Cyberint

The Ultimate Guide to Selecting a Managed Detection and Response Service Provider

The Ultimate Guide to Selecting an MDR

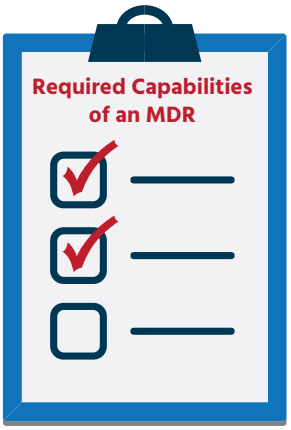
Managed Detection and Response services (MDRs) providers remove the heavy burden of cybersecurity from companies that don't have the staffing, technological resources or know how to combat advanced cyber threats. An MDR's overwhelming strength is the ability to identify and act upon threats and attacks that would otherwise go unnoticed by standard security controls. Additionally, the incident response capabilities, both automated and manual, are an important part of their offerings.

Companies don't have to abandon their existing security monitoring solutions in favor of an MDR. An MDR that can supplement and enhance your existing security tools allows your business to quickly implement mature threat detection and response capabilities – rather than having to build a solution from scratch while your business is left exposed to cyber risk.

Utilizing an MDR augments your in-house security operations by giving you access to highly specialized expertise and know-how that help you identify and respond to advanced threats. But not all MDRs are the same. MDRs differ in capabilities, service offerings, and are differentiated by focus on specific industries, verticals and operational security maturity levels. Finding an MDR that perfectly complements your company's security needs is of crucial importance for a well-rounded cybersecurity strategy in the age of advanced persistent threats.

An MDR that can supplement and enhance your existing security tools allows your business to quickly implement mature threat detection and response capabilities.

What to Look For in an MDR



Your selection process should start with an evaluation of what is most critical to your organization. For example, if compliance and regulation is of highest priority, than the "ideal" MDR needs to demonstrate strengths in those areas. If your business is mainly digital, then you will need an MDR that focuses on the digital aspects of the business.

Ultimately, you need to determine how well an MDR can align with your existing security tools, expertise and business requirements, while filling in the gaps in your cybersecurity coverage. We've provided a list of factors and criteria to take into consideration when selecting an MDR:

- Every MDR offers a unique solution that is focused on specific issues. Some may focus on threats facing medium sized enterprises, while others, will CyberInt focus on digital channels and online businesses. It is recommended to look for an MDR which offers the most value to your particular business model.

- Can the prospective MDR offer proven use cases within your specific industry with a strong focus on risk management? The MDR should be able to demonstrate specialized expertise in their area of operations in order to help your business through a wide range of industry-specific risk challenges, including compliance, brand and reputational risk, and fraud.

- What is more important- detecting threats within your network or beyond? Digital MDRs are focused on the digital world and look beyond the perimeter to detect threats before they become business affecting incidents, while other vendors are focused on detecting threats that successfully bypassed traditional perimeter security controls, and focus on networks, endpoints and traffic. Where do you need a boost?

- Determine if the MDR can provide comprehensive security coverage specifically where your cyber defences are lacking. There is sufficient variability in offerings, delivery models, target customer market and vertical, and pricing, so having a strong set of requirements is necessary for an efficient selection process. Decide whether you need help with managing risk across a broad set of digital channels (social, mobile, and web) or is detecting and mitigating all forms of corporate risk online of higher priority to you? Find an MDR that can help you cover your unique security gaps. Ideally, the MDR service should augment your existing security monitoring capabilities, in-house staff and expertise.

You Need Advanced Security in Order to Deflect Advanced Threats

Many companies recognize that the old approach to cybersecurity focuses on prevention and relies heavily on technology. However, the problem is, it doesn't fully protect them in the era of complex and persistent threats. Digital MDRs venture beyond the perimeter into the digital channels such as code-sharing sites, web communities and dark web domains, where most advanced persistent threats originate. Other MDR services are much more focused on detecting threats once they bypass traditional perimeter security controls, regardless whether the threats are in a customer's data center or public cloud services provider.

Digital MDRs detect attacks before they happen by comprehensively and persistently monitoring risk across digital channels, within as well as beyond the perimeter.

Investing in an MDR to close the gaps in your cybersecurity posture is more cost effective than purchasing yet more technology or recruiting more staff. You will also be utilising the brain power of some of the cybersecurity industry's best and most experienced human talent. A carefully chosen MDR will become your cybersecurity partner; selecting the right one will be the best decision your company can make in a troubled time of advanced persistent threats.

Digital MDR detect attacks before they happen by comprehensively and persistently monitoring risk across digital channels, within as well as beyond the perimeter.

Cyberint
Protection Beyond the Perimeter

United Kingdom
Tel: +442035141515
sales@cyberint.com
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +972-3-7286-777
sales@cyberint.com
3 Columbus Circle | NY 10019 | New York | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
sales@cyberint.com
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
sales@cyberint.com
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com **www.cyberint.com**