GUIDE

Questions To Ask When You're Evaluating an MDR Provider

Discerning MDR fact from fiction in a confusing marketplace

Emerging from the traditional Managed Security Services Provider model in the early 2010s, MDR represented a tectonic shift from an alert-driven to a 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.

Fast forward to present day, as organisations continue to be under-resourced and struggle to protect a growing attack surface, the need for MDR services has exploded. There are now 600+ providers who claim to offer MDR services.

While MDR growth has been good for the evolution of cybersecurity, the increasing number of service providers jumping on the MDR bandwagon has led to confusion and risk for unsuspecting buyers. Recognising lucrative opportunities in the MDR market, MSSPs adjusted their marketing with clever claims that masquerade traditional alert-based services as MDR. In this saturated market, many vendors overpromise and under deliver on security outcomes.

The growing varieties of true MDR providers has led many organisations to ask themselves:

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

Real Managed Detection and Response addresses five measurable components of your protection:

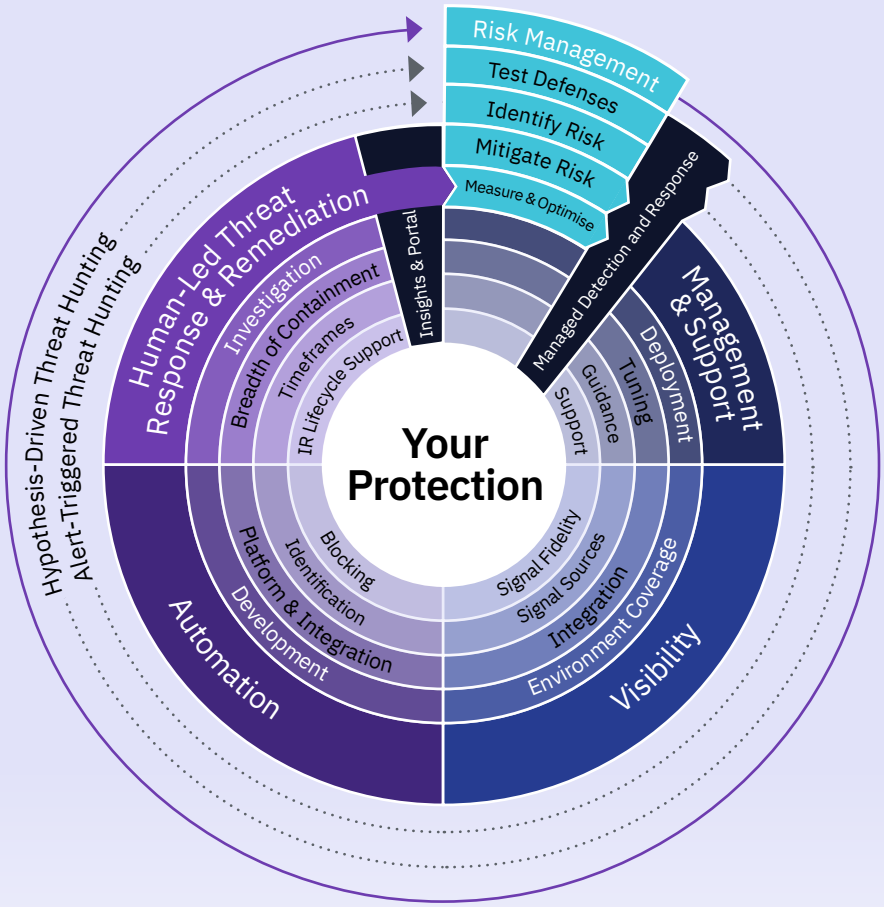
How is my provider leveraging data and lessons from ongoing MDR operations to reduce my risk over time?

How does the provider alleviate complexity and resource constraints?

How is my provider accounting for sensitive data and potential blind spots?

How many threats am I able to automatically block?

How fast is my provider able to investigate, respond and remediate identified threats?



These questions, aligned to macro level outcomes, are applicable to any MDR provider regardless of the variation of MDR they deliver. As a result, you should be confident that your MDR provider and by extension, your organisation, is keeping up with the evolving threat landscape.

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 organisation is looking to achieve.

The following 20+ questions should serve to qualify or disqualify a potential vendor from consideration in relation to their ability to deliver against your unique MDR requirements:

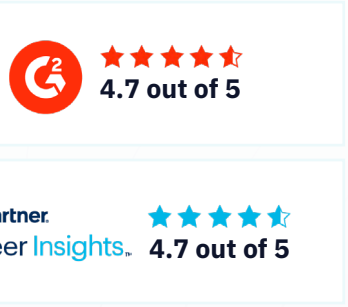
Question	Expected Outcomes
Can you test the efficacy of my current defenses?	Identifies gaps in prevention and detection capabilities before attacks do.
Can you systematically identify risk?	Identifies systemic weaknesses and roadmaps improvements that harden your security program over time.
Can you operationalise 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 optimise 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 optimising 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 optimised for your environment.
Are you providing guidance on tool/ service efficacy?	Optimises 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 organisation 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?	Minimises 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 that could meet your specific requirements.

Organisations considering an MDR provider should ask for customer references, conduct an in-person, or participate in a virtual, Security Operations Center (SOC) tour, participate in demonstrations of delivery in real-world scenarios and poll peers as well as industry analysts for experiences with vendor satisfaction.



eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organisations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organisation's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organisations with 65% of its global base recognised as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organisations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.