eSENTIRE

20 Questions To Ask When You're Evaluating an MDR Provider

Discerning fact from fiction in a confusing marketplace

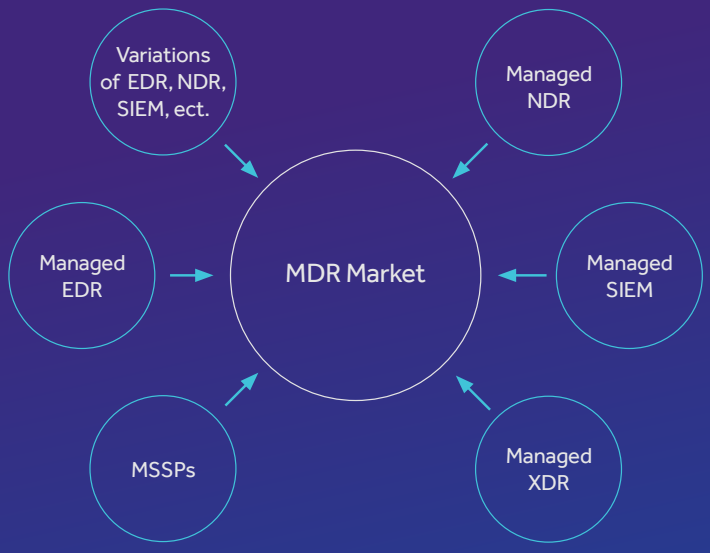
In the latest Managed Detection and Response (MDR) market guide, Gartner estimates there are now over two hundred organizations delivering MDR services globally.

Emerging from the traditional Managed Security Services Provider model in the early 2010s, MDR represented a tectonic shift from an alert-driven to response-driven service model. Acknowledging that attackers were not only increasing in sophistication but in the speed with which they could accomplish their objectives, MDR sought to help under-resourced security teams identify advanced threat actors and stop them before they could cause irreparable damage.

> Security leaders are increasingly cognizant that reducing the time to detect a threat is meaningless without a corresponding reduction in the time to respond to a threat to enable a return to a known good state.
>
> - Gartner 2021

Fast forwarding to the present day, the need for MDR services has exploded as organizations continue to be under-resourced while struggling to protect a growing attack surface.

While MDR growth has been good for the evolution of cyber security, the increasing number of organizations jumping on the MDR bandwagon has led to confusion and risk for unsuspecting buyers. Recognizing lucrative opportunities in the MDR market space, MSSPs adjusted their marketing with clever claims that masquerade traditional alert-based services as MDR. In addition, the growing varieties of true MDR providers has led many organizations to ask themselves:



"What is MDR and how do I select the right provider for my organization?"

As the market continues to take shape, five recurring and measurable components have emerged that are applicable to the challenges Managed Detection and Response Services address:

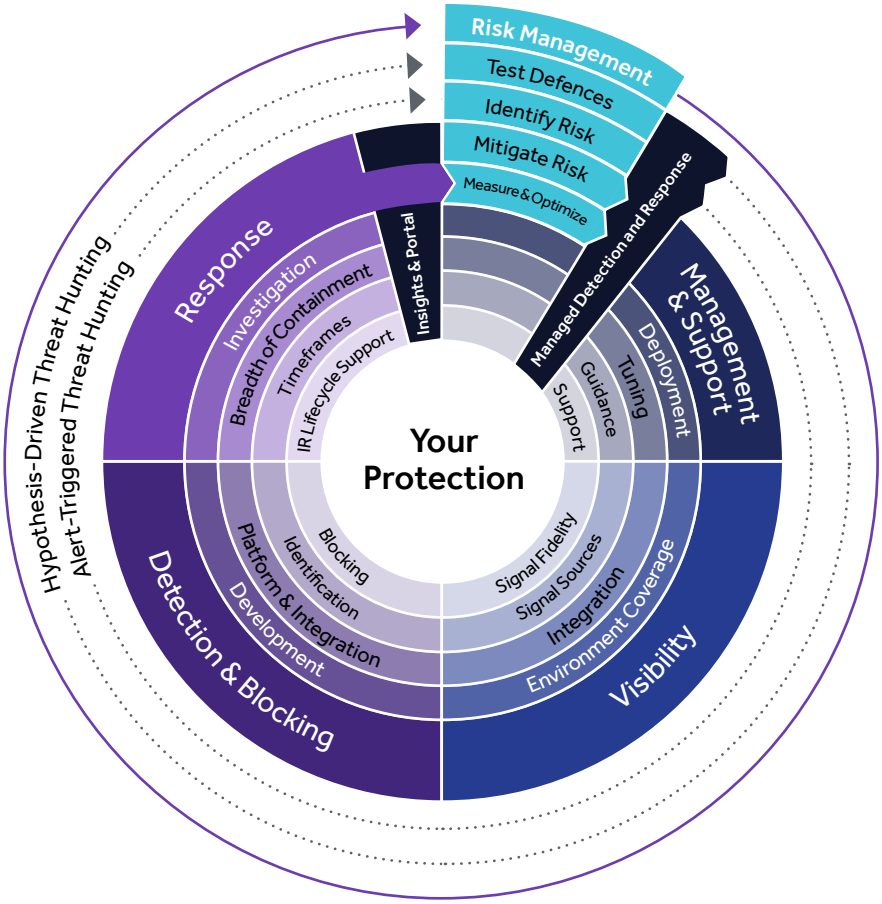
How does the provider identify risk, improve resiliency and optimize MDR accordingly?

How does the provider alleviate complexity and resource constraints?

How does the provider integrate with existing and future environments and what can they see?

How does the provider detect the latest threats?

How does the provider minimize dwell time and support incident response?



These questions, aligned to macro level outcomes, are applicable to any MDR provider regardless of the variation of MDR they deliver.

We recommend supporting these questions with the critical follow ups outlined below to ensure any MDR provider you are evaluating can produce the outcomes your organization is looking to achieve.

The 20 questions here should serve to qualify or disqualify a potential vendor from consideration in relation to their ability to deliver against your unique Managed Detection and Response requirements:

Question	Expected Outcomes
Can you test the efficacy of my current defenses?	Identifies gaps in prevention and detection capabilities before attacks do
Can you systematically identify risk?	Identifies systemic weaknesses and roadmaps improvements that harden your security program over time
Can you operationalize MDR contextual to that risk?	Implements MDR against your identified areas of greatest risk, not just blindly placing MDR anywhere across your environment
Can you measure the efficacy of MDR and optimize against my business changes?	Ensures services deliver on targeted outcomes and adapts protections that keep pace with your business requirements

Question	Expected Outcomes
Do you deploy the technology and get us operational quickly?	Removes the burden of deploying and optimizing technologies so you get rapid return on investment
Are you continuously tuning and maintaining contextual awareness?	Alleviates complexity and resource drain while ensuring protection is optimized for your environment
Are you providing guidance on tool/ service efficacy?	Optimizes services based on your security events with supporting recommendations that harden your environment against further attack
Are you supporting my security team in a timely manner?	Ensures your security team has the support it needs when it needs it from SOC, Customer Success, Support etc. Confirm the wait times and communication process
What is the extent of your coverage across cloud, on-premise, users, etc.?	Delivers comprehensive visibility across your growing attack surface and users
How do you leverage my existing tech?	Derives value out of existing security investments that enhances visibility into your environment
What signals can you pull from the environment?	Provides critical threat visibility into different layers of your attack surface
What depth of information are you using from the signals for detection and investigation?	Performs deeper investigations that leads to discovery of advanced and elusive attackers
How are you developing detections that exceed commodity threat intelligence?	Ensures your environment is protected against the latest attacker tactics and techniques
How are you rapidly integrating detections into a platform that can correlate information?	Correlates disparate information from your network and users that facilitates discovery of advanced and elusive attackers
What methods are being used to identify potential threats?	Puts your organization on the cutting-edge of threat detection leveraging methods that exceed the limitations of signatures and IoCs
How are you blocking known threats that are identified?	Automatically stops attackers from gaining an initial foothold within your environment
To what degree are you investigating potential threats and confirming presence?	Verifies attacker presence and root cause without the false positives that would normally consume your security team
How and where are you able to contain threats on the customer's behalf?	Stops attackers earlier in the kill chain preventing lateral spread
How quickly are you triaging, investigating, alerting and responding	Minimizes the time attackers can dwell within your network and achieve their objectives
To what degree do you support the Incident Response lifecycle?	Alleviates the need for costly incident response retainers and boots on ground Incident Response engagements

Question	Expected Outcomes
How are customers able to derive insights from the MDR service?	Delivers easy to consume information on security events, system health and security posture for your security team
To what degree are insights able to convey value from the MDR service?	Delivers Executive level reporting and insights that justifies MDR spend and return on investment
How do you comprehensively conduct reactive threat hunting?	Rapidly detects and contains attackers that bypass your security controls before they can accomplish their objectives
How do you proactively hunt threats across the customer's environment?	Discovers and stops attackers that have previously established a foothold within your environment

While these questions do not cover every facet of consideration for MDR vendors, they should provide the basis for desired outcomes and critical criteria for vendors that could meet your specific requirements. Organizations considering a Managed Detection and Response provider are encouraged to ask for customer references, visit in person or participate in virtual Security Operations Center tours, participate in demonstrations of delivery in real-world scenarios and poll peers as well as industry analysts for experiences with vendor satisfaction.

To learn more about eSentire Managed Detection and Response, and how we can protect your organization from business disrupting threats, connect with an eSentire security specialist today.

Contact Us

If you're experiencing a security incident or breach contact us  **1-866-579-2200**

eSENTIRE

eSentire Inc., is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Thre at Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.