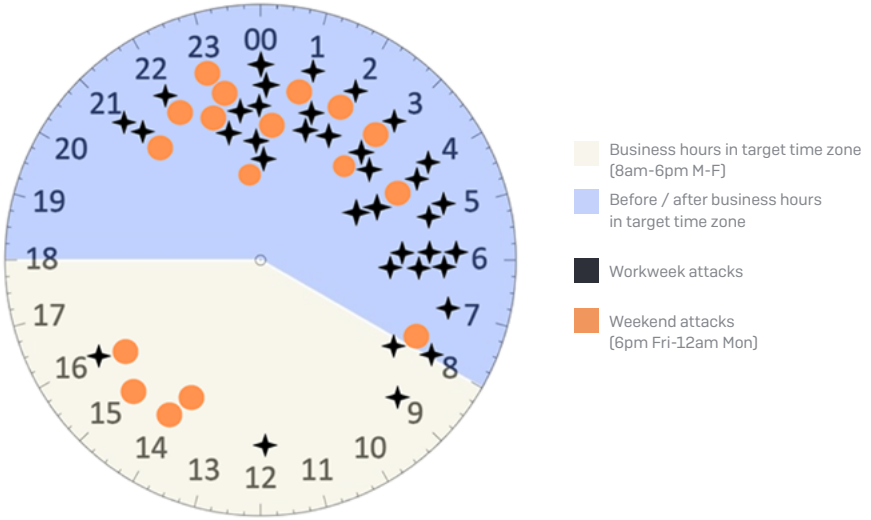
Active Adversaries are highly skilled cyber criminals, often equipped with sophisticated software and networking skills, who gain entry to an organization's systems, evade detection, and continuously adapt their techniques using hands-on-keyboard and AI-assisted methods to circumvent preventative security controls and execute their attack.

These attacks, which often result in devastating ransomware and data breach incidents, are among the hardest to stop. They have also become highly prevalent, with 23% of small and mid-sized organizations reporting that they experienced an attack involving an Active Adversary in the last year[2].

These skilled and persistent attackers deploy multiple approaches to achieve their goals, including:

- **Exploiting security weaknesses** to penetrate organizations and move laterally once inside the network, including stolen credentials, unpatched vulnerabilities, and security tool misconfigurations.
- **Abusing legitimate IT tools** to avoid triggering detections, including PowerShell, PsExec, and RDP.
- **Modifying their attacks in real-time in response to security controls** by pivoting to new techniques (such as Remote Ransomware) until they can achieve their goals.
- **Emulating authorized users and taking advantage of weaknesses in an organization's defenses** to avoid triggering automated detection technologies that struggle to differentiate between legitimate users and attackers.
- **Executing multi-stage attacks**, from initial access, to lateral movement, to privilege escalation, etc. Due to the nature of multi-stage attacks, it is important to have visibility and insight across key attack surfaces to identify an attack faster as individual technologies (endpoint, firewall, identity, etc.) may only contain one piece of the puzzle.
- **Actively targeting organizations when there's a higher chance they won't be detected** – 91% of ransomware attacks remediated by Sophos Incident Responders start outside of regular working hours in the victim's time zone (i.e., outside 8 am to 6 pm Monday to Friday)[3].

The time of day ransomware attacks start[4]



Challenges in Security Operations Delivery

Compounding the threat landscape challenges are recent changes in the business environment. Users may be in the office, working remotely, or constantly on the move. At the same time, company data can be on-premises, in the cloud, and on the devices of geographically dispersed employees.

These complexities mean it is no surprise that over half of organizations (52%) say cyberthreats are now too advanced for their organization to deal with on their own[5].

Key challenges faced by IT teams in delivering effective security operations include:

Shortage of specialist skills – 93% of IT teams find security operations challenging[6], and skilled employees continue to be hard to recruit. A lack of experience means team members often struggle to determine if a security alert is malicious or benign, which creates a domino effect: investigating alerts takes longer, which, in turn, reduces the team's capacity and increases risk exposure.

Lack of 24/7 coverage - Organizations struggle to actively monitor and respond to alerts and suspicious activity outside standard business hours (nights, weekends, and holidays). Analysts need to actively identify, investigate, and respond to suspicious activity immediately as it happens.

Noise overload – 71% of organizations struggle to identify which alerts to investigate. Too many alerts from different systems overwhelm operators who often don't know how to prioritize which signals/alerts to investigate, potentially missing indicators of an attack.

Siloed data – Threat signals are limited to specific technologies, preventing IT teams from seeing the big picture, identifying multi-stage attacks, and promptly remediating malicious alerts or incidents.

Lack of integration – Security tools don't integrate with each other or the business's IT infrastructure, increasing complexity.

Manual processes – IT teams spend many hours correlating events, logs, and information to understand what is happening. This manual effort delays attack identification and response.

Reactive response – Many IT teams are on the back foot, responding to threats only after they've caused damage rather than stopping them earlier in the attack chain.

Focus on firefighting – Day-to-day efforts to stop threats prevent long-term enhancements. When IT teams are firefighting, they often don't have the opportunity to identify and address the root causes of incidents.

Organizations Are Turning to MDR Services

As a result of these threats and operational challenges, organizations are increasingly turning to MDR service providers to supplement and extend their in-house security operations capabilities.. Gartner® predicts that 60% of organizations will use MDR service providers by 2025, up from 30% in 2023[7].

MDR Fundamentals

MDR offerings are fully managed 24/7 services delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Ideally, the MDR Service will provide full incident response and act on your behalf, not just alert you to a threat.

By combining human expertise with powerful protection technologies and artificial intelligence, security analysts can detect, investigate, and respond to even the most advanced human-led attacks, stopping ransomware, preventing data breaches, and avoiding operational disruption.

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 an organization's security analysts to hunt for and investigate potential threats; with MDR, a specialist security provider's team of analysts hunt for, investigate, and neutralize threats on the organization's behalf.

At a bare minimum, an MDR service provider should provide:

- **24/7 threat monitoring** – a team of experts watching your environment to identify suspicious behaviors that may indicate a compromise or breach.
- **Human-led response** – immediate remote mitigative response, investigation, and containment activities beyond alerting and notification—with no limitations on volumes or time dedicated to the discovery, investigation, and response process.
- **Comprehensive visibility** – a provider-operated technology stack (either proprietary or curated from select partners) is used to provide visibility across endpoint, firewall, identity, email, network, cloud, backup and other security data sources.
- **Human-led threat hunting** – focused on finding "unknown unknowns" (i.e., threats not currently detectable by current prevention or detection technologies).
- **Threat intelligence** – threat-focused content and analytics, also known as detection engineering, is used to detect new, novel, and emerging threats.
- **Elevated threat detection** – specialist MDR service providers detect more cyberthreats than security tools can identify on their own.

MDR Benefits: Superior Security and Business Outcomes

Now that we've outlined what an MDR service should do at a functional level, when selecting an MDR provider it's essential to take a broader view of how MDR can benefit your organization. MDR services should work to deliver optimal security and business outcomes.

Elevated Cyber Defenses and Reduced Cyber Risk

One significant advantage of using an MDR provider over in-house security operations programs is elevated protection (and reduced risk) from ransomware and other advanced cyberthreats.

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

MDR teams also investigate and respond to incidents daily, giving them 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 most 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. Experienced MDR teams collate runbooks or playbooks (documented processes and protocols) for each threat or unique adversary they encounter. Once an adversary is identified during an investigation, rather than needing to carry out widespread research at the time of an attack, analysts reference the runbook and then leap straight into action.

A further advantage of an MDR service is that it can apply intelligence across customers that share the same target profile, enabling them to prevent similar attacks in that cohort proactively. Should analysts detect any suspicious signals, they can swiftly investigate and remediate the situation, creating community immunity for the targeted group.

Increased IT Efficiency

64% of businesses want their IT teams to spend less time firefighting cyberattacks and more time on strategic issues[8]. MDR services should enable this goal.

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

Given the potential impact of an attack on the organization, when suspicious activity is detected, you must drop everything so the threat can be investigated and acted upon 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.

Additional Expertise, Not Headcount

Another advantage of using an MDR service is that it eliminates the challenge of recruiting specialized threat hunters and security analysts. Threat hunting is a highly complex operation. Individuals in this field must possess a specific and niche set of skills, which makes recruiting an uphill — if not impossible — task for many organizations.

Improved Cybersecurity Return on Investment (ROI)

Best-in-class MDR providers help you get more from your existing security investments by integrating with your current cybersecurity technology stack. This vendor-agnostic approach enables analysts to leverage telemetry from your existing technologies to increase visibility across multiple security control points and accelerate threat detection, investigation, and response. The more analysts can see, the faster they can act.

If, however, you're at an earlier stage in your cybersecurity journey, look for an MDR provider that also offers a broad portfolio of security solutions that are deeply integrated with their detection and response toolset, as you can achieve significant operational and financial benefits by consolidating with a single platform vendor. Rather than paying one provider for endpoint protection and another for an MDR service, working with the same vendor can reduce your licensing costs and day-to-day management overheads while offering an integrated experience.

Also, by elevating your protection, MDR services also significantly reduce the risk of a costly data breach or ransomware event and avoid the financial pain of dealing with a significant incident. In 2023, the average cost to remediate a ransomware attack was a staggering $1.82M[9]. Therefore, investing in a service such as MDR makes good financial sense.

Optimized Cyber Insurance Position

Cyber insurance premiums have risen significantly in recent years, and policy applications have become more complex and time-consuming. Insurers are demanding stronger cyber controls – in fact, 95% of organizations that purchased insurance in the last year said the quality of their defenses directly affected their insurance position[10].

The key to optimizing your insurance position is to minimize your cyber risk. Investing in strong defenses, including 24/7 security services and industry-leading detection and response tools, delivers multiple insurance benefits:

1. It makes it easier to obtain cyber insurance coverage (i.e., improves insurability).
2. It helps reduce premiums and enhances terms.
3. It reduces the likelihood of a claim – and the resulting higher premiums.
4. It reduces the risk of non-payment in the event of a claim.

Services that deliver optimized detection and response capabilities and, therefore, minimize the risk of a cyber incident occurring are considered the 'gold standard' by cyber insurers. Organizations that use MDR services are often considered "Tier 1" customers by insurers, as they represent the lowest level of risk.

Key Considerations

Now that you have a clearer idea of what a best-in-class MDR service looks like, here are some factors to consider before evaluating potential vendors.

1. **Identify what you want to achieve.**
   What is the definition of success for your organization? This will be influenced by your current challenges and motivations for using an MDR service.
2. **Identify how you want to work with the MDR service.**
   Consider your current IT/cybersecurity organization, the role (if any) you want your current team to play, and what you want the MDR service to do. Are you looking for additional coverage for nights, weekends, and holidays? Do you want the MDR service to notify you of issues so you can act, or do you want the MDR service to execute response actions on your behalf?
3. **Identify your current security investments.**
   Understand the IT and security technologies you already use, such as endpoint protection, network firewalls, email gateways, identity solutions, etc. Ideally, the MDR service can consume telemetry from those products to give them more visibility into your environment with the view to detect, investigate and respond faster.

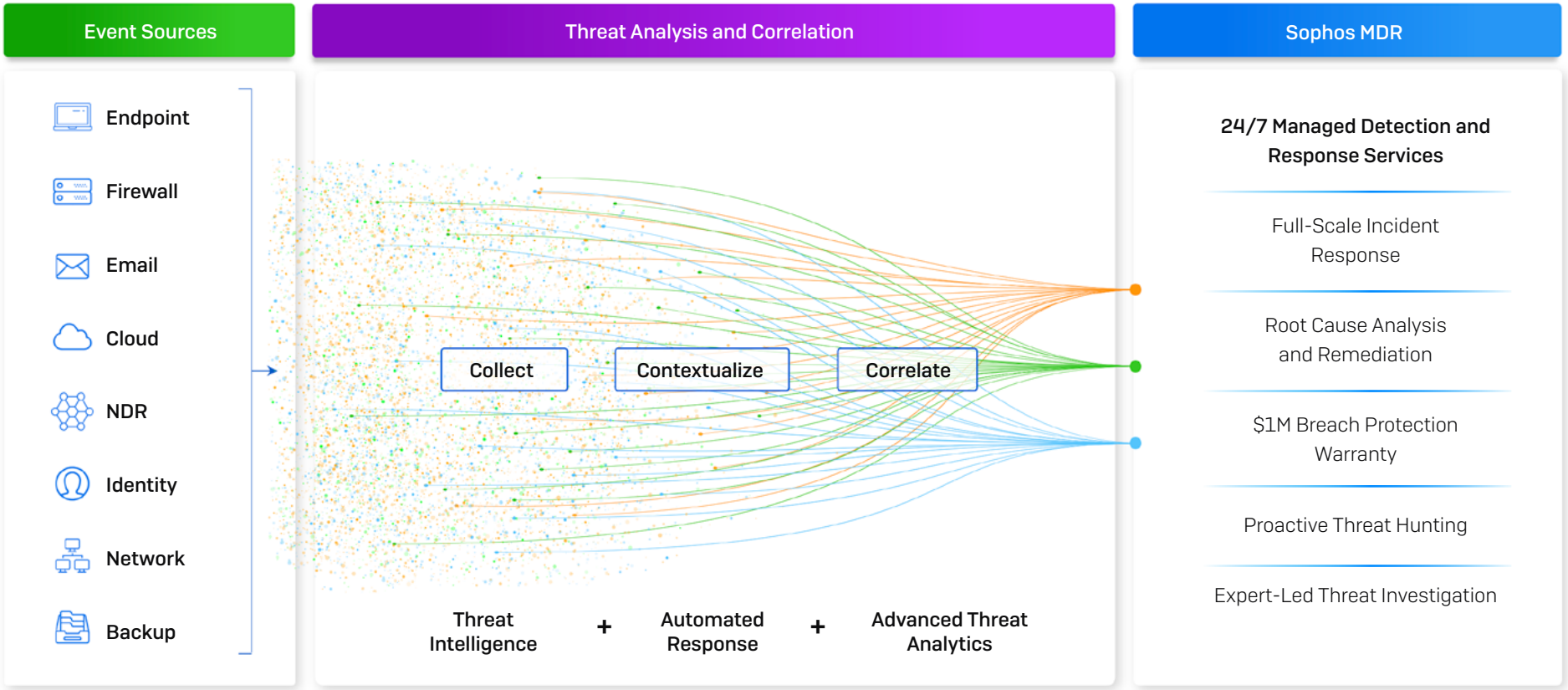
Evaluating MDR Services: Top 10 Questions to Ask

Once you've established your requirements, here are suggested questions to ask of a potential vendor.

1. What native security solutions do you provide that your MDR analysts leverage (e.g. Endpoint Protection, Email Security, etc.)?
2. Can the service integrate with my existing cybersecurity solutions from other vendors?
3. What value do these integrations provide for your MDR analysts?
4. How long does it typically take your team to respond to threats?
5. What response actions can your team execute on my behalf and what actions must be performed by my team?
6. If my organization experiences sudden growth, can the MDR service scale with it?
7. Which levels of support and interaction do you offer? Do you offer customized levels of service?
8. What do your existing customers say about your service?
9. Does your service include full-scale Incident Response to disrupt, contain, and fully eliminate active threats, and is this capability included in the core service or is it considered extra?
10. Do you provide a breach protection warranty?

Sophos Managed Detection and Response (MDR)

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. With Sophos MDR, our expert team stops advanced human-led attacks and takes immediate action to neutralize threats before they can disrupt your business operations or compromise your sensitive data.



MDR That Meets You Where You Are

Sophos MDR is the world's most widely used Managed Detection and Response service. It protects organizations across all sectors, from small companies with limited IT resources to large enterprises with in-house security operations teams. The three most popular Sophos MDR response models are:

- Sophos MDR manages threat response on your behalf.
- Sophos MDR works with your in-house security team, co-managing threat detection and response activity.
- Sophos MDR supports and supplements your in-house team, alerting them to incidents that require attention and providing threat insights and remediation guidance.

Our flexible approach enables Sophos to meet your organization's specific needs. From a fully managed 24/7 service to supplementing your in-house team, we meet you where you are.

24/7 Coverage from Seven Global Security Operations Centers (SOCs)

Threats are investigated and remediated by a global team of threat detection and response experts based out of seven global security operations centers (SOCs) across North America (Indiana, Utah, Hawaii), Europe (UK/Ireland, Germany), and Asia Pacific (India, Australia).

With over 500 experienced analysts covering the entire threat environment, including malware, automation, AI, and remediation experts, Sophos MDR has a breadth and depth of expertise that is almost impossible to replicate in-house.

World-Leading Detection and Response Times

This unique combination of human, technology, and threat expertise enables Sophos MDR to deliver a world-leading incident response time of just 38 minutes that, in turn, drives superior cybersecurity outcomes:

- Mean Time to Detect (MTTD): 1 minute
- Mean Time to Investigate (MTTI): 25 minutes
- Mean Time to Respond (MTTR): 12 minutes

Sophos Breach Protection Warranty

More organizations trust Sophos for MDR than any other security vendor. With the Sophos Breach Protection Warranty, Sophos MDR Complete customers enjoy the reassurance and peace of mind of having financial coverage in the event of a breach.

The Sophos Breach Protection Warranty is included at no additional charge with our **Sophos MDR Complete** subscription. It covers:

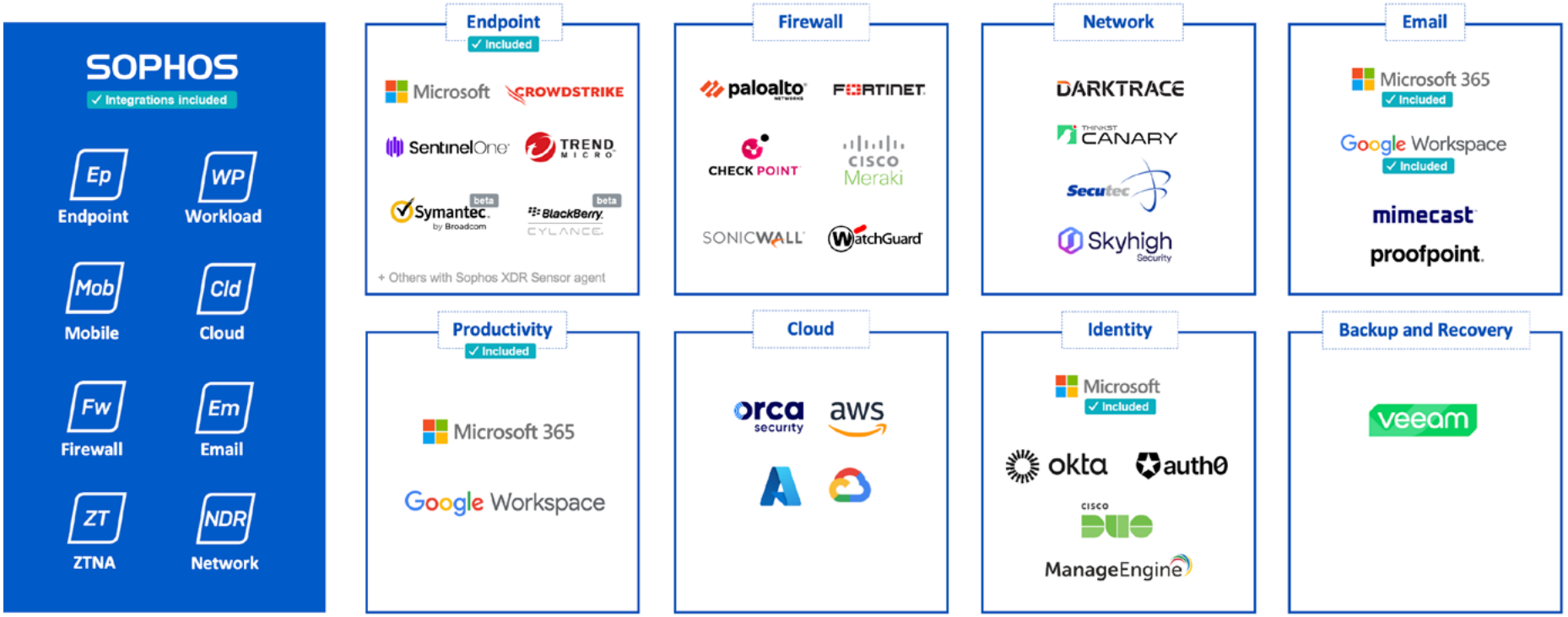
- Up to $1 million in total response expenses for qualifying customers.
- Up to $100,000 for ransom payment (as part of the per-device limit).
- Up to $1,000 per breached machine.
- Covers a range of incurred expenses, including data breach notification, PR, legal, and compliance.

For full terms and conditions of the warranty, visit www.sophos.com/legal

Industry-Leading Compatibility

Whether you want to use Sophos tools, your existing technologies, or a mixture of them, Sophos MDR boasts extensive integrations across the full IT stack, including native and third-party endpoint, network, cloud, email, and Microsoft 365 solutions.

Our vendor-agnostic approach enables analysts to gain broad visibility across your entire IT environment, elevating threat detection, investigation, and response. Furthermore, these integrations increase the return on your existing investments. Integrations include (but are not limited to):



Sophos Endpoint and Sophos Workload Protection solutions are included with Sophos XDR and MDR. Other Sophos product integrations require a subscription to the applicable solution.

Third-party Endpoint, Microsoft, and Google Workspace integrations are included with Sophos XDR and MDR subscriptions at no additional charge.

Integration Packs for other non-Sophos solutions are available as add-on subscriptions for each integration category. Licensing is based on the total number of users and servers.

Integrations as of February 8, 2024. To get an up-to-date list, please contact your Sophos representative or Sophos partner.

Sophos MDR: Delivering Superior Security and Business Outcomes

Earlier in this guide we discussed the outcomes any MDR service should deliver. Let's now highlight how Sophos MDR delivers superior security and business outcomes.

Elevated Cyber Defenses and Reduced Cyber Risk

Sophos analysts have breadth and depth of experience and fluency in using telemetry and threat-hunting tools that are almost impossible to replicate in-house. This enables them to respond quickly and accurately at all stages of the process — from identifying the signals that matter to investigating potential incidents and neutralizing malicious activities.

Sophos MDR secures more organizations than any other provider, enabling us to provide unrivaled 'community immunity'. Intelligence from defending one customer is automatically applied to others with a similar profile, enabling Sophos to proactively prevent similar attacks in that cohort.

"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

Increase The Efficiency and Impact of Your Security Investments

Sophos MDR enables you to increase the efficiency and impact of your people and your security tools. Threat detection and response consume vast amounts of IT capacity. Sophos MDR takes on this burden, freeing up valuable IT resources for strategic program delivery.

In parallel, 24/7 phone access to Sophos security operations experts and detailed reporting on threat activity via the Sophos Central platform accelerates in-house teams by enabling them to respond more quickly and accurately to alerts.

Sophos MDR elevates your defenses by using telemetry from your existing security tools to increase visibility and accelerate threat detection and response. This enables you to increase the return on your existing investments.

"Instead of spending the time doing investigations and doing manual threat intelligence searches etc., I have a great team of subject matter experts with the MDR team at Sophos essentially maintaining these alerts for me."

United Musculoskeletal Partners, U.S

"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

Additional Expertise, Not Headcount

At Sophos, over 500 expert analysts provide continuous MDR services to over 20,000 customers across the globe. Sophos MDR enables organizations to expand their security operations capabilities without expanding headcount.

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

Hammondcare, Australia

"With a seasoned MDR team, like Sophos', you're essentially getting folks that are masters at their craft."

United Musculoskeletal Partners, U.S.

"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

Optimized Cyber Insurance Position

Sophos MDR enables organizations to achieve many of the cyber controls key to insurability and superior policy offers, including 24/7 detection and response, cyber incident response planning, logging and monitoring, and more.

Sophos MDR customers report improved access to insurance coverage and policies recognizing and rewarding their reduced cyber risk. Furthermore, several leading insurance providers recognize our service's reduced cyber risk and offer exclusive premium discounts and automatic qualification for Sophos MDR customers. For more information, contact your Sophos partner.

Our decision to partner with Sophos for XDR and MDR was a big factor in achieving a decrease in cybersecurity premiums versus what we were told walking into this would be a doubling of those premiums. That's a big win that shows real value... I actually got a note from the CFO thanking our team for what we put together and MDR was a huge part of that."

Bob Pellerin, CISO, The Fresh Market, U.S.

The World's Most Trusted MDR Service

Sophos is the number one MDR provider globally, securing more organizations than any other vendor against ransomware, breaches, and other threats that technology alone cannot stop. Sophos MDR protects organizations across all industries worldwide, giving us unparalleled depth and breadth of expertise into threats facing individual sectors.

Gartner® Peer Insights™

Sophos is the highest-rated and most reviewed MDR solution on Gartner® Peer Insights™ with a 4.8/5 rating across 435 reviews (more than any other vendor) as of January 23, 2024, and 97% of customers saying they would recommend us. Furthermore, Sophos was the only vendor named 2023 Gartner Customers' Choice across all these categories:

- Managed Detection and Response
- Endpoint Protection Platforms
- Network Firewalls
- Mobile Threat Defense

Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Sophos was named a Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP), marking our 14th consecutive recognition as a Leader in this category.

The report provides readers with a comprehensive evaluation of the industry's most prevalent endpoint prevention solutions and evaluates XDR and MDR offerings. The strength of both our XDR platform and MDR service helped contribute to our continued position as a leader in this evaluation.

2024 IDC MarketScape For Worldwide Modern Endpoint Security for Small and Midsize Businesses

These IDC MarketScape assessments evaluate vendors based on how their endpoint prevention, EDR, and MDR capabilities meet the needs of both small and midsize businesses. The strength of our MDR service helped contribute to our position as a Leader in both of these assessments.

G2 Grid® Reports

Sophos is named a Leader in the G2 Grid® Reports for Managed Detection and Response and a Leader for MDR in the G2 Overall, Mid-market, and Enterprise grids. In G2's Winter 2024 reports, Sophos was named a Leader in multiple categories, including XDR, EDR, Network Firewall, and Endpoint Protection.

2023 MITRE Engenuity ATT&CK Evaluations

Sophos excelled in the 2023 MITRE Engenuity ATT&CK® Evaluations, which focused explicitly on threat detection and response. Our XDR solution, Sophos XDR, detected 99% of the adversary behaviors in the evaluation and recorded rich analytic data on 98% of the substeps in the valuations.

The result is significant as Sophos XDR underpins our MDR service. Sophos MDR analysts use our XDR capabilities to aid and accelerate threat detection and response.

2022 MITRE Engenuity ATT&CK Evaluation for Security Service Providers

Sophos MDR excelled in every component of the 2022 ATT&CK® Evaluation for Security Services Providers – the first-ever ATT&CK Evaluation for Managed Services. Sophos recorded exceptional performance across analytic detections, sub-step coverage, alert consolidation, and human analysis during the evaluation.

Summary

As adversaries evolve and adapt, MDR is rapidly becoming a must-have protection for organizations of all sizes. Working with a trusted, proven MDR vendor like Sophos 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. Increase your IT efficiency.
3. Add expertise, not headcount.
4. Improve your cybersecurity ROI.
5. Optimize your cyber insurance position.

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

1 Microsoft Digital Defense Report 2023
2 The State of Cybersecurity 2023: The Business Impact of Adversaries – Sophos
3 Stopping Active Adversaries: Lessons From The Cyber Frontline – Sophos [references ransomware attacks because they had the most reliable and objective indicators in the analysis]
4 Stopping Active Adversaries: Lessons From The Cyber Frontline – Sophos
5 The State of Cybersecurity 2023: The Business Impact of Adversaries – Sophos
6 The State of Cybersecurity 2023: The Business Impact of Adversaries – Sophos
7 2023 Gartner® Market Guide for Managed Detection and Response Services
8 The State of Cybersecurity 2023: The Business Impact of Adversaries – Sophos
9 The State of Ransomware 2023 - Sophos
10 Sophos Guide to Cyber Insurance – Sophos

To learn more about Sophos MDR and how it enables organizations to reduce cyber risk, increase the efficiency and impact of security investments, and improve insurability, visit www.sophos.com/mdr

2023-02-27 (WP-NP)

SOPHOS