UnderDefense
CYBERSECURITY

Managed Detection and Response Buyer's Guide

Essential questions you should be asking when evaluating MDR solutions

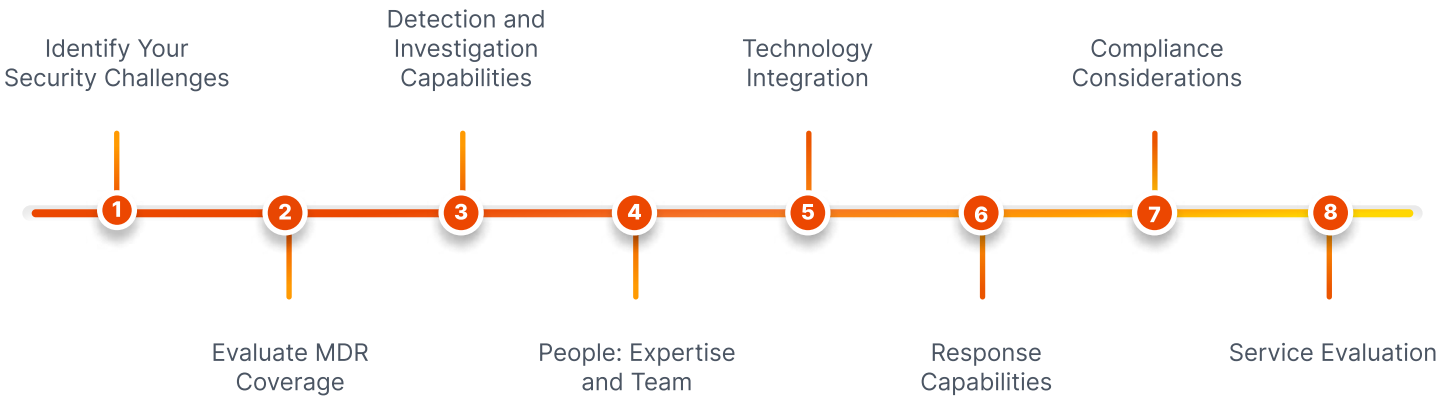
Introduction

> *"By 2025, 50 percent of organizations will be using MDR services for threat monitoring, detection, and response functions that offer threat containment and mitigation capabilities."*
>
> Gartner.

The cybersecurity landscape is relentless. Threats are ever-evolving, and traditional security solutions often struggle to keep pace. MDR bridges the gap between cutting-edge security technology and human expertise. As a managed service, MDR offers organizations access to a Security Operations Center (SOC) focused on rapidly investigating and neutralizing cyber threats. MDR vendors collect data from various sources, including endpoints, networks, and cloud environments, using this comprehensive telemetry to empower their team of security experts in threat hunting and incident response.

Choosing the right MDR provider is a critical decision. The ideal MDR provider becomes a trusted partner, freeing your internal security team to focus on core business functions while providing 24/7 vigilance against cyber threats.

However, navigating the MDR landscape and selecting the right vendor can feel overwhelming. This guide is designed to be your roadmap to a robust security posture. We'll cut through the noise and equip you with the essential questions to ask before making your final decision.



Identify your security challenges

Utilize the checklist below to identify the specific security challenges you aim to address. For each challenge marked as "yes," assess Managed Detection and Response (MDR) providers based on their ability to mitigate these issues effectively. Providers that offer solutions tailored to your security needs should be prioritized and considered at the forefront of your selection process.

Problem statement	YES	No
1. We cannot achieve 24×7×365 coverage.		
2. Our team is not large enough and lacks dedicated resources to process each alert.		
3.We aim to focus on confirmed threats rather than diving into routine alert reviews.		
4. We switch between multiple security tools because we lack a singular platform that integrates everything.		
5. Investigating, responding to, and remediating threats on time is challenging.		
6. We're concerned that we may be missing or detecting threats too late.		
7. We currently use network, SaaS, Cloud, and/or identity products.		
8. We need fully managed or co-managed SIEM with access to log data to meet compliance requirements.		
9. While our DevOps team manages our Cloud security, we must ensure they don't put our business at risk.		
10. When we require expert security advice, we lack a trusted source to ask.		
11. We lack the contextual information needed to make accurate security decisions.		
12. We need assistance in containing and remediating threats.		

Evaluation matrix: the depth and breadth of MDR coverage

Within the MDR market, a crucial distinction is the depth and breadth of MDR coverage a provider offers. Like a well-rounded security posture, an effective MDR solution must address both aspects to safeguard your organization.

This section of the guide explores the depth and breadth of MDR coverage. We'll find out how to evaluate potential MDR providers to ensure they deliver the level of protection your business needs.

Detection and investigation capabilities

1. **Do they create their detections?**
   The MDR vendor should be able to create its detections based on threat intelligence, behavioral analytics, and machine learning algorithms to identify novel and emerging threats.

2. **Are detections and investigations primarily determined by humans, machines, or a combination?**
   It should be a combination of both. While machines (such as AI and automation) can handle routine alerts and initial triage, human analysts are essential for in-depth investigations, context analysis, and decision-making.

3. **Does the MDR vendor have an integrated XDR platform**?
   Integrating an eXtended Detection and Response (XDR) platform enhances visibility and correlation across multiple security layers, enabling more effective threat detection and response capabilities.

4. **Does the MDR vendor integrate with existing technologies?**
   The MDR vendor should offer seamless integration with existing technologies, including endpoints, identity management systems, and cloud platforms like AWS, GCP, and Azure, to provide comprehensive coverage and streamline security operations.

5. **Endpoints**
   The MDR solution should integrate with endpoint security tools to monitor and protect endpoints from malware, ransomware, and unauthorized access.

6. **Identity**
   Integration with identity management systems enables the MDR solution to monitor user authentication, access controls, and user behavior to detect and prevent insider threats and unauthorized access attempts.

7. **Cloud (AWS, GCP, Azure) integration**
   Integration with major cloud platforms allows the MDR solution to monitor and secure cloud environments, providing visibility into configuration errors, suspicious activities, and unauthorized access attempts.

8. **Kubernetes native support**
   Native support for Kubernetes environments ensures that the MDR solution can effectively monitor and protect containerized applications and microservices deployed in Kubernetes clusters against security threats and vulnerabilities.

9. **What is the level of investigation and incident reporting that the vendor provides?**
   The vendor must provide comprehensive investigation, root cause analysis, timely incident reporting, detailed incident analysis, customized reporting, and post-incident recommendations.

People: expertise and team

1. **Concierge service (SOC analysts directly available for customers)**
   The vendor should offer a concierge service where SOC analysts are directly available to customers, providing personalized support and guidance for security incidents and inquiries.

2. **SOC team with 24+ engineers to cover 24×7**
   The vendor must maintain a SOC team comprising 24 or more engineers to ensure round-the-clock coverage for monitoring, detection, and response to security threats.

3. **Handle multi-step investigations: trace activities associated with compromised systems and apply the MITRE & Kill-chain methodology to see the attack lifecycle**
   The vendor should handle multi-step investigations, trace activities related to compromised systems, and apply methodologies such as MITRE ATT&CK and the Kill Chain model to analyze the attack lifecycle and identify threat actors' tactics, techniques, and procedures (TTPs).

Technology integrations

1. **Do they utilize machine learning and AI?**
   The MDR provider employs machine learning and AI algorithms to analyze vast datasets, recognize patterns, and identify anomalies indicative of potential threats. This enhances threat detection accuracy by reducing false positives and enables the prioritization of alerts based on their severity and likelihood of being malicious. Additionally, AI-driven automation streamlines security processes, enabling faster response times to security incidents.

2. **Are they capable of providing everything and SIEM integration?**
   The MDR provider can offer a comprehensive security solution that includes managed detection and response (MDR) services and SIEM (security information and event management) integration. This integration allows for centralized log management, correlation of security events, and enhanced visibility into the organization's security posture across various IT environments.

3. **Do they utilize User Behavior Analytics and Anomaly Detection?**
   The MDR provider leverages User Behavior Analytics (UBA) and anomaly detection techniques to monitor user activities and identify deviations from normal behavior. By analyzing patterns and trends, the system can detect suspicious activities, insider threats, and unusual network behavior, helping to mitigate risks and prevent security breaches.

Response capabilities

1. **Does the MDR provider offer automated response capabilities?**
   The MDR provider offers automated response capabilities to address security incidents and threats swiftly.

2. **Does the MDR provider utilize SOAR (Security Orchestration, Automation, and Response) playbooks for incident response?**
   The MDR provider employs SOAR playbooks to automate and orchestrate incident response processes, enhancing efficiency and effectiveness

3. **How quickly does the MDR provider respond to security alerts?**
   The MDR provider ensures a rapid response to security alerts to minimize the impact of potential threats on the organization.

4. **Does the MDR provider offer human-led response capabilities?**
   In addition to automated response, the MDR provider must offer human-led response capabilities to provide expertise and decision-making in complex security incidents.

5. **Does the MDR provider offer hands-on keyboard response services?**
   The MDR provider offers hands-on-keyboard response services, allowing skilled analysts to address security incidents as needed directly.

6. **What is the MDR provider's average response time for security alerts?**
   The MDR provider's average response time for security alerts is [insert specific timeframe], ensuring timely investigation and action to mitigate potential threats.

7. **How quickly does the MDR provider typically reply to emails regarding technical inquiries?**
   The MDR provider aims to respond promptly to technical inquiries via email, typically within [insert specific timeframe].

8. **To what degree is the MDR provider's response machine-led?**
   While the MDR provider employs automation and machine learning for swift response, human expertise also plays a crucial role in decision-making and complex incident handling.

Compliance considerations

1. **Does the MDR solution consider cloud-specific compliance regulations, such as HIPAA, PCI DSS, or SOC 2, and assist in meeting those requirements through robust security practices?**
   The MDR solution considers cloud-specific compliance regulations like HIPAA, PCI DSS, and SOC 2. It implements robust security practices tailored to these requirements, helping organizations comply with relevant standards and regulations.

Service evaluation

1. **Can the MDR provider develop custom integrations tailored to my organization's specific needs?**
   The MDR provider can develop custom integrations to meet your organization's unique requirements and enhance the effectiveness of your security infrastructure.

2. **How will I interact with the MDR team?**
   The MDR provider typically offers various communication channels such as email, phone, and ticketing systems for seamless interaction with their team. Regular meetings and status updates may also be scheduled to ensure alignment and transparency.

3. **Does the MDR service include expert advice?**
   The MDR service often includes access to experienced security professionals who provide expert advice, guidance, and recommendations to address security challenges and enhance your organization's security posture.

4. **Is there a limit on communication with the MDR provider?**
   Typically, communication with the MDR provider is uncapped. Organizations must maintain open communication channels to facilitate effective collaboration and timely responses to security incidents and inquiries.

5. **What is the MDR vendor's pricing model?**
   The MDR vendor typically offers a flexible pricing model tailored to the organization's needs and requirements. Common pricing models include subscription-based pricing, which may be determined by factors such as the number of endpoints, users, or level of service required. Additionally, some vendors offer tiered pricing based on the features and level of support provided. It's essential to discuss pricing details directly with the vendor to understand the specific terms and factors influencing the cost of the MDR service.

Compliance considerations

1. **Does the MDR solution consider cloud-specific compliance regulations, such as HIPAA, PCI DSS, or SOC 2, and assist in meeting those requirements through robust security practices?**
   The MDR solution considers cloud-specific compliance regulations like HIPAA, PCI DSS, and SOC 2. It implements robust security practices tailored to these requirements, helping organizations comply with relevant standards and regulations.

About UnderDefense MDR

UnderDefense Managed Detection and Response (MDR) - where cutting-edge security technology meets expert human oversight to detect and thwart threats across your IT landscape swiftly and decisively.

At UnderDefense, we understand the importance of proactive threat detection and rapid response. Our MDR service empowers organizations with advanced technology and skilled security professionals to identify and neutralize threats that would otherwise evade detection. With our UnderDefense MAXI MDR, 24×7 SOC/Threat Hunting team, and comprehensive threat intelligence, we ensure that no threat goes unnoticed.

Our approach goes beyond mere feature checklists; we prioritize positive security outcomes and strive to be an extension of your team. By eliminating alert fatigue and providing unlimited access to our threat hunters and subject-matter experts, we enable you to focus on strategic initiatives while we handle the security frontline.

Choosing the right MDR vendor can be daunting, but with UnderDefense, it doesn't have to be. Let us help you achieve your security goals and more. Discover how UnderDefense MDR can be your partner to safeguard your organization's mission.

BOOK A MEETING