Malwarebytes™

# MSPs: YOUR MDR BUYER'S GUIDE

The essential requirements for MSPs to select an MDR service that enables high business growth and maximum security for customers.

# EXECUTIVE SUMMARY

It's an exciting time to be in the managed service provider (MSP) market. Businesses both large and small have a high demand for security services that help them defend against cyber threats, which is one of the key factors driving the MSP market's double-digit growth. Yet, if there's one thing we've learned about delivering security services, it's that it's a complex effort to get the security staff, time, and tools to keep up with attackers. In fact, research finds that the innovation gap between attackers' capabilities and an organization's security defenses is three months.[1]

Over the past few years, the inherent complexities organizations face in handling threat detection and response has given rise to managed detection and response (MDR) services. MDR services provide 24-by-7 monitoring of an organization's environment for signs of a cyber-attack, and when the inevitable attack is detected, highly skilled security analysts deliver swift incident response actions. It makes sense, then, that the MDR market provides an exciting opportunity for MSPs to augment their existing security services portfolio with a new, high value offering.

As MSPs consider expanding their business with an MDR offering, there's the big question on how to proceed and deliver the best MDR solution. MSPs are different than business buyers and have different needs. To start, there's the question of whether to build an in-house MDR service or to partner with a vendor. Next, there's the actual scoping of what features should and must be included in the service that will ultimately support the end goal of providing customers with an exemplary 24x7 service that also drives business growth and profitability for the MSP.

Whether you're just kicking the tires or are actively sketching your go-to-market plans for a new MDR service, this MDR buyer's guide, specifically for MSPs, will provide helpful guidance on the critical MDR capabilities and market entry considerations that will provide your MSP business with the best fit to support your business goals now and in years to come.

# MSP TRENDS AND INHIBITORS

Managed service providers are an important part of the IT environment, providing the knowledge and trusted partnerships that enable businesses of all sizes to embrace innovations made available by our era of digital transformation. MSPs provide such meaningful value for businesses that the market is experiencing steady growth with projections that it will reach $557.10 billion in 2028, which is an impressive 12.6% CAGR in the 2021 to 2028 forecast period.[2]

While there has never been a more exciting time to be in the MSP business, MSPs must navigate many challenges to acquire and preserve long-lasting client relationships. Indeed, there are many factors that keep MSP owners awake at night. With the steady market growth consistently attracting newcomers, 34% of MSPs cite competitive pressures as their top challenge while 27% point to revenue growth and 22% note hiring staff as some of the top business issues.[3]

With nearly all MSPs offering managed security services in their portfolio, this introduces another set of unique challenges, including:

## Security staff resources and skills shortage

While, overall, nearly a quarter of MSPs struggle with hiring staff, this issue is further complicated for MSPs when it comes to hiring and retaining seasoned cybersecurity practitioners. This isn't surprising when the global cybersecurity workforce is experiencing a massive 2.72 million shortfall of skilled workers.[4]

**The security staff shortage isn't a simple issue, and MSPs feel the pain in the following areas:**

- Keeping up with the never-ending volume of alerts with limited team bandwidth.
- Attaining deep security expertise for 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 MSP business to grow.

## Detecting advanced attacks

Depending on the endpoint security tools used, it can be very hard for MSPs to uncover threats in a customer's 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, MSPs 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 an MSPs reactive investigation actions (i.e., responding to a threat after an EDR detection). For MSPs to provide customers with proactive threat hunting investigations based on IOCs, they 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, an MSP's security team is 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 43% require days to weeks to remediate an incident.[5]

### Disconnected, complex toolsets

Managing an organization's security architecture requires multiple consoles across disparate technologies. Notably, 45% 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.[6]

## THE RISE AND VALUE OF MDR SERVICES

Given the inherent complexities in providing managed security services, MSPs are pursuing strategic approaches to overcome the challenges mentioned above. Notably, 44% are engaging new partnerships with MDR service providers who can fill in these gaps.[7]

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. For MSPs, that means an MDR service provider is always watching the MSP's customer endpoints so the MSP team isn't burdened with the time and resources the effort requires. This offers MSPs a sure-fire way to navigate past some of the business complexities in providing security services while also creating new opportunities to grow the business with an MDR service offering.

Notably, the MDR security services market is experiencing accelerated growth with projections to reach $2.2 billion by 2027, which represents a strong 16.7% CAGR in the 2021 to 2027 forecast period.[8] 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 favorable revenue potential for MSPs.

**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).

## BENEFITS TO MSPs

When an MSP outsources MDR to a third-party vendor, the MDR service is delivered to the MSP's customers on behalf of the MSP, which allows MSPs to seamlessly augment their security team while closing any bandwidth or security skills gaps. Offering MDR services also empowers MSPs to create market differentiation that provides valuable benefits by shoring up a customer's security posture and mitigating potential impact of malware threats to the customer's business.

Adopting third-party MDR services as part of your MSP portfolio provides many other advantages as well:

### Business benefits

- Grow business with new monthly recurring revenue (MRR) by adding MDR to your service offerings.
- Improve your competitive business value and stand out in your local region.
- Remain relevant and competitive today and in the future by offering a service that meets growing market demand from small- to medium-sized businesses.

### Customer benefits

- Improve your customer satisfaction and retention rates by reducing endpoint issues and mitigating disruptive infections that can lead to a breach and interrupt business operations.
- Reduce business risk by having 24x7 coverage by top-tier security analysts.

### 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 the service in house or partner with a third party.**
3. **If outsourcing, the top considerations for selecting your ideal MDR partner.**

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

# 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 the customer's 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 MSP offering needs:

## 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.[9] 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 that you can provide customers is 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.

## 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 that a customer's MDR service is focusing on the threats that are most relevant and likely to be launched against them.

## 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 newly emerging attack methods and vulnerabilities that can pose a risk to a customer's 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 an organization's network traffic and system logs to uncover 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 here to select an MDR offering that offers both active and research-based threat hunting. This will give you the flexibility to determine what business outcomes are most important for each of your customers and provide the level of service that meets their use cases and requirements.

### REQUIREMENT #6: Reporting

Once you select an MDR provider, it should run like a well-oiled machine that addresses security issues that come up and takes care of your customers' 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 provides makes available either via a central dashboard or email. This empowers you to deeply understand what's happening in your customers' environments and provides the opportunity to include this information in regular service reviews with your customers. Equally important, these reports allow you to assess the quality of service you are receiving from your MDR provider and to see how the MDR provider is responding to detected threats.

### REQUIREMENT #7: Multi-tenancy

Like so many other aspects of running an MSP business, multi-tenancy is an essential MDR requirement. Your MDR offering should have a multi-tenant architecture that allows you to manage and monitor multiple security systems for numerous customers all in one place.

Likewise, the multi-tenancy capabilities should have granular settings that allow you to provide MDR services to specific customers, as well as a select group of endpoints within a customer site. For example, it should be easy for you to select specific servers and business-critical endpoints that your customer wants to include under MDR management, while excluding others. When you can centrally manage everything with multitenancy, you can increase scalability, reduce costs, and improve security.

## BUILD IN-HOUSE OR PARTNER WITH A THIRD-PARTY MDR VENDOR

For your first go-to-market decision, you must choose to either build your own MDR service or partner with an MDR vendor. As market research shows, MSPs are more frequently choosing to partner as their preferred approach to enter the MDR market, 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 service:

### 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 an in-house MDR service is a time, expense, and effort equivalent to starting a new MSP business. Alternatively, partnering with an MDR vendor provides several key advantages:

- Gives you fast time-to-market to immediately address market demand.
- Enables you to offer 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 offer a service that is backed by staff with advanced security expertise.
- Makes it easy to scale and grow your MDR service with a fully staffed MDR service partner.

## TOP CONSIDERATIONS FOR SELECTING THE IDEAL MDR VENDOR

With more than 100 vendors in the MDR market, you'll have no shortage of choices when selecting one as your partner. Finding an MDR provider is easy, but how do you find a good one? Ultimately, this will be a long-lasting relationship so you'll want to ask questions that let you evaluate a vendor from multiple angles to ensure they'll provide the most value to your MSP business and your customers.

Investigative questions across the following criteria will help you identify your preferred MDR partner:

### 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 your customers can restore access to their files?

### Trusted brand

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

### Ease of EDR deployment and onboarding

- What's the typical amount of time to install the EDR agents on customer 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 MSP's team?

### Threat hunting expertise

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

### Vendor communications

- What method will the MDR team use to communicate with you and how often?
- Can your team easily connect with the MDR partner 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?

### Tenancy

- Will the MDR service provide multi-tenancy across your various customers?
- Can you easily apply MDR to specific customer sites and endpoints and keep track of licensing and billing?

### Marketing and sales support

- Does the MDR vendor provide marketing and sales support to help you launch your new offering?
- Does the vendor provide sales and marketing kits that help you expedite your service promotion to attract new customers?

### Predictable pricing

- Does the MDR company provide transparent and scalable pricing?
- Is the pricing model easy to understand so you can forecast monthly costs and easily invoice customers?

### Reporting

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

### Threat enrichment via SIEM

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

## CONCLUSION

As an MSP, you have a prime opportunity to enter the MDR market and grow your business. With Gartner predicting that half of organizations will be using an MDR service by 2025, you'll undoubtedly attract strong interest from existing and new customers.

Building an in-house MDR service can get expensive, especially considering the staffing and technology infrastructure costs. That's why, at 44%, partnering with an MDR vendor is one of the most popular ways MSPs are acquiring security expertise and introducing a new MDR offering.[10] Finding an MDR vendor that perfectly complements your MSP business needs and customer use cases is essential to execute on your well-rounded MDR business strategy.

Partnering with an MDR vendor that has a purpose-built service for MSPs along with powerful EDR capabilities, highly seasoned security practitioners, and a pricing model that offers favorable margins will provide your MSP business with a strong alliance to launch a successful MDR offering that supports your business goals now and well into the future.

# MALWAREBYTES: MDR PURPOSE-BUILT FOR MSPS

At Malwarebytes, we're deeply invested in enabling you to grow your MSP business. We stand by that commitment by providing our MSP partners with a purpose-built MDR service that makes it easy, efficient, and profitable to detect and respond to threats in your customer environments.

Malwarebytes MDR gives your MSP business a powerful and affordable threat detection and remediation offering with 24x7 monitoring and investigations, perfectly suited for your small-to-medium business customers. Your customers will gain a posture of cyber resilience with expert services that accelerate threat detection and perform incident response with precision. Malwarebytes MDR delivers thorough remediation as attacks occur, powered by our proprietary remediation technology that removes dynamic and related artifacts.

## Priced and packaged for your MSP business growth

With our affordably priced offering, you can realize high margins that accelerate your profits and growth opportunities.

Our pre-built selling and marketing kits make it easy for you to attract new customers and drive net new business with a high value offering.

## Powered by the Malwarebytes EDR platform

Malwarebytes EDR provides powerful and effective threat detection, isolation, and remediation. Along with Malwarebytes' patented ransomware detection, it includes seven layers of protection, multi-mode isolation, and automated malware clean up. Other feature highlights include:

- Provides the industry's only 72-hour ransomware rollback, enabling full recovery from ransomware attacks in minutes.
- Applies multiple detection techniques to provide full attack chain protection.
- Delivers advanced remediation capabilities that uncover and remove hidden malware artifacts to provide thorough endpoint clean up.

## TAKE THE FIRST STEP TO PURPOSE-BUILT MDR SERVICES FOR YOUR MSP BUSINESS

To learn more about how Malwarebytes MDR can help you grow your MSP business visit:
www.malwarebytes.com/MDR-for-MSPs

## TRUSTED BY YOUR PEERS

[1] Immersive Labs. Cyber Workforce Benchmark. 2022.
[2] Fortune Business Insights. Managed Service Provider Market Size. September 2021.
[3] Datto. Global State of the MSP Report. 2021.
[4] (ISC)2. Cybersecurity Workforce Study. 2021.
[5] Computing Research. Best practice makes perfect: malware response in the new normal. 2020.
[6] Ponemon Institute. Cyber Resilient Organization Report. 2020.
[7] Datto. Global State of the MSP Report. 2021.
[8] MSSP Alert. Security Research Brief: MDR Market Growth Forecast. December 2021.
[9] ZDNet. Most ransomware attacks take place during the night or over the weekend. March 2020.
[10] Datto. Global State of the MSP Report. 2021.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediations, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. for more information, visit https://www.malwarebytes.com.