Managed Detection & Response (MDR)

Buyer's Guide

Table of Contents

Why do you need MDR?

The technical security controls implemented to block cyber attacks are often ineffective against new and evolving threats. Accepting that an attacker will penetrate these defences, new technologies are constantly being implemented. The most common of these are technologies that aid the detection of, and response to, in-progress attacks.

To be effective, detection and response tools require continuous monitoring and input from expert security operations (SecOps) personnel. MDR services have emerged to remove the burden from organisations that struggle to build their own high-quality security function. This guide explores your choices for outsourcing your detection and response capability.

> "MDR services provide customers with remotely delivered, human-led, turnkey, modern SOC functions; ultimately delivering threat disruption and containment."
>
> — Gartner

The key takeaway from this definition is the term "human-led". MDR providers use their economies of scale to deliver a service at a lower cost than organisations can achieve by insourcing. However, MDR services differ significantly, with many not providing the complete turnkey solution to which Gartner refers.

Make detection and response a priority

According to the World Economic Forum, 4 million professionals are needed to plug the talent gap in the global cybersecurity industry, and this could reach 85 million by 2030.

Few but the largest businesses have the budget to employ all the IT and security personnel required to implement and manage an enterprise-grade, mature security programme. Those that do have this capability must still overcome the challenge of finding and keeping the right people, in a highly competitive market.

Below, we outline your choices for improving your security posture and building a programme that enables you to rapidly respond to, contain and recover from a cyber attack that evades your primary defences. Your action is to balance the benefits and challenges associated with each approach and find the one that is most appropriate for your needs.

Outsourcing and partnering

Information and cyber security programmes require many different teams and personnel. When evaluating your needs from an outsourcing provider, you should consider the following disciplines, and which are a priority to fill your gaps.

- Governance, risk and compliance (GRC)
- Security policy, architecture and technology evaluation
- SecOps focused primarily on incident detection and response

	BENEFITS	BARRIERS TO SUCCESS
Outsource some aspects of the information and cyber security programmes Many organisations opt to outsource some elements of their programmes whilst maintaining some in-house.	Reduces the challenge of hiring and retaining your own workforce. You can outsource to experts and dedicated companies who pass on the cost savings achieved from their economies of scale, in the form of competitive pricing. Provides flexibility to choose which elements/roles to outsource based on your available skillsets. Enables outsourcing tactical activities while keeping strategic functions in-house.	Maintaining multiple relationships with, for example, VCISO, advisory companies, consultants and managed security service providers (MSSP). High total cost of ownership (TCO) – cost to onboard and manage a complex "supply chain", which itself introduces risks that you must mitigate: • Who owns which parts of your programme? • Lack of clarity around roles and responsibilities could create a blame culture. • Managing multiple SLAs will create an admin and management overhead.
Outsource monitoring to a managed security services provider (MSSP) This option is used by organisations of all types and sizes. An MSSP provides remote monitoring of security products and incident response services from its SOC.	Removes the requirement to build and own a SOC or hire and retain your SecOps team. You can outsource to experts and dedicated companies who pass on the cost savings achieved from their economies of scale. The high-priority detection and response activities will be managed and remove the burden from your team. You get 24/7 coverage.	Many of the barriers above are equally applicable with this option. An MSSP might not support all your products. Monitoring every one could be cost-prohibitive. MSSPs might not perform threat hunting and full incident response. Many just triage alerts and pass response capabilities back to their customers. MSSPs will likely not help build your security programme or perform proactive activities, like attack surface management (ASM) and vulnerability hunting.
Outsource to an MDR provider Many organisations are recognising that, given the priority that should be provided to detection and response, having an expert MDR provider remotely manage this process is critical.	A cost-effective method of implementing the priority security mechanisms to reduce the risk of a successful attack, such as ransomware. MDR providers are experts who are laser focused on the highest priority – reducing the risk of breach. They support a limited number of technologies, with purpose-built tooling, removing the complexities and costs that an MSSP incurs from managing 100s of products. These savings will be passed on to customers. Reduced complexity results in rapid deployment and reduced time-to-protection.	Barriers to success are similar to the other outsourcing options above. However, many MDR providers recognise that, in a highly competitive market, they must bundle additional value-add services. Some are laser focused on the mid-market and are creating significant value targeted at their customer base.

Mid-market organisations, with limited time, budget and resources, must outsource elements of their cybersecurity programme. Focusing on the highest priority to mitigate the risk of breach means outsourcing to an MDR provider.

Choose an MDR partner that adds value across all strategic and tactical elements of your security programme

You have many providers to choose from and they offer very different services, from basic alert triage, event correlation and reporting to a true partnership, where they become an extension of your IT and security function.

Key evaluation criteria for MDR providers

The criteria you should use to evaluate MDR providers can be broadly described under three headings. This will enable you to fully understand how a provider can help you across your end-to-end security programme.

Understand what you need from your MDR provider to enable you, your team and your organisation to achieve your business goals.

Choose a partner, not a supplier	Look for a partner who can become an extension of your IT and security teams and enable them for success. They should be adaptable, able to fill the gaps in your skillsets and support you across your complete security programme.
Local language support	Assess how important local language support is. Does the provider offer it from a fully staffed SOC during your business hours? Many large, multi-national providers will have local language first-line support only. This can result in information being relayed from the SecOps team doing the actual work, through first line, resulting in potential delays and risk of reduced clarity in communications. Ensure that every level of staff required to support you is available during your business hours.
Data residency	This is a challenge for many organisations, more so in some EU countries than others. If information must leave the EU, you might have to evaluate the risk of non-compliance, audit your provider and sign data processing agreements. Further complexities could be introduced if you already have back-to-back data processing agreements with supply chain partners that need to be revisited.

Integrated visibility into your security posture	Look for value-added functionality and services that reduce the risk of a data breach, such as ASM, vulnerability management and proactive vulnerability hunting, backed by human-led insights from expert security professionals. Your provider's customer portal should offer visibility of your attack surface with easy to understand, actionable insights to enable you to prioritise your remedial actions and manage risk.
Integrated user enablement and user risk visibility	Look for integrated value-added services that help you strengthen your security posture by enabling your users. Regular security awareness training (SAT) and testing programmes are mandated by many regulations, and most even non-regulated organisations recognise the value of creating a security culture. The concept of human risk management is gathering pace. This helps organisations understand the risks associated with their users. These might be intrinsic risk associated with their position in the organisation and their access to high-value assets, or that risk identified through training exercises. Look for SAT that is integrated into your MDR providers portal, so that you have visibility of your overall security posture and risk across your human as well as technical assets.
Demonstrating value to justify your spend and unlock incremental budget	Look for a provider with a portal, dashboards and reporting that helps you justify your security spend and unlock incremental budget for you and your team. An understanding of your security posture and how it changes over time helps you measure the effectiveness of your MDR provider and the proactive security measures they bring. By understanding your attack surface and vulnerabilities and being able to report the associated risks to your business, you can drive the agenda and argument for increased budget.
Demonstrating security levels to customers and business partners	Many businesses have a complex chain of suppliers and customers that vet each other during an onboarding process. Look for a provider that helps simplify and reduce the time to complete this process by enabling you to demonstrate that your security programme is mature, your business resilient and even in the worst-case scenario, if an attack was successful, you could quickly recover.

Detection and Response

Reduce the risk of a data breach or successful ransomware attack by ensuring you have the best possible chance of detecting, containing and responding to an in-progress attack.

The value of proactive enablement in containing and responding to an attack	Your starting point is looking beyond just incident response. Your provider should recognise that by enabling you, as described above, they are also enabling themselves. By helping you manage vulnerabilities, the likelihood of a successful incursion or the attacker compromising a device, host or user is reduced. If the attacker does gain a foothold, by understanding your IT environment, users and the assets the attacker is targeting, the attack can be slowed down and contained. This minimises the risk of a data breach or successful ransomware attack.
Maintaining protection and enabling rapid response as threats evolve	Look for a provider who is technology agnostic and has deployed a best-of-breed and flexible technology stack that enables them to rapidly switch/deploy new security tools as the threat landscape evolves. They should be adding value by developing applications and tooling to integrate with and fill gaps left by third-party tools. This ensures they can maximise their event correlation efforts, minimise triage time and respond quickly.
Time to protection and value	Linked with the above point, if your provider has architected their technology stack effectively, they can automate much of their deployment and integration with your environment, reducing your time to protection and to realise value from the service.
Full coverage	Look for a partner that provides full incident response, threat hunting, containment and helps with recovery. Many simply act as a monitoring point to triage alerts and pass the information on to you for you to respond to and recover from an attack.
Substantiated, transparent metrics	Ensure the providers you are evaluating have SLAs that meet your requirements and can produce quantifiable metrics, in formats consumable by all your stakeholders, that demonstrate they are achieving them.
Report on value add	This is linked to the above and of high importance. You must be able to demonstrate the value that any bundled or add-on functionality and services is bringing. This should be communicated in a consumable manner to all stakeholders, via a portal or offline reporting.

Recovery and cyber insurance

In the worst-case scenario, when an attack is successful, what can your MDR provider do to mitigate the risk and financial impact of a successful attack.

DFIR, root cause analysis and advice	Your provider should have DFIR capabilities in-house to support the MDR team in their root cause analysis within SLA, to report on an incident lifecycle, from incursion to final containment. They should offer advice and optional hands-on expertise to help you remediate and recover from an incident.
Ransomware negotiations	Most organisations do not want to consider this outcome, but many do opt to pay the ransom. However, to stand the best chance of successfully recovering your data, even when agreeing to pay, you need the help of a specialised negotiator. Some providers have the expertise to help with this task.
Source cyber insurance from an MDR provider	Many businesses recognise the importance of cyber insurance. There are various drivers, including regulatory necessity, appeasing partners up and down your supply chain and mitigation of the financial risks associated with business disruption. Look for an MDR provider that has proactively partnered with insurance underwriters to help reduce its cost and the complexity of the application process.
Simplify the insurance application process	Insurers need to understand the risk associated with insuring you by assessing your security posture. Sourcing insurance from a provider that has proactively partnered with insurance underwriters and had their services reviewed, can reduce the number of questions you must answer, often by up to 80%.
Lower costs	MDR providers offering insurance through partner underwriters should have proactively negotiated discounts on behalf of all their customers. These can range from 25% to 35%.
Simplified renewal	Along with the simplified initial application process, renewal should also be a trivial process.

Carefully choose your MDR provider type

Your first decision is to determine which foundational technology you would like your detection and response service to be based around. The choices are:

- Endpoint detection and response (EDR)
- Network detection and response (NDR)
- Extended detection and response (XDR)

The majority of MDR providers offer an element of XDR and many call their service MXDR. They absorb signals from point security measures and correlate them with those from EDR or NDR. However, one of these two technologies will form the foundation of their service. Your decision is which to choose.

PROVIDER TYPE	BENEFITS	CHALLENGES
Vendors of endpoint, cloud and network security software	Experts in their own technology. Global coverage with multiple SOCs providing follow-the-sun support.	Support only their own point products; no/little correlation of alerts across multiple enforcement points to enable rapid triage and response. Primary focus is large, multi-national enterprise customers.
Large MDR providers and telcos/large MSSPs	Experts across the range of products they support. Global coverage with multiple SOCs often providing follow-the-sun support.	Diverse range of technologies supported results in slow integration and service deployment. Limited incident response and recovery offered; often inflexible. Primary focus is large enterprise customers.
Local MDR provider	Typically, laser focused with experts across the range of products they support, enabling rapid deployment and response. Flexible business partners with high levels of engagement and value-add. Local language and data residency.	Might not support all products in your environment.
Cyber insurance-led MDR provider	Strong, competitive insurance products.	No cybersecurity expertise and outsource the complete function to a third party. No direct relationship with the MDR provider on whom you are relying to prevent a data breach.

In a crowded market with many choices, it is imperative that you understand exactly what MDR providers are offering so that you can identify gaps that need to be filled by internal resources. Even when a provider claims to cover all your needs, ascertain what is included as part of the basic package and what is an additional cost.

Ask these questions to help you choose the right MDR partner

Enablement

Local support	• Do you provide local language support on a 24/7 basis? • Will any of my data be processed in a different country?
ASM and vulnerability management	• Is ASM bundled? • Do you provide digital asset and user/identity discovery? • Is your discovery process at a point in time or continuously updated at regular intervals? • Is vulnerability hunting bundled? • Are they point in time scans or continuous? • Do you provide advice around vulnerability management? • Do you monitor domains, hosts and device configurations for weaknesses and make recommendations to improve security? • Do cybersecurity professionals provide advice around attack surface insights? How is it presented?
User enablement and user risk visibility	• Do you monitor domains, hosts and device configurations for weaknesses and make recommendations to improve security? • Do cybersecurity professionals provide advice around attack surface insights? How is it presented?
Reporting	• Do you provide visibility of all my users? • Do you provide SAT? • Is SAT reporting integrated into your customer portal to give me a single pane of glass view of user risk alongside other assets?
Human-led insights	• Is expert advice included across all proactive elements of the service as well as incident response? • Do you offer a VCISO service?

Detection and response

ASM and vulnerability management	• Do you use information gathered during the ASM process to aid detection and response?
SOC tooling	• Do you rely on only third-party tools or do you have your own integrated technology stack to enable rapid response across your supported environments?
User enablement and user risk visibility	• Do you correlate alerts and triage incidents to determine their priority? • Do you take remedial action to contain an attack? What actions do you support? Do you support these examples? - For devices – terminate a process or isolate an endpoint - For cloud applications – disable user accounts, revoke sessions or force a password reset
Reporting and communication	• What is your communications process during an incident? • What information do you make available following containment?
SLAs and reports	• What SLAs do you provide? • How do you report compliance with them? • How do your service average metrics compare with your SLAs?

Recovery and cyber insurance

Reporting	• Do you provide root cause analysis reporting highlighting each incident lifecycle? • Do you provide expert advice to minimise the risk of a similar incident? What form does it take?
Cyber insurance	• Do you have relationships with insurance underwriters? • Have you negotiated discounts? • If I purchase via your underwriter partners, does it simplify the application and renewal processes?
Human, expert-led value-add	• Can you provide consultancy advice to help during recovery? • Can you help with ransomware negotiations?

Case Studies

Jan de Rijk Logistics

For Jan de Rijk Logistics, the industry's heavy reliance on automated processes makes cybersecurity more critical than ever. Customers now expect increased accountability from logistics partners, recognising the far-reaching consequences of operational failures. Find out why Eye was the right cybersecurity partner.

Avi Medical

Avi Medical is unlocking the benefits of digitised healthcare by integrating AI-driven services. With the company's highly connected approach, securing sensitive patient data is a priority. So is business continuity. With Eye Security at their side, Avi Medical can keep innovating and providing a holistic healthcare experience.

KeyTec Netherlands

As reports of ransomware in their industry soared, manufacturing company KeyTec Netherlands decided to act. Find out how Eye Security helped them proactively bolster their defences and create a cyber-savvy work culture.

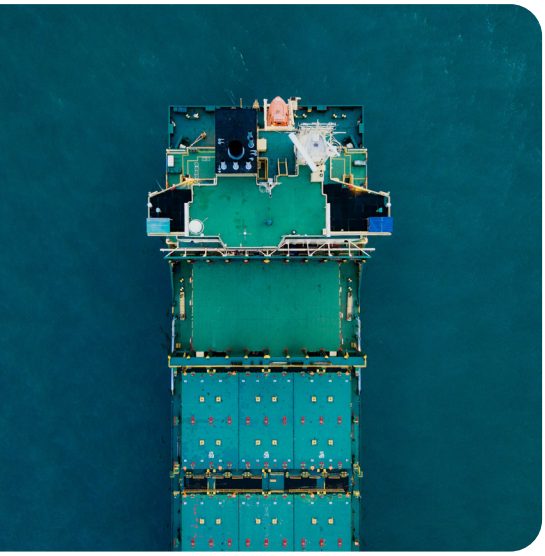
Signature Foods

As cyber crime becomes increasingly sophisticated, companies racing to keep up are turning to external suppliers. Find out how we helped Signature Foods get blanket cyber protection in just a few weeks.

Testimonials

Eye Security was the most approachable, accessible – and fair. Their focus on mid-sized-plus companies like us made it feel like a partnership from the start."

— Fred Westdijk
CEO, Jan de Rijk Logistics



A pen test alone to identify all the threats would have cost us as much as our annual cost for Eye's all-round service."

— Thorsten Spieker
Director of Engineering, Avi Medical

Eye Security helps European companies stay safe with 24/7 MDR, rapid incident response, security awareness, and integrated cyber insurance. We make cybersecurity straightforward and effective so you can focus on maintaining operations.

www.eye.security