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. May 2025

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.

Proactive cybersecurity is no longer optional

While ransomware remains the top threat, data-focused attacks are growing, and new tactics continue to emerge. Software-as-a-service (SaaS) platforms — widely adopted during the COVID-19 pandemic to support remote work and strengthen security — are now being exploited for social engineering, initial access, and malware delivery. Business email compromise (BEC) is also on the rise, increasingly used for malware deployment, credential theft, and a range of social engineering attacks.

Keeping pace requires more than reactive measures — it's a strategic necessity. Failing to act doesn't just risk technical disruption, it opens the door to substantial financial loss, reputational harm, and long-term operational setbacks.

To learn more, read The Sophos Annual Threat Report: Cybercrime on Main Street 2025

Ransomware: More impactful than ever

Ransomware remains a widespread threat — but even more alarming is the escalating financial impact. Our annual State of Ransomware survey revealed that the average cost of recovering from a ransomware attack has surged to $2.73 million — a 50% increase over the previous year. This sharp rise underscores the growing severity of ransomware incidents and the urgent need for fast, effective incident response.

2021	2022	2023	2024
$1.85M	$1.4M	$1.82M	$2.73M

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=2,974 (2024)/ 1,974 (2023)/ 3,702 (2022)/ 2,006 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

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

The rise of remote ransomware

Remote ransomware is a fast-growing threat that can have a huge impact on victims. Used in around 70% 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 an endpoint security solution.

Adversaries don't break in – they log in

Every organization has some investment in cyber-risk mitigation technology, but no matter the strength of that defense, a determined and highly skilled attacker may eventually succeed in evading such tools.

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.

How adversaries gain entry

Although initial access methods can vary widely, active adversaries typically rely on two primary techniques to gain entry:

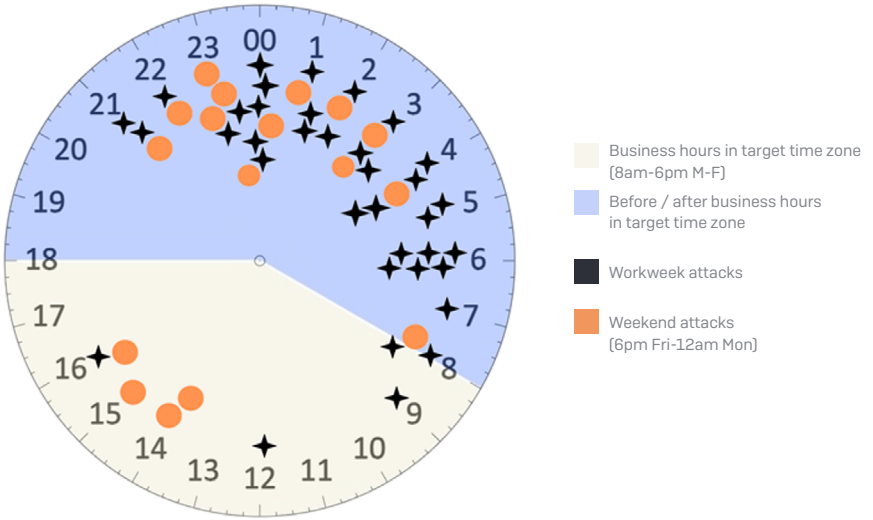
41%	22%
Compromised credentials	**Exploited vulnerabilities**

The 2025 Sophos Active Adversary Report

These attacks, which often result in devastating ransomware and data breach incidents, are among the hardest to stop with attackers deploying 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 (to name but a few).
- **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** that involve actions that start in one area and end in another — such as initial access, lateral movement, and privilege escalation. Since each stage may only be visible in isolated systems like endpoints, firewalls, or identity platforms, broad visibility across key attack surfaces is critical to detect and understand the full threat.
- **Actively targeting organizations when there's a higher chance they won't be detected** – 88% of ransomware attacks remediated by Sophos Incident Responders start outside of regular working hours in the victim's time zone (i.e., outside 8 a.m. to 6 p.m. Monday to Friday)[2].

The time of day ransomware attacks start[3]



Challenges in security operations delivery

Changes in the business environment are compounding the challenges of an already complex threat landscape. With users working from offices, remotely, or while on the move — and company data distributed across on-premises systems, the cloud, and employee devices — IT teams face mounting difficulties in delivering effective security operations. Key challenges include:

Shortage of specialist skills – 96% of IT teams in small and mid-sized organizations find security operations challenging[4], and skilled employees continue to be difficult and expensive to hire, train, and retain. 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 - One-third (33%) of the time, small and mid-sized organizations have no one actively monitoring, investigating, or responding to alerts[5]. This gap is especially critical outside standard business hours — nights, weekends, and holidays — when organizations often struggle to maintain coverage. Yet immediate detection and response by analysts is essential to staying ahead of suspicious activity.[6]

Noise overload – 74% of small and mid-sized organizations struggle to identify which alerts to investigate.[7] 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 we could add that this gives adversaries the advantage - they can take advantage of these delays to progress their attacks unchallenged.

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.

As a result of these threats and operational challenges, organizations are increasingly turning to MDR service providers to supplement and extend or outsource their in-house security operations capabilities.

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). EDR and XDR are tools that enable an organization's in-house security operations team — if they have one - to investigate, hunt for, and respond to threats. With MDR, organizations leverage a security provider's specialist team of analysts, threat hunters, researchers, and incident responders, to identify and neutralize threats on their behalf.

At a bare minimum, an MDR service 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 threat containment and full-scale incident response to neutralize threats and establish root cause - with no caps on hours spent, or additional fees.
- **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 and other IT tools.
- **Expert-led threat hunting** – focused on finding "unknown unknowns" (i.e., threats not currently detectable by current prevention or detection technologies).
- **Threat Intelligence –** this involves using threat-focused analytics to identify emerging threats. The MDR provider should continuously update and apply detection rules based on current threat intelligence to stay ahead of evolving threats.
- **Elevated threat detection** – specialist MDR service providers detect and stop 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 cyber threats.

With MDR, you benefit from the provider's threat analysts' breadth and depth of experience. An MDR vendor with a large customer base 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, enabling 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.

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 both time-consuming and unpredictable. For IT professionals managing multiple tasks and priorities, keeping up with reviewing logs to detect suspicious signals or activities can be a significant challenge.

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 hiring, training, and retaining specialized threat hunters and security analysts. 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 2024, the average cost to remediate a ransomware attack was a staggering $2.73M[9]. Therefore, investing in a service such as MDR makes good financial sense.

Optimized cyber insurance position

Cyber insurance premiums have surged in recent years, and the application process has become increasingly complex and time-consuming. Insurers are now placing greater emphasis on robust cybersecurity controls — using insurance requirements as a "stick" to encourage stronger defenses. In fact, 97% of organizations that purchased a cyber insurance policy in the past year reported making investments to strengthen their security posture to optimize their insurance position[10].

By prioritizing strong cyber defenses — such as 24/7 security monitoring and best-in-class detection and response tools — organizations can unlock a range of insurance-related 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 claims — and the resulting higher premiums.
4. It reduces the risk of non-payment in the event of a claim.

Cyber insurers view services that deliver optimized detection and response capabilities as the gold standard for minimizing cyber risk. Organizations leveraging MDR services are therefore often considered "Tier 1" customers by insurers, as they represent the lowest level of risk.

This distinction isn't just theoretical: data shows that organizations using MDR services file claims that are, on average, 97.5% lower than those relying solely on endpoint protection ($75K vs. $3M)[11]. This significant reduction in potential loss makes MDR-enabled organizations especially attractive to insurers.

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, backup and recovery, and productivity solutions such as Microsoft 365 and Google Workspace. 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.

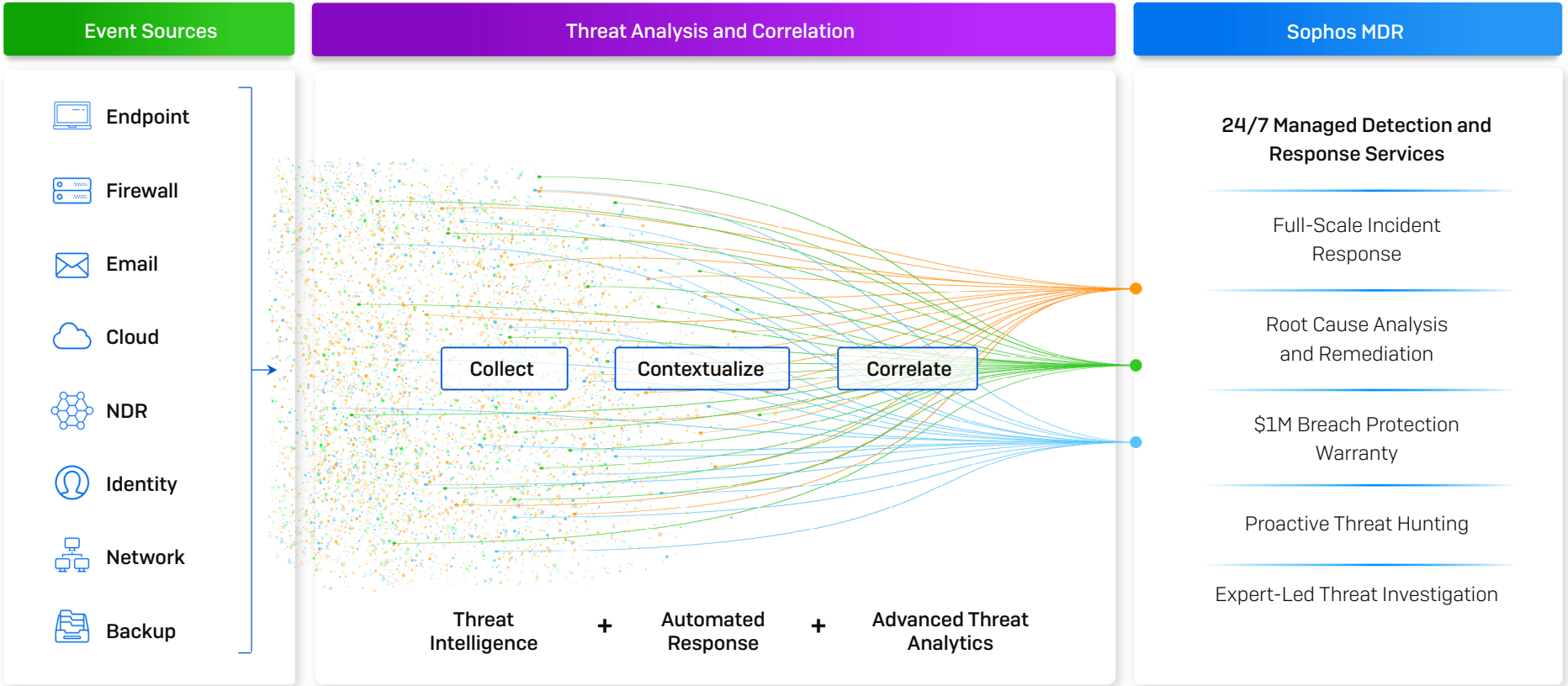
Evaluating MDR services: Top 10 questions to ask

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. As of May 2025, we secure more than 30,000 diverse organizations worldwide. This unmatched breadth of customer coverage provides our analysts with unparalleled insights into threats and adversary behaviors, allowing us to stop more attacks, faster. We protect organizations across all sectors — from small businesses 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 experts in threat intelligence, analysis, data engineering, data science, threat hunting, adversary tracking, and incident response 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 — 96% faster than the industry average for internal SOC teams — 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, 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 integrations require an applicable subscription for the Sophos product.

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 May 2025.. To get an up-to-date list, please contact your Sophos representative or Sophos partner.

The most robust MDR service for Microsoft environments

Sophos MDR for Microsoft Defender augments your team with Microsoft Certified experts who monitor, investigate, and respond to Microsoft Security alerts 24/7 and execute immediate, human-led response actions to confirmed threats.

Stop threats Microsoft security tools miss

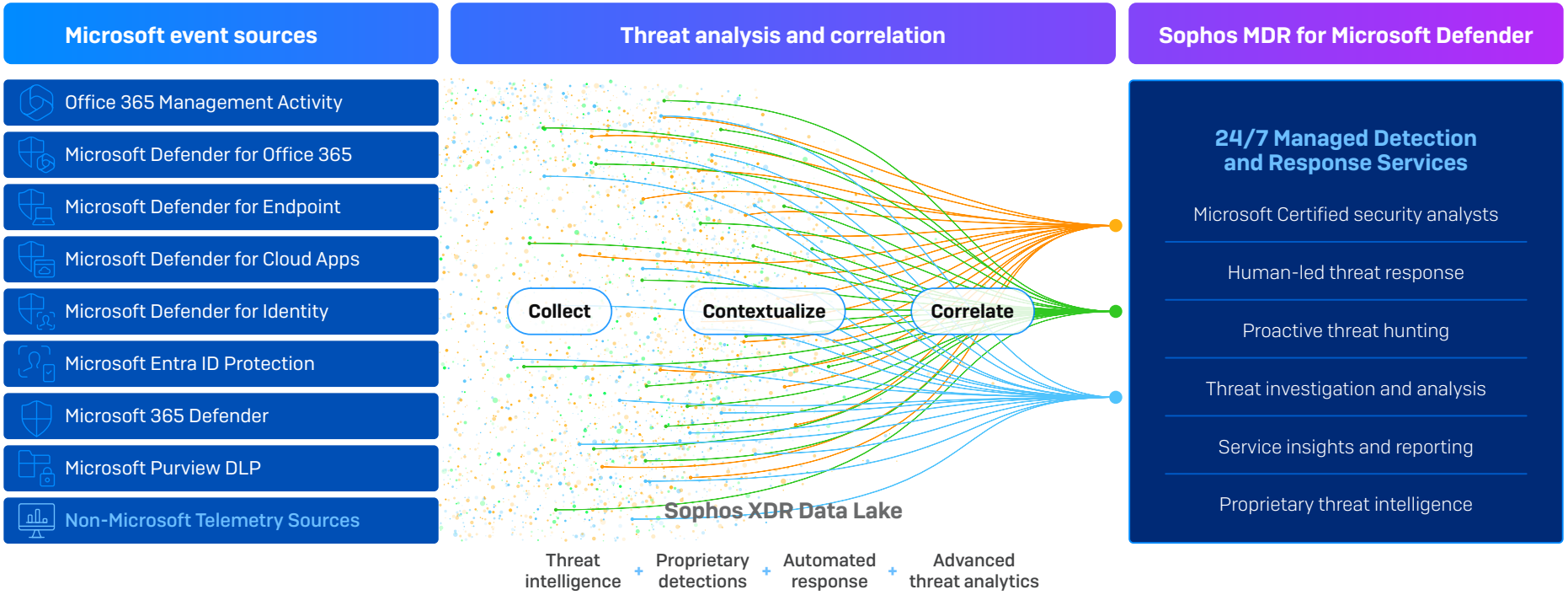
Sophos MDR uses proprietary threat detection rules and world-class threat intelligence to identify sophisticated adversary activities that may bypass Microsoft security tools. Sophos can protect your organization from attacks including business email compromise (BEC) with any Microsoft 365 Business plan.

Effective response to threats targeting Microsoft 365

Sophos MDR analysts can execute a range of response actions in Microsoft 365 on your behalf — such as blocking user sign-ins, terminating active sessions, and disabling suspicious inbox rules — to rapidly contain threats with no action required by you.

Support for a comprehensive range of Microsoft tools

Included with at no additional cost, Sophos MDR's turnkey integrations support the most popular Microsoft solutions. Data from Microsoft 365, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and more, is collected, analyzed, correlated, and prioritized.



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 experts provide continuous MDR services to over 30,000 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™ Customers' Choice for Managed Detection and Response Services

Sophos was named a Customers' Choice vendor in the 2024 Gartner Voice of the Customer report for Managed Detection and Response for the second year running.

Based on verified customer reviews, Sophos is **the highest-rated** (4.9/5.0) and **most-reviewed** (344 reviews) vendor in the report. And, with this recognition, Sophos is the **only vendor** named a 2024 Customers' Choice vendor across Endpoint Protection Platforms, Network Firewalls, and Managed Detection and Response categories.

Gartner® Magic Quadrant™ for Endpoint Protection Platforms

Sophos was named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP), marking our 15th 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 Managed Detection and Response (MDR)

Sophos was named a Leader in the IDC MarketScape: Worldwide Managed Detection and Response (MDR) 2024 Vendor Assessment. The IDC MarketScape study evaluates the capabilities and business strategies of MDR service vendors, and positions Sophos in the Leaders Category.

Sophos was also named a Leader in the European version of this MDR evaluation.

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 Spring 2025 reports, Sophos was named a Leader in multiple categories, including XDR, EDR, Firewall Software and Endpoint Protection Suites.

2024 MITRE ATT&CK Evaluations

Sophos achieved exceptional results in the 2024 MITRE ATT&CK Evaluations for Enterprise. In this evaluation, Sophos XDR achieved:

- The highest possible ('Technique') ratings for 100% of adversary activities in the Windows and Linux ransomware attack scenarios.
- The highest possible ('Technique') ratings for 78 out of 80 total adversary activities across all three comprehensive scenarios.
- Analytic coverage' ratings for 79 out of 80 total adversary activities.

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.

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 2024
2 The 2025 Sophos Active Adversary Report
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 Addressing the cybersecurity skills shortage in SMBs - Sophos
5 Addressing the cybersecurity skills shortage in SMBs - Sophos
6 Addressing the cybersecurity skills shortage in SMBs - Sophos
7 Addressing the cybersecurity skills shortage in SMBs - Sophos
8 The State of Cybersecurity 2023: The Business Impact of Adversaries – Sophos
9 The State of Ransomware 2024
10 Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leader - Sophos
11 Quantifying ROI: Understanding the impact of cybersecurity products and services on cyber insurance claims - 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

2025-06-09 (WP-DD)

SOPHOS