

The Complete MDR Buyer's Guide

Your handbook to confidently evaluating a Managed Detection and Response (MDR) solution for your security program

Today's security teams struggle against 3 outsized challenges: technology, headcount, and expertise. But that doesn't have to be the case. By 2025, half of all businesses are expected to turn to a Managed Detection and Response (MDR) service for their Security Operations Center (SOC) needs. Here's what you need to know about selecting the right provider for you.

TABLE OF CONTENTS

Executive Summary	3
Cost Justification	4
MDR vs MSSP vs MEDR	6
Key Capabilities of MDR	8
Headcount and Expertise	10
Technology	12
Collaboration and Partnership	13
Threat Hunting	14
Process and Service Expectations	16
Managed Response and Incident Response (IR)	17
Security Orchestration, Automation, and Response (SOAR)	18
Simple Pricing That Works With You	19
MDR Vendors: Key Questions and Considerations Recap	20
MDR Power Moves	22
About Rapid7 Managed Detection and Response	23

Executive Summary

MDR Extends Your Security Team Faster Than You Can Add to It



While cyber threats are now the #1 concern of CEOs, their companies are at a persistent disadvantage. Even if security teams were given blank checks to add the best technology and armies of experts — staffed 24x7x365 — they couldn't.

Cybersecurity has a 0% unemployment rate. Of candidates applying for open positions, fewer than 1 in 4 are qualified.¹ Globally, 3.5 million cybersecurity jobs and counting are unfilled.²

MDR is an instant extension of your internal team. You'll have 24/7 threat monitoring, detection and incident response services, technology deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response.

Don't think of it as "outsourcing." The right MDR service is a partner, working alongside you and freeing your team to focus on what matters most. These services focus on "outcomes" as a force multiplier that integrates into your own internal incident response processes. But choosing that right partner can be difficult.

Almost every provider says the same thing: "We have the best people that use the best technology to detect and respond to threats across your network." But separating fluff from fiction is almost as difficult as sifting through the alert noise in your old SIEM.

This guide will help you understand the top decision criteria and questions you should ask each provider. It is based on thousands of MDR evaluations, hundreds of RFPs, and research from objective industry analyst experts. We've made it easy for you with a list of key questions to ask as well as additional worksheets and tools to help you find the right partner for your business.

According to Gartner®, "Many customers fail with their threat monitoring and detection and response initiatives because of the focus on wide-scale collection of data and generic security monitoring. Instead, they should focus on risks and outcomes that will directly impact their business objectives."³

¹ MIT Technology Review

² PricewaterhouseCoopers 2020

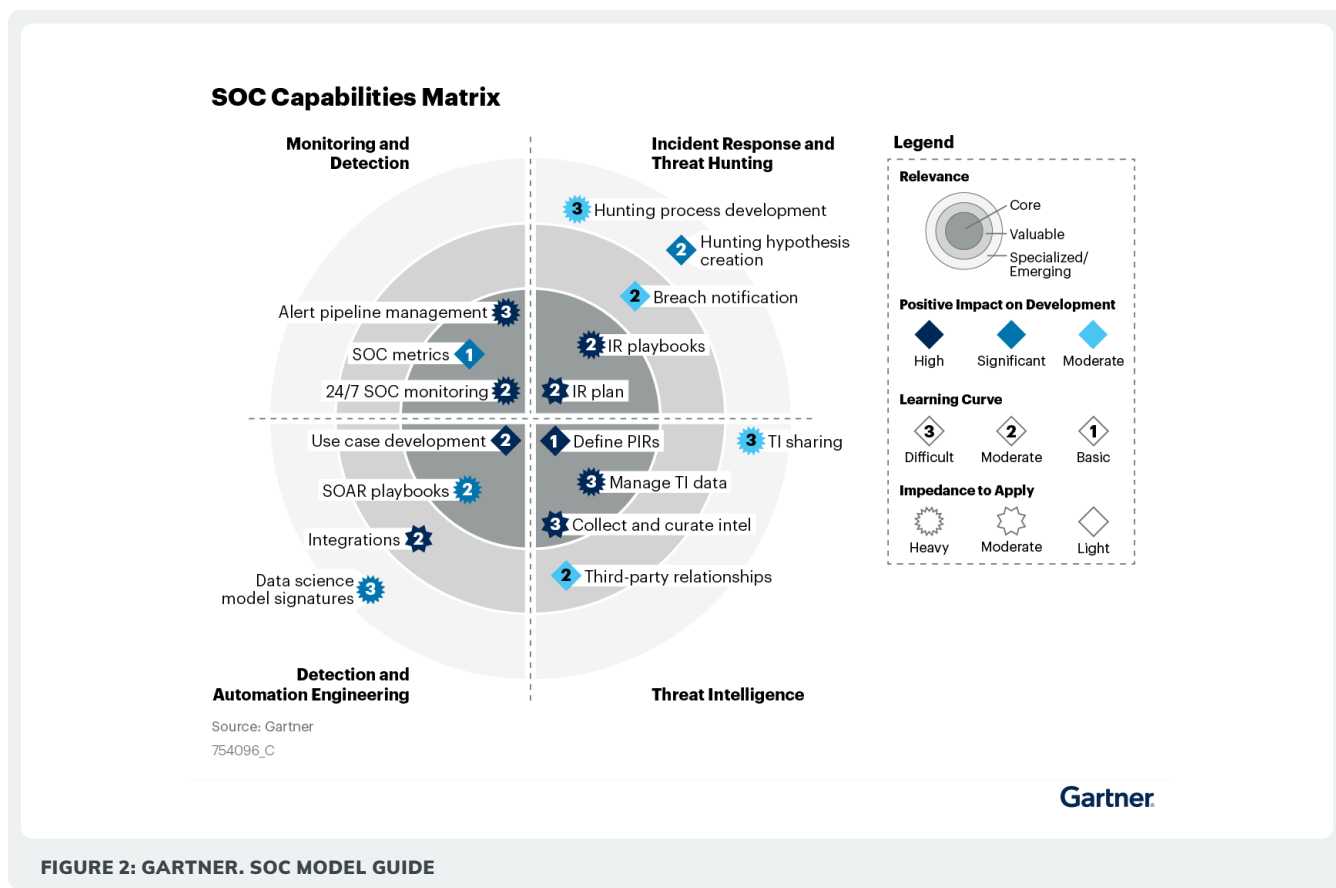
³ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021

Cost Justification

Managed Services Offer an Affordable SOC Option

While cyber threats are now the #1 concern of CEOs, their companies are at a persistent disadvantage. Even if security teams were given blank checks to add the best technology and armies of experts — staffed 24x7x365 — they couldn't. Cybersecurity has a 0% unemployment rate. Of candidates applying for open positions, fewer than 1 in 4 are qualified. Globally, 3.5 million cybersecurity jobs and counting are unfilled.

It's expensive to invest in cybersecurity. Without sugarcoating, a good MDR provider can cost a lot. But it's a whole lot more economical than standing up your own SOC team.



Building a modern SOC today requires you to go beyond the “core” capabilities shown in Gartner’s illustration above. According to Gartner, “Internal SOC’s are usually suited for well-funded organizations that can afford at least 10-12 personnel for 24/7 coverage, and that have a large array of security tool licenses and a library of comprehensive processes and playbooks.”

By adding these personnel and the technology solutions and capabilities to detect threats across your environment, you’re easily looking at a multi-million dollar investment.

And that's not to mention challenges like:

- One-by-one interviewing and hiring of highly sought after, experienced staff
- Finding ways to retain that SOC staff and keep them happy (like not working night shifts)
- Depending on new personnel to quickly learn what's at stake and then source appropriate hardware and software
- Implementing machine learning to tailor future automated processes
- Focusing on the massively important task of building out your SOC, which means not focusing on other parts of your growing business
- Proving the value and ROI of detection and response, especially to budget-controlling stakeholders outside of the security organization

MDR will be a significant consideration when slicing and dicing your budget. But if you haven't already built out a proven SOC and have stakeholders in urgent need of comprehensive detection-and-response capabilities, a rapidly engaged and deployed managed services solution might be for you.

By 2025, 33% of organizations that currently have internal security functions will attempt and fail to build an effective internal SOC due to resource constraints, such as lack of budget, expertise, and staffing.⁴

Key Questions and Considerations

- Will your provider be available for non-emergency communication, either by email or phone?

⁴ Gartner. SOC Model Guide. Collins, Schneider, Shoard. October 19, 2021.

MDR vs MSSP vs MEDR

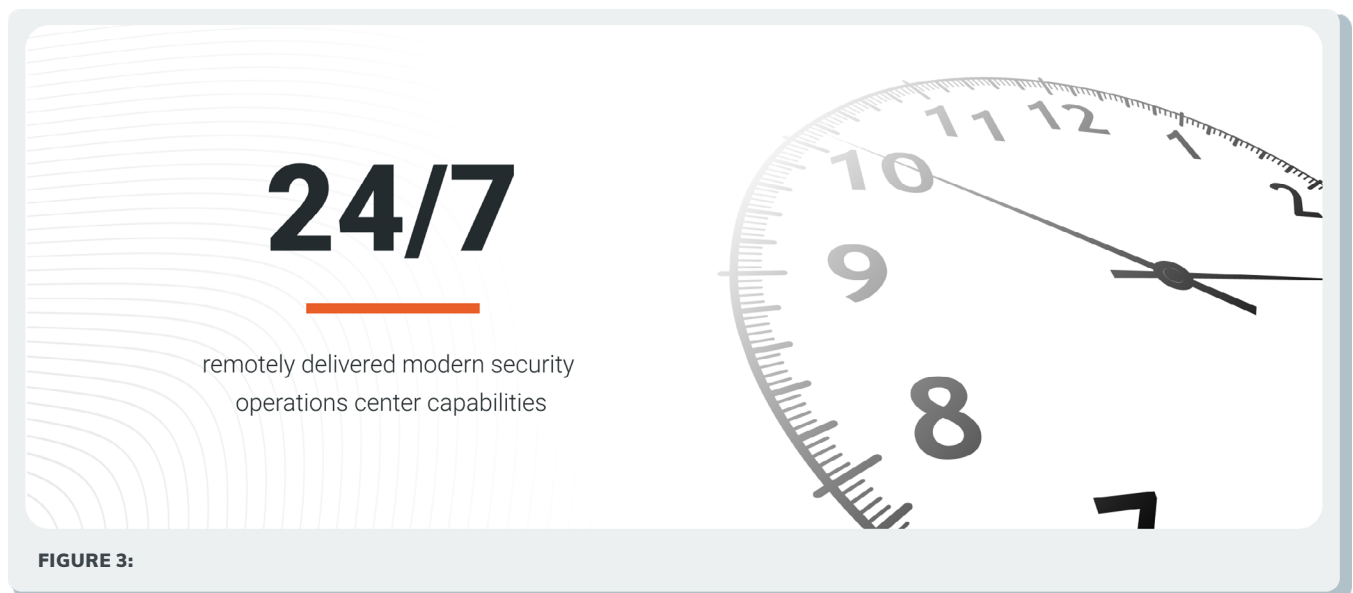
Is MDR the right fit? A quick look at your first, big choice.

Security teams often choose from one of three approaches to managed services. Choosing the best one for your business can make or break your success. Your first decision is which path to take:

MSSP is a Managed Security Service Provider. MSSP is a broad term often used to describe a wide array of Service Providers, with varying degrees of service maturity. Legacy services may be limited to alert-forwarding to your in-house team, while more mature providers may manage alert investigations but stop short of remediation. Recently, some MSSPs have begun to develop dedicated MDR offerings, but the scope of these can vary significantly across providers. When assessing MSSPs, be sure you have a detailed understanding of their scope of service to ensure their combination of people, process, and technology will meet your needs.

MEDR is a Managed Endpoint Detection and Response. This is typically an MSSP add-on service focused specifically on endpoints, though it is available as a standalone offering. Providers that have endpoint protection agents will often augment their offering by providing MDR specifically for their software. Here too, the actual “response” is in your team’s hands.

MDR is Managed Detection and Response. This is an end-to-end, turnkey solution, providing threat detection, incident validation, and response, such as threat containment in your environment. MDR is available 24x7x365 as an extension of your in-house team. It can be a game-changer, with some providers adding features such as threat intelligence, human-led threat hunting, behavior analytics, automation, and more to your capabilities. One of the biggest differentiating factors for MDR providers is their reporting which dives much deeper into the attack details than an MSSP or MEDR would convey.



While MDR is more expensive, it is arguably a better option. Detection and response requires a dedicated SOC staffed with highly skilled security experts using the best technology, cutting edge threat intelligence, and forensic tools to reveal — and report — problems and ensure stealthy attackers have nowhere to hide.

Use MDR services to obtain 24/7, remotely delivered modern security operations center capabilities when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing security operations capabilities.⁵

Key Questions and Considerations

- How did the attacker get in?
- What tactics, techniques, and procedures (TTPs) did the attacker use?
- Where did the attacker move?
- What credentials were used?
- What data was accessible and/or exfiltrated?
- How should we prevent this type of incident from happening in the future?

⁵ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021.

Key Capabilities of MDR

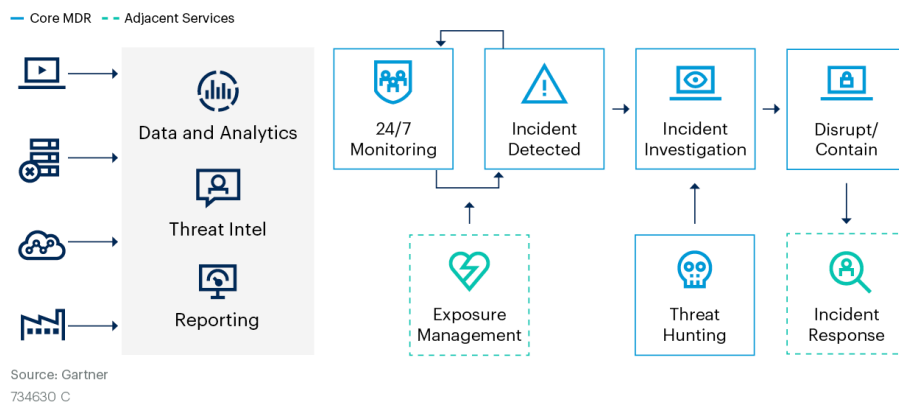
Evaluating MDR on 8 Core Capabilities

Almost every MDR buyer's journey for finding their MDR partner starts with feeling the pain of one or more core challenges for their security program:

- Their organization has minimal in-house threat detection and response capabilities
- They don't have enough resources to achieve off-hours or 24x7 monitoring
- They lack technologies or skills to take on forensic analysis or extended detection and response (XDR) coverage
- They don't have the staff or budget to expand their capabilities
- They're not capable of collecting and acting on threat intelligence
- They need a "second set of eyes" to augment their SOC
- By using an MDR service, they may feel like it can make their existing team more efficient

While these challenges are a thorn in your side, rest assured, you're not alone. MDR services can help alleviate all of these issues, but first you must ensure you're finding the right solution that helps your team achieve the desired security and business outcomes.

Managed Detection and Response and Adjacent Services



Gartner.

FIGURE 4: MARKET GUIDE FOR MANAGED DETECTION AND RESPONSE SERVICES ⁽⁶⁾

MDR service delivery is split into Core and Adjacent capabilities. Gartner says the right MDR vendor will be able to "deliver these capabilities using technologies — at the endpoint, network, application and, increasingly, cloud services layers — that generate or collect security log data and alerts. In addition, telemetry provides contextual information (for example, identity and user, vulnerabilities and business-criticality) to improve and validate threat detection. Providers develop threat-focused content and analytics (also known as detection engineering). They apply threat intelligence (whether it is developed in-house, purchased from third parties or a combination of both approaches) and manual and automated incident mitigation activities — such as host isolation, account lockout, and network blocking."⁷

⁶ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021.

⁷ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021.

But as you've probably seen, almost every vendor says they can do these things. It's hard to tell fact from fiction. To navigate the crowded market for MDR service providers, you should make sure you're evaluating each across 8 of the most critical core capabilities:

1. Headcount and Expertise	How experienced are the MDR analysts that will be working alongside your team?
2. Technology	What level of visibility and detection methods will be used for real-time threat monitoring and investigation?
3. Collaboration and Partnership	What do day-to-day and monthly service interactions look like?
4. Threat Hunting	Will the MDR vendor go beyond real-time threat monitoring to provide proactive, reactive, and targeted threat hunting?
5. Process and Service expectations	How will your MDR provider help you achieve rapid time to value and ensure you're making progress over time?
6. Managed Response and IR expertise	How will your MDR provider help you respond on your behalf, and what happens if that incident becomes a breach?
7. Security Orchestration, Automation, and Response	Does the provider leverage SOAR to automate their processes, and is there a way that you can leverage SOAR capabilities?
8. Pricing	How does the MDR provider price their solution to ensure it's transparent, predictable, and aligned to the value you'll receive?

1. Headcount and Expertise

It's one thing for an MDR provider to say something like, "We can detect threats across your entire ecosystem and attack surface." It's quite another for a provider to say they do all that with world-class expertise and effectiveness 24 hours a day, 365 days a year.

Technology can only go so far. Round-the-clock monitoring by SOC experts is crucial in the seemingly forever-war against today's attackers. They don't sleep, so why should your MDR? You want your headcount and specialist personnel freed up to innovate, push forward long-tail security initiatives, and provide increasing value to the business.

Staffing and Headcount

If your company is facing staffing issues in skilled security and IT positions, you're not alone. As the pandemic has forced companies to adapt to remote work on a never-before-seen scale, the race for skilled talent that can work from anywhere is heating up. Therefore, small-to-midsize companies may not be able to pay ultra-competitive salaries that some world-dominating firms can.

What does that particular context mean? That you may be facing a shortage of security personnel now or in the near future. And in this era of increasing attacks — particularly of the ransomware variety — it's necessary to find value for money in your MDR provider of choice. If an MDR partner is focusing solely on your organization's detection-and-response capabilities, you should ultimately experience shorter detection times. This leads to shorter response times, especially when automated workflow becomes prevalent.

Therefore, as mentioned above, it's key for the specialists you do have to be able to focus less on endless vulnerability chases and more on projects that will move the organization forward as well as keep the business secure and competitive.

Expertise

When it comes to the expertise your MDR provider should bring to the table, let's look at a medical analogy: you go to your primary care physician for an annual checkup, for referrals, and to check on your overall health. But if you needed open-heart surgery, you wouldn't go to your primary-care physician. You'd go to a Cardiothoracic Surgeon, someone who specializes in those types of procedures and has performed hundreds of them. Sure, your primary-care physician knows about general medicine, but they won't be successful performing a specialized surgery.

The same is true for cybersecurity. A security generalist might be able to monitor technology for alerts, but they're certainly not going to be able to do deep investigations, malware forensics, or scope and respond to an incident when there's a breach. So when it comes to your program, it's a good idea to engage a service that brings those specialized capabilities like:

- **Integrated Threat Intelligence** — Pulling in data and insights from multiple telemetry sources — internal and external — is the basis of XDR. This type of advanced threat intelligence leads to smarter, more actionable, and more precise threat-hunting capabilities. Taking all of this into account, an MDR provider should be able to alleviate SOC teams from dealing with the sheer number of false positives pouring in as organizations race to adopt cloud infrastructure and scale up.
- **Breach-response Capabilities** — When it comes to "incident response," make sure you're going to get what you pay for. Every MDR vendor will tell you their people are experts, but how can they prove it? The best MDR providers are staffed with analysts AND Digital Forensic and Incident Response (DFIR) experts who have hundreds to thousands of hours experience handling some of the most advanced data breaches in history.

Key Questions and Considerations

- What is the experience level of the MDR SOC team that will be monitoring my environment?
- What is the tenure and attrition rate of the team?
- How many MDR analysts are assigned to monitor my environment?
- Where did the MDR provider locate their security operations teams? Did they choose locations with the highest concentrations of threat detection and response expertise? Or were they focused only on minimizing operational cost?
- How does the MDR provider ensure 24x7 coverage?
- How does the provider integrate threat intelligence into the service?
- What's the process if the MDR provider misses a confirmed breach in the environment?
- Does the MDR provider have in-house, incident-response expertise on staff and ready to take action in the event of a breach?

2. Technology

The best MDR services combine deep observation of endpoints with real-time forensics, authentication, network, and log data. More recently, experts are extending MDR functionality to tackle rapidly scaling cloud environments. This is an effective approach to XDR: a cloud-native platform that optimizes threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation. It simplifies SecOps, and gives analysts the freedom to focus on what matters most.

Since threats are coming from anywhere and everywhere along modern networks, XDR's greater scope of visibility means having a more cohesive view of related events so you can detect threats faster, and elevate outcomes. Without multiple sources of telemetry, your depth of defense could be lacking, leaving your environment exposed to a breach.

User-endpoint Telemetry — User telemetry provides insights on file and network access, registry access or manipulation, memory management, and start-and-stop activity. Unusual behavior detected can include processes that spawn command shells, memory injection attempts, or accessing unusual file locations.

Server-endpoint Telemetry — Server telemetry provides information on extremely differentiated data. Since servers handle so much crucial organizational functionality, XDR telemetry can help prioritize investigations and remediations of incidents on a more macro level.

Network Telemetry — Network telemetry provides insights on traffic, particularly a sudden increase in volume, new network protocols, or anomalous privilege escalations. Advanced encryption methods can often hinder deeper network analysis that could otherwise thwart threat actors. But make no mistake, combined with endpoint telemetry network traffic analysis can be a cornerstone of an XDR offense.

Cloud Telemetry — Cloud telemetry provides insights on infrastructure. This can include detecting security anomalies for any cloud workloads or components deployed. Attackers specifically targeting an organization's cloud components can easily gain access with the proper credentials, so it is of critical importance to leverage the advanced detection technology of XDR to hunt threats faster and fortify cloud environments.

Investigate whether the MDR provider's technology stack or supported set of technologies fits with existing security controls and IT environment, from on-premises to cloud.⁸

⁸ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021.

3. Collaboration and Partnership

An MDR provider should be a true partnership — they should work in step with your existing security program to help alleviate the pressure and around-the-clock expectations of your team. The best providers strive to understand each customer and then meet and exceed their unique needs.

Named Security Advisor as Your Main POC

The best MDR providers also work to build cyber resilience in the present as well as into the future. This often means appointing security-program advisors as each customer's point of contact (POC); advisors should learn about customer environments, goals, and limitations so they can provide the fastest breach notification and response, as well as guidance for program improvement.

As a prospective customer, try to dig deep into what your relationship and engagement model will look like so an MDR partner brings real benefits to your team and acts as a true partner rather than a "human SMS" system. Your Security Advisors should be available to provide regular updates in the form of monthly consultations and/or service report reviews.

SOC Team

Your Security Advisor may be the face of your MDR relationship, but the SOC team of threat analysts will be the heart of the service. This team might come in one of two models. A SOC "concierge" model would focus on triaging your alerts quickly, and would spend less time focusing on actual threats. However, in-house analysts at any reputable MDR firm are often deployed as a SOC "squad" model to ensure your environment will be covered as the MDR partner scales their operations.

The squad model assembles SOC analysts into teams (squads) and assigns each squad to customer clusters so that, over time, they learn about their unique user environments. Squad methodologies allow teams to triage customer alerts and prioritize the highest-risk threats in a fast and efficient manner. The Forrester Wave™: Managed Detection and Response Q1 2021 says:

"Many MDR vendors offer the squad model for a customized delivery experience — a dedicated team of analysts, responders, and customer support specialists that work within a given vertical and geography.

The strongest MDR vendors work with customers while building each squad to ensure the team members are the best fit for personality, team culture, and desired capabilities. Customers noted the importance of the customized squad approach and appreciated that they were able to swap out team members during the early stages to get the most out of their MDR provider."⁹

Key Questions and Considerations

- What does the interface look like — both digital and via humans — when customers need to connect with the MDR team?
- Is the MDR team using a concierge model or a SOC squad model?
- How does the MDR operations team plan to scale as the number of customers grows?
- What is the ratio of MDR SOC analysts to customers? Security Advisors to customers?
- How quickly can your SOC team scale up to detect and respond to larger incidents, like a supply chain breach?

⁹ The Forrester Wave™: Managed Detection and Response, Q1 2021. Forrester Research, Inc. March, 2021.

4. Threat Hunting

Paring down data into actionable insights and detecting anomalies in customer environments is the foundation of a successful threat-hunting methodology. Ideally, your MDR provider should quickly be able to parse a suite of host- and network-based forensics to get a clear sense of a customer environment at a given moment in time.

Threat hunting is human-led and is based on risk analysis and integrated threat intelligence feeds that augment indicators of compromise. A provider should first get to know the ins and outs of your IT/security stacks, then implement a tailored plan to begin offensive tactics across your systems and application environments. Let's now take a look at different types of threat hunting you should make sure your provider is offering in their services package.

Reactive Threat Hunting

1. **Identification of malicious processes based on suspicious network activity** — The monthly collection of process snapshot data allows for the extraction of network connection data for each running process. This data can then be used for the identification of undetected malicious processes via the analysis of suspicious network connections.
2. **Detection of suspicious ingress events** — The aggregation and analysis of all external ingress authentications that occurred in the customer's environment for a given month allows an MDR provider to detect suspicious authentications not detected by real-time alerting.
3. **Imposter domains** — Threat hunts should uncover all types of threats to your business, not just hackers. For example, the hunt reports should be able to find multiple registered domains that are potentially designed to be imposters of your registered domain. We call these look-alike domains: those not owned by your organization and possibly used for malicious (often phishing) purposes — like "Rapld7.com" instead of "rapid7.com". The easy way to solve this problem is to review and block the identified domains, if they serve no business need. But without your MDR provider telling you which domains are out there in their threat hunt analysis, you're left to figure this out on your own.
4. **Malicious PowerShell activity** — For some providers, this is common practice and is picked up with real-time detections. But if the provider is unable to monitor for malicious powershell commands in their technology-driven detections, make sure it gets picked up in their monthly hunts. This is all activity regarding PowerShell execution in your environment.
5. **Reconnaissance and lateral movement via "net" commands** — If real-time detections are not set up for lateral movement, ensure that manual review is set up to aggregate and review all net command execution in your environment to detect any potential reconnaissance/lateral movement/post-exploitation that may have evaded real-time detections. This should be core to any MDR provider's abilities.

Proactive Threat Hunting

1. **Forensic data collection and ingestion** — In this process, forensic data is normalized and enriched. Informational tagging is then applied to data, e.g: "Remote Access Software," "Cloud Storage Software," etc. Persistence based alerts are generated via detection rules being applied to the forensic data, which are then independently triaged by the SOC. Normalized and enriched data is then ingested into hunt databases.
2. **Real-time data aggregation** — Available real-time data should be aggregated for analysis. But in the off-chance that the real-time detections cannot trigger alerts on this activity, ensure your provider includes command line data of all PowerShell executions and of all net commands that occurred during the month in their threat hunting. Doing this should also account for asset authentication data depicting successful Remote Desktop (Type 10) authentications from public IPs, firewall logs depicting any external SMB traffic observed during the month, and source address data for all successful ingress authentication events

3. **Analyst review** — Alerts generated from forensic data should be triaged by MDR analysts. They should perform a review of a stacked representation of forensic data and aggregated real-time data to identify suspicious entries. If determined to be malicious, a full investigation should be conducted and a report produced by your MDR provider as if it was any other incident. The report usually includes identification of documents and files that likely contain password information, an overview of remote access applications found, and an overview of cloud-storage applications found.

Targeted Threat Hunting

1. **Combine elements outlined in both proactive and reactive threat hunting** — Your MDR provider should be able to perform ad-hoc hunts against any asset or asset group in an organization.
2. **Monthly threat hunts** — These should target all available assets, looking for unknowns across the entire environment. When a new threat is discovered — like the Solarwinds hack or the Microsoft 0-day exploit — a provider often will perform retro-hunts in your environment to ensure nothing is exposed and/or TTPs not identified using analytical detections haven't been exploited.

Key Questions and Considerations

- Is your provider doing real-time, reactive, proactive, and targeted hunts?
- How often are proactive threat hunts performed?
- What type of reporting is delivered after each hunt?
- When new threats are discovered, how does the team do targeted threat hunts?
- Will the MDR provider assess and alert you to potential look-alike, imposter domains?
- Is powershell activity logged and alerted in real-time, or will it be reviewed after a manual threat hunt?
- Is lateral movement activity logged and alerted in real-time, or will it be reviewed after a manual threat hunt?

5. Process and Service Expectations

Despite alert fatigue, validation is always required. These days, the average attacker dwell time is about 270 days. That is anything but good. So, how can organizations be faster and build resilience for the future? MDR services hold the key.

270 days

the average attacker
dwell time



FIGURE 5

Deployment and Onboarding

Every security organization is different, so it stands to reason that MDR provider onboarding should be customized to each individual client. Deployment and onboarding is a journey, therefore expectations should be kept in check as far as the first day online versus the first year online with a new provider. However, you can look for service providers who will start protecting you as soon as you start and ramp up the process, rather than waiting until everything is complete to begin delivering value. The machine-learning capabilities at the heart of a service will need time to, well, learn a particular organization's activities to ensure detections are tuned for your specific environment. After all, you're getting a service that extends your team, so your service should be tailored to your environment as well.

Compromise Assessment

Want to know what's worse than getting breached with an MDR service? If you were already popped before the MDR service even started. Before you begin your service, understand how your MDR provider will ensure you're not compromised before you begin. Otherwise, they could be pointing the finger back at you for the blame. A compromise assessment should utilize the exact same approach and methodology as the monthly threat hunts to spot known and unknown threats in your environment and ensure you're starting out with a clean baseline.

Metrics

You'll need more than an incident report when something happens in order to justify your MDR purchase. That's where detailed reporting comes in, down to the alerts by disposition, metrics around mean time to detection (MTTD), and mean time to respond (MTTR) to provide your team (and your executives) the analytics that prove out your MDR partner's value.

Key Questions and Considerations

- Would a human be involved in any part of that automated response?
- Is threat intelligence derived from research, previous investigations, monitoring findings, and third-party sources?
- Does machine learning eventually establish benchmark metrics for detection within your environment that would enable future automated response?

6. Managed Response and Incident Response

Limiting an attacker's ability to execute is perhaps the most crucial consideration after detection, especially if an attacker is proficient at bypassing proactive security controls. So there are 2 considerations for effective incident response:

- Acting with urgency
- Leverage a strategy that goes beyond only securing affected endpoints

An effective response should include cutting attackers off at both the endpoint and user-account levels, and your MDR provider should take action immediately in the wake of detecting confirmed malicious activity.

Managed Response

The worst thing your MDR partner can do is tell you "we found this threat, now you have to go take care of it." You should find an MDR provider that can help you take action at any time, day or night, with whatever level of collaboration and control you specify. Gartner sees this as a core capability for MDR providers: "A key value proposition of MDR is performing the initial mitigation steps when a threat is identified to enable an effective incident response and remediation process. By providing deeper investigation, analysis, and validation of threats, and taking action to disrupt or contain an attack, the MDR provider can buy time for the customer to perform further investigation and remediation."¹⁰

This type of provider is more aligned as a partner for your business than a transactional, service-oriented relationship. Look for a service provider who will be working shoulder-to-shoulder with your team should a breach occur. Being able to quickly engage a team of in-house breach-response experts at your MDR provider speeds up the process in the event of a breach, since the same team monitoring your environment can quickly pivot to incident-response mode. No time should be lost when minutes are critical.

Digital Forensics and Incident Response

When something really bad happens, who you gonna call? Hopefully it's not like many providers who actually refer you down the line to another third-party with extensive breach-response expertise because their MDR SOC can't handle it. And who wants to deal with yet another provider when you only thought you'd be dealing with one? The best MDR providers have breach-response expertise on staff and are included as part of their MDR service. This level of integrated, in-house team should be able to quickly pivot to DFIR mode once a confirmed breach is detected, and that has multiple affected endpoints, lateral movement, or data exfiltration.



Warning: Be aware of "assurance guarantees" or "warranty" clauses

Who wouldn't want a "\$1 million guarantee" if something happened? The problem is, it's often too good to be true. If you get breached while under that MDR's watchful eye, they're going to make you jump through a ton of hoops to get anywhere near that \$1 million. Oftentimes it's only reserved for customers who have many of that provider's products, and only under certain circumstances, with allotments reserved by each element of the breach. The point is: If you're getting all that guaranteed money, you've got bigger problems on your hands. And chances are, you'll be back to searching for a new MDR provider soon after. At the end of the day, you want your MDR partner to be on your side - not trying to find ways to pay you off (or worse, they say, "sorry, you only qualify for this much").

Key Questions and Considerations

- What types of managed response actions can your SOC advisors take?
- How can I deny the containment response if I don't want the SOC team to take action, especially if the action is automated?

¹⁰ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Lawson, Schneider, Collins, Wah, Davies. October 25, 2021.

7. Security Orchestration, Automation, and Response (SOAR)

Security orchestration, automation, and response (SOAR) includes a range of services typically designed to help you leverage automation to lower your average incident-response time, expedite eradication processes, and free up more time by automating tedious and repetitive tasks. As a customer, you should also be able to quickly leverage “out-of-the-box” automated workflows inside your provider’s detection-and-response tool so you can eliminate low-value work.

Alert Enrichment

Event sources and agent data are great for detections, but the SOC needs as much data as possible to do their job. This is where SOAR comes in to automatically enrich the quality of your security alerts with more data and then help analysts weed out false positives. Not only is your MDR partner’s SOC operating at optimal speed and with the right context using SOAR enrichment, but their deliverables to you (the incident reports) are stronger and more detailed.

Threat Response

SOAR is often the back-bone for Managed Response actions. It provides both flexibility and integration to fit into your workflow instead of you accepting automated actions taken on your behalf. For example, when threats are validated, an MDR provider should be able to kick off an automated response workflow to contain a threat. While the action is often automated, it should include a human-review component and initiation by that human.

Key Questions and Considerations

- What SOAR workflows are included for me to use?
- Is there an ability to add more automation to expedite my remediation process when MDR finds something?
- In what instances will the MDR service take response action on my behalf?
- Is there an ability to create an exceptions list?
- Will you be able to look up indicator reputation with open-source threat intelligence, kill malicious processes, quarantine infected endpoints from the network, deprovision users, reset passwords, and more — all from day one?
- What about blacklisting hashes or blocking IP addresses, URLs, domains, and ports using automated workflows?

At the end of the day, your MDR provider should be able to advise on which areas/processes within your organization can benefit most from automated responses and how threat hunting can be further accelerated by connecting disparate technology solutions so you get the most benefit from your security and IT workflows.

8. Simple Pricing that Works With You

Much like when buying into anything that requires a larger budgetary commitment — and protects what makes your business run — pricing should be transparent, predictable, and customized to your environment. It should be based on:

- The number of assets (workstations, servers, etc.) in your environment
- The expectation there will be continuous, 24/7 real-time alert monitoring
- The expectation there will be a dedicated security advisor as the main POC for technical and day-to-day service delivery
- The expectation the MDR technology will begin learning its way around your systems on day 1 and be able to quickly start threat protection
- Receiving detailed analysis and regular reports with tailored remediation guidance and recommendations

What it shouldn't be based on:

- How many egress points or locations you have — MDR is about monitoring your environment, no matter how big or spread out it is. You shouldn't be penalized for having multiple offices.
- How many servers you have — A threat on an endpoint is similar to a threat on a server. You shouldn't be charged for looking at endpoint threats on different machines.
- How much data you can send to MDR — Detection and response is about finding threats with context and correlation, not charging for collecting events per second. Your MDR provider should want to see the data you have, so make sure that if there is a data allotment it's enough to cover the most important sources used to detect threats.

Key Questions and Considerations

- Does the provider offer volume-based discounts for number of assets?
- Are costs for additional services — digital forensics, major IR engagements, data overage fees — built in or priced a la carte?
- How do they determine the price of their MDR service? What happens if I go over my allotted data limit?

MDR Vendors: Key Questions and Considerations Recap

Cost Justification

- Will your provider be available for non-emergency communication, either by email or phone?

MDR vs MSSP vs MEDR

- How did the attacker get in?
- What tactics, techniques, and procedures (TTPs) did the attacker use?
- Where did the attacker move?
- What credentials were used?
- What data was accessible and/or exfiltrated?
- How should we prevent this type of incident from happening in the future?

Key Capabilities of MDR: Headcount and Expertise

- What is the experience level of the MDR SOC team that will be monitoring my environment?
- What is the tenure and attrition rate of the team?
- How many MDR analysts are assigned to monitor my environment?
- How does the MDR provider ensure 24x7 coverage?
- How does the provider integrate Threat Intelligence into the service?
- What's the process if the MDR provider misses a confirmed breach in the environment?
- Does the MDR provider have in-house, incident-response expertise on staff and ready to take action in the event of a breach? Is there an added cost for this?

Key Capabilities of MDR: Technology

- How does the provider detect threats that bypass preventative controls?
- Will you have full access to the MDR partner's back-end technology?
- If full access is not provided, can you self-service log search and dashboards?
- Can your MDR provider tell if a potential threat is an outside attacker impersonating an employee?
- How does your MDR provider detect if an actual employee is presenting risk, whether through negligence or malice?
- What's your MDR provider's process for detecting and responding to unusual user behavior?
- Can the provider support other assets and environments like public and private clouds (IaaS, SaaS, PaaS), Operational Technologies (ICS/SCADA), and IoT (medical devices, building controls)?

Key Capabilities of MDR: Collaboration and Partnership

- What does the interface look like — both digital and via humans — when customers need to connect with the MDR team?
- Is the MDR team using a concierge model or a SOC squad model?
- How does the MDR operations team plan to scale as the number of customers grows?
- What is the ratio of MDR SOC analysts to customers? Security Advisors to customers?
- How quickly can your SOC team scale up to detect and respond to larger incidents, like a supply chain breach?

Key Capabilities of MDR: Threat Hunting

- Is your provider doing real-time, reactive, proactive, and targeted hunts?
- How often are proactive threat hunts performed?
- What type of reporting is delivered after each hunt?
- When new threats are discovered, how does the team do targeted threat hunts?
- Will the MDR provider assess and alert you to potential look-alike, imposter domains?
- Is powershell activity logged and alerted in real-time, or will it be reviewed after a manual threat hunt?
- Is lateral movement activity logged and alerted in real-time, or will it be reviewed after a manual threat hunt?

Key Capabilities of MDR: Process and Service Expectations

- Does machine learning eventually establish benchmark metrics for detection within your environment that would enable future automated response?
- Would a human be involved in any part of that automated response?
- Is threat intelligence derived from research, previous investigations, monitoring findings, and third-party sources?

Key Capabilities of MDR: Managed Response and IR

- What types of managed response actions can your SOC advisors take?
- How can I deny the containment response if I don't want the SOC team to take action, especially if the action is automated?

Key capabilities of MDR: Security Orchestration, Automation, and Response (SOAR)

- What SOAR workflows are included for me to use?
- Is there an ability to add more automation to expedite my remediation process when MDR finds something?
- In what instances will the MDR service take response action on my behalf?
- Is there an ability to create an exceptions list?
- Will you be able to look up indicator reputation with open-source threat intelligence, kill malicious processes, quarantine infected endpoints from the network, deprovision users, reset passwords, and more — all from day one?
- What about blacklisting hashes or blocking IP addresses, URLs, domains, and ports using automated workflows?

Key Capabilities of MDR: Simple Pricing That Works With You

- Does the provider offer volume-based discounts for number of assets?
- Are costs for additional services — digital forensics, major IR engagements, data overage fees — built in or priced a la carte?
- How do they determine the price of their MDR service?
- What happens if I go over my allotted data limit?

MDR Vendor Evaluation Reference Sheet

- After reading this buyer's guide, you may find it obvious that there are many criteria to evaluate when choosing the right managed detection and response partner for your organization. That's why Rapid7 has compiled this information into a handy, quick-reference sheet.
- You'll find comprehensive considerations and corresponding questions to ask so you'll have confidence that you're able to compare different MDR vendors across criteria to find one that's best for your business.

[Read reference sheet](#)

MDR Power Moves

Security organizations across the globe continue to struggle with headcount and the expertise needed to effectively solve detection and response challenges in today's world. Even in the midst of all this, you should still be able to gain freedom from everyday cybersecurity fatigue, have more time to recharge, and be able to focus more on positive initiatives that help your organization move forward.

- Should your MDR partner tailor their service to your organization's desired outcomes? **Yes.**
- Should they bring a team of detection and response experts that enable you to find and stop threats anywhere they arise? **Yes.**
- And should they partner with you to drive your business forward and mature your security program? **Absolutely!**

More than anything though, your MDR partner's power should be to provide you and your team with the peace of mind and relief that help you all sleep better at night. Managed detection and response is a partnership that should help you achieve successful outcomes. At the same time, it is a significant investment — in budget, time, and resources. But, here's one last question: what is the likelihood that, with the right partner, you can ensure you're able to achieve those outcomes and save money in the long run?

Lots of MDR vendors bring similar solutions, but it's up to you to find the right fit for your business.

About Rapid7 Managed Detection and Response

Rapid7 MDR was recognized as a “Leader” in the 2021 IDC MarketScape U.S. MDR Provider Assessment (IDC #US48129921), The Forrester Wave™: Mid-Size Managed Security Service Providers (Q3 2020), and is a “Strong Performer” in The Forrester Wave™: Managed Detection And Response (Q1 2021). Rapid7 MDR offers:

- Proprietary threat intelligence and research
- Full access to [InsightIDR](#), our industry-leading, unified SIEM & XDR technology
- Behavioral detections for user and host anomalies
- Intruder traps and proactive, human-led threat hunting
- 24x7x365 monitoring, delivered from multiple global SOCs
- A security advisor who acts as your trusted guide
- Incident investigations and Active Response

Customers have full access to the Rapid7 Insight Platform to run their own investigations, create dashboards, and more. All of this, combined with uncapped incident-response hours and uncapped access to your Security Advisor for any questions and security-related collaboration, adds up to a true partnership.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our [website](#), check out our [blog](#), or follow us on [Twitter](#).

[Click here](#) to learn more from a Rapid7 expert. You can also reach out to sales@rapid7.com or call 866.7.RAPID7