eBook

ThreatDown™
Powered by Malwarebytes

Your MDR Buyer's Guide

The essential requirements for resource-constrained organizations to select an MDR service that delivers maximum security.

ThreatDown™ Powered by Malwarebytes

Contents

ThreatDown™ Powered by Malwarebytes

Executive Summary

Managing an organization's cybersecurity is a big effort. A strong cyber program is an essential component to a company's success in the present speed-driven digital world. While cybersecurity is an indispensable aspect of every business strategy, for most small- and medium-sized businesses (SMBs) defined as under a thousand employees by Gartner[1], delivering on that strategy with an in-house IT team is increasingly challenged by constrained budget, time, talent, and resources.

Over the past few years, the inherent complexities that organizations face in handling threat detection and response have given rise to managed detection and response (MDR) services. MDR services provide 24x7 monitoring of an organization's environment for signs of a cyberattack, and when the inevitable attack is detected, highly skilled security analysts deliver swift incident response actions. MDR services provide a valuable opportunity to outsource critical security tasks so that organizations' internal IT teams can focus on strategic priorities rather than chasing down alerts.

As organizations consider fortifying their security practices with an MDR service, how to select the ideal MDR solution becomes an important question. MDR services can vary in capabilities and some can come with a hefty price tag. For organizations with limited IT resources, an important consideration is what should and must be included in the service—at an affordable price point—that will support the end goal of keeping the business, its users, and operations secure and productive 24x7.

Whether you're just kicking the tires or are actively sketching requirements for an MDR service, this MDR buyer's guide will provide helpful guidance on the critical MDR capabilities to consider based on your cybersecurity goals now and in years to come.

[1] https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

Trends and Inhibitors in Managing Threat Detection and Response, In House

Undoubtedly, cybersecurity is hard. Threats and adversary techniques are evolving in ways that make them harder to predict and even harder to stop.

A recent survey, by our partner ThreatDown, showed that organizations with fewer than 1,000 employees have on average 450 devices to maintain and just three IT staff. For them, security is one task among many, and they don't have time to waste.[2]

68%

of mid-size organizations said managing limited time and resources is their biggest challenge

Security staff resources and skills shortage

Hiring and retaining seasoned cybersecurity practitioners is a challenge that continues to increase year after year. In 2022, the gap between supply and demand for skilled cybersecurity professionals was estimated at 3.4 million; in 2023, it reached 4 million.[3]

Organizations with limited IT budgets to attract security staff experience the shortage in the following areas:

- **Keeping up with the never-ending volume of alerts with limited team bandwidth**
- **Training junior analysts to effectively investigate and prioritize threat response efforts**
- **Hiring and retaining top security talent to fill skills and resource gaps, as well as enable the business to grow**

[2] Why complexity has become a security issue
[3] (ISC)2. Cybersecurity Workforce Study. 2023

ThreatDown™ Powered by Malwarebytes

Trends and Inhibitors in Managing Threat Detection and Response, In House (continued)

Detecting advanced attacks

Depending on the endpoint security tools used, it can be extremely hard for a security team to uncover threats in the business environment. Advanced attacks are commonplace because innovation is the name of the profitability game for cybercriminals. Attackers use "low and slow" tactics, techniques, and procedures (TTPs) that can individually pass for normal activity. This means, even with a great EDR tool, the security team may need external threat intelligence feeds to enrich alerts and support analyst investigations. And what about those alerts? They require in-depth investigation by seasoned analysts to truly understand the threat. Not to mention, the EDR only supports reactive investigation actions (i.e., responding to a threat after an EDR detection). To enable proactive threat hunting investigations based on IOCs, the organization need security staff, which takes us back to the staff resourcing challenges.

Time-consuming alert management and triage

With a constant overwhelming volume of alerts to prioritize and triage, security teams are stretched thin. Security analysts don't have the time to assess and validate every alert or set priorities on those that require further investigation. Avoiding the potential negative outcomes from a breach requires fast response to halt an attack, yet it takes 277 days on average to identify and contain a breach: 207 days to identify and 70 days to contain according to IBM.

Disconnected, complex toolsets

Managing an organization's security architecture requires multiple consoles across disparate technologies. Notably, 45% of organizations use more than 20 tools when specifically investigating and responding to a cybersecurity incident. However, use of disconnected tools creates complex environments, which can weaken cyber resilience.

ThreatDown™ Powered by Malwarebytes

The Rise and Value of MDR Services

Given the inherent complexities in managing threat detection and response in house, organizations are pursuing strategic approaches to overcome the challenges mentioned above.

Notably, many are pursuing new partnerships with MDR service providers who can fill in these gaps. MDR is an outsourced service that provides around-the-clock monitoring of an organization's environment for signs of a cyber-attack. Leveraging a combination of EDR technology and human-delivered security expertise, an MDR service provides advanced attack prevention, detection, and remediation, as well as targeted and risk-based threat hunting. That means an MDR service provider is always watching the organization's endpoints so the company's internal IT team isn't burdened with the time and resources the effort requires. This offers organizations a sure-fire way to navigate past some of the business complexities in managing cybersecurity while also freeing team resources to focus on other priorities.

The MDR security services market is experiencing accelerated growth with projections to reach $236 billion by 2028, which represents a strong 26.1% CAGR in the 2023 to 2028 forecast period.[4] According to Gartner, "By 2025, 50% of organizations will be using MDR services for threat monitoring, detection, and response functions that offer threat containment capabilities." Collectively, these projections represent a strong push for organiztions to investigate the value an MDR service can provide their organization.

At a high level, MDR is an outsourced cybersecurity service designed to protect an organization's data and assets even if a threat eludes EDR security detection. The core service capabilities include:

- **24x7 monitoring of an organization's environment for threats**
- **Threat detection, alerting, and response from highly experienced security analysts**
- **Correlation of endpoint alerts with other data sources to identify threats and response measures more effectively**
- **Proactive threat hunting based on past indicators of compromise (IOCs)**

[4] IDC Worldwide and U.S. Comprehensive Security Services Forecast, 2024–2028

ThreatDown Powered by Malwarebytes

The Rise and Value of MDR Services (continued)

The Benefits of Third-Party MDR

When an organization outsources threat detection and response to a third-party MDR service provider, they can seamlessly augment their security team while closing any bandwidth or security skills gaps. Adopting an MDR service also provides valuable business benefits by shoring up the organization's security posture and mitigating potential impact of malware threats to the business.

Adopting an MDR service provides many other advantages as well:

Business benefits

- Reduce risk of a data breach. With data breaches costing $4.45 million on average and putting many out of business the increased security level gain by an MDR service provides significant benefits to a company's continued growth and longevity.
- Maintain continuity and employee productivity by avoiding downtime from malware and other threat infections.

Team benefits

- Increase your team's morale and job satisfaction with fewer alerts and response efforts to navigate.
- Open your team's resources to focus on net new billable projects.
- Expand your team's skillset by learning how the third-party MDR experts respond to threats.

Before you make your move into the MDR market, there are several things to consider given MDR services can vary. As you embark on the strategy planning, there are three core areas to evaluate:

1. **The essential capabilities that should be included in the MDR service**
2. **Whether to build and manage your MDR in house or adopt a third-party service**
3. **If outsourcing, the top considerations for selecting your ideal MDR vendor**

Let's review the criteria for each of these core areas.

ThreatDown™ Powered by Malwarebytes

Essential MDR Capabilities

No doubt, MDR services include a range of features with a lot of "bells and whistles." Ultimately, your MDR must provide the capabilities to address the biggest security need: to identify and remediate IOCs quickly and accurately across your environment.

It's important to segment your MDR evaluation into sections that take a close look at the technology capabilities and human-driven functions that, collectively, provide strong assurance the offering will deliver rapid detection and response of new IOCs, as they emerge.

Evaluating the MDR capabilities across the following areas will ensure it provides a strong fit for your organization's needs.

Adopting an MDR service provides many other advantages as well:

Requirement #1: 24x7 real-time threat detection

Not all companies operate around the clock, but attackers do. In fact, 76% of ransomware attacks take place at night or over the weekend. For this reason, it's a necessity to have a security operations center (SOC) that monitors an environment full time. Ensuring your MDR service provides 24x7 coverage is table stakes to provide constant vigilance against malware attacks.

Requirement #2: Powered by EDR and SIEM technologies

An MDR service is only as strong as the technology that powers it. There are a range of approaches, so it's important to dig into the behind-the-scenes details when evaluating MDR providers. Good security hygiene is about "defense-in-depth" to counter the many possible attack vectors, so your MDR offering should include two essential technologies: security information and event management (SIEM), as well as endpoint detection and response (EDR)

A managed SIEM solution enriches threat analytics with endpoint alerts, correlated with log events and network flow, providing greater context that enables an MDR team to efficiently identify critical threats and IOCs. A robust EDR system is the go-to tool to deal with attacks that land on an endpoint. A high-caliber EDR solution should provide advanced threat prevention, detection, and automated response actions.

Requirement #3: Effective threat response

Responding to incidents has been a challenging area for organizations, often taking teams days to weeks to contain and remediate a threat. One of the biggest values from an MDR service is that you can fortify your organization's security with fast and efficient incident investigation and response.

To make that a reality, a high quality MDR service should provide incident response that is supported by both security analysts and the EDR platform. An MDR service provider with top tier security analysts will have the skills to tackle complex threats. This will reduce an organization's mean time to response (MTTR) and ensure they receive appropriate response actions for each type of incident.

ThreatDown™ Powered by Malwarebytes

Essential MDR Capabilities (continued)

Requirement #4: Threat intelligence

To keep data safe from zero-day attacks and advanced persistent threats (APTs), your MDR solution should include threat intelligence that applies specific tools and practices. Threat intelligence, or cyber threat intelligence, is information security experts use to understand the threats that have, will, or are currently targeting the organization. This provides insights into who attackers are, where they can access the network, and specific actions that can be taken to strengthen defenses against a future attack.

Your MDR solution should use curated threat intelligence from multiple sources. This important feature reduces false positive alerts and ensures your service is focusing on the threats that are most relevant and likely to be launched against your organization.

Requirement #5: Threat hunting

Threat hunting typically includes two essential functions in the delivery of MDR services. The first one is research-based threat hunting where security analysts look, or "hunt," for past IOCs and vulnerabilities that can pose a risk to your environment. When an analyst identifies a potential exploit, this information drives the team's priorities to provide related detection and response functions.

The second approach is active threat hunting where the security analysts systematically reviews your organization's environment to uncover any current suspicious activity or newly emerging IOCs that are in progress. Of course, when an IOC is detected, your MDR provider's response efforts should kick into action.

Depending on an MDR's service levels, they may only provide threat hunting based on an identified threat, so you should dig into the fine print to select an MDR offering that offers both active and research-based threat hunting.

Requirement #6: Reporting

Once you select an MDR provider, the partnership should run like a well-oiled machine addressing any security issues that come up in your environment. In like manner, MDR service providers should also have transparent and consistent communication, sharing details about their threat detection and response activities.

As part of this communication, you should receive summary reports that an MDR provider makes available either via a central dashboard or email. This empowers you to deeply understand what's happening in your environment and provides the opportunity to make other improvements to your security posture. Equally important, these reports allow you to assess the quality of service you are receiving from your MDR provider and to see how they respond to detected threats.

ThreatDown™ Powered by Malwarebytes

Build In-House or Select an MDR Partner

For your purchase decision, you must choose to either build your own MDR capabilities in house, or select an MDR partner. As market research shows, organizations are frequently choosing to partner as their preferred approach to enable the maximum benefits from an MDR service, and there are a lot of good reasons for moving in that direction. Partnering with an MDR provider gives you quick entry-to-market and alleviates the time, cost, staffing, and maintenance entry barriers.

Still thinking about building your MDR in house? Here are the staffing and facility aspects you'll want to consider before launching your in-house MDR capabilities:

MDR staffing requirements

- Hire a minimum of five, full-time employees to provide 24/7 coverage
- Identify effective avenues to find, hire, and replenish high-caliber security talent
- Develop an employee loyalty and retention program

MDR facilities requirements

- Build out SOC facilities
- Purchase, implement, and maintain the hardware and software for your SOC
- Project manage the facility operations and day-to-day MDR functions
- Provide ongoing security training, certifications, and red team exercises to expand staff expertise
- Purchase and manage third-party security intelligence feeds
- Engage periodic outside consultation to assess the caliber of your detection and response services and invest in appropriate items to make any recommended improvements

In short, building in-house MDR capabilities is a time, expense, and effort equivalent to starting an entirely new IT security department. Alternatively, partnering with an MDR vendor provides several key advantages:

- Gives you fast time-to-market to immediately address your organization's security needs
- Enables you to adopt a service that uses the best security technology and tools
- Removes the full-time employee staffing costs of hiring five analysts to run a 24/7 SOC
- Alleviates the capital expenditures (CapEx) of purchasing a SIEM or other security tools
- Empowers you to leverage a service that is backed by staff with advanced security expertise

ThreatDown™ Powered by Malwarebytes

Top Considerations for Selecting the Ideal MDR Partner

With hundreds of vendors in the MDR market, you'll have no shortage of choices when selecting one as your service provider. Finding an MDR partner is easy, but how do you find a good one? Ultimately, this should be a long-lasting relationship that will let you evaluate and question your vendor from multiple angles. Investigative questions across the following criteria will help you identify your preferred MDR service:

✔ Breadth of threat detection and response capabilities

- How effective are they at detecting new and obfuscated malware?
- What technologies do they use to power the MDR service, such as EDR, SIEM, and threat intelligence feeds?
- How often do they update the threat definitions on their EDR software agents?
- Do they support all the threat response requirements such as network, process, and desktop isolation, as well as automated remediation and rollback of ransomware encryptions so you can restore access to their files?

✔ Trusted brand

- Do you know and trust the brand to be hands-on with their customers' endpoints?
- How is the partner perceived in the market, and what kind of customer ratings do they receive?

✔ Ease of EDR deployment and onboarding

- What's the typical amount of time to install the EDR agents on machines? Is it a process that can be done in days, or will it take weeks?
- Once the EDR solution is set up, how much time will it take to establish a baseline profile for alerts?
- How long will it take before the MDR can enable communications with your internal IT security team?

✔ Threat hunting expertise

- How many security analysts will be supporting your organization? What are their qualifications?
- Does the MDR partner have cyber security practitioners with well-established and seasoned pedigrees?
- Do you have strong confidence in the MDR partner's ability to identify all levels of threats and swiftly deliver appropriate incident response efforts?

ThreatDown™ Powered by Malwarebytes

Top Considerations for Selecting the Ideal MDR Partner (continued)

✔ Partner

- What method will the MDR team use to communicate with you and how often?
- Can your team easily connect with the MDR service provider when you need support? How about outside of business hours?
- Are you satisfied with the level of communication offered by the vendor? Does it align with your business needs?

✔ Affordable pricing

- Does the MDR partner provide transparent and cost-effective pricing? Is it competitive and does it fit within your company's budget?
- Is the pricing model easy to understand so you can forecast your annual security budget for years to come?

✔ Reporting

- Does the MDR partner provide reports that allow you to review their recent and historic security activities?
- What details does the partner provide to help you understand the volume and types of threats targeting your organization?
- Do the MDR partner reports detail weaknesses in your organization's security posture?

✔ Threat enrichment via SIEM

- How many and which type of security data sources does the MDR partner use to monitor and identify threats?
- Does the partner use MITRE data, network, and third-party threat intelligence feeds to enrich their threat intelligence telemetry data and increase their threat detection effectiveness?

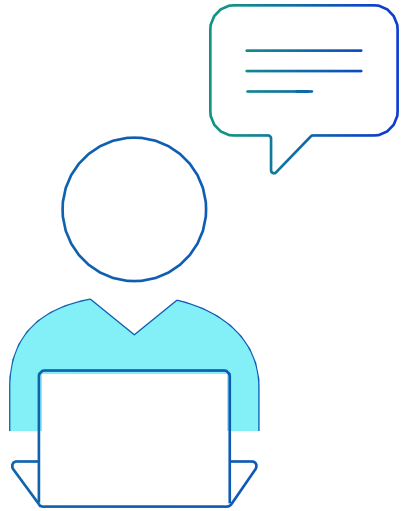
ThreatDown™ Powered by Malwarebytes

Considerations for Future Growth

Organizations today have a lot to navigate in managing security while prioritizing investments that help the company innovate and grow. Adopting an MDR provides organizations with a strong opportunity to offload resource-constraining security tasks. As well as strengthen the company's overall security posture while freeing budget, time, and talent to focus on projects that provide strategic value to the business.

Building MDR in-house can get expensive, especially considering the staffing and technology infrastructure costs. That's why partnering with an MDR vendor is one of the most popular method organizations are tapping into valuable security expertise to manage threat detection and remediation. Finding an MDR partner that aligns with your business requirements, budget, and use cases is essential to execute on your cybersecurity strategy and business goals.

With an MDR vender purpose built for partners who are supporting resource constrained organizations along with powerful EDR capabilities, highly seasoned security practitioners, and an affordable licensing model will provide your business with a strong service provider that will support your business goals now and well into the future.



ThreatDown™ Powered by Malwarebytes

ThreatDown: MDR Purpose-Built for Resource-Constrained Organizations

Our trusted partner, Malwarebytes, offers ThreatDown MDR to give 24x7 monitoring and investigations, perfectly suited for your resource-constrained organizations. From the ThreatDown team of of specially-recruited experienced threat researchers, expert security analysts, and veteran service leaders; your organization will gain a posture of cyber resilience with expert services that accelerate threat detection and perform incident response with precision. ThreatDown MDR delivers thorough remediation as attacks occur, powered by our proprietary remediation technology that removes dynamic and related artifacts.

Priced and packaged to meet your budget

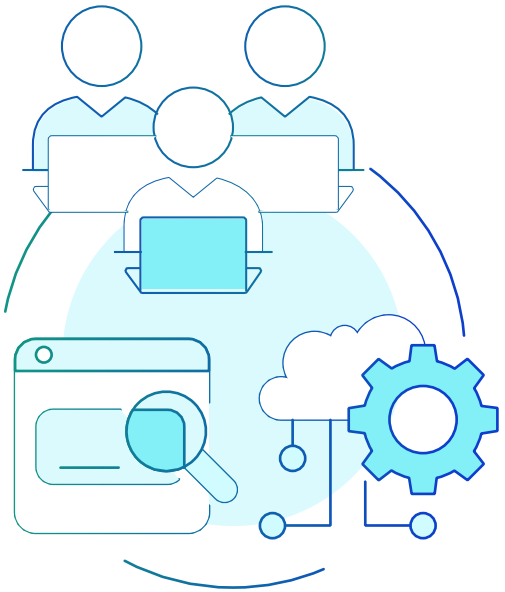
We work closely with Malwarebytes to offer organizations award-winning, customizable and scalable ThreatDown MDR service at a highly competitive and affordable rate.

Powered by ThreatDown EDR

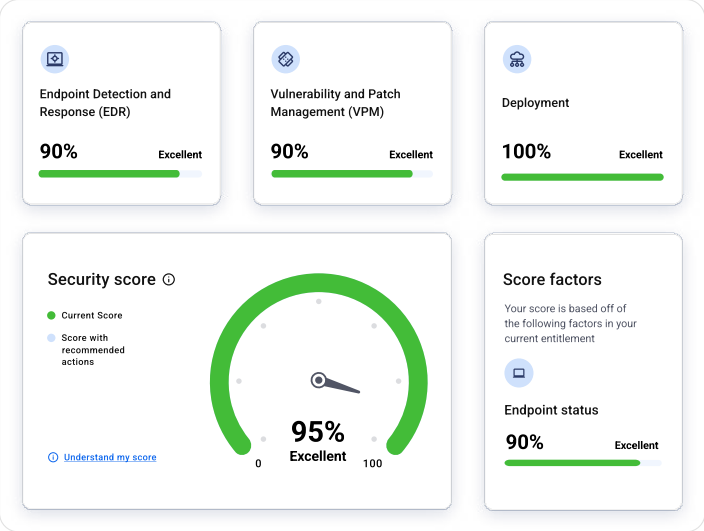
ThreatDown EDR provides powerful and effective threat detection, isolation, and remediation. Along with Malwarebytes' patented ransomware detection and remediation engine, exists many advanced layers of protection, multi-mode isolation, and automated malware clean up.

Other feature highlights include:

- **Providing the industry's only 7-day ransomware rollback, enabling full recovery from ransomware attacks in minutes.**
- **Applying multiple detection techniques to provide full attack chain protection.**
- **Delivering advanced remediation capabilities that uncover and remove hidden malware artifacts to provide thorough endpoint clean up.**



Detect and Neutralize Threats 24x7 with MDR



Learn more about how ThreatDown MDR can help your business.

Speak with us today

"Cyber threats are 24/7, and my team needs to sleep. The ThreatDown MDR team watching our network around-the-clock gives us a chance to sleep without worry."

Dennis Davis,

IT Systems Manager, Drummond