Quick Answer: What Key Questions Should I Ask When Selecting an MDR Provider?

Published 10 November 2021 - ID G00753739 - 7 min read

By John Collins, Andrew Davies, **and 1 more**

It is critical to ask questions that reflect key requirements when engaging a managed detection and response service provider. Security and risk management leaders should use this research when evaluating and procuring MDR services.

Quick Answer

What key questions should I ask when selecting an MDR provider?

The number of MDR service providers, and range of styles, continues to increase, causing challenges for buyers who are unprepared for the evaluation, proof of concept (POC) and selection process activities. It is therefore essential that security and risk management leaders define and document the desired outcomes of the necessary requirements and the expectations before engaging providers, especially factoring in the needs of their internal incident response capabilities.

Many buyers struggle to formulate effective RFPs that can solicit relevant information from providers to help in the initial evaluation and down-select process. Therefore, it is critical that buyers construct the must have, should have, could have and won't have (MoSCoW) framework. Using these criteria will ensure they are able to effectively make selection choices based on genuine business needs.

Once these requirements are defined and documented, leverage the following critical questions and factors when evaluating MDR service providers. This is not an exhaustive list of questions and evaluation criteria. However, knowledge of these questions and answers is key before engaging with a provider.

Questions to ask yourself to prepare for buying MDR services:

- Are we looking for providers that can improve our incident response capabilities?
- What business risks and threats relating to security are our highest concern or priority?
- Do we require the MDR provider to bring its own tech stack? Do we want it to use ours? Do we want it to use a mix?
- Do we have use cases specific to our environment that the MDR provider needs to accommodate?
- What is our use of OT environments and/or cloud services, like cloud infrastructure and platform services (CIPS) and software as a service? How might these impact the scope and coverage required from an MDR provider?
- What geographies do we need the provider to operate in, and where does data need to be located?
- Are there specific languages we need the provider to support?
- What functionality do we anticipate needing via the provider's portal?
- Do we need the provider to ensure service continuity, recovery and resiliency of its operations?
- Do we have effective internal incident response processes and procedures for a service to integrate with?
- Do we have effective internal incident management tooling to allow us to record, measure and improve how we respond to incidents?
- What other security services might be required in the future, and will the MDR provider be able to support them (for example, vulnerability management, cloud security, digital forensics and incident response, log management)?

Questions to ask MDR service providers:

- How good is the provider at detecting threats that have bypassed existing, preventative controls? Is there a dependence on third-party tools to provide the alerting/detection?
- What types of response are provided as a component of the MDR service, and what is the limit of those response activities?
- How are response actions managed? Does the provider have a change authorization process and tool that needs to be integrated, and can the provider support that integration?
- What communication mechanisms are available and permitted with the provider's analysts (for example, chat, email, phone)? Are there limits to levels of communication/support?
- How does the provider price its services? Are they ala carte or available as bundles? For example, is threat hunting included in the core service or available as an add-on at additional cost?
- How does the provider define threat hunting, and what is its process for finding unknowns, even to them, in the environment? (see Are You Getting What You Thought From Outsourced Threat Hunting?)
- Are additional services available, like digital forensics and major incident response (on-site and/or remote)? Are they included or available as a retainer agreement?
- What is the provider's support for other assets and environments like public and private cloud (CIPS, SaaS)?
- Does the provider offer access to data (logs, alerts, incidents) in a format that could be leveraged for compliance reporting use cases?
- How is the data that is collected and used by the provider secured? How long is it retained?
- How does a customer get its data returned at contract termination, and is there an attestation by the provider that it has removed/returned all the data in its possession?
- How is scaling of the service managed? Can it scale down as well as up?
- What remedies are available if SLAs (if they exist) are not met, or services are not delivered as contracted or do not meet expectations?

More Detail

Selecting an MDR service provider to obtain modern SOC services can be a challenging process that requires the appropriate planning and evaluation processes before, during and after an agreement. Gartner clients face several unique challenges when evaluating and implementing MDR services. The MDR market is quite dynamic, with an increasing number of providers to choose from, which makes identifying, evaluating and selecting a provider difficult. Effective and well-defined evaluation and selection criteria are essential.

The relative newness of the MDR market (at least compared to the managed security service market, which has been around for more than 20 years) presents risks that need to be considered and addressed, but tend to be overlooked by first-time, and even experienced, buyers in the market.

To be successful with outsourcing MDR services, organizations must define and document requirements and use cases before engaging with providers.

Figure 1 describes how MDR service buyers should approach their evaluation and selection process, whether it's for an initial MDR service engagement or for changing providers. The questions provided to support the development process were identified through hundreds of inquiries with Gartner clients over several years.

Figure 1: MDR Buying Approach

Steps for Evaluating and Procuring MDR Services

Source: Gartner
753739_C

Gartner

Define and Document the Desired Outcomes From Outsourcing to an MDR Provider

Organizations are recognizing the need to implement and enhance their threat monitoring, detection and response capabilities; however, prior to engaging with service providers, many still struggle to properly define and document their desired outcomes. While this is true for most security monitoring services, it is especially pertinent when contracting services such as MDR, as they can be far less flexible when it comes to meeting custom requirements. For example, a limited number of EDR solutions is likely supported or the provider may mandate its own technologies be deployed to get services. The process for scoping use cases and requirements, and assessing MDR service offerings, often includes a negotiation and evaluation exercise where a "best match" and "ideal partner" is identified. Prior to starting any outsourcing initiative, requirements need to be documented and ratified (and continuously updated post onboarding), or else the old adage of "garbage in, garbage out" is likely to be realized.

Defining the steady state after outsourcing to an MDR provider need not be complicated. The process should involve the appropriate stakeholders in the decision making and management of the service. They should brainstorm what the ideal future state or outcome looks like in a few sentences that follow a structure such as who requires the monitoring, the coverage period (e.g., 8/5, 24/7), environments to be monitored, highest-priority threats, style of response, required complementary capabilities and technologies, and the goals to be achieved via the engagement.

For example:

"Our organization, consisting of the parent holding company and all of its subsidiaries, is targeting the following outcomes upon agreement and implementation of services and associated technology from the provider selected as part of this effort. We will have 24/7 monitoring of threats against our organization across all sites and environments, including on-premises assets, critical SaaS applications and services delivered from public cloud service providers (both IaaS and PaaS). Additionally, we will have improved capabilities that allow a threat that is able to infiltrate our environments to be contained or disrupted within minutes of detection to mitigate the impact from that threat. This will allow us to improve both our mean time to detect (MTTD) and respond (MTTR), reducing the risks from all forms of external threats (opportunistic, cybercriminal and nation states). Finally, we will have

access to a central log repository for all data from our environments that will aid our, and the service provider's, ability to triage incidents, especially those where having the capability to look back across our logs to uncover undetected threats as new information and intelligence arises."

Once this has been achieved, the use cases aligned to this outcome can be identified and specific requirements of the service provider can be documented. These requirements will feed into any RFI, RFP and POC/proof of value (POV) activities. The following research should be used when evaluating MDR providers:

- What Makes a Successful Security Service RFP?
- Successfully Align Your Threat Detection and Incident Response Requirements to Your Service Providers
- How to Deploy Foundational Threat Detection and Response

Recommended by the Authors

Market Guide for Managed Detection and Response Services

How and When to Change Your Managed Security Service Provider

Evidence

This research is based on existing Gartner research, client interactions and vendor briefings with Gartner.