ESET ®

Digital Security
Progress. Protected.

9 THINGS TO LOOK FOR WHEN CHOOSING AN MDR SERVICE

Progress. Protected.

9 Things to Look For When Choosing an MDR Service

MDR can help overcome gaps in security capacity and expertise — but choosing the right provider is key.

Among businesses of all sizes, there is growing recognition for the need for more proactive security. The continued adoption of cloud computing, new hybrid working practices and the digital supply chain have increased the attack surface, and threat actors have become more inventive at finding ways to burrow into networks.

However, only larger enterprises operate at a scale that allows tooling up a full security operations center and staffing it with full-time security analysts. Even if you have the funding, cybersecurity specialists are in short supply. If yours is a midsize organization or small business, you likely have to rely on IT generalists to shoulder the responsibility of defending the IT environment.

Managed detection and response (MDR) services fill the void for organizations that need to overcome gaps in security capacity and expertise. They provide access to services manned by cybersecurity professionals and the specialized toolsets they need to practice their craft.

Those who use the term MDR to describe their offerings, though, have a wide variety of delivery models. If you have decided it's time to step up your security and engage with an outsourced MDR service, you need to do some homework to find the provider who is the right fit for your organization. Here are the questions you should ask.

1. WHAT IS THE PROVIDER'S ONBOARDING AND TUNING PROCESS?

Onboarding times vary, as do the various MDR providers' tools of choice and delivery models. Get clarity over the onboarding process and the degree to which your IT team needs to be involved so there are no surprises.

There should be some customization of detection rules, exclusions and parameters to fit the needs of your IT environment and the threats your organization faces. Faster onboarding is always desirable, but there may be a bit of a trade-off here, striking a balance between getting the MDR service up and running as quickly as possible and getting up and running with optimal detection performance on day one

Also, keep in mind that the protection afforded by an MDR service improves over time. It takes some amount of fine-tuning as the tools and the human analysts gain hands-on experience and learn what is normal versus abnormal in your environment.is the right fit for your organization.

2. IS THE SERVICE 24/7

Adversarial gangs operate from countries and time zones all around the globe, which means an MDR service has to be a 24/7 endeavor. Indicators of compromise and indicators of attack need to be investigated immediately, in real time, so a proper response may be initiated.

A local service has some advantages, but those disappear quickly if staffing during the overnight hours isn't adequate. Your best option might be a service that can provide you with a local representative but that maintains fully staffed security operations centers in locations around the globe for a true 24/7 operation.

3. WHAT IS THE TECHNOLOGY STACK? WHAT FEEDS ARE USED?

Fundamental to an MDR service is a provider-supplied technology stack that handles detection, investigation, mitigation and response. It can be a technology set developed by the provider or a set of third-party tools linked by APIs. The tools would most likely include endpoint or extended detection and response (EDR or XDR), security information and event management (SIEM), and security orchestration and response (SOAR) and should integrate with your endpoint protection platform.

The hallmark of an XDR as opposed to an EDR system is incorporation of feeds from outside the endpoints, including network traffic and various log files. Ask what feeds will be used as part of the monitoring effort. One advantage of a service provided by an endpoint-protection provider is that the endpoint platform can not only directly feed the XDR but also furnish telemetry that gathers unique data about attacks.

Cyber adversaries are becoming increasingly adept at using cloud-borne services as an attack vector or part of the attack chain, so be sure your MDR provider is able to detect and monitor activities in the cloud..

4. WHAT ROLES DOES AUTOMATION PLAY IN THE OFFERING? WHAT ROLES DO HUMAN ANALYSTS PLAY?

A robust technology stack is important, but what makes an MDR service MDR is the attention of human-in-the-loop cybersecurity analysts.

Artificial intelligence can play a valuable role in identifying anomalous behavior and sifting through seemingly unrelated actions to recognize correlations and the signs of compromise or attack. Automation can quickly execute a set of actions that isolate systems or stop an attack in its tracks. These are assistive and do not replace the expertise of human analysts.

In their rush to get to market or make their services more affordable, some MDR providers over-rely on automation for some parts of their offerings (for more, see "Who handles mitigation and remediation?" below). Some offer tiered services, with the higher tiers making more expert-led services available, such as dedicated incident-response leads, digital forensic incident (DFIR) response and expert malware analysis.

5. WHAT THREAT INTELLIGENCE SOURCES ARE USED?

Updated threat intelligence about the activities of global cyber adversaries is a key component of a maximally effective MDR service. Gathered from telemetry and curated by threat intelligence teams, these updates reveal attack methods and share countermeasures.

Threat intelligence feeds can be generated by the MDR service provider or obtained from one or more third parties. Understand the sources of the provider's intelligence, how it is gathered and how it is made actionable within the service.

Putting regularly updated and current threat intelligence in front of security analysts is key to uncovering latent threats within your environment (next topic).

6. WHAT TYPES OF THREAT HUNTING ARE OFFERED?

The adversary's goal is to establish an unknown presence on the network by employing tactics, techniques and procedures that evade the existing detection mechanisms. Finding these evasive, hidden threats is the province of proactive threat hunting.

The inclusion of threat hunting and the scope of the services is one of the key differentiators among MDR services. Look for ongoing, systematic threat hunting — it should be considered part of the baseline requirements for an MDR service.

Some providers specifically offer customized threat hunting on either a planned or recurring basis that focuses on current trending threats or offer hypothesis-driven historical threat hunting that draws from data on past detections and attack methods.

7. WHO HANDLES MITIGATION AND REMEDIATION?

Among MDR vendors, there is no shared vision about which party — the service provider or the buyer — is responsible for the "response" piece of MDR. While detecting compromised systems and active attacks is a universal part of MDR services, they vary in their approaches to mitigating the threat (containment to prevent further damage) and remediating it (restoring data and system function).

Some providers will only take responsive action if it can be automated — if not, they only offer to assist the customer's IT staff. Others offer response as part of a higher-tiered service, under a retainer or for an additional price.

Customers are different, too, in their comfort levels with third-party changes. You might be reluctant to allow the MDR service to remediate your systems because they lack intimate knowledge of the potential impact on business processes. You might prefer an approach that relies on the MDR service to contain the threat and remove it and leave full restoration to your IT staff.

8. HOW DOES THE PROVIDER'S APPROACH ALIGN WITH YOUR BUSINESS?

When incidents happen, the impact of the MDR service reaches outside of security and touches other parts of your business. Take a look at the provider's approach to containment and consider how the actions taken will align with the requirements of your business.

Operationally, consider how and whether its activities and outputs can or should be integrated with your ticket management systems and internal workflows.

The provider should also be able to furnish or allow you to generate reports about pending and resolved incidents, the status of your environment, and any other details it handles on your behalf.

9. IF YOU HAVE PARTICULAR REGULATORY OR COMPLIANCE REQUIREMENTS, CAN THE SERVICE MEET THEM?

If you have data privacy, residency or retention requirements, verify that the MDR provider is able to adhere to them. It may need to adjust or make special exceptions to its standard processes to comply with your local statutes.

If you are pursuing or have cybersecurity insurance coverage, compare the elements of the provider's service with the insurance requirements. The additional cyber controls that are part of the MDR service can qualify you for coverage or lower your premium.

CONCLUSION

MDR is a fast-growing market category. According to Gartner, there are more than 600 providers offering MDR services (or services that they call MDR); 30% of organizations are actively using MDR, and that number will double by 2025.

Broadly speaking, MDR vendors who have stepped up to serve the growing demand fall into two categories: (1) companies that provide managed IT services on an outsourced basis and have added MDR to their offerings and (2) security software companies that have added a services component. Beyond this broad categorization, there are widely differing models for how an MDR service should be architected and delivered. Understanding those differences is important.

We applaud your recognition of the need to retain an MDR service and hope this guide will be useful to you in finding the right fit for your organization.

Read on to learn about ESET's MDR services.

About ESET Managed Detection and Response

ESET MDR services are built on a strong foundation: award-winning ESET endpoint protection; ESET Extended Detection and Response, which provides hands-on security analyst tools; and human security experts who man the consoles. They work across a global network of operations centers to monitor and respond to threats, gather and curate threat intelligence, and vigilantly track international cyber adversaries and their tactics, techniques and procedures.

The service is available in two tiers, one designed to offer small and midsize businesses sophisticated protection and the other effectively constituting an enterprise-class SOC. Both tiers include the key components of an MDR service, including ongoing threat hunting and hands-on monitoring, containment, and threat eradication. The higher tier offers greater access to customized or specialized services from ESET cyber experts.

ESET MDR offers:

- Threat hunting, monitoring and response for customers of any size and security maturity level

- Always-on, 24/7 service that applies a combination of AI-powered automation and human expertise

- A pre-built library of behavior detection patterns, further customized and matched to the customer environment

- A Global Threat Intelligence team that tracks current, critical incidents and takes coordinated action to counter threats

About ESET

AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global cyber threat intelligence**, including our **extensive R&D network** led by industry-acclaimed researchers.

ESET PROTECT, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection and proactive threat-hunting capabilities with a wide range of security services, including **managed detection and response** (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening. ESET protects your business so you can unlock the full potential of technology.

(ESET) ® Digital Security
Progress. Protected.