Market Guide for Managed Detection and Response Services

Published 14 February 2023 - ID G00761083 - 25 min read

By Analyst(s): Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies

Initiatives: Security Operations; Build and Optimize Cybersecurity Programs

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.

Additional Perspectives

- Invest Implications: Market Guide for Managed Detection and Response Services (22 February 2023)
- Summary Translation: Market Guide for Managed Detection and Response Services (27 March 2023)

Overview

Key Findings

- Misnamed technology-centric offerings and vendor-delivered service wrappers (VDSW), that fail to deliver human-driven managed detection and response (MDR) services, are causing challenges for 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.
- MDR buyers must focus on the ability to provide context-driven insights that will directly impact their business objectives, as wide-scale collection of telemetry and automated analysis are insufficient when facing uncommon threats.
- An increasing number of MDR customers demand that providers are able to 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 consuming organization affect adoption.

Recommendations

As a security and risk management leader responsible for security operations, you should:

- Use MDR services to obtain 24/7, remotely delivered, human-led security operations capabilities when there are no existing internal capabilities, or 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 and 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 to ensure a business-centric response.
- Investigate whether the MDR provider's service is able to align with your business-driven requirements and 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 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today.

Market Definition

This document was revised on 23 February 2023. For more information, see the Corrections *page on gartner.com.*

Managed detection and response (MDR) services provide customers with remotely delivered security operations center (SOC) functions. These functions allow organizations to rapidly detect, analyze, investigate and actively respond through threat disruption and containment. They offer a turnkey experience, using a predefined technology stack that commonly covers endpoint, network, logs and cloud. Telemetry is analyzed within the provider's platform using a range of techniques. This process allows for investigation by experts skilled in threat hunting and incident management, who deliver outcomes that businesses can act upon.

Core capabilities include:

- 24/7 remotely delivered detection and response functions.
- A provider-operated technology stack that enables and coordinates real-time threat detection, investigation and active mitigating response. Whether it is developed by the MDR provider, an integrated set of commercial technologies that use modern techniques (like APIs) to exchange data and instructions, or a combination of both approaches.
- Staff that engage daily with individual customer data and have skills and expertise in threat monitoring, detection and hunting, threat intelligence (TI) and incident response.
- Turnkey delivery, with predefined and pretuned processes and detection content. This includes a standard playbook of workflows, procedures and analytics, and requires a minimum viable set of telemetry to deliver services; offering integration with third-party detection and response technologies beyond provider-owned technologies.
- The availability of immediate remote mitigative response, investigation and containment activities (such as quarantining hosts and deauthenticating users) beyond alerting and notification, delivered and coordinated by service provider staff.

- Triage, investigate and manage responses to all discovered threats, regardless of priority with no limitations on volumes or time dedicated to the discovery and investigation process.

Optional capabilities include:

- Additional contextual data sources providing details of security exposures such as vulnerabilities, attack surface visibility, and brand and reputational analysis.
- Digital forensics and incident response retainer capabilities (DFIR) offering call-off remote or deployable staff to carry out deep dive incident and root cause analysis.
- Security assessment and validation capabilities, such as breach and attack simulation (BAS), that analyze the efficacy of security controls and response processes, and provide clients with guidance on how to improve their defensive posture.
- 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. Different from threat hunting, which is included as part of MDR and hunts for known threat techniques.

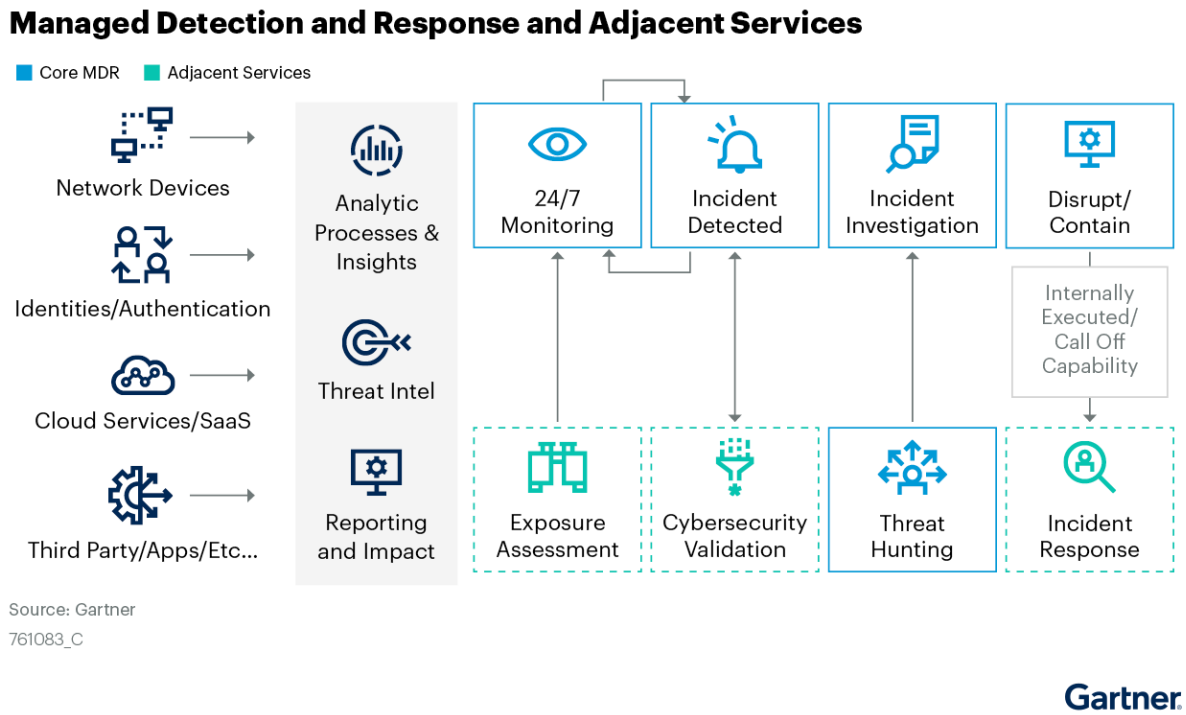
Market Description

MDR provides customers with remotely delivered, human-led SOC functions for the purposes of reporting, rapid detection, analysis and investigation of threats as well as remote mitigative response to those threats (see Note 1).

MDR service providers deliver these capabilities using a variable combination of 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, 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 nonexistence of a threat 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 which 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.

Figure 1: Managed Detection and Response and Adjacent Services



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

Market Direction

MDR is a high-growth, established market (see Market Share: Managed Security Services, Worldwide, 2021 where MDR is a distinct segment, the MDR market grew 48.9% from 2020 to 2021).

Successful MDR service providers offer a focus on high-fidelity threat detection, investigation and mitigative response with high verbosity, and human interpretable reporting aligned to business-focused risks. The provider takes responsibility for determining how threats are detected. Customers may 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-led services as part of the core MDR service, as this may possibly 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 TI 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 and then 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, beyond traditional vulnerability analysis:**
  - Exposure management capabilities help with the prevention of attacks through increased awareness of their attack surface, 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 300 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, or offer detection and response as well as wider IT security specific services. MDR services are also available through managed services providers (see Market Guide for Managed Security Services), 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 (such as critical infrastructure and manufacturing, or healthcare, which all have privacy, safety and reliability risk concerns). For more information, see Innovation Insight for Cyber-Physical Systems Protection Platforms.

Detecting a threat is meaningless without a preplanned, timely response to that threat.

Market Analysis

The key value proposition of MDR is the human interpretation of security incidents, providing guidance, as well as performing the initial mitigation steps, that would otherwise be complex to understand and enact. By providing context-led investigation, analysis and threat validation (and 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.

Capabilities providing mitigative response, to disrupt or contain threats, is a core capability of MDR service providers. Many of these mitigative response actions are centered around using EDR solutions to disrupt or contain a threat, for example to isolate an endpoint or kill malicious processes. However, response actions are increasingly focused on modern corporate architecture and identity-centric functions (such as account restrictions in authentication systems) which enable an MDR provider's response to be effective across platforms, into cloud and SaaS as well as on-premises.

MDR Service Delivery Styles Vary, Beware of Lesser Services That Mimic MDR

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

- Organizations that have threat detection, investigation and response (TDIR) capability investments, but consider themselves to be unable to manage these 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.
- Organizations that have a long-term vision of owning TDIR internally but need to achieve a level of maturity quickly, and wish to use services to provide interim coverage while they hire, skill up and develop requirements for SOC operations.

MDR providers must operate technology centrally, in a multitenant fashion to achieve the scale and consistency that buyers demand, and to 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-, 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, but rarely called out separately from core IT security requirements; organizations recognize that cyberthreats are cyberthreats, no matter the system they reside in.

Buyers have faced challenges with service naming and marketing language that has often overpromised and under delivered. Core service capabilities and components 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. There are many areas where new terminology, buzzwords and acronyms have surfaced and provided confusion in the market:

- **Simply delivering a managed technology service** — Services which deliver a light overlay to either existing technology investments, such as endpoint detection and response (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 managed EDR (MEDR). Commonly delivered by technology providers, greater internal staffing, skill sets and engagement is required to truly get value from these services. Such services are also often delivered using security information and event management (SIEM) technology (see Gartner's Market Guide for Managed SIEM Services).

- **Managed extended detection and response** — An attempt to appear more in-depth than MDR services, managed extended detection and response is commonly interchanged with MDR as a service term, but it is not yet proven to actually deliver more capability or better outcomes. As suggested by the name, managed extended detection and response technology utilizes a broader range of telemetry than, for example, EDR alone. However, MDR services typically utilize telemetry from a wide number of sources. Buyers should scrutinize managed extended detection and response offerings more closely to ensure they are not simply being offered a managed technology offering (similar to that of MEDR) if they require the MDR capabilities defined within this research.

- **Renamed historic threat detection services** — Some vendors have offered services for a number of years that provide SOC capabilities as a service. Many of these services could be described as being more aligned to managed SIEM or heavily customized on a per-customer basis. 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. These services can provide high levels of quality and detail in outputs but regularly take longer to deliver, are more expensive and require far more direction from the buyer in regards to scope and evolution.

Some MDR providers are more flexible about using security technologies already owned by buyers. These providers will have a defined set of technologies and vendors that are supported, and usually depend on the ease of integration (e.g., through APIs) and the utility of that technology (e.g., the ability to produce useful telemetry, detect threats and support incident response activities).

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 agnosticism. 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.

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, giving third-party providers access and control on top of existing internal access for security teams.

The willingness to use more technology-agnostic services is increasing the need to mandate a minimum set of telemetry to 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 Services Must Demonstrate Ability to Address Threats in Modern Infrastructure

Modern infrastructure includes the use of SaaS, IaaS, third-party subscriptions, open-source tools and a wide variety of internally developed applications. The traditional model of on-premises devices, boundary firewalls and business-specific endpoint devices is beginning to fade. MDR buyers must demand compatibility for the areas of their infrastructure that are most critical to their mission. This means not only visibility into those areas, but also mitigative response. “Identity” is fast becoming an 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 Tier 1 and 2 analyst cohort or an extended part of their existing SOC. Clients expect their providers to be able to perform investigation and containment on their behalf. This is most visible as customers allow MDR providers to perform remote disruption and containment activities to support internal incident response processes.

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 on their behalf.

When buyers are uncomfortable with the providers directly performing the actions, they want easy mechanisms to approve or initiate any threat disruption or containment actions themselves. The full response to a threat is not typically something performed by MDR providers. However, security and risk management leaders should be demanding threat disruption and containment from their service providers. Remediation activities 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, this 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. Although some of the most progressive MDR providers are able to be business-risk aligned, it is important to qualify whether the service they offer stems from your organization's specific risk-focused requirements and delivers outcomes internal teams will be able to act on. Focus on the detail of the outcomes MDR providers offer, and identify the best way to integrate an MDR service provider's outputs and coverage into your own internal incident response processes. Fine-tuning the security processes is critical if you hope to improve overall outcomes. It is also important to allow internal resources to work with your providers, as this will improve outcomes and help maintain good working relationships with providers.

Evolution of the MDR Market

Increase in the Relevance of Threat Exposure

An organization's exposure to security threats is more than just vulnerability, and with the SaaS and IaaS expansion of infrastructure, managing discovered issues is harder and more voluminous. MDR providers have begun looking at how they can approach a connection between traditional threat detection, reducing a client's attack surface (see Innovation Insight for Attack Surface Management), and discovery of threats and exposures in modern infrastructure. Presenting a risk-based view of threat exposures that clients are able to prioritize should be the core objective of such a capability. This should be executed through effective communication of the business impact of hypothesized security scenarios. There is still a large amount of immaturity in cloud platform visibility, but the relevance of including preventative exposure-driven analysis will likely match and possibly exceed the reactive nature of traditional threat detection in the next few years (see Predicts 2023: Enterprises Must Expand From Threat to Exposure Management).

MDR 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, and 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 exactly 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 agnostic in the way they deliver their services. This approach starts to resemble traditional SOC services from managed security services providers (MSSPs), but with a stronger emphasis on disruption and containment activities in addition to the typical alerting and notification.

Complementary Cybersecurity Validation

Buyers continue to struggle to test the claims of security service vendors — especially those vendors that overprotect the intellectual property (detection content) that they develop to detect threats for the services offered. BAS and automated penetration testing capabilities are commonly seen as an effective way to validate vendor claims regarding coverage and complexity of detection mechanisms. An attractive approach for buyers is having a third-party, independent testing and simulations provider offer the ability to validate capabilities and harden security posture during the course of an engagement.

Self-Service Technology Availability

An expanding presence in the managed security market and an increase in "as-a-service" demands have driven a number MDR providers to offer their technology platforms 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." It will also support a natural maturity evolution for clients that want more control over and visibility into their security events and issues. These clients may find that as-a-service options support potential migration away from tools and technologies that they no longer want responsibility for managing.

MDR Market Merger and Acquisition Activity

During the past 12 months, there have been many acquisitions in this market.

In 1Q22 and 2Q22:

- Google Buys Mandiant
- Herjavec Group and Fishtech Group Agree Merger
- ReliaQuest Buys Digital Shadows
- Fortra Buys Alert Logic
- Arctic Wolf Buys Tetra Defense
- Forescout Buys Cysiv

In 3Q22 and 4Q22:

- Open Systems Buys Tiberium
- Security On-Demand Buys/Unifies with Booz Allen Hamilton's MTS service to Create DeepSeas

- Allurity Buys Aiuken
- CrowdStrike Buys Reposify
- Fortra Buys Alert Logic

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.

Market Introduction

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 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

(Enlarged table in Appendix)

Provider	Service Name	Headquarters
Ackcent	Managed Detection and Response	Barcelona, Spain
Aiuken	Managed Detection and Response	Madrid, Spain
Arctic Wolf Networks	Managed Detection and Response	Eden Prairie, Minnesota
Atos	Managed Detection and Response	Bezons, France
Binary Defense	Managed Detection & Response	Stow, Ohio
Bitdefender	MDR Advanced/Enterprise	Bucharest, Romania
BlueVoyant	Managed Detection and Response	New York, New York
Critical Insight	Managed Detection and Response	Seattle, Washington
Critical Start	Managed Detection and Response	Plano, Texas
CrowdStrike	Falcon Complete	Sunnyvale, California
Cybereason	Cybereason MDR Complete	Boston, Massachusetts
CYBEROO	Managed Detection and Response	Reggio Emilia, Italy
Cyderes [2]	Enterprise Managed Detection & Response	Kansas City, Missouri
Cysiv	SOC-as-a-Service	San Jose, California
DeepSeas [1]	Managed Threat Services (MTS)	McLean, Virginia
Deepwatch	Managed Detection and Response	Denver, Colorado
eSentire	Managed Detection and Response	Waterloo, Ontario
Expel	Expel MDR	Herndon, Virginia
Fortra	Managed Detection and Response	Eden Prairie, Minnesota
Integrity360	Managed Detection and Response	Dublin, Ireland
IBM	Managed Detection and Response	Armonk, New York
Kroll	Kroll Responder	New York, New York
Kudelski Security	Managed Detection and Response	Cheseaux-sur-Lausanne, Switzerland; and Phoenix, Arizona
Mandiant	Managed Defense	Alexandria, Virginia
mnemonic	Argus Managed Defence	Oslo, Norway
NCC Group	Managed Detection and Response	Manchester, U.K.
Obrela Security Industries	Managed Threat Detection and Response	London, U.K.
Ontinue (the MDR division of Open Systems)	Managed Detection and Response	Zurich, Switzerland
Optiv	Managed Detection and Response	Denver, Colorado
Orange Cyberdefense	Managed Detection and Response	Paris, France
Pondurance	Managed Detection and Response	Indianapolis, Indiana
Proficio	Managed Detection and Response	Carlsbad, California
Quorum Cyber	Azure Sentinel SOC & MDR	Edinburgh, U.K.
Rapid7	Managed Detection and Response	Boston, Massachusetts
Red Canary	Managed Detection and Response	Denver, Colorado
Secureworks	Managed Detection and Response	Atlanta, Georgia
Sophos	Managed Detection and Response	Santa Clara, California
Trustwave	Managed Detection and Response	Chicago, Illinois
Verizon	Managed Detection and Response	New York City, New York
WithSecure	Countercept Managed Detection and Response	Helsinki, Finland

[1] Formerly Booz Allen Hamilton
[2] Merger between Herjavaec and Fishtech

Source: Gartner (February 2023)

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, including co-managed, SOC-as-a-service engagements or an internal 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 What Makes a Successful Security Service RFP?). Buyers should also be cautious of overemphasizing the value of SLAs as part of detection-and-response-driven services.
- As MDR services are "consumable," buyers must develop and operate their own internal incident response policies and procedures, to 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).
- Organizations must perform sufficient due diligence on the MDR providers before signing a contract. Use an RFP and a proof of concept (POC), and 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 and attack simulation
CAGR	compound annual growth rate
CASB	cloud access security broker
CIPS	cloud infrastructure and platform services
CNAPP	cloud-native application protection platform
CWPP	cloud workload protection platform
DFIR	digital forensics and incident response
EDR	endpoint detection and response
EPP	endpoint protection platform
IoT	Internet of Things
MDR	managed detection and response
MSSP	managed security services provider
NSM	network security monitoring
OT/ICS	operational technology and industrial control systems
SOAR	security orchestration, automation and response
SOC	security operations center
TI	threat intelligence
PTaaS	penetration testing as a service
TTPs	tactics, techniques and procedures

Note 1: Managed Detection and Response

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

Document Revision History

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: What Key Questions Should I Ask When Selecting an MDR Provider?

Market Guide for Digital Forensics and Incident Response Services

What Makes a Successful Security Service RFP?

Market Share: Managed Security Services, Worldwide, 2021

Emerging Tech: Adoption Growth Insights for Managed Detection and Response

Table 1: Representative Vendors

Provider	Service Name	Headquarters
Ackcent	Managed Detection and Response	Barcelona, Spain
Aiuken	Managed Detection and Response	Madrid, Spain
Arctic Wolf Networks	Managed Detection and Response	Eden Prairie, Minnesota
Atos	Managed Detection and Response	Bezons, France
Binary Defense	Managed Detection & Response	Stow, Ohio
Bitdefender	MDR Advanced/Enterprise	Bucharest, Romania
BlueVoyant	Managed Detection and Response	New York, New York
Critical Insight	Managed Detection and Response	Seattle, Washington
Critical Start	Managed Detection and Response	Plano, Texas
CrowdStrike	Falcon Complete	Sunnyvale, California
Cybereason	Cybereason MDR Complete	Boston, Massachusetts
CYBEROO	Managed Detection and Response	Reggio Emilia, Italy
Cyderes [2]	Enterprise Managed Detection & Response	Kansas City, Missouri
Cysiv	SOC-as-a-Service	San Jose, California
DeepSeas [1]	Managed Threat Services (MTS)	McLean, Virginia

Deepwatch	Managed Detection and Response	Denver, Colorado
eSentire	Managed Detection and Response	Waterloo, Ontario
Expel	Expel MDR	Herndon, Virginia
Fortra	Managed Detection and Response	Eden Prairie, Minnesota
Integrity360	Managed Detection and Response	Dublin, Ireland
IBM	Managed Detection and Response	Armonk, New York
Kroll	Kroll Responder	New York, New York
Kudelski Security	Managed Detection and Response	Cheseaux-sur-Lausanne, Switzerland; and Phoenix, Arizona
Mandiant	Managed Defense	Alexandria, Virginia
mnemonic	Argus Managed Defence	Oslo, Norway
NCC Group	Managed Detection and Response	Manchester, U.K.
Obrela Security Industries	Managed Threat Detection and Response	London, U.K.
Ontinue (the MDR division of Open Systems)	Managed Detection and Response	Zurich, Switzerland
Optiv	Managed Detection and Response	Denver, Colorado
Orange Cyberdefense	Managed Detection and Response	Paris, France
Pondurance	Managed Detection and Response	Indianapolis, Indiana
Proficio	Managed Detection and Response	Carlsbad, California
Quorum Cyber	Azure Sentinel SOC & MDR	Edinburgh, U.K.

Rapid7	Managed Detection and Response	Boston, Massachusetts
Red Canary	Managed Detection and Response	Denver, Colorado
Secureworks	Managed Detection and Response	Atlanta, Georgia
Sophos	Managed Detection and Response	Santa Clara, California
Trustwave	Managed Detection and Response	Chicago, Illinois
Verizon	Managed Detection and Response	New York City, New York
WithSecure	Countercept Managed Detection and Response	Helsinki, Finland

[1] Formerly Booz Allen Hamilton
[2] Merger between Herjavaec and Fishtech

Source: Gartner (February 2023)