RAPID7

SERVICES GUIDE

The 10 Things Your MDR Service Must Do

When assessing Managed Detection and Response (MDR) vendors, we recommend evaluating each based on 10 tactical prescriptions for what a provider should be able to offer your business:

1. Deep observation of the endpoint in real time

Whether these are workstations, laptops, servers, or cloud assets, few significant breaches occur without attacker activity on the endpoint. The best MDR services combine deep visibility at the endpoint, including real-time forensics capabilities with authentication, network, and log data. WIthout leveraging the endpoint agent, it's impossible to see start/stop processes and correlate notable events to determine if there's anomalous activity indicative of an attacker.

This doesn't mean EDR is always the answer; it takes a combination of User Behavior Analytics (UBA), Endpoint Log Analysis, and Attacker Behavior Analytics (ABA) to correlate and detect attackers with higher fidelity.

MDR services that only place sensors on the endpoint will not only miss attacks, but they'll lack context on "who does what" in the company. Unlike your internal team, third-party analysts don't know who's regularly on the road or who requires anomalous privileges for their job. For example, employees may need to expose themselves to interesting extensions when delivering webcasts with third-party providers. This would be a less-than-ideal time for their asset to be "contained" mid-demo.

The job of your MDR provider is to tell you exactly what happened, including:

- How did the attacker get in?
- What tools did the attacker use?
- Where did the attacker move to?
- What credentials were used?
- What data was accessible?
- What data was stolen?
- Is the attacker still in the environment?
- What specific steps can you take to remediate?
- What can you do to prevent these kinds of attacks from happening in the future?

While some of the above can be answered with network data, thoughtful endpoint data collection captures authentication, file system, process execution, and forensic artifacts critical across the entire incident response lifecycle.

How Rapid7 MDR does it:

Our Insight Agent securely streams endpoint data to our Insight cloud to run analytics detections. With close attention to running processes (especially parent-child relationships) and anomalous behavior on the asset, this produces faster and stronger detections and thorough incident investigations. We also pair your team with an assigned Customer Advisor, who promptly notifies you of malicious findings. MDR triages any investigations beforehand so you only are alerted to the incidents that require action.

2. Ingestion of network device data

Having endpoint visibility does not mean analysts should not value the information from netflow or network device data. On the contrary, attackers will inevitably use the network in their attack. Network data is lightweight, easily searchable, and can quickly identify the exact location of an attacker throughout the network to identify the scope of the breach. Leveraging this data allows analysts to take action and understand what's going on across the network layer, while correlating events to the endpoints.

How Rapid7 MDR does it:

The MDR SOC leverages this information to correlate network data to endpoint data against processes and actions on the endpoint. Our agent sends network level activity on the host to the Insight Cloud; we analyze process level and network connections, correlate these with firewall events to see if it was accepted or blocked, and assign a severity to the event. This gives our analysts more data points and evidence to understand if a connection is malicious, for example, malware calling an external IP address.

3. Ingestion of security device data

By the time you're ready to invest in an MDR service, you've likely already invested in a number of different security tools aimed at preventing threats and detecting breaches. The best MDR providers will want to use that data as part of delivering the service. More data means more visibility, more ways to validate threats, and more ways to track attackers.

How Rapid7 MDR does it:

Rapid7 MDR is able to reuse existing security technology investments to gather more, and deeper, logs and event data into activities across the user, endpoint, network, and application layers. This allows our team to perform further analysis than what is solely enabled by the Insight Agent.

4. Ingestion of cloud service data

The modern network extends beyond your perimeter. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) are now the norm for the modern enterprise. To complicate things, your users are mobile, working remotely, and traveling while using traditional remote access solutions (in addition to modern cloud-based services). Your MDR provider must be able to identify and respond to threats regardless of where these threats are materializing.

How Rapid7 MDR does it:

Your operating footprint has moved outside of the traditional four walls. Any vendor you choose must adapt at a similar pace. Our MDR service is designed to monitor your expanding enterprise network, including data, applications, and endpoints—wherever they are. With many businesses moving data to the cloud, it's important for your MDR vendor to find threats wherever the data lives.

5. Ingestion of authentication data across local, domain, and cloud sources

There isn't a single threat or breach that doesn't involve attackers using legitimate credentials to cause harm. Unfortunately, our credential footprint has grown beyond the traditional local accounts and directory services to online service accounts, SSO, and other web-based authentication mechanisms. The best MDR providers are not only equipped to detect authentication regardless of where they occur, but also possess the intelligence and visibility needed to detect when an attacker might be looking to compromise those credentials through social engineering.

How Rapid7 MDR does it:

Many traditional SIEM solutions claim to utilize User Behavior Analytics (UBA) detections, but SIEM engines aren't built for real-time attribution. Users and assets constantly move around in a modern network architecture, leading to an engine that cannot accurately map events to entities. This requires more than out-of-the-box detections: It requires advanced analytics and human threat detectors.

Our team is able to leverage real-time attribution from these UBA indicators within InsightIDR to more easily determine if a potential threat is an outside attacker impersonating an employee or an actual employee who presents risk, whether through negligence or malice. UBA utilizes our purpose-built proprietary attribution engine to detect behaviors indicative of true threats, while sorting out users who may be doing unusual tasks but are not actually compromised. This enables our team to connect network activity to a specific user, as opposed to an IP address or asset, to detect compromised credentials, lateral movement, and other malicious behavior. This combination allows the MDR analysts to dynamically prioritize and rank alert criticality by:

- **Detecting unknown threats** based on single occurrences, or groups of notable events based on specific user behaviors or deviations from known-good baselines.
- **Detecting insider threats** based on groups of notable events describing the sequence of events typically associated with information theft by an authorized party.
- **Associating user behaviors** based on notable events with alerts and investigations to improve the validation and investigation analyst workflows.
- **Providing the data and evidence needed** to associate technical analysis with human behaviors for threat reporting.

6. Multiple threat detection methodologies, including deep analysis on attacker behaviors

Threats and attackers come in all shapes and sizes, and each type of threat and attacker requires different ways to detect and respond. Common threats that affect every business require up-to-date and well-managed threat intelligence to quickly identify and remediate. Targeted attacks perpetrated through sophisticated attackers require equally adaptive detections as their tools will be unknown to the threat intelligence industry. The best MDR providers use a combination of threat intelligence, User Behavior Analytics, Attacker Behavior Analytics, and human threat hunts to provide detection for threats and attackers.

How Rapid7 MDR does it:

Rapid7 MDR's layered Attacker Behavior Analytics (ABA) and highly skilled SOC analysts clear the fog around attacker techniques. The information we see from our honeypot network (Project Heisenberg) and our hundreds of MDR customers is infused with context from our threat intel teams and ultimately formed into proactive detections that help us differentiate unusual admin activity from attacker activity.

For example, when Rapid7 MDR adds ABA against real-time endpoint data and combines that with UBA information, we understand who logged on to a system, their location, and the specific actions taken. Furthermore, Rapid7 MDR is able to look much earlier in the attack lifecycle to find scenarios where:

- **Log collection and endpoint event analysis is required** from the most critical systems/applications (including systems and apps outside of the traditional network, such as cloud services) and your existing security technology.
- **Efficient detection** of malicious tools, tactics, and procedures requires visibility across the entire attack lifecycle.
- **Attackers hide** behind routine actions on the machine where it's necessary to leverage start/stop process data to correlate events to uncover malice.
- **Attackers impersonate** one of your employees.

Why does this matter?

- **High-fidelity alerts grant context to take action**: Alerts include context from our analysts and threat intel teams, so you can make better decisions, remediate the problem, mitigate risk, and contain the alert from directly inside your Findings Report.
- **Detections based on behaviors, not signatures**: By leveraging InsightIDR and top security experts, your team can feel confident that we're able to detect attackers with high-fidelity endpoint data to identify novel variations of new attacker techniques.
  Found once, applied everywhere: Your security team gets the benefit of the learnings from Rapid7 customer detections. For example, when our SOC team finds new attack methodologies—either by way of our SOC, threat intelligence team, or Rapid7 research—those TTPs are updated in InsightIDR investigations.
- **Speed**: By including ABA as a threat detection methodology, Rapid7's threat intelligence team can quickly develop new rules for emerging attacker behavior, and push detections out within minutes of discovering a new technique or trend.
- **Defense-in-Depth**: UBA is adept at identifying breaches in the "lateral movement" phase of the attack chain. ABA allows us to detect attacker activities in all other phases of the attack lifecycle.
- **Constantly evolving ABA detections**: Whenever possible, the alert will detail known, recent adversary groups using a similar technique in a confirmed attack. As a key advantage of our cloud deployment model, our detections are updated automatically to our entire user population of customers after a thorough prototyping, testing, and validation process. All new indicators are applied to one month's historic data so your environment is instantly protected.
- **Context**: Indicators of attack are now surfaced on the InsightIDR visual timeline along with unusual behaviors. This combination makes it even easier for the Rapid7 MDR SOC (or your team) to perform investigations and have confidence in the results of the Findings reports.

7. Threat validation and reporting

Engaging a managed security service provider—either a traditional MSSP or MDR provider—should never involve wasting your time. When you've decided to partner with a provider to manage your threat detection and incident response program, the last thing you want is hundreds of reports a day to become more overwhelming than the alerts themselves. The best MDR providers perform alert validation up front to minimize the number of false positives in order to accelerate alert validation. Reports should provide a high level of detail to determine validity of the findings, as well as concrete steps to remediate. At the end of the day, you shouldn't pay for a list of things that you must validate before you figure out what's actually important.

How Rapid7 MDR does it:

Rapid7's global MDR SOC teams are composed of security experts with unparalleled experience—both red team and blue team—who use this in-depth knowledge of attacker tools, tactics, and procedures to catch malicious activity early in the attack lifecycle and validate each potential threat. Each of our SOC analysts acts as an extension of your security team and tailors the MDR service specifically to your industry and your business. This includes threat hunting, validation of threats, and guidance (e.g. containment, remediation, and mitigation recommendations) for only true threats. Once alerts are investigated and verified, our SOC analysts produce a Findings Report delivered via the Customer Services Portal (with alerts via email or phone call, per the customer's request). This report provides a summary of the incident with detailed evidence of the threat, recommended containment actions, remediation guidance, and mitigation recommendations. You'll be able to quickly see the problem, its importance, and the solution.

8. Incident response support

Having the best threat detection methodologies, a streamlined and efficient process for validating threats, and a rock solid reporting standard may still leave you open to unexpected costs. The best MDR providers will also bundle a certain amount of incident response hours to assist you in your time of greatest need. The worst thing to hear after "you have been breached" is "you have to pay us extra to continue the investigation" to resolve your worst nightmare.

How Rapid7 MDR does it:

At Rapid7, we consider our managed services customers as much more than customers: you're our partners. It's our commitment to help you protect your business against attackers and breaches. That's why we include a number of Remote Incident Response hours in each MDR contract, just in case something happens. In the event of a validated breach, MDR customers will have the option to exercise up to a maximum of 60 Remote IR engagement hours included in the MDR service per year. This includes remote technical analysis and incident scoping, daily reporting, and conclusion report of the breach and our findings.

9. Assigned analysts and security program advisors

Every organization is unique with different goals, different technologies, different missions, different security program maturities, different staffing models, and different incident detection and response program needs. The best MDR providers know this and tailor the solution delivery to meet the customer needs. To achieve this, SOC analysts should be assembled into teams (pods) and assigned customer clusters so that they learn about the technology and user environments over time. Additionally, the best MDR providers provide security program advisors that learn about their customers, their goals, and their limitations so that only the best and most effective guidance is provided to remediate against threats and build up the security programs.

How Rapid7 MDR does it:

We believe our analysts get better at their job the more they know about each customer's specific environment. That's why we assign analyst pods to specific customer clusters, so each environment is deeply understood by a group of analysts—not just one member of the team. We believe the more our analysts know about you and your environment, the better they will be at supporting you with the recommendations that you need.

10. Automation and orchestration

Even the most adept security teams with the best-in-class MDR provider need ways to respond efficiently to security threats. And while today's security organizations continuously procure new, best-of-breed software to bolster their programs, many teams often tell us that they struggle to integrate their security tools. As a result, context switching between a large toolset begets inefficient utilization of man-hours and underutilization of tools. What's more, traditional MDR providers do nothing to operationalize a security organization's stack and often rely on users to take recommendations and remediate on their own. Because every second between a finding and closure risks a growing blast radius, it is crucial that MDR providers integrate automated incident response processes so action can be taken to quickly mitigate and remediate threats leveraging existing tools.

How Rapid7 MDR does it:

Since Rapid7 MDR customers have full access to InsightIDR, customers can leverage the automated workflows built inside the tool—accessed directly from the MDR Findings Report—to take containment actions instantly. These automation workflows streamline response and eliminate repetitive, low value work. For example, through InsightIDR, you can kill malicious processes, quarantine infected endpoints from the network, deprovision users, reset passwords, and more, from day one.

For more bespoke use cases, Rapid7's InsightConnect SOAR solution expands this ability, allowing users to automate additional tasks. InsightConnect extends automation abilities to allow users to build workflows leveraging over 290 plugins for well known and oft-used security tools, as well as create custom integrations. In this way, time to response is minimized and you can sleep easy knowing that applying recommendations is as easy as a simple deployment of pre-built workflows.