RAPID7

2024 EDITION

The Complete MDR Buyer's Guide

Confidently evaluate a Managed Detection and Response (MDR) solution for your security program.

Today's security teams struggle against three outsized challenges: technology, headcount, and expertise. But that doesn't have to be the case. Per Gartner, **60% of all businesses are expected to turn to a Managed Detection and Response (MDR) service to help consolidate** and ultimately extend the capabilities of their Security Operations Centers (SOCs) by 2025. Read on for a deep dive into the how-to of selecting the right provider for you.

Contents

Executive Summary

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

While cyber risk is 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. 75% of teams view the current threat landscape as the most challenging it has been in 5 years, and 52% don't feel they have the tools and people they need to effectively respond.

Cybersecurity has a 0% unemployment rate. For teams that are able to hire, 92% report a persistent skills gap in their team, commonly in cloud security, AI/ML and zero-trust.[1]

Managed Extended Detection and Response (MDR) is an instant extension of your internal SOC team. You'll have 24/7 threat monitoring, extended detection and incident response services, covering native and 3rd party sources technology deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise – all in an effort to extend your team and enable your SOC to more efficiently tackle incident investigation and response.

The right MDR service is a partner that should be able to help you focus on outcomes tailored to your business. They should act as a force multiplier that integrates into your own internal incident response processes. Don't think of it as outsourcing; instead focus on how it can help you tackle record numbers of CVEs, bridge the cybersecurity skills gap, and address an overload of tools and complexity.

This guide will help you understand the top decision criteria and questions to 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 categorical lists of key questions to ask as well as additional tools to help you find the right partner for your business so you can extend the power of your SOC and take command of your attack surface.

[1] ICS2 2023

Cost Justification

Consolidated Managed Services Offer an Affordable SOC Option

In the spirit of transparency, a good MDR provider can cost a lot. But it's a whole lot more economical than standing up your own 'round-the-clock SOC team. Even the most well-heeled security operations struggle with 24/7/365 staffing of a diverse team of security experts.

Building a modern SOC today requires you to go beyond the "core" capabilities. According to Gartner, "Internal SOCs 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 for a bespoke SOC.

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
- The building impact of ransomware that ultimately leaves teams defenseless against the latest attacker tactics, techniques, and procedures (TTPs)

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.[2]

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.

Key Questions and Considerations

- Will your provider be available for non-emergency communication, by email, phone, chat, or otherwise?
- Is the provider able to offer all components of core MDR services, including 24x7 monitoring, detections, investigation, containment, and threat hunting?
- Is the provider able to provide any adjacent services as part of their MDR service, such as exposure assessment, cybersecurity validation, or incident response?

[2] **Gartner. SOC Model Guide.** Collins, Schneider, Shoard. October 19, 2021.

MSSP, MEDR, MXDR, MDR - What do you choose?

Is MDR the right fit? The game is changing.

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. Which path is the right one?

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 consolidated technology will meet your needs.

Managed Endpoint Detection and Response (MEDR) is typically a specific version of a Managed Detection and Response that is focused almost exclusively on endpoint protection, but sometimes can fall short of ingesting telemetry from additional, equally impactful sources such as network, user, logs, and cloud. When assessing MEDR providers, focus on understanding if and how they are able to collect and correlate telemetry from these additional sources.

Managed Extended Detection and Response (MXDR) is a version of a MDR service that extends threat coverage to multiple telemetry sources. Whereas some MDR providers build their service around a core telemetry source, MXDR providers ingest and correlate data from endpoints, networks, identities, the cloud, and more. This comprehensive view of the attack surface helps SOC's accelerate triage, investigation, response, and containment of threats. MXDR providers can either have native visibility into these different sources, ingest and respond to telemetry from other providers, or a combination of both.

Managed Extended Detection and Response (MDR) 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 more intelligent features to address the full attack surface. MDR solutions can include the features such as:

- Threat intelligence and human-led threat hunting
- Security assessment capabilities
- Behavior analytics
- Automation
- Remote containment
- Exposure management
- Digital forensics and incident response (DFIR)
- Next generation antivirus (NGAV)
- Digital risk protection (DRP)
- Ransomware coverage

As you can see, MDR vendors are leveling up their programs' abilities to address more sophisticated threats across the entire attack surface. The effectiveness of solutions that work together to pick up where another has ended – all through a single pane of glass – is helping to extend the SOC's reach and enable faster threat takedowns.

This new generation of multifaceted 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 to ensure stealthy attackers have nowhere to hide.

Key Questions and Considerations

- Which components of a managed service are most important to your organization?
- Is consolidating functionality into a single service a priority? What can be consolidated and what do you want to remain an in-house function?
- What does your existing workflow between detecting and responding to threats look like?
- Where, along that workflow, is most important to augment and reduce overall Mean Time to Respond (MTTR)?
- How would you prioritize extending the visibility and efficacy of your internal security team?

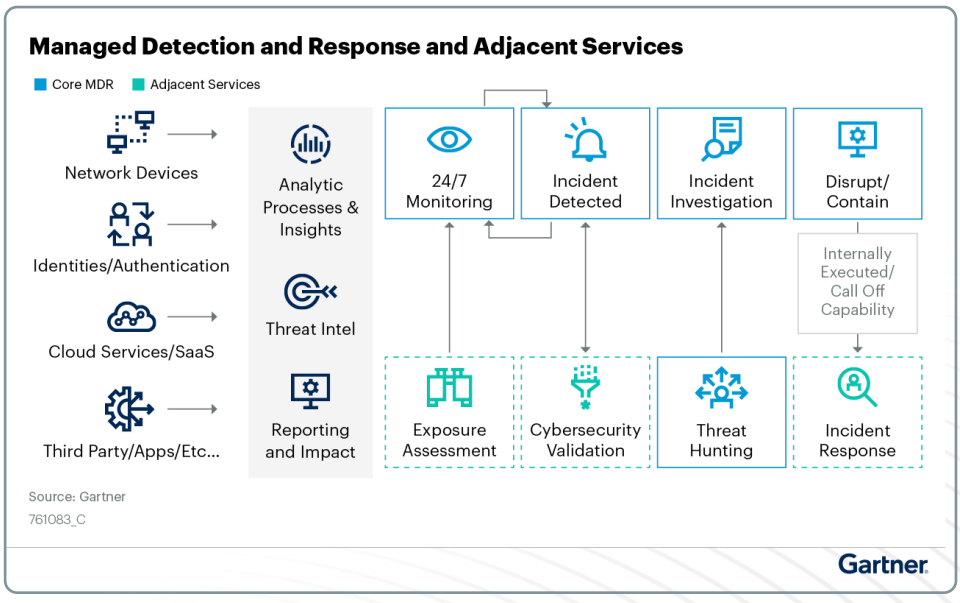
Seven Core Capabilities

Key Capabilities of a Consolidated MDR Solution

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're not capable of collecting and acting on threat intelligence or risk exposure data.
- A recent breach has expedited the need for a managed partner to accelerate their program maturity and coverage.
- They're overwhelmed by alerts and unable to respond effectively.
- They need to comply with cybersecurity or data regulations within their industry.

While these challenges can become a thorn in your side, rest assured, you're not alone. MDR services can help alleviate these issues, but first you must ensure you're finding the right consolidated solution that helps your team command the attack surface and achieve desired outcomes.



As mentioned, MDR service delivery is split into Core and Adjacent capabilities. Gartner says the right MDR vendor will be able to "deliver these capabilities using a variable combination of technologies — these are commonly endpoint- and network-driven, involve cloud services layers, SaaS and custom applications. In addition, connectivity to adjacent capabilities provides contextual information (e.g., identity and user, threat exposure and business-criticality) to improve and validate threat detection. Providers develop threat-focused content and analytics, also known as detection engineering, and apply threat intelligence, whether developed in-house, purchased from third parties or a combination of both approaches. Providers also apply manual/automated disruption and containment activities — such as host isolation, account lockout and network blocking."[3]

But as you've probably seen, almost every vendor claims they are consolidating these many solutions to offer a more empowered MDR program – which is why it's so difficult to begin to tell fact from fiction when launching the search for a vendor. To navigate the crowded market, try to ensure you're evaluating each vendor across seven of the most critical core capabilities:

1. Headcount, Expertise, and Collaboration	• How experienced are the MDR analysts that will work alongside your team? • What do day-to-day and monthly service interactions look like? • What reports, dashboards, and deliverables can you expect as part of your service?
2. Technology	• What level of visibility and detection methods will be used for real-time threat monitoring and investigation? • What technological capabilities does the service provider provision to end users? Are teams able to create custom alerts, run investigations, and pull logs?
3. Threat Hunting	• Will the MDR vendor go beyond real-time threat monitoring to provide proactive, reactive, and targeted threat hunting? • What data does the vendor utilize in their threat hunts? • Are hunts human-led or run through automation?
4. Process and Service Expectations	• How will your MDR provider help you achieve rapid time-to-value and ensure you're progressing over time? • What is the cadence of interactions with the vendor's team?

[3] Gartner. Market Guide for Managed Detection and Response Services. Shoard, Price, Schneider, Lawson, Davies. February 14, 2023.

5. Managed Response and IR Expertise	• How will your MDR provider respond on your behalf, and what happens if an incident becomes a breach? • Do you need an additional retainer with an Incident Response consulting firm? • How will they leverage DFIR to provide advanced attacker analysis?
6. Security Orchestration, Automation, and Response (SOAR)	• Does the provider leverage SOAR to automate their processes, and is there a way that you can leverage SOAR capabilities? • Is the provider able to respond and contain on your behalf?
7. Pricing	• How does the MDR provider price their solution to ensure it's transparent, predictable, and aligned to the value you'll receive? • Is it a truly connected and "consolidated" approach that provides greater value?

1. Headcount and Expertise

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? In most instances, attackers target organizations when they're likely to be weakest, in their off hours. 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. The post-pandemic world still places a premium on security talent – no matter where they're located. Therefore, small-to-midsize companies may not be able to pay ultra-competitive salaries that some world-dominating firms can.

So, if you see a shortage of security personnel now or in the near future, it will become extremely necessary to find value in your MDR provider of choice. If a vendor is focusing solely on your organization's detection-and-response capabilities, you should ultimately experience shorter response times after a detection is validated, especially in an automated-workflow world.

Therefore, it's critical for the specialists you do have to push strategic objectives, implement security best-practices, and build resilience within their organization and overall program.

Expertise

When it comes to the expertise your MDR provider should bring to the table consider this: You wouldn't trust your primary-care physician to do open heart surgery. There are specialists for that.

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 a breach. That's why it's critical to bring in 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 who can respond to incidents. But most are minor incidents. The best MDR providers are staffed with analysts and DFIR experts able to fully respond to major incidents within an organization's environment to fuel faster response and reduce downtime. They have logged thousands of hours of experience handling some of the most advanced data breaches in history.
- **Digital risk protection (DRP)** – This capability extends service beyond the network perimeter or a unique environment, and provides deeper visibility and understanding of threats from around the clear, deep, and dark web. DRP leverages the earliest signals of a targeted threat against an organization – those earliest indicators of someone choreographing an attack against a company – and takes defensive action on a customer's behalf.

Named Security Advisor as Your Main POC

Appointing a security-program advisor as each customer's point of contact (POC) is a main piece of criteria against which an MDRs provider's effectiveness will be judged. 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.

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?
- How does the MDR provider ensure 24x7 coverage? Is it a follow-the-sun model?
- How does the provider integrate threat intelligence into the service?
- What is the process if the MDR provider misses a confirmed breach in the environment?
- 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?

2. Technology

The best MDR services combine deep observation of endpoints, real-time forensics (DFIR), authentication, network, and log data with functionality that tackles rapidly scaling cloud environments and pulls in context from native and 3rd party sources. More recently, experts are extending MDR SOC functionality to tackle rapidly scaling cloud environments. This combined approach is true XDR – a cloud-native platform that enables security teams to optimize threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation.

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

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 (NTA) 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.

When an MDR solution is built on top of native XDR technology, customers get deep visibility into their scaling environments and coverage from advanced threats. It's important to note that increasingly, MDR providers are tasked with understanding customers' risk profiles and remediating – exposures, vulnerabilities, misconfigurations, and more – before an environment is breached.

Key Questions and Considerations

- 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?
- Is there any ability to create customizations within the technology?
- Is there an included or adjacent SOAR tool that allows for custom automation based on your environment's needs?
- 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 internet-of-things (IoT) devices?

3. 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 based on risk analysis and integrated threat intelligence feeds that augment indicators of compromise (IoCs).

A provider should first get to know the ins and outs of your IT and security stacks, then implement a tailored plan that incorporates multiple angles of threat hunting, allowing them to make sure they're hunting through the right information, with the right checks, at the right time to identify undetected, lingering threats. Let's now take a look at different types of threat hunting to ensure a provider is offering in a services package.

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.

Reactive Threat Hunting

4. **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.

5. **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.

6. **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 if your MDR provider fails to tell you which domains are out there in their threat hunt analysis, you could be left to figure this out on your own.

7. **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.

8. **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.

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.

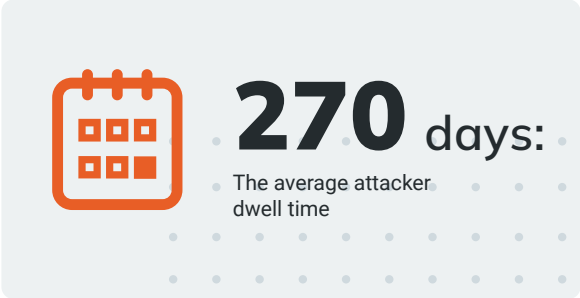
2. **Hypothesis-Based threat hunts** — These should target all available assets, looking for unknowns across the entire environment. When a new threat is discovered — like the Solarwinds hack or the Microsoft 0-day exploit — a provider often will perform retro-hunts in your environment to ensure nothing is exposed and/or TTPs not identified using analytical detections haven't been exploited.

Key Questions and Considerations

- Does your provider leverage the right technology to execute 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?

4. Process and Service Expectations

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



Deployment and Onboarding

Every security organization is different, so it stands to reason that MDR provider onboarding should be customized to each client. Many organizations look for fast time to value, looking for their managed security provider to quickly enable them to deploy the necessary cloud-based or on-prem technologies and begin actively monitoring within the first couple of months of the service. Of course, baselining an environment takes time to best provide actionable insights, but the quicker providers are able to get their new customers into their service delivery the better.

Look for service providers who will start protecting you as soon as you start the process, rather than waiting until everything is complete to begin delivering value. You're looking to buy into a service that extends your team, protects your environment around the clock, and saves you time.

Compromise Assessment

Before you begin your service, understand how your MDR provider will ensure you're not compromised. Otherwise, they could be pointing the finger back at you. A compromise assessment should utilize a similar approach and methodology as threat hunts to spot known and unknown threats in your environment and ensure you're starting out with a clean baseline.

Metrics

To justify your MDR purchase, you'll need more than a brief alert notification when something happens. That's where detailed incident reporting comes in, down to the alerts by disposition, mapping to MITRE ATT&CK Framework, incident rebuilding, timelines, detailed mitigation and remediation recommendations, and detail around

affected assets, accounts, and their relevant IOCs. This provides your team – as well as your C-Suite – the analytics that prove your MDR partner's value.

All this integration and scale adds up to a future where teams feel confident in a consolidated approach from their SecOps partner. The future isn't buying more and more tools – it's your team, supercharged with the right partner to help them succeed.

Key Questions and Considerations

- Would a human be involved in any part of an automated response?
- Is threat intelligence derived from research, previous investigations, monitoring findings, and third-party sources?
- What baseline assessment is done at the start of the service to make sure you aren't already compromised?
- What detail can you regularly expect from the provider after an investigation? How do you receive that information, and at what cadence?
- Does machine learning eventually establish benchmark metrics for detection within your environment that would enable future automated response?

5. 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 two considerations for effective incident response:

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

An effective response should include commanding your attack surface to cut attackers off at both the endpoint and user-account levels, and your MDR provider should be able to 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: "The key value proposition of MDR is the human interpretation of security incidents, providing guidance, as well as performing the initial mitigation steps, that would otherwise be complex to understand and enact. By providing context-led investigation, analysis and threat

validation (and taking action to disrupt or contain an attack), the MDR provider can buy time for the customer to perform further investigation and ultimately remediate discovered issues utilizing their internal standardized response processes."[4]

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 in the event of a breach. No time should be lost when minutes are critical.

Digital Forensics and Incident Response

When something really bad happens, you don't want to be referred down the line to another third-party – all because your MDR provider's SOC "can't handle it." And who wants to deal with fighting for incremental budget for 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 forensic investigation mode once a confirmed breach is detected, particularly if it has affected multiple endpoints, lateral movement is occuring, or there is active data exfiltration.

Continuous Monitoring

In the spirit of assuming full command of the attack surface, the SecOps loop continues unabated. Because after the incident has seen proper response and the investigation has concluded, vigilance must remain. This means continued and always-on monitoring for vulnerabilities as well as regularly enlisting your managed vulnerability management partner to help ensure your resilience isn't revoked. They can do this by accelerating your ability to:

- Discover risk
- Prioritize vulnerabilities
- Remediate accordingly
- Track progress
- Optimize your program

Because after a breach is contained, it's critical to keep proactively closing doors before attackers have a chance to break through.

[4] Gartner. Market Guide for Managed Detection and Response Services. Shoard, Price, Schneider, Lawson, Davies. February 14, 2023.

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, you'll not only have to deal with the damage to your environment and the rippling effects, but those providers will make you jump through 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 their SOC 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?
- Can the provider articulate a top-level before, during, and after attack plan for cyber resilience?
- What types of responses are in-scope for the provider? What will you be on the hook for?

6. Security Orchestration, Automation, and Response

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
- Free up more time by automating tedious and repetitive tasks

As a customer, you should also be able to connect your ecosystem and accelerate operations by quickly leveraging "out-of-the-box" extensions and automated workflows so you can eliminate low-value work. These can typically be found inside your provider's detection-and-response tool and/or extensions library.

Alert Enrichment

Event sources and agent data are great for detections, but the SOC needs as much data as possible so security practitioners can confidently do their jobs. SOAR can automatically enrich the quality of your security alerts with more data and then help analysts weed out false positives and pinpoint real threats anywhere.

Not only is your MDR partner's SOC operating at optimal speed and with the right context using SOAR enrichment and AI-added context, but their deliverables to you (the incident reports) are stronger and more detailed.

Threat Response

SOAR 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 out-of-the-box SOAR workflows are included? • Is there an ability to add more automation to expedite my remediation process when MDR finds something? • What role does artificial intelligence play in the MDR provider's automated responses? • 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, quarantine infected endpoints from the network, deprovision users, 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. They should be able to demonstrate how threat hunting can be further accelerated by connecting and consolidating disparate technology solutions so you get the most benefit from the provider's security and IT workflows.

7. 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 one and be able to quickly start monitoring and 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 — vulnerability management, digital forensics, major IR engagements, data overage fees, SOAR — 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 MDR partner. That's why we've compiled it all into a handy, quick-reference sheet so you can get to the decision-making part faster.

Get reference sheet

MDR Power Moves

Security organizations around 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, a consolidated MDR solution should be able to extend your SOC capabilities so that your team can gain freedom from everyday cybersecurity fatigue, have more time to recharge, and be able to focus more on positive initiatives that help the organization move forward.

- Should your partner tailor their service to your organization's desired outcomes? **Yes.**
- Should they extend your SOC with 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!**

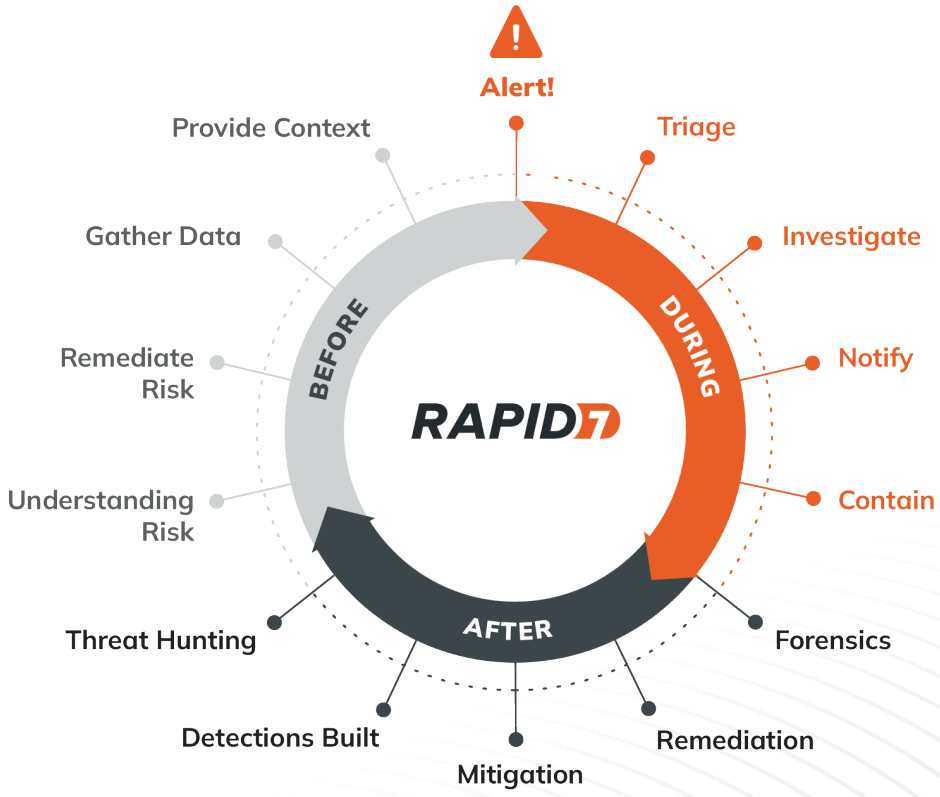
At the same time, MDR is a significant investment — in budget, time, and resources. But, here's one last question: What is the likelihood that, with the right partner, you can ensure you're able to achieve successful outcomes and save money in the long run?

Lots of MDR vendors bring similar solutions, but it's up to you to find the right fit that can provide your team with peace of mind and better sleep at night.

Consolidate Threat Coverage with Rapid7 Managed Threat Complete

Standing up an effective detection and response program isn't as simple as buying and implementing the latest security products. It requires a dedicated SOC, staffed with highly skilled and specialized security experts that are harder-than-ever to source and hire. It also requires 24x7x365 vigilance. Creating this kind of program in-house can be expensive, complex, and difficult to maintain.

Rapid7's Managed Threat Complete is an MXDR service that delivers the most effective detection and response and vulnerability management capabilities – all in one program. With native and 3rd party visibility into extended environments, organizations get true context and correlation of malicious activity across their attack surface. Managed Threat Complete enables teams to shrink the attack surface by consolidating, simplifying, and reducing security workloads, so they can focus on strategy as well as mission-critical efforts. Experience the full threat-protection lifecycle:



BEFORE

Mitigate Risk and Contain Impact

- Unlimited Vulnerability Scanning
- Visibility into Internal, & External Environment
- Digital Risk Protection
- Threat Hunting
- Next-Gen Antivirus and Ransomware Prevention
- Security Posture Assessment
- IR Planning and Readiness Assessment

DURING

Rapidly Identify and Contain

- 24x7x365 Elite SOC Monitoring
- SIEM Tooling & XDR Coverage
- Unlimited Incident Response
- Robust Detections Library
- Forensic Investigations & Reports
- Active Response for Remote Containment
- Unlimited Data Ingestion, 13 Month Retention

AFTER

Eradicate and Build Resilience

- Remediation and Mitigation Guidance
- Detailed Monthly Reporting
- Ransomware & Data Leakage Monitoring
- Strategic Security Program Advisory
- Built-in DFIR Tooling, Velociraptor
- Monthly Security Posture Reviews
- Critical Security Controls Assessment
- Executive Trend Report & Readout

Gain full command of your attack surface with Managed Threat Complete.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. In recognition of this, Rapid7 was recognized as a "Strong Performer"in the The Forrester Wave™: Managed Detection And Response (Q2 2023). Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web.

We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.