Market Guide for Managed Detection and Response

24 June 2024 - ID G00788157 - 29 min read

By Analyst(s): Pete Shoard, Andrew Davies, Mitchell Schneider, Angel Berrios, Craig Lawson

Initiatives: Security Operations; Build and Optimize Cybersecurity Programs; Meet Daily Cybersecurity Needs

MDR services provide customers with remotely delivered, human-led, turnkey, modern SOC functions, ultimately delivering threat disruption and containment. Security and risk management leaders should use this research to identify MDR services that meet their business-driven risk requirements.

Overview

Key Findings

- Misnamed technology-first offerings that fail to deliver human-driven managed detection and response (MDR) services are confusing buyers looking to identify and select an outcome-driven provider.
- Turnkey threat detection, investigation and response (TDIR) capabilities are a core requirement for buyers of MDR services, who demand remotely delivered services deployed quickly and predictably.
- Increasingly, MDR buyers are asking providers to extend their requirements beyond the detection of and response to threats, to include the proactive identification of threat exposures and preemptive security responses.
- An increasing number of MDR customers demand that providers can remotely initiate measures for active containment or disruption of a threat, yet vendor autonomy still varies. Factors including trust, geography and the security maturity of the organization affect adoption.

Recommendations

Security and risk management leader responsible for security operations should:

- Use MDR services to obtain 24/7, remotely delivered, human-driven security operations capabilities when there are no existing internal capabilities. MDR services also should be used when the organization needs to accelerate or augment existing security operations capabilities.
- Assess how the MDR provider's containment approach and incident reporting can integrate with your organization. Also decide whether actions can be performed on your behalf to align with business requirements as well as compliance/legal policy/government regulation.
- Attain the maximum benefit from MDR services by preparing response workflow processes and integrating existing ticket management systems. This will ensure an outcome-driven response for the business.
- Investigate whether the MDR provider's service can align with your business-driven requirements by using RFPs and proofs of concept (POCs), and if necessary, by validating core, must-have requirements, such as data residency requirements. Determine whether it can provide actionable findings that internal teams can successfully react to, rather than settling for regurgitated technology outputs with no added analysis.

Strategic Planning Assumption

By 2028, 50% of findings from managed detection and response providers will be focused on, or include detail on, threat exposures, up from 10% today.

Market Definition

Gartner defines managed detection and response (MDR) services as those that provide customers with remotely delivered security operations center (SOC) functions. These functions allow organizations to perform rapid detection, analysis, investigation and response through threat disruption and containment. They offer a turnkey experience, using a predefined technology stack that commonly covers endpoints, networks, logs and cloud. Telemetry is analyzed within a provider's platform using a range of techniques. The MDR provider's analyst team then performs threat hunting and incident management to deliver recommended actions to their clients.

MDR offers outcome-driven security incident management that is predicated on the detection, analysis and investigation of potentially impactful security events and the delivery of active threat disruption and containment actions to respond to and mitigate the impact of cyber breaches.

Must-Have Capabilities

The must-have capabilities for this market include:

- A remotely delivered, provider-hosted and provider-operated shared technology stack that enables and coordinates real-time threat detection, investigation and active mitigating response. This technology stack can be developed by the MDR provider, or an integrated set of commercial technologies that use modern techniques (like APIs) to exchange data and instructions. This capability can also be achieved through a combination of both approaches.
- 24/7 staffing that recognises customer-specific cyber-risk-based use cases, engages daily with individual customer data, and has skills and expertise in threat monitoring, detection and hunting, threat intelligence (TI) and remote response.
- The availability of immediate remote mitigative response, investigation and containment activities (such as quarantining hosts), beyond alerting and notification, delivered and coordinated by service providers' staff and preapproved by end users.

Standard Capabilities

The standard capabilities for this market include:

- Turnkey delivery, with predefined and pretuned processes and regularly evolving detection content. It includes a standard playbook of workflows, procedures and analytics, requires a minimum viable set of telemetry to deliver services, and offers integration with third-party detection and response technologies beyond provider-owned technologies.
- Triaging, investigating and managing responses to all discovered threats, regardless of priority and the provision of "incident tickets" that include likely objectives of attacks, degrees of success, impact on the business and remedial actions that the client must take. There must be no limitations on volumes or time dedicated to the discovery and investigation process.

Optional Capabilities

The optional capabilities for this market include:

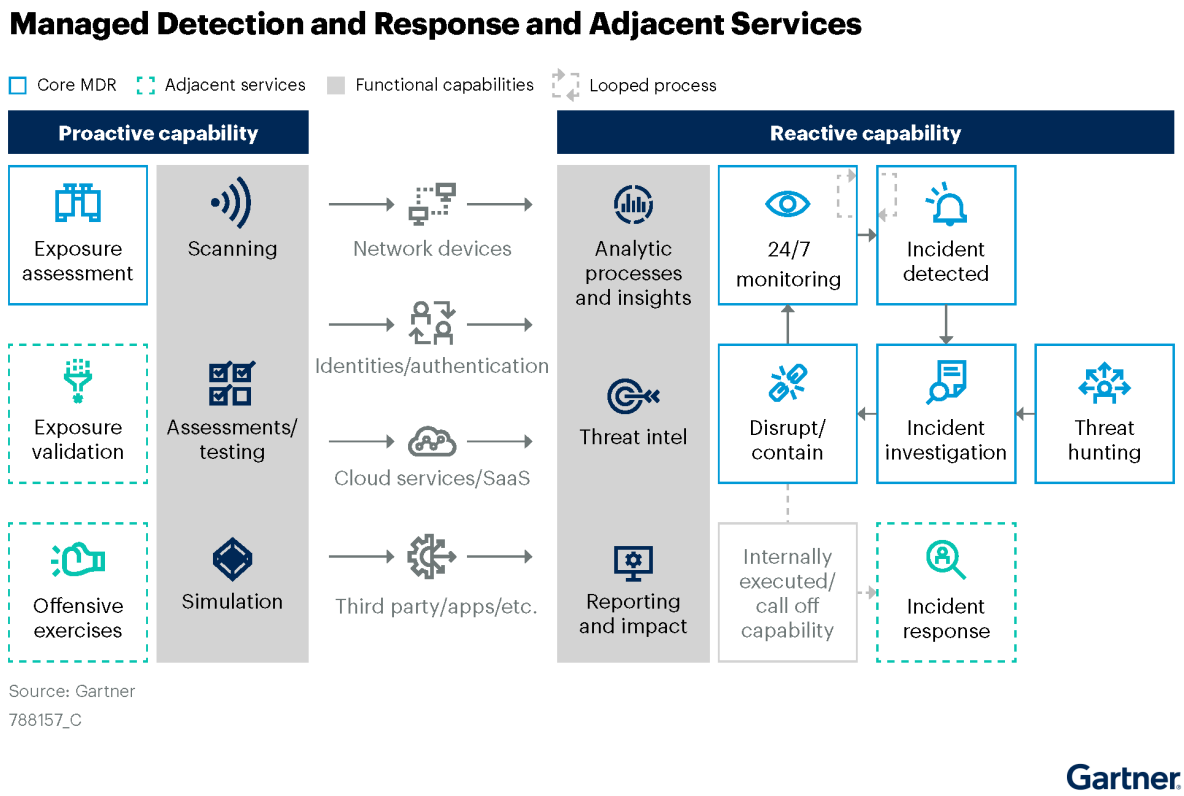
- Additional contextual data sources providing details of security exposures such as vulnerabilities, attack surface visibility, and brand and reputational analysis, as well as security assessment and validation capabilities, such as breach and attack simulation (BAS), which analyze the efficacy of security controls and response processes, and provide clients with guidance on how to improve their defensive posture and remediate misconfigured security controls.
- Digital forensics and incident response (DFIR) retainer capabilities offering call-off remote or deployable staff to carry out deep dive incident and root cause analysis.
- Incident management capabilities that track, measure and suggest improvements and automation opportunities for the remediation actions involved in response workflows.
- Hypothesis-driven threat hunting, where clients are able to identify specific threat hunt targets to determine if a threat actor was to blame. The focus would be on users of interest or where privileged data is known to have entered public circulation. This capability is different from threat hunting, which is included as part of MDR and hunts for known threat techniques.
- Telemetry coverage of identity and email/collaboration tools as well as Internet of Things (IoT) and operational technology (OT) device monitoring, cloud services, particularly SaaS and identity data from an array of common identity and access management (IAM) providers.

MDR service providers deliver these capabilities using a range of security technologies — these are commonly endpoint- and network-driven but increasingly involve cloud services layers, SaaS and custom applications. In addition, connectivity to adjacent capabilities provides contextual information (e.g., identity and user, threat exposure and business criticality) to improve and validate threat detection. Providers develop threat-focused content and analytics, also known as detection engineering, and apply threat intelligence (TI), whether developed in-house, purchased from third parties or a combination of both approaches. Providers also apply manual/automated disruption and containment activities — such as host isolation, account lockout and network blocking (see Figure 1).

Threat hunting augments real-time threat detection. It can find attackers employing tactics, techniques and procedures (TTPs) that have avoided customers' prevention and detection capabilities or validate the lack of threat evidence in an environment. Additionally, requests for more ad hoc business-led, hypothesis-driven threat hunting has gained popularity. This type of threat hunting should not be confused with everyday threat hunting that should be included as a standard part of an MDR service. Instead, it should be seen as an additional service, driven by consumer requests for specific findings and aligned with call-off consultancy pricing models.

Extensions to the detection of threats include the assessment of exposures. MDR services regularly detect and respond to proactively discovered issues with configuration, vulnerability and leaked digital assets (such as credentials). Services carry out scanning and regular assessments of both the internal and external components of client infrastructure to provide alerting on high-risk issues. These services also provide suggested remedial actions for the organization to take to reduce cyber risk.

Figure 1: Managed Detection and Response and Adjacent Services



MDR services are designed primarily to reduce the time between detecting and responding to threats and provide assessment of current exposures to threats. Additional security operations functions have emerged, including digital forensics and incident response (DFIR), exposure validation capabilities (such as breach and attack simulation [BAS]) and offensive exercises. These complement and enrich the threat detection, analysis, investigation as well as the mitigative response to threats.

Market Description

MDR provides customers with remotely delivered, human-led security operations center (SOC) functions for the purposes of reporting, rapid detection, analysis and investigation of threats and exposures. MDR also provides remote mitigative response to such threats (see Note 1).

Market Direction

MDR is a high-adoption growth and established detection and response market (see Emerging Tech: Security — Adoption Growth Insights for Managed Detection and Response). MDR mind share increased 29.14% year over year with MDR adoption growth increasing 67% from 2021 through 2022

Successful MDR service providers offer a focus on high-fidelity threat detection, investigation and mitigative response with meaningful and human interpretable reporting aligned to business-focused risks. The provider takes responsibility for determining how threats are detected. Customers have little opportunity to customize threat detection use cases relative to their environment but are encouraged to communicate risk-based requirements to ensure relevant use cases are implemented. Such requirements might include identifying critical business functions and the assets they depend on, or significant personnel or data and the impact their disruption or compromise may cause.

Buyers should not expect distinct or specific customization that would be available in more consultancy and/or professional services-led efforts as part of the core MDR service. This is because customization may be offered as an add-on or adjacent service capability. To achieve the required scale, a common delivery platform for all customers providing centralized reporting is essential. A common delivery platform ensures all customers receive a common set of threat intelligence and detection content, and therefore a comparable service experience. This provides both maturity to established SOC capabilities within organizations or an immediate level of maturity to those with little existing capability.

Other elements of MDR are emerging in the market but are not yet commonplace. The following traits may appeal to buyers, especially as they look for differentiation in their markets. A typical pattern observed among organizations that are less mature in their security operations is to start with threat detection and response capabilities. From there, they expand the services used from the provider to improve other areas of security operations. Emerging areas include:

- **Expanding into other security operations functions, such as exposure management and beyond traditional vulnerability analysis:**
  - Exposure management capabilities help with the prevention of attacks through increased awareness of their attack surface (see Innovation Insight: Attack Surface Management). It also helps with effective prioritization of exposures in the customer's environment, user accounts and cloud applications, and validation that these exposures genuinely represent risk.
  - The ability to monitor infrastructure as a service (IaaS) and SaaS platforms, as well as popular online applications — especially apps like Google Workspace, Microsoft 365, Salesforce, SAP and Workday.
- **Self-service additions to the common platform, also known as "co-management":**
  - These enable organizations to expand their security maturity, graduating from using an MDR service and include capabilities such as data investigation and reporting tools. These capabilities enable internal customer security staff to use the data collected by the provider for custom searches and functions, such as threat hunting or compliance reporting.

MDR services are available from a range of providers (well above 600 providers as of this research). These providers may be focused specifically on the MDR market opportunity and dedicated to providing only detection and response services. Additionally, these providers may offer detection and response as well as wider IT security-specific services. MDR services are also available through managed security services providers (MSSPs), who offer MDR as part of a larger catalog of managed technology, security and risk management services or consultancy.

Many MDR providers also target verticals where they can offer industry-specific expertise and services and compatibility for niche technologies in the operational technology (OT) space. This includes critical infrastructure and manufacturing, or healthcare, which all have privacy, safety and reliability risk concerns.

Having an MDR provider detect a threat is meaningless without your own preplanned, timely response processes to deal with the potential impacts of that threat.

Market Analysis

The key value proposition of MDR is the human interpretation of security incidents and their impact on an organization. MDR also provides guidance on, as well as performing the initial mitigation steps, which would otherwise be complex to understand and enact. By providing context-led investigation, analysis and mitigation (taking action to disrupt or contain an attack), the MDR provider can buy time for the customer to perform further investigation and ultimately remediate discovered issues utilizing their internal standardized response processes.

Providing mitigative response to disrupt or contain threats is a core capability of MDR service providers. Due to the prevalence of endpoint detection and response (EDR) technology providers offering an MDR service wrapper for their technology, many of these mitigative response actions are centered around using EDR solutions. However, with the increased prevalence of cloud-based and application-centric business, response requirements from end users are predominantly focused on identity-centric functions (such as account restrictions in authentication systems).

Struggling Differentiation Between MDR Services Is Causing Providers to Diversify

A variety of MDR service approaches address a range of buyers. Buyer types include:

- **Organizations that have** TDIR capability investments but consider themselves to be unable to manage these technology investments effectively due to inadequate team size or skill sets.
- **Organizations that have not** invested or developed TDIR capabilities and require support in both grassroots setup and long-term maintenance and oversight of a capability.

- **Organizations that have** a SOC and want to use services to create efficiency in their teams and expand the availability of existing resources to carry out more business-focused threat defense. This includes where requirements align with key business objectives and risks; for example, manufacturers focusing on the availability of OT environments).
- **Organizations that have** a long-term vision of owning TDIR capabilities internally but need to achieve a level of maturity quickly. Additionally, these organizations want to use services to provide interim coverage while they hire, skill up and develop requirements for SOC operations.

Expectations from buyers of MDR is that providers must operate a single technology centrally in a multitenant fashion to achieve the scale and consistency demanded. In addition, MDR must achieve the benefits of the provider's global visibility around detection content and relevance. There is no mandated technology type choice, nor set of telemetry that is required to deliver an MDR service. However, for most engagements, a breadth of experience with endpoint-, network-, identity-, cloud-SaaS- and application-driven detection platforms and telemetry is preferable for most. Extensions into Internet of Things (IoT) and cyber-physical security (CPS) systems or operational technology (OT) are available. However, they are rarely called out by buyers separately from core IT security requirements; organizations recognize that cyberthreats are cyberthreats, no matter the system they reside in.

Buyers continue to face challenges with service naming and marketing language that has often overpromised and underdelivered. Core service deliverables and outcomes should broadly be the same for all providers in this market. However, some providers describe and offer their services as MDR when they are not delivered as a buyer might expect or in alignment with how MDR is described in this guide. Alternative delivery styles sometimes described as MDR include:

- **Co-managed security monitoring:** Services which deliver an overlay to either existing technology investments, such as EDR technologies, are frequently named MDR. These services deliver a far less human-driven experience, depending on the technology for the bulk of the delivery. Although still valuable, these offerings are often promoted as being more engaged than they actually are and would be better described as co-managed security monitoring (see Market Guide for Co-Managed Security Monitoring Services). Commonly delivered by technology providers or systems integrators (SI), greater internal staffing, skill sets and engagement is required to truly get value from these services.

- **SOC as a service:** Some vendors have offered services for a number of years that provide SOC capabilities as a service, often under the MSSP umbrella. Many of these services could be described as being more aligned to consultancy and staff augmentation. They are commonly heavily customized on a per-customer basis, providing dedicated technology and staffing. The variation in these services and the lack of turnkey offering can sometimes be disguised behind a renaming of a historical service to MDR. Buyers should evaluate these services in alignment with their requirements and budget. These services can provide high levels of quality and detail in outputs but regularly take longer to deliver. They are also more expensive and require far more direction from the buyer in regard to scope and evolution.

However, there exists a trend where organizations invest in their own security technology stacks and then look to adopt MDR services. In reaction, service provider flexibility regarding data sources is shifting to full data-source neutral. Buyers that are unwilling or unable to replace the security technology investments they have made require an MDR provider who can adapt to or integrate with their adopted security technologies.

Some MDR providers are more flexible about using security technologies already owned by buyers, however, this is not without limitation. MDR providers that offer this flexibility will still have a preferred set of technologies and vendors that are supported, and limitations often focus on how telemetry is utilized (investigational use cases versus detection use cases). Usually, willingness to take on alternative data sources will depend on the ease of integration (e.g., through APIs) and the utility of that technology (e.g., the ability to mimic existing preferred telemetry sources or support incident response activities).

There are also a number of circumstances under which security investments are included as part of wider infrastructure and SaaS subscriptions. These are now commonplace as the primary supported technology, with some technology vendors specifically developing capabilities to enable tiered management of the platforms. These technology vendors give third-party providers access and control on top of existing internal access for security teams.

The willingness to use more technology-neutral services is increasing the need to mandate a minimum set of telemetry. This will enable providers to deliver consistent and high-quality services. MDR providers supporting this approach risk losing control of the quality and fidelity of the sources for threat detection. Without this, they will be unable to effectively investigate and respond to threats, and therefore, unable to truly deliver against the needs of the MDR buyer.

MDR Service Compatibility With Threats to Modern Infrastructure

Modern infrastructure includes the use of SaaS, IaaS, third-party subscriptions, social media, open-source tools and a wide variety of internally developed applications, often using more modern tools like serverless computing. The traditional model of on-premises devices, boundary firewalls and endpoint devices are commonly becoming irrelevant to the core risks faced by businesses. Importantly, there are two focus areas for threat management in modern infrastructures, exposure and identity.

MDR buyers are demanding compatibility for the areas of their infrastructure that are most critical to their mission. This means greater visibility into not just active threats but exposure to potential threats. With a lack of direct security control on aspects of third-party services used by businesses, reducing exposure to threats through more granular configuration, access control and reducing data visibility, is sometimes the only mechanism available. Furthermore, being able to take immediate and direct mitigative action to reduce exposure in those areas, and mitigative response to active threats, is essential for an effective MDR service. “Identity” is arguably the most important piece in the puzzle, and it is one of the few areas of commonality among a soup of different technologies, providers, applications and subscriptions (see Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response).

Gartner clients look to MDR providers to be their entire SOC Level 1 senior analyst cohort (see The Security Operation Leader’s First 100 Days) or an extended part of their existing SOC. Clients expect their providers to be able to perform investigation, containment and exposure reduction on their behalf. Customers regularly allow MDR providers to perform remote disruption and containment activities to support internal incident response processes with larger numbers of preagreed actions and scenarios.

Organizations that depend on MDR services for the bulk of their security operations functions have reported that they are highly likely to reject MDR providers that cannot take mitigative response actions against threats and exposures on their behalf.

Buyers can be uncomfortable with the providers directly performing actions on their behalf. Therefore, buyers want easy mechanisms to approve or initiate any exposure reduction, threat disruption or containment actions themselves. Preagreed actions and scenario playbooks provide transparency for specific threats and often limit the actions of MDR providers to low impact or easily reversible actions.

A full response or remediation of a threat event is not typically something performed by MDR providers. However, security and risk management leaders must demand threat disruption and containment from their service providers. Remediation activities self-administered by the client should be a logical set of well-established, follow-on internal processes that are put into action once MDR providers have disrupted or contained threats. Remediation must be internal because it is difficult for an MDR provider to carry out full response activities and know, categorically, that it won't impact legitimate business functions unnecessarily. As an additional service, some MDR providers that offer incident response retainers may also assist with the recovery phase. However, this is most often a purely investigational and advisory capability, and it is not the same as the mitigative response included in MDR.

Security Operations Processes Cannot Be Fully Outsourced

MDR can be a compelling offering, but like all varieties of managed security, it is not an all-encompassing solution. Some of the most progressive MDR providers are business-risk aligned. However, it is important to quantify whether the service they offer stems from your organization's specific risk-focused requirements and delivers outcomes internal teams can act on. Focus on the detail of the outcomes MDR providers (see Note 2) offer and identify the best way to integrate an MDR service provider's outputs and coverage into your own internal incident response processes. Integrating and fine-tuning both MDR and internal security processes is critical if you hope to improve overall outcomes. It is also important to allow internal resources to work with your providers. Offering details regarding new risks, business changes, updates to infrastructure (new apps, networks, etc.) will improve outcomes and help maintain good working relationships with providers.

Maturation of the MDR Market

Adoption by More-Mature Buyers

Consistency in delivery is a key feature of MDR services, as this enables them to achieve scale. But it also allows clients to get a better understanding of what the service will specifically deliver. Consistency is something beneficial to both less mature and mature buyers alike. For less mature buyers, consistency allows the use of existing MDR clients to act as a benchmark to service quality and assurance. Conversely, for more-mature buyers, it becomes a guarantee of efficiency. MDR services do not have to provide cutting-edge detection capabilities or be at the front of the threat intelligence market to provide value. Clear consistent deliverables that improve the operational efficiency and the maturity of a business's security team is often what is required.

Some MDR providers do specifically target more mature buyers, focusing on providing a tailored solution for organizations with existing investments in security tools. Some providers are particularly neutral in the way they deliver their services. This approach starts to resemble traditional SOC services from MSSPs, but with a stronger emphasis on disruption and containment activities in addition to the typical alerting and notification.

Expansion Into Exposure Management Services

Exposure to potential threats is becoming more critical than reactivity to current threats. This is because of a reduction in technology ownership in favor of subscriptions is moving the emphasis from monitoring platforms to protecting data. With this in mind, buyers want to introduce initiatives around exposure management (EM) within current constraints for technology acquisition. Gartner's continuous threat exposure management (CTEM) program provides a route to enhance existing vulnerability management programs (see Implement a Continuous Threat Exposure Management (CTEM) Program). However, organizations still struggle to deal with the volume and complexity of the discovered issues. Services provide governance, expertise and well-integrated technology to enable the detection and response to discovered exposures as well as discovered threats.

Furthermore, understanding this context enhances detection and response effectiveness. Service providers have been offering proactive exposure visibility and mitigation guidance for some time, predominantly focused on vulnerability and threat intelligence. Doing so can significantly reduce the volume of reactive issues, converting the service focus onto proactive challenges which allow for more time and consideration to be given to resolution actions.

While exposure assessment is now a common function of MDR services, expansion and adjacent services that provide exposure validation functions, such as subscriptions to regular attack simulations using BAS toolsets and offensive exercises (red teaming), are becoming more commonplace.

Self-Service Technology Availability

A divestiture of some service provider offerings toward directly competing with technology and an increase in "as-a-service" demands have driven a number MDR providers to offer their security service delivery platforms (SSDPs) to more-mature or maturing buyers. This addition to portfolios is not a direct expansion of MDR capabilities. However, it does show willingness and openness from MDR vendors to let clients see "under the hood (of the car)." It will also support a natural maturity evolution for clients that want more control over, and visibility into, their security events and issues. Buyers that do want more control over this and want to mature internal security operations are now investing in co-managed security monitoring services more frequently, in addition to an MDR service.

A number of providers have created branding for their SSDPs and encouraged end users to migrate away from service offerings. With many reaching a "peak" of scalability for their MDR businesses, they have proactively looked at other revenue streams. End users should be careful not to choose the do-it-yourself option when they need MDR-level support. Overall, the availability of self-service capabilities should provide some diversity in content and functionality, broadening the pool of available talent to improve detections. This operating model is highlighted in Emerging Tech: Rise of the Detection and Response Security Service Delivery Platform. Yet, no extensions into the exposure assessment space have been observed in these areas. As a more recently emerged capability for MDR providers, it is expected that some maturity in the platforms and integrations will be required before a formal self-service option appears on the open market.

MDR Market Merger and Acquisition Activity

During the past 12 months, there have been many acquisitions in this market, examples include:

In 2Q23 and 3Q23:

- Arctic Wolf Networks acquired Revelstoke
- Integrity360 acquired Advantio
- Rapid7 acquired Minerva Labs

In 4Q23 and 1Q24:

- BlueVoyant acquired Conquest Cyber
- Allurity (Aiuken) acquired SRLabs
- Chertoff Group acquired Trustwave
- CrowdStrike acquired Flow Security
- SentinelOne Acquires PingSafe

Security and risk management leaders need to be prepared for the fact that, in a rapidly growing market, providers will continue to be acquired.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Selection

Gartner has included a range of providers in this research to ensure coverage from a geographical, vertical and capabilities perspective. Gartner estimates that more than 600 providers in this market claim to offer MDR services. Those included in this Market Guide:

- Are consistently visible to Gartner clients (based on inquiries)
- Are variable in size and distribution as to reflect the buying population
- Have a clear end-user and outcome-focused offering distinct from pure technology-driven offerings

A list of representative vendors is provided in Table 1. This is not intended to be a list of all the providers in the MDR services market. It is not, nor is it intended to be, a competitive analysis of the providers.

Table 1: Representative Vendors for Managed Detection and Response

(Enlarged table in Appendix)

Provider	Service Name	Headquarters
Ackcent	Managed Detection and Response	Barcelona, Spain
Aiuken Cybersecurity	MDR SOC	Madrid, Spain
Arctic Wolf Networks	Managed Detection and Response	Eden Prairie, Minnesota, U.S.
Binary Defense	Managed Detection & Response	Stow, Ohio, U.S.
Bitdefender	MDR Advanced/Enterprise	Bucharest, Romania
BlackBerry	Cylance MDR	Irvine, California, U.S.
Critical Insight	Managed Detection and Response	Seattle, Washington, U.S.
Critical Start	Managed Detection and Response	Plano, Texas, U.S.
CrowdStrike	Falcon Complete	Sunnyvale, California, U.S.
Cybereason	Cybereason MDR Complete	Boston, Massachusetts
CYBEROO	Managed Detection and Response	Reggio Emilia, Italy
Cyderes	Enterprise Managed Detection & Response	Kansas City, Missouri, U.S.
Deepwatch	Managed Detection and Response	Denver, Colorado, U.S.
eSentire	Managed Detection and Response	Waterloo, Ontario, Canada
ESET	PROTECT MDR	Bratislava, Slovakia
Eviden	Eviden MDR	Bezons, France
Expel	Expel MDR	Herndon, Virginia, U.S.
Fortra	Managed Detection and Response	Eden Prairie, Minnesota, U.S.
Integrity360	Managed Detection and Response	Dublin, Ireland
Kroll	Kroll Responder	New York, New York, U.S.
Kudelski Security	MDR ONE Resolute	Cheseaux-sur-Lausanne, Switzerland; and Phoenix, Arizona
Lmntrix	Managed Detection and Response	Orange, California, U.S.
Mandiant	Managed Defense	Reston, Virginia, U.S.
mnemonic	Managed Detection and Response	Oslo, Norway
Obrela Security Industries	MDR Core	London, U.K.
Ontinue	Ontinue ION Cyber Defense	Zurich, Switzerland
Optiv	Managed Detection and Response	Denver, Colorado, U.S.
Orange Cyberdefense	Managed Threat Detection	Paris, France
Pondurance	Risk-Based Managed Detection and Response	Indianapolis, Indiana, U.S.
Proficio	ProSOC Managed Detection and Response	Carlsbad, California, U.S.
Quorum Cyber	Managed Detection and Response	Edinburgh, U.K.
Rapid7	Managed Detection and Response	Boston, Massachusetts, U.S.
Red Canary	Managed Detection and Response	Denver, Colorado, U.S.
SentinelOne	Vigilance Respond MDR	Mountain View, California, U.S.
Smarttech247	Managed Detection & Response	Cork, Ireland
Sophos	Managed Detection and Response	Santa Clara, California, U.S.
Stratejm	enhanced Managed Detection & Response	Ontario, Canada
Trustwave	Managed Detection and Response	Chicago, Illinois, U.S.
Verizon	Managed Detection and Response	New York City, New York, U.S.
WithSecure	Countercept Managed Detection and Response	Helsinki, Finland

Source: Gartner (June 2024)

Market Recommendations

- MDR services are not a good fit for every organization. As discussed in the Market Analysis section, a variety of delivery styles for MDR services exist, and some are MDR only in name. As part of a drive to increase maturity, organizations must identify whether they will benefit from a combination of service capabilities both inside and outside of MDR. This includes co-managed, SOC-as-a-service engagements or an internal do-it-yourself (DIY) approach.

- Define specific required outputs (incident ticket structure, reports) and goals that address defined use cases before engaging with a provider. As with any outsourcing initiative, if outcomes are not defined, regardless of what service provider is used, the chance of success will be lessened (see How to Make a Successful Security Services RFP). Buyers should also be cautious of overemphasizing the value of SLAs as part of detection-and-response-driven services. This is especially true when many buyers are not able to consume the SLAs that they are constraining their services with.

- As MDR services are "consumable," buyers must develop and operate their own internal incident response policies and procedures. This will ensure that full value of the MDR service can be obtained. Relevant, internal business understanding is critical for the "right" response to a discovered threat. Some MDR providers are positioned to help their customers develop policies and processes if they don't exist or require updating. Internal departments, such as HR and legal, may need to be involved as may incident response service providers (see Market Guide for Digital Forensics and Incident Response Retainer Services).

- Organizations must perform sufficient due diligence on MDR providers before signing a contract. Use an RFP and a proof of concept (POC), and assess the willingness of prospective providers to assess the current state/maturity of the environment. Most importantly, ask for sample deliverables to validate claims and fitness-for-purpose with your organization's requirements. Use other sources as well, such as your peer network and Gartner Peer Insights.

- If you have data residency and strong privacy or other compliance requirements, validate that the MDR providers can comply with them. Focus on MDR providers in your geographic region or those using a data collection architecture that adheres to data residency requirements. Separate log retention may be required as an addition to any MDR service to ensure alignment to regulatory requirements.

Acronym Key and Glossary Terms

BAS	breach attack simulation
CPS	cyber-physical systems
CTEM	continuous threat exposure management
DFIR	digital forensics and incident response
EDR	endpoint detection and response
IaaS	Infrastructure as a service
IoT	Internet of Things
MDR	managed detection and response
MSSP	managed security services provider
OT	operational technology
POC	proof of concept
RFP	request for proposal
SaaS	software as a service
SI	systems integrator
SOC	security operations center
TDIR	threat detection, investigation and response
TI	threat intelligence
TTPs	tactics, techniques and procedures

Note 1: Remote Mitigative Response

Remote mitigative response is defined as disruption or containment actions, such as quarantining hosts and deauthenticating users.

Note 2: Incident Template

Reporting may include:

- A description of the incident, how it was discovered and when it was reported.

- Any findings regarding how the incident occurred.
- A review of the incident timeline and actions taken.
- Recommendations to mitigate future incidents of a similar nature.

Table 2: Example of Typical Security Incident Ticket

(Enlarged table in Appendix)

Detail	Description
Subject	An outline of the issue containing a reference to the priority of the incident.
Notification time	A date and time stamp indicating the send time of the incident.
References	Reference number generated by the provider and internal customer references, if applicable.
Priority	A numerical representation of the priority/intended severity of the issue (usually on a scale of one to four, where one is the highest).
Classification/category	Single-word classification of the type of issue, such as "misconfiguration," "malware" or "phishing."
Date and time of activity	A date and time stamp indicating the time the activity took place; may include specific enrichment details, such as hostnames to separate events across a common incident (could be a window of time or single event).
Source entities	If applicable, the details of hostnames, email addresses, IP addresses, vulnerability details or other identifying factors that pinpoint the sources of the issue.
Destination entities	The details of hostnames, email addresses, IP addresses or other identifying factors that pinpoint the affected assets.
Activity details	A descriptive set of sentences or bullet points that outlines the series of events, specific issues or any other details relevant to the issue that explains the problem discovered.
Risks	A descriptive set of sentences or bullet points that outlines the risks to the business as a result of an activity that may have already occurred or may occur in the future.
Recommended actions	Simple-to-follow, intelligence-led instructions that outline follow-up remedial actions based on the providers' mitigation actions and actions that the business needs to take following notification. This is often opinion-driven and nonmandatory advice.
Mitigation/response actions taken	Details of assets that have been quarantined, users that have been subject to password changes or lockouts, and other details, such as processes/files that have been stopped or deleted, or temporary firewall rules that have been activated.

Source: Gartner

Document Revision History

Market Guide for Managed Detection and Response Services - 14 February 2023

Market Guide for Managed Detection and Response Services - 25 October 2021

Market Guide for Managed Detection and Response Services - 26 August 2020

Market Guide for Managed Detection and Response Services - 15 July 2019

Market Guide for Managed Detection and Response Services - 11 June 2018

Market Guide for Managed Detection and Response Services - 31 May 2017

Market Guide for Managed Detection and Response Services - 10 May 2016

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Quick Answer: Key Questions to Ask When Selecting a Managed Detection and Response (MDR) Provider

Market Guide for Digital Forensics and Incident Response Retainer Services

Implement a Continuous Threat Exposure Management (CTEM) Program

How to Make a Successful Security Services RFP

Emerging Tech: Security — Adoption Growth Insights for Managed Detection and Response

Table 1: Representative Vendors for Managed Detection and Response

Provider	Service Name	Headquarters
Ackcent	Managed Detection and Response	Barcelona, Spain
Aiuken Cybersecurity	MDR SOC	Madrid, Spain
Arctic Wolf Networks	Managed Detection and Response	Eden Prairie, Minnesota, U.S.
Binary Defense	Managed Detection & Response	Stow, Ohio, U.S.
Bitdefender	MDR Advanced/Enterprise	Bucharest, Romania
BlackBerry	Cylance MDR	Irvine, California, U.S.
Critical Insight	Managed Detection and Response	Seattle, Washington, U.S.
Critical Start	Managed Detection and Response	Plano, Texas, U.S.
CrowdStrike	Falcon Complete	Sunnyvale, California, U.S.
Cybereason	Cybereason MDR Complete	Boston, Massachusetts
CYBEROO	Managed Detection and Response	Reggio Emilia, Italy
Cyderes	Enterprise Managed Detection & Response	Kansas City, Missouri, U.S.
Deepwatch	Managed Detection and Response	Denver, Colorado, U.S.
eSentire	Managed Detection and Response	Waterloo, Ontario, Canada
ESET	PROTECT MDR	Bratislava, Slovakia

Eviden	Eviden MDR	Bezons, France
Expel	Expel MDR	Herndon, Virginia, U.S.
Fortra	Managed Detection and Response	Eden Prairie, Minnesota, U.S.
Integrity360	Managed Detection and Response	Dublin, Ireland
Kroll	Kroll Responder	New York, New York, U.S.
Kudelski Security	MDR ONE Resolute	Cheseaux-sur-Lausanne, Switzerland; and Phoenix, Arizona
Lmntrix	Managed Detection and Response	Orange, California, U.S.
Mandiant	Managed Defense	Reston, Virginia, U.S.
mnemonic	Managed Detection and Response	Oslo, Norway
Obrela Security Industries	MDR Core	London, U.K.
Ontinue	Ontinue ION Cyber Defense	Zurich, Switzerland
Optiv	Managed Detection and Response	Denver, Colorado, U.S.
Orange Cyberdefense	Managed Threat Detection	Paris, France
Pondurance	Risk-Based Managed Detection and Response	Indianapolis, Indiana, U.S.
Proficio	ProSOC Managed Detection and Response	Carlsbad, California, U.S.
Quorum Cyber	Managed Detection and Response	Edinburgh, U.K.
Rapid7	Managed Detection and Response	Boston, Massachusetts, U.S.
Red Canary	Managed Detection and Response	Denver, Colorado, U.S.

SentinelOne	Vigilance Respond MDR	Mountain View, California, U.S.
Smarttech247	Managed Detection & Response	Cork, Ireland
Sophos	Managed Detection and Response	Santa Clara, California, U.S.
Stratejm	enhanced Managed Detection & Response	Ontario, Canada
Trustwave	Managed Detection and Response	Chicago, Illinois, U.S.
Verizon	Managed Detection and Response	New York City, New York, U.S.
WithSecure	Countercept Managed Detection and Response	Helsinki, Finland

Source: Gartner (June 2024)

Table 2: Example of Typical Security Incident Ticket

Detail	Description
Subject	An outline of the issue containing a reference to the priority of the incident.
Notification time	A date and time stamp indicating the send time of the incident.
References	Reference number generated by the provider and internal customer references, if applicable.
Priority	A numerical representation of the priority/intended severity of the issue (usually on a scale of one to four, where one is the highest).
Classification/category	Single-word classification of the type of issue, such as “misconfiguration,” “malware” or “phishing.”
Date and time of activity	A date and time stamp indicating the time the activity took place; may include specific enrichment details, such as hostnames to separate events across a common incident (could be a window of time or single event).
Source entities	If applicable, the details of hostnames, email addresses, IP addresses, vulnerability details or other identifying factors that pinpoint the sources of the issue.
Destination entities	The details of hostnames, email addresses, IP addresses or other identifying factors that pinpoint the affected assets.
Activity details	A descriptive set of sentences or bullet points that outlines the series of events, specific issues or any other details relevant to the issue that explains the problem discovered.

Risks	A descriptive set of sentences or bullet points that outlines the risks to the business as a result of an activity that may have already occurred or may occur in the future.
Recommended actions	Simple-to-follow, intelligence-led instructions that outline follow-up remedial actions based on the providers' mitigation actions and actions that the business needs to take following notification. This is often opinion-driven and nonmandatory advice.
Mitigation/response actions taken	Details of assets that have been quarantined, users that have been subject to password changes or lockouts, and other details, such as processes/files that have been stopped or deleted, or temporary firewall rules that have been activated.

Source: Gartner