

COMMON QUESTIONS AND ANSWERS

Understanding how Managed Detection and Response (MDR) compares to Managed Security Service Providers (MSSPs)

zscaler™

Introduction

Managed Detection and Response (MDR) offers enterprises the technology and expertise they need to stop threats that have bypassed other security controls.

Until recently, organizations that have lacked the resources to build an internal detection and response capability have been without options. Purchasing advanced products that are not properly staffed has little effect. And while Managed Security Service Providers (MSSPs) support many different parts of a security program, detecting and responding to advanced threats is not where they specialize. Organizations have been looking for sophisticated vendors who can identify malicious activity within their environment and ensure a quick response. This is the void MDR is filling.

As organizations consider MDR it is important that they understand key differences when compared against the traditional outsourcing option of MSSPs. Many organizations that are predisposed to pass over MSSP detection and response offerings will find that MDR can help them fill gaps within their internal capabilities.

This guide walks through eight questions asked by security teams as they seek to understand what services will make the biggest positive impact on their security program.

1. What is MDR?
2. How does the MDR model differ from an MSSP?
3. Why would I use MDR?
4. Can MSSPs provide MDR?
5. What types of organizations typically use MDR?
6. Can I replace my MSSP with MDR?
7. Would I ever use MDR and an MSSP?
8. How does Managed Endpoint Detection and Response (MEDR) fit into MDR?

1 What Is Managed Detection and Response (MDR)?

MDR services are designed to quickly detect threats and improve an organization's response once compromises have been found. The solutions deliver an operational capability to organizations that often lack the resources to build it themselves.

MDR solutions approach detection and response the same way an internal security team would.

- **Collect**
  MDR services require a robust data set to perform their detection. Organizations should expect their MDR to either request access to the existing security stack or require deployment of additional technology for greater visibility.

- **Detect**
  A hallmark of MDR solutions is advanced detection capabilities that use multiple sophisticated technologies. These include improved analytics engines, behavioral based detection, machine learning, and anomaly detection.

- **Respond**
  MDR providers vary in the degree of response delivered but at a minimum it includes remote investigation of potential threats. They employ a team of knowledgeable experts who understand how to interpret the events produced by the detection technology. These individuals often have years of investigative experience and know how to accurately identify advanced attackers. These services will also typically provide a high degree of support in containing and responding to threats once they have been detected (and some even perform the response).

The best MDR offerings closely integrate into an organization's security team, continually learn about the environment, and use that information to support investigations and threat hunting. The end result is that MDR users have a team of experts who are continually monitoring and searching through their environment to quickly detect threats and strengthen response.

Buyer Beware:
Not all MDR solutions are created equally. Offerings differ greatly across what data is collected, the technology analyzing for threats, and the response performed. And because this is a managed offering, a vendor's ability to execute is equally important. Use pages 8 and 9 to assess specific parts of an MDR offering.

2 How does the MDR model differ from an MSSP?

MSSPs typically focus on basic security tasks like monitoring standard ingress-egress traffic on perimeter products and vulnerability management. They are meant to provide high-level security coverage for basic and repetitive tasks across an organization's entire security stack. It is not uncommon to find an MSSP advertising that they use hundreds of security tools. A detailed look will often show that they employ inexperienced staffers trained to capably operate only a small fraction of those.

See the next page for a detailed comparison chart.

MSSPs mostly rely on signatures and rule-based detection and frequently miss advanced threats (and increasingly even basic attack tactics). When incidents are discovered, many MSSP customers are still responsible for managing containment and mitigation unless they pay the provider's Incident Response team extra for help. Even then, the MSSP's staff may not be specifically trained to effectively respond to an incident.

Conversely, MDR services focus specifically on improving an organization's advanced threat detection, investigation, and response. They are used to augment and enhance internal capabilities. They frequently examine similar data sets as MSSPs such as network logs or endpoint telemetry, but at a much greater depth. They are specifically tailored to use advanced technologies such as Endpoint Detection and Response (EDR), behavioral analytics, specialized forensics tools, and custom security event management platforms. The most sophisticated MDR providers focus heavily on detecting behaviors like lateral movement, credential theft, and credential escalation, all behaviors of today's advanced attacks. Some even operate large software and security engineering teams to design their own detection and response technology.

MDR services are usually built with integration in mind so that they can be plugged into a pre-existing security program and workflow.

The foundation of MDR usually lies in three key areas:



Technology

A unique data analytics platform that evaluates an organization's activity using multiple detection technologies and techniques



Expertise

Highly technical security analysts and threat hunters capable of conducting in-depth investigations, malware analysis, and threat research



Process

A well-refined process that relies on data science, efficient security operations, and incident response best practices

MDR vs MSSP: At-a-Glance Comparison

Capabilities	MSSP	MDR
Collection, Detection, and Response Platform	Perimeter technology; signature/rule-based detection to identify known threats	Inspection across endpoints and networks; behavioral analysis and machine learning to detect threatening behaviors
Triage, Investigation, and Response	Focused on meeting SLAs by quickly performing cursory triage that often results in high false positives	Designed to investigate and confirm threats at Tier 1 and Tier 2 levels and provide a more complete understanding of incidents
Role In internal Security Program	Meant to supplant basic internal security functions	Augments and enhances an existing security program with advanced technology and highly specialized analysts, threat hunters, and incident responders
Integration Across Security Program	Technology frequently lacks integration points with internal tools	Usually designed to plug into organization's SIEM, workflow, and SecOp tools. Some include additional data source ingestion options
Threats Detected	Known vulnerabilities, known malware, and common, high-volume attacks	Malware, targeted attacks, zero-days, and insider threats
Staff Specialization	Basic log management, monitoring, and investigation via playbook or script	Advanced malware analysis, threat hunting, forensics, incident response, data science and security analytics, and security research

3 Why would I choose to use MDR?

Enterprise, mid-market, and SMB firms are turning to MDR because they want the benefits of today's most advanced detection technology and practitioners to defend their organization. They might not have the resources to build a highly specialized team, or they might want to layer a specialized solution on top of their existing security program.

Advanced collection and detection technology is the first step to detecting previously unseen threats and remediating them. These new tools—Endpoint Detection and Response (EDR), User Behavior Analytics (UBA), thorough network analysis engines examining full PCAP records, etc.—require constant monitoring, tuning, and process improvement. Additionally, advanced detection tools detect potential threats. They will generate hundreds to thousands of events per day that need to be investigated prior to mitigation.

Investments in these advanced tools will be largely wasted without an advanced security team who knows how to run an in-depth investigation, understands malware analysis, and has a sixth sense about how attackers operate. A true detection and response capability requires equal investments in advanced technology, experienced security practitioners, and a process that focuses on efficiency and accuracy.

Organizations that partner with an MDR provider have a reliable team who stands by their side to defend against the worst types of threats.

With this in mind, organizations are choosing MDR for two primary reasons:

1. The opportunity costs and actual costs of acquiring advanced technology and talent and building an operational capability are extremely high and sometimes unrealistic. MDR providers offer organizations a full capability that doesn't require a dozen individual investments and months to years of implementation. Most MDR providers are priced significantly below what it would cost an organization to build internally.

2. MDR solutions work. They accurately detect threats ranging from malware to advanced attackers and support customers to ensure threats are addressed. Organizations that enlist an MDR provider have a reliable partner who stands by their side to defend against the worst types of threats.

4 Can MSSPs provide MDR?

In theory: yes, MSSPs could provide MDR services. But the majority of MSSPs are not offering true MDR capabilities at this time—even when they advertise that they do. The current business model used by traditional MSSPs cannot support a specialty service like MDR.

MSSP infrastructure is typically designed around signature-based detection and perimeter defense. And generally MSSPs employ Tier 1 SOC analysts who are there to monitor rather than investigate. To add MDR services, most MSSPs would need to completely retrofit their SOC architecture and hire veteran security engineers with experience in threat hunting, malware analysis, incident response, and data science. Complicating the matter, the most mature MDR providers are technology companies that run full software development, PM, QA, and DevOps teams.

These changes require a massive investment and culture shift that most MSSPs cannot make. In fact, these service providers' inability to deliver MDR services is partially what drove the rise of MDR.

As the MDR market grows, buyers must be careful when considering a detection and response solution from an MSSP. Many MSSPs may try to dress up existing offerings without making the necessary investments.

Red Flags That an MSSP May Not Be Able to Provide True MDR

There are many different ways to identify an MSSP overselling its detection and response offering. Organizations need to ask the right questions and require technical substantiation. Your questions should help you gain an understanding of the provider's team, technology, philosophy about detection and response, and standard operating procedures.

Questions to Ask MSSPs (and MDR Providers):

- ☐ What is your team's expertise across the following disciplines: security research, advanced detection methodologies, threat hunting, security analysis, incident response, forensics, security operations, security engineering, data science, and IT operations?

  

  TIP: To really do due diligence, ask to interview specific individuals on the security team. Learn about what they do every day and their areas of expertise.

- ☐ How do you ensure you always have enough analysts and incident responders in your SOC? How do you maintain a pipeline of recruits?

- ☐ What is your process for detection, investigation, and response?

- ☐ What technologies are core to your MDR offering? How do you train your SOC to ensure proficiency?

- ☐ Can you automatically orchestrate data and suppress events to limit investigation of false positives?

- ☐ Are you able to provide metrics showing continuous improvements in analysis time?

- ☐ Can you detect XYZ activity?

  - ☐ For each scenario you present, ask which artifacts will be collected to enable detection and what aspects of the attack will be detected.

- ☐ What is the false positive rate on some of your detectors? Not the false positive rate customers report, rather the false positive rate the provider's internal SOC reports from its own detection technology. (The key here is that internal false positives are okay. You want your MDR provider examining a lot of different activity, even if it doesn't convert to a threat.)

- [ ] What are three new types of threatening behavior you can now identify due to improvements you've made in the last 3 months? (The key here is you don't want the MSSP driving their detection with threat intelligence and you want a provider who is continually improving their detection.)
- [ ] What types of threats are you unable to detect?
- [ ] What is your customer reported false positive rate? False negative rate?
- [ ] What is your average time to detection? Response?
- [ ] Have you ever had a customer get breached? Walk through through how that event happened and what your response was. Can a conversation with that customer be arranged?
- [ ] Who do customers typically interact with when they have questions on detections, response best practices, implementation of the MDR service, etc.?
- [ ] Explain your detection and response roadmap. What new techniques and technologies will you incorporate into your offering?
- [ ] How do customers hold you accountable? (You do not want an MDR provider focused on traditional SLAs. They should be focused on breadth and timeliness of detection and response)

This line of questioning is useful for assessing all MDR offerings, not just those from MSSPs.

5 What types of organizations typically use MDR?

Organizations of all sizes across all industries are enlisting MDR solutions to support their detection and response efforts. These organizations recognize their existing security program stops a percentage of threats but can never realistically stop every threat.

Commonly held beliefs by organizations using MDR:

- ☐ Satisfying compliance requirements is no longer enough and additional security investments must be made to reduce risk.
- ☐ Prevention will fail. No matter how many products are put in place, attackers will always find a way in.
- ☐ Visibility, monitoring, detection, and response is the only way to reliably identify attackers within an environment.
- ☐ Detection and response is a capability, not a product. The capability requires equal parts technology, process, and expertise.
- ☐ Building an internal detection and response capability will be burdensome and there are new advanced services delivering a true capability that can be trusted to help secure an environment.

Organizations using MDR might have a SOC with dedicated threat hunters who want a second set of eyes watching their environment. Or, they might have a lean security team managing day-to-day security operations with no extra time to build a full detection and response capability. All are investing in MDR to accomplish one goal: quickly identify new threats and limit an attacker's dwell time within an environment.

6 Can I replace my MSSP with MDR?

It depends on how the MSSP is used. Some MDR offerings are including more of the services associated with a traditional MSSP. Others are staying focused on detection and response. Ensure you clearly understand what the MDR can support and supplement with internal resources or an MSSP.

7 Would I ever use MDR and an MSSP?

Yes. It is very common for organizations to use an MSSP in addition to MDR. This is a common combination with the MSSP handling the basic security functions while the MDR provider is specifically focused on identifying threats.

It is not uncommon for an organization to prefer the simplicity of partnering with only one managed vendor. For organizations that use this strategy, that will mean enlisting an MSSP for MDR. This approach opens the organization up to a high likelihood of relying on a sub-par MDR offering. As a result, the organization will either be continually disappointed with the MDR offering or disillusioned with its security.

Many organizations recognize there is great value in partnering with two managed vendors. The vendors can backstop each other, hold each other accountable, and each can focus on their proficiencies.

8 How does Managed Endpoint Detection and Response (MEDR) fit into MDR?

It has been said before that the endpoint never lies. With increasingly more distributed organizations and more sophisticated attacks, this has never been more true. Attackers are more adept at disguising their tactics and techniques. Endpoint Detection and Response (EDR) is a solution that can help organizations take control. But many internal teams and MSSP staffers come from a network security background and lack expertise in the intricacies of endpoint security.

Endpoint detection and response requires a dedicated team with both the skill set and the time to surface potential threats, efficiently investigate incidents, and hunt for previously unknown threats. The specialized nature of EDR and the intensive time necessary to use this product makes this a great use case for MDR. Providers delivering MEDR are hyperfocused on the endpoint, deeply analyzing the robust data to detect attackers as they try to hide on customers' laptops and servers.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.™