ThreatDown™
Powered by Malwarebytes

Is MDR Right for Your Organization?

An assessment of MDR's value proposition for small to midsized organizations

Contents

Introduction **3**

MDR is an option—but is it right for you? **4**

Question ᵗ#1: Does your security team lack sufficient staff, skills, and budget to deliver 24x7 services? **5**

Question #2: Is your security team overwhelmed by seemingly endless alerts? **6**

Question #3: Is your dwell-and-response time above average? **7**

Question #4: Do you need to mitigate the risk of regulatory violations? **8**

Question #5: Does the ROI of MDR justify its expense for your organization? **9**

Conclusion **10**

The Ideal MDR Partner **11**

Glossary of Cybersecurity Terms **13**

Introduction

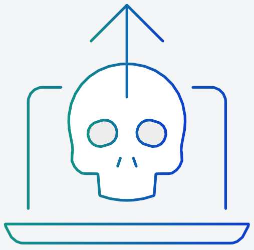
2023 broke records with its total number of 4,475 ransomware attacks, a 70% increase from 2022.[1] Numbers that large tend to feel somewhat abstract, but this statistic is easy to grasp and crystal clear: Nearly three-quarters (73%) of global organizations experienced a ransomware attack in 2023.[2]

You might be thinking, "Those are 'just' attacks. What about breaches?" Glad you asked. 95% of studied organizations have experienced more than one breach in 2023.[3]

The potential impact of cybercrime looks even more bleak when you consider the cost of a data breach. In 2023, the cost of a data breach reached an all-time high at an average of $4.45 million.[4] And that global average pales compared to the US average of $9.48 million, the highest of any country.[5]

This state of affairs has not gone unnoticed: Less than 40% of executives think they are fully mitigating different cybersecurity risks.[6] And yet every organization in every country in every vertical needs to reduce risk. The trouble is organizations simultaneously need to reduce complexity and cost.

95%



95% of studied organizations have experienced more than one breach in 2023.

[1] Ransomware in 2023 recap: 5 key takeaways, https://www.malwarebytes.com/blog/threat-intelligence/2024/02/ransomware-in-2023-recap-5-key-takeaways
[2] Statista, Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023.
[3] 2023 IBM Cost of a Data Breach Report
[4] 2023 IBM Cost of a Data Breach Report
[5] 2023 IBM Cost of a Data Breach Report
[6] PwC 2023 Global Digital Trust Insights Report

MDR is an option—but is it right for you?

So, how do you increase protection while reducing complexity and costs?

No doubt, your organization will explore several avenues to improve its cybersecurity posture. However, one avenue to consider is managed detection and response (MDR), which some industry analysts consider essential in today's world.

Managed detection and response (MDR) is a service that provides proactive, purpose-built threat hunting, monitoring, and response capabilities powered by a team of advanced cybersecurity technicians combined with the analysis of robust correlated data.

With MDR, organizations accelerate threat detection analysis, investigation, and response, which can include automated and managed threat containment and mitigation. Depending on the provider, an MDR service can be an affordable solution, tailored to meet your organization's needs.

But is MDR right for your organization? The goal of this document is to help you answer that larger question by guiding you through five smaller questions:

1. **Does your security team lack sufficient staff, skill and budget to deliver 24x7 services?**
2. **Is your security team overwhelmed by seemingly endless alerts?**
3. **Is your dwell-and-response-time above average?**
4. **Do you need to mitigate the risk of regulatory violations?**
5. **Does the ROI of MDR justify the expense for your organization?**

"Would you buy a security system that only worked between 8 a.m. and 5 p.m.? What about one that set off an alarm but didn't alert your phone or the police? … Having a cybersecurity plan without managed detection and response (MDR) is like having that security system."[7]

[7] Watne, Holden, "Why Your Organization Needs Managed Detection and Response (MDR)," GenIX, May 16, 2023.

Question #1:

Does your security team lack sufficient staff, skill and budget to deliver 24x7 services?

If your security team is operational only 40 to 50 hours (about two 24-hr days) each week, then you are at an increased risk for a malware attack. The Federal Bureau of Investigations (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have issued more than one alert reminding organizations that cybercriminals "may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses."[8]

To offset 24x7 threats, it stands to reason that you need 24x7 security. However, your organization might lack the cybersecurity staff and skill necessary for delivering continual security services.

A ESG and ISSA survey demonstrated that the "ongoing cybersecurity skills shortage impacted 71% of organizations and left two-thirds of cybersecurity professionals stating that the job itself has become more difficult over the past two years."[9]

A 2023 (ISC)2 study further reveals that organizations lacking sufficient staff are concerned about their organization's ability to protect itself. When asked why the shortage was happening, "41% believed it was due to a lack of qualified talent, 34% mentioned budgetary constraints, and 27% mentioned challenges with turnover and staff attrition."[10]

Study participants who reported insufficient staff felt they would have mitigated more threats if they had enough cybersecurity staff:

- Not enough time for proper risk assessment and management: **50%**
- Oversights in process and procedure: **48%**
- Misconfigured systems: **38%**
- Slow to patch critical systems: **38%**

The seemingly obvious solution would be to hire more cybersecurity team members.

Unfortunately, and not surprisingly, in a workforce shortage, organizations struggle to find qualified candidates and pay a competitive wage.

If you answer "Yes" to #1….

Your security team is experiencing limited staff, skill gaps, and budget constraints, then partnering with an MDR provider would be a sensible choice.

Doing so would enable you to:

- **Minimize your business risk**
- **Maximize your cybersecurity posture—starting now—without the difficulty and expense of hiring staff to do so**
- **Free your team to turn attention toward critical projects, such as creating (and training on) security policies and fine-tuning procedures that ensure ongoing compliance**

[8] CISA, Ransomware Awareness for Holidays and Weekends, Alert Code: AA21-243A, February 20, 2022.
[9] ESG and ISSA, "The Life and Times of Cybersecurity Professionals," September 6, 2023.
[10] 2023 (ISC)2 ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap

Question #2:

Is your security team overwhelmed by seemingly endless alerts?

According to Cybersecurity Ventures, if cybercrime were measured as a country, then it would rank third on a list of the world's largest economies, after the US and China.[11] This analogy points to the prolific nature of cyberattacks and the costly impact of seemingly endless security alerts on IT teams.

Security professionals spend a significant portion of every day investigating alerts—which often isn't enough time to address every alert, especially if encountering false alerts.

A Vectra AI report on alert overload notes that security analysts are unable to deal with 67% of the daily alerts received. On average, the report found, SOC teams receive 4,484 alerts daily and spend nearly three hours a day manually triaging alerts.[12] Excessive alerts can lead to alert fatigue and drops in worker productivity as well as security effectiveness.

> *"The current approach to threat detection is broken [...] disparate, siloed tools have created too much detection noise for SOC analysts to successfully manage and instead fosters a noisy environment that's ideal for attackers to invade."*
>
> **Kevin Kennedy,** SVP of products, Vectra AI

If you answer "Yes" to #2....

Many organizations have found it helpful to outsource 24x7 alert monitoring to an MDR service provider.

By partnering with an MDR provider, you gain a team of experts who prioritize the top critical threats, provide hands-on assistance for speedy response, or can resolve the threat on your behalf.

Armed with this additional security expertise, your team:

- **Receives fewer alerts, which in turn, reduces the teams' susceptibility to alert overload**
- **Is less likely to miss critical threats**
- **Regains time previously wasted on investigating lower-level or false-positive alerts**
- **Gains more time to respond appropriately to threats that matter**

[11] 2023 Official Cybercrime Report by Cybersecurity Ventures.
[12] 2023 State of Threat Detection Research Report.

Question #3:

Is your dwell-and-response time above average?

In cybersecurity, dwell time refers to the hours, days, or months that attackers lurk undetected in your network. Ideally, dwell time would be measured in minutes—or, even better, seconds.

But your organization doesn't live in an ideal world—and it isn't alone in the real world. According to a 2023 report by Ponemon Institute, organizations take an average of 204 days (about 6 and a half months) to identify a breach and another 73 days (about 2 and a half months) to contain it.[13]

To help reduce dwell time, your organization might have deployed endpoint detection and response (EDR), the de facto cybersecurity standard for endpoint protection. When properly configured, EDR can stop malware, detect suspicious activity, and automate responses.

EDR offers a solid start to protection. However, without experienced cybersecurity analysts dedicated to monitoring EDR, investigating priority alerts and taking action, organizations are not fully protected.

Your team may not have the time to respond to EDR alerts, notifications, and logs. Or perhaps team members lack the experience required to analyze this telemetry. Seasoned professionals can use EDR telemetry not only to stop attacks but to detect signs of attacks in progress sooner, thereby reducing dwell time.

If you answer "Yes" to #3....

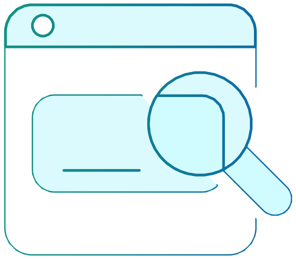
The power behind MDR starts with the automated detection and response that EDR offers—but it doesn't stop there.

With MDR, you partner with experienced cybersecurity professionals who continually monitor EDR telemetry, which to the inexperienced can be difficult to decipher. An MDR team may have years or even decades of experience analyzing EDR telemetry, which is critical: **Human expertise can find and stop attacks that software—no matter how advanced—misses.**

Augmenting your own team with an MDR team of seasoned threat hunters, forensic analysts, and incident responders vastly improves your cybersecurity posture.

For example, MDR security experts strengthen protection by:

- **Uncovering brute force attacks against remote desktop protocols**
- **Recognizing patterns of unfamiliar activity coming from a single account (indicating potential compromise)**
- **Creating rules to block activity they recognize as ransomware—even before a new variant has even been officially identified or named**



[13] Ponemon Institute, Cost of a Data Breach Report 2023.

Question #4:

Do you need to mitigate the risk of regulatory violations?

The stakes associated with cybersecurity (or lack thereof) involve more than the threats themselves. Your organization might need to verify compliance with regulations.

Many organizations collect and process data that is safeguarded under one or more data protection regulations, such as the EU's General Data Protection Regulation (GDPR). Other organizations collect payments subject to regulations, such as those dictated by the Payment Card Industry (PCI). If protected health information is collected, Health Insurance Portability and Accountability Act (HIPAA) requirements must be met to safeguard its privacy.

Non-compliance with rules and regulations can result in fines, which can be substantial. For example, violation fines associated with the GDPR are very high. Violators face fines of anywhere from €10 million to €20 million or two – four percent of their global revenue—whichever amount is higher.

And the potential cost of non-compliance doesn't stop there: anyone whose data was leaked has the right to seek compensation for damages.[14]

If you answer "Yes" to #4….

IndustryARC cites the need for compliance as one of the top three drivers of the MDR Market, which the firm projects will reach US $2.2 billion (about $7 per person in the US) by 2025.[16]

If you are subject to compliance mandates, then partnering with an MDR provider is likely a sensible option for you. MDR will help you:

- **Bolster your cybersecurity and provide evidence of improvements**
- **Dramatically reduce your risk of a breach**
- **Comply with most data protection regulations by implementing many of the critical steps required for doing so**

> "Compliance is a critical aspect of modern business operations…. MDR providers are well-versed in the compliance requirements… [and] can help businesses maintain compliance with regulations such as GDPR, HIPAA, PCI-DSS and others."[15]

[14] Wolford, Ben, "What is GDPR, the EU's new data protection law," GDPR.EU, July 18, 2023.
[15] "5 Reasons Your Business Needs MDR Solution for Proactive Cybersecurity and Compliance," SISA, March 8, 2023.
[16] IndustryARC, "Managed Detection and Response Market – Forecast (2023 – 2028)," July 18, 2023.

Question #5:

Does the ROI of MDR justify its expense for your organization?

If your organization is like most, your goal is to increase your profit. To that end, the business will require justification for every expense.

Can you justify the expense of MDR? If so, by what standard of measurement?

Compare the cost of a breach with the cost of improved protection to justify the expense of MDR. You'll also need to consider the cost of in-house cybersecurity professionals. As noted earlier, 73% of organizations experienced a ransomware attack in 2023 and 95% experienced more than one data breach.

The cost of a breach is staggering. For example, the average cost of a ransom paid in Q3 2023 was $850,70019.[17] But the ransom payment is not the only cost. Other costs include network downtime, legal liability, operational disruption, and lost personal data. When factoring all costs, the average cost of a data breach (across all industries) in 2023 was $4.45 million.[18]

Evidence of the clear and present danger of a breach should convince even the most cybersecurity illiterate of the need for always-current, always-available defenses. But that brings you no closer to justifying the expense of MDR.

One way to justify the expense of MDR is to estimate its return on investment (ROI). Research suggests that for most organizations, MDR pays for itself in approximately two months, compared to the cost of hiring internal staff.[19]

For example, at a cost of $3 - $6 per endpoint (for 24x7x365 monitoring, investigations, triage, and remediation), an organization with 1,000 endpoints would pay $3,000 - $6,000 per month. Now weigh that cost against the expense of hiring and maintaining in-house cybersecurity professionals to work the same hours and accomplish similar tasks. A scenario such as this yields an ROI as great as 425% with a payback on MDR in as few as 2.3 months.[20]

In addition, by some estimates and depending on the solution, MDR may reduce the risk of a breach by 99%.[21] When you consider that statistic against the cost of a breach, deploying MDR seems a sensible choice indeed.

If you answer "Yes" to #5....

To assess whether MDR makes financial sense for your organization, run a risk assessment, calculate the ROI, and see where you stand.

MDR offers the following benefits:

- **Reduces time-to-value**
- **Maximizes ROI**
- **Avoids the high total cost of ownership (TCO) associated with creating and running a 24x7 SOC inhouse**

[17] Statista 2024, https://www.statista.com/statistics/1409510/ransom-payment-us-quarterly-amount/
[18] 2023 IBM Cost of a Data Breach Report
[19] ThreatDown internal research.
[20] Ibid.
[21] Ibid.

Conclusion

If you answered "Yes" to one or more of the above five questions, then partnering with an MDR provider is likely a sensible choice for your organization. Not surprisingly, MDR is growing in popularity faster than other cybersecurity options: Gartner estimates that by 2025, 60% of organizations "will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today."[22]

Given its increasing popularity, MDR might raise the bar for baseline security. Not partnering with an MDR provider could leave your organization well below the baseline security bar.

> "Spoiler alert: Building an in-house SOC costs a heck of a lot more than partnering with an MDR provider…. Some estimates place the capital costs to establish a SOC at close to $1.3 million—and annual recurring costs running up almost $1.5 million. Not exactly dirt-cheap, to say the least."[23]

[22] Shoard, Pete, Al Price, et al, "Market Guide for Managed Detection and Response Services," Gartner, February 14, 2023.
[23] Cozens, Bill, "Is an Outsourced SOC Worth It? Looking at the ROI of MDR," December 15, 2022.

The Ideal MDR Partner

Ready to find your ideal MDR partner? Here are two critical areas to discuss with prospective MDR partners:

1. The MDR technology stack:

Each MDR provider has a unique technology stack, some are provider-owned, and some are only managed by the MDR provider. What is most important is that the stack is continually monitoring your environment to automatically detect, investigate, and remediate threats. Ask what is the provided or preferred EDR solution: a good one will be powerful and simple to use out-of-the-box without complex configurations or a hefty agent.

Award-winning EDR:

Industry-proven through award-winning protection, ThreatDown EDR stops attacks against workstations and servers with security that catches what other solutions miss. The ThreatDown Elite bundle combines EDR with threat prevention technologies and a skilled MDR analyst team to provide a simple, powerful, all-in-one cybersecurity solution that frees security teams to spend time on other projects.

2. The MDR team:

Each MDR provider will offer different degrees of collective experience; wouldn't you like to know what you're getting? Ask. MDR analysts should be experienced cybersecurity professionals with expertise in threat detection, forensic analysis, incident response and, ideally, data regulation requirements and compliance issues.

Skilled MDR analysts:

The ThreatDown MDR team features threat hunters with deep incident response backgrounds and decades of experience triaging and mitigating complex malware threats and protecting organizations from cyberattacks.

3. Deployment and setup:

Once you have selected an MDR partner, you want them to become an extension of your team, readily available and proactively monitoring, investigating and remediating threats as soon as they are discovered or provide you with easy guidance to follow if you prefer to take remediation actions yourself. What you don't want is to wonder what is happening, or for setup to take days, weeks or months. Adversaries won't wait. Why should you?

Immediate onboarding:

ThreatDown MDR is activated within minutes with our MDR analysts instantly monitoring your environment. Detection data is ingested into the MDR Security Orchestration, Automation, and Response (SOAR) platform where it is enriched with internal and external threat intelligence feeds. This process speeds the identification, analysis, and triage (response prioritization and investigation) of security events.

Introducing ThreatDown Elite

✓	**Managed Detection & Response**	24x7x365 monitoring by our experts, who analyze, respond to, and remediate threats on your behalf (even those that escape technological detection)
✓	**Endpoint Detection & Response**	Award-winning solution that provides continual active detection and response, suspicious activity monitoring, integrated cloud sandbox, and Ransomware Rollback
✓	**Threat Hunting**	Automated alert scanning that correlates EDR data against external and internal threat intelligence feeds, prioritizing threats and escalating the most critical with clear, step-by-step, response guidance
✓	**Endpoint Protection**	Defense-in-depth prevention that stops signature-based, fileless, and zero-day attacks before they infiltrate your system
✓	**Vulnerability Assessment**	Run scans on demand or on schedule to search for operating system and application vulnerabilities
✓	**Patch Management**	Automate the patching process to lock up potential access points
✓	**Application Block**	Easily block unauthorized programs to enforce acceptable-use policies
✓	**Incident Response**	Built on our proprietary Linking Engine that not only removes malware executables but finds and automatically eradicates all associated files and changes to prevent re-infection
✓	**7-Day Ransomware Rollback**	"Dial back the clock" instantly on ransomware and reverse ransomware encryption to restore files to their original state the previous week
✓	**31-day lookbacks**	Our team of experts, who search for Indicators of Compromise to stop attacks and refine detections and alerts going forward

Talk to an expert

Learn more about how ThreatDown MDR can help reduce cyber risk in your organization.

Glossary of Cybersecurity Terms

Alert fatigue is a condition to which cybersecurity professionals are susceptible that is characterized by desensitization to overwhelming numbers of alerts; alert fatigue can lead to ignored or missed security alerts. See "fear of missing incidents (FOMI)."

Endpoint detection and response (EDR) is a cybersecurity technology that continually scans endpoints (e.g., laptop, PC, server) to thwart cyberattacks. An EDR should meet these three critical requirements:

1. Detect, isolate, prevent, and remediate known and unknown threats
2. Investigate, threat hunt, and roll back systems infected with ransomware
3. Deploy, manage, integrate, and report with ease

False positives are behaviors that incorrectly trigger an alert indicating the presence of a cybersecurity threat, which poses a serious problem for SOC teams. According to the Enterprise Strategy Group, nearly half of all alerts are false positives.

Fear of missing incidents (FOMI) is an anxiety or dread that some cybersecurity professionals experience because they simply cannot investigate all of the alerts they receive; closely related to "alert fatigue." (FOMI is derived from "fear of missing out," or FOMO.)

Indicators of Compromise (IoCs) are clues or traces that attackers leave behind that show not only that a system intrusion or data breach has occurred but might also show how it happened and who is to blame. Unlike threat hunting, which can thwart an attack before it occurs, IoCs show you only what has already happened.

MITRE ATT&CK was created in 2013 based on real-world observations as a framework for describing and categorizing cyberattacks (according to their tactics and techniques). MITRE uses its ATT&CK framework to mimic known tactics and techniques as a way of testing and evaluating products.

Threat detection is a reactive search for IoCs to uncover what happened and who is to blame. Efficient threat detection is necessary for prompt incident response and remediation.

Threat hunting is a proactive search for threats aided by both machine learning (ML) tools and by trained security analysts. ML tools automatically and continually scan a network to observe user and device behaviors; the purpose is to detect anomalous and, therefore, suspicious behavioral patterns that might point to malware with an unknown signature. Once alerted, analysts investigate the potential risks to assess the validity of the ML tool's hypothesis.

Zero-day threats are software flaws that are vulnerable to attack and have not yet been patched.

Zero-day attack is an attack by way of an unpatched software flaw.

ThreatDown™
Powered by Malwarebytes

threatdown.com/mdr