Market Guide for Managed Detection and Response Services

Published 26 August 2020 - ID G00722909 - 22 min read

By Analysts Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

Initiatives: Security Operations

MDR services offer turnkey threat detection and response via modern, remotely delivered, 24/7 security operations center capabilities and technology. Security and risk management leaders should use this research to determine whether MDR is a good fit with their operational security requirements.

Overview

Key Findings

- The number and variety of MDR providers continues to grow rapidly in an established, but competitive market.
- Buyers are challenged to differentiate among the variations in delivery approaches and technologies used by MDR service providers.
- The acceptance of active responses, such as containing or disrupting a threat, by MDR customers is increasing. However, adoption varies according to the trust level with the provider, the customer's geography, the organization's size and the maturity of security operations.
- Coverage for cloud services, such as software as a service and infrastructure as a service, has improved during the past 12 months; however, it is still a work in progress for many MDR service providers.

Recommendations

Security and risk management leaders responsible for security operations should:

- Use MDR services to add remotely delivered modern 24/7 security operations center functions in a turnkey approach when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing capabilities.
- Embrace containment actions as an incident response capability of MDR service providers when there are no internal 24/7 operations to respond to threats that require immediate attention.

- Assess how the MDR provider's containment approach can integrate with your organization's policies and procedures.
- Ensure the MDR providers technology stack fits well with your existing security controls and IT environment, from on-premises to cloud.
- Use MDR providers that have experience with use cases appropriate to your organization's size, location and industry vertical. Use any unique challenges in your industry vertical to differentiate potential providers.
- Consider managed security service providers that offer MDR services when security technology and device management, and compliance use cases are required. Data residency requirements may also drive consideration of an MSSP over an MDR service provider.

Strategic Planning Assumption

By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities.

Market Definition

Threat monitoring, detection and response (MDR) services provide customers with remotely delivered modern security operations center (SOC) capabilities to rapidly detect, analyze, investigate and actively respond to threats (e.g., containment or disruption). MDR service providers offer a turnkey experience, with many using a predefined technology stack covering endpoints, networks, cloud services, operational technology (OT)/Internet of Things (IoT) and other sources, to collect relevant logs, data and other telemetry (e.g., forensic data, contextual information). This telemetry is analyzed via the provider's platform using a range of analytics, threat intelligence (TI) and manual analysis from experts skilled in incident detection and response. Human-performed, threat-hunting services complement real-time monitoring and detection capabilities to find novel and sophisticated threats.

MDR services offer turnkey threat detection and response via modern, remotely delivered, 24/7 security operations center (SOC) capabilities and technologies. Security and risk management (SRM) leaders should use this research to determine whether MDR services are a good fit for their security operations requirements.

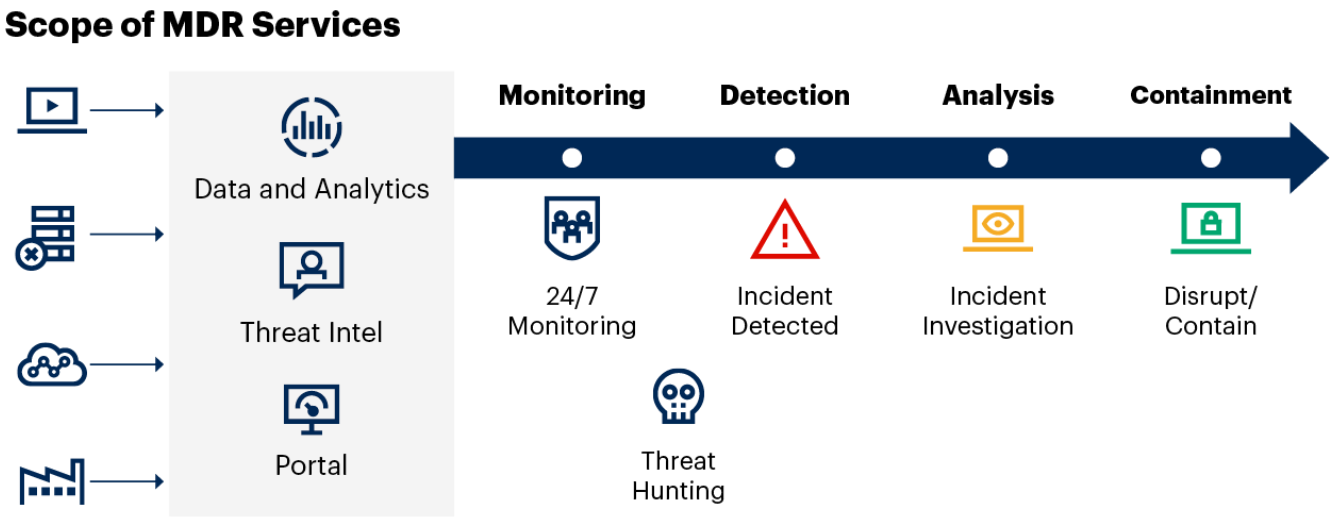
Market Description

The MDR services market is composed of providers offering 24/7 threat MDR services. They emphasize performing incident response functions and activities on behalf of the customer (e.g., acting like an extension of the customer's security team) across on-premises locations, remote assets, cloud services and OT/ICS environments. MDR services are designed to reduce the time to detect, as well as the time to respond to threats. They deliver customers the people, expertise, processes and technologies of a modern SOC in an easy-to-consume and standardized approach

(see "Selecting the Right SOC Model for Your Organization"). Additional security operations functions, such as vulnerability management and log management, which are typically offered by managed security service providers (MSSPs), have emerged to complement the threat monitoring, detection and response offerings.

MDR service providers deliver these capabilities using technologies — at the host, network, application and, increasingly, the cloud services layers — that generate and/or collect security log data and alerts. In addition, telemetry provides contextual information (e.g., identity and user, vulnerabilities and business criticality). Providers develop threat-focused content and analytics (aka detection engineering), use of TI, and manual and automated incident response activities, such as triage, investigation and containment actions (see Figure 1). Threat hunting can augment real-time threat detection to find attacks employing tactics, techniques and procedures (TTPs) that bypassed existing prevention and detection capabilities.

Figure 1: Scope of MDR Services



Source: Gartner
722909_C

MDR services are characterized by the following attributes:

- They provide customers with a modern, remotely delivered 24/7 SOC outcome. A modern SOC requires:
  - Applicable technologies to detect, investigate and respond to threats.
  - Staff that have skills and expertise in threat monitoring, detection and hunting, threat intelligence (TI), and incident response.
  - Processes that include a standard playbook of workflows and procedures.

- Successful MDR services providers deliver these capabilities in a packaged delivery model to buyers:
  - A focus on high-fidelity threat detection and validation, geared toward attacks that have bypassed preventative security controls.
  - Remote incident response investigation and containment activities beyond alerting and notification. Threats move too fast for most organizations these days. Depending on the type of threat and the environment targeted, this could have an impact on data confidentiality, availability to operations (e.g., a destructive ransomware event), an impact on privacy (e.g., breach of customer data), or even an impact on physical safety (e.g., an attack on industrial control system [ICS]/supervisory control and data acquisition [SCADA] systems or medical devices).
  - Selective use of technologies and a turnkey model to enable the MDR provider's team to quickly implement and deliver services. To support the activities performed and the outcomes being delivered depends on and, in many cases, mandates a specific set of technologies (see "Tips for Selecting the Right Tools for Your Security Operations Center").
  - A common delivery platform for all customers. The platform uses TI and custom analytics. In some cases, the platform may use behavioral and machine learning (ML)-powered analytics too.
  - The provider takes responsibility for determining what and how threats are detected. Customers may have little opportunity to customize threat detection use cases relative to their environment. For example, the MDR providers might be looking for specific TTPs that indicate a threat is active in a customer's environment. However, if the customer wants some rules specific to their environment, that level of customization may not be supported.

Other elements of MDR are emerging in the market, but are not yet commonplace. These may appeal to buyers, especially as they look for differentiation in a market:

- Expanding into other security operations functions, such as vulnerability management. The typical pattern observed with many Gartner clients that are less mature in their security operations, is to start with threat detection and response capabilities. Expansion into vulnerability management capabilities can be used to address compliance mandates and help with the prevention of attacks by reducing the exposures in the customers environment proactively, and for better incident enrichment and response guidance. Once that has been addressed, and assuming trust and a solid relationship has been established, buyers may look to that provider to help them address other security operations challenges, such as log management (usually for compliance requirements).
- Exposing security orchestration and automation (SOA) capabilities to customers. In addition to the MDR provider using SOA capabilities internally to improve operations, some MDR providers

are exposing orchestration and automation to enable their customers to define response workflows and activities.

- Expanding the technology stacks to detect and mitigate threats earlier in the cyber kill chain. This includes the use of email monitoring and Domain Name System (DNS) monitoring.

Market Direction

MDR market growth and awareness continues. Gartner has observed a 44% growth in end users' inquiries during the past 12 months.

MDR services are available from an increasing number of providers, some net new and others, such as MSSPs, that are shifting their offerings to better align with the characteristics of MDR. After limited concern during the past couple of years, traditional MSSPs are now adding MDR service offerings to their portfolios. This has been achieved organically by acquisition, with large MSSPs acquiring existing MDR providers, and some building them from the ground up.

Many MDR providers target a few verticals where they can offer more-specific expertise and services, such as critical infrastructure and manufacturing, or healthcare, which have privacy, safety and reliability risk concerns (see "How to Develop a Security Vision and Strategy for Cyber-Physical Systems").

> **Security leaders are increasingly cognizant that reducing the time to detect a threat is meaningless without a corresponding reduction in the time to respond to a threat to enable a return to a known good state.**

A key value proposition of MDR is performing most of the incident response process. Timely and accurate incident response takes time and skill, which many organizations just don't have, especially when multiple threats need to be addressed simultaneously. By providing deeper investigation, analysis and validation of threats, and taking action to disrupt or contain an attack, the MDR provider can buy time for the customer to perform further investigation and remediation. This can result in reduced risk to an organization from increasingly hostile and impactful threats (see "How to Respond to the 2020 Threat Landscape").

Market Analysis

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

- Organizations that have minimal in-house threat MDR capabilities, where an MDR service forms the primary (sometimes only) security operations capability. These buyers usually have few, if

any, security-specific experts, and often have security operations responsibilities federated across the IT teams. They buy preventative controls, such as multifunction network firewalls and endpoint protection platforms (EPPs). They may lack security technologies that provide forensic data, such as endpoint detection and response (EDR) or network packet capture, or address the security of cloud services. 24/7 IT or security operations are usually not available to support response activities.

- Organizations that have threat detection technologies, but are not going to build and operate their own SOC. Such organizations prefer engaging MDR providers that can support their technology of choice (such as EDR).
- Organizations that don't have the staff to expand their capabilities, nor the experience required to run some of the advanced technologies that MDR providers use and to have this managed, maintained and operated by specialists 24/7.
- Organizations that just want to obtain "a modern SOC" by outsourcing to a provider, leaving them to focus their internal resources on other security and risk activities.
- Organizations that have a SOC and want to use MDR services to fill in gaps in their capabilities (such as threat hunting) or act as a "second set of eyes" for their SOCs.
- Organizations that are not capable of maintaining the mapping of threats against security technologies. The ability to answer the question, "Do we have all that is necessary to detect the most common and known threats?" is not trivial. MDR services are a good way to gain this expertise.

Different MDR Service Delivery Styles Address the Various Buyers in the Market

A number of MDR providers bring their own proprietary technologies to the engagement. Typically, the delivery platform is centrally managed and multitenant, providing functions like log and data management, analytics, orchestration and automation, and the user interface (UI) to customers.

Some MDR providers are more flexible about using security technologies already owned by buyers, but most are not entirely technology-agnostic. These providers will have a defined set of technologies and vendors that are supported, and usually depend on the ease of integration and the utility of that technology (e.g., the ability to produce useful telemetry, detect threats, and support incident response activities).

- **Full technology stack from the provider** — This style involves the provider leveraging two or more threat-detection-oriented technologies to deliver MDR services. These technologies are selected and provided by the provider. That is, the customer doesn't get a choice in the technologies used, because it's delivered "as a service," or might have a limited choice, such as which of two EDR products will be used. The two most common components are a multifunction network security monitoring (NSM) sensor or appliance and an EDR agent. Both of

these technologies provide capabilities oriented toward near-real-time threat detection, as well as forensic data for investigations. Some providers may also use other technologies to detect threats, such as deception technologies, and will also monitor other attack vectors, such as cloud services, email and DNS. This is a "multimode" type of service and is recommended for the ability to provide better outcomes.

- **Technologies for monitoring cloud services, OT/ICS and IoT** — Some MDR vendors have proprietary technologies and approaches to support assets and environments beyond standard on-premises IT. They may be available as add-on or even stand-alone MDR services, such as in the case of monitoring ICS and SCADA systems, or IoT devices in medical provider environments. Increasingly, MDR providers are starting to support cloud environments as add-ons through their own technologies (e.g., through the use of integrations and their analytics platform) and partnerships with other vendors as cloud access security brokers (CASBs), cloud security posture management (CSPM; see "Innovation Insight for Cloud Security Posture Management") and cloud security workload protection (CWPP; see "Market Guide for Cloud Workload Protection Platforms.") This is still a work in progress for many MDR service providers.

- **Managed point solutions** — Managed EDR is often used interchangeably with MDR, when it's actually one style or a "single mode." Managed EDR may have limited visibility of threats in a customer's environment, depending on the assets and environments that need to be monitored. For example, you can't install an EDR agent on a multifunction printer/scanner device or a programmable logic controller (PLC).

- **BYO technology stack** — These providers deliver modern SOC functions that leverage customers' technologies, with the caveat that they are not data-source-agnostic and implementation needs to be as turnkey as possible. MDR providers tend to heavily curate the range of the technologies and vendors they will support. Providers may mandate a minimum set of technologies (likely with a subset of supported vendors), which will allow the MDR provider to:

  - Easily onboard the technology (e.g., API connectivity is necessary)
  - Generate high-enough fidelity detections
  - Provide enough forensic and/or contextual information to investigate incidents
  - Allow the provider to execute active response actions (containment) on behalf of the customer

An example of this might be a mandated set of technologies that includes network firewalls with support for advanced threat detection features (see "Magic Quadrant for Network Firewalls"), EDR telemetry and Active Directory (AD) logs, covering identities, endpoints and the network.

The Importance of Rapid Incident Response to Augment Threat Monitoring and Detection Is Growing

Buyers continue to push MDR providers to do more. Gartner clients look to MDR providers to be the security team or an extended part of their team for security operations. Clients expect their providers to perform thorough incident response work on their behalf. This is most visible as customers allow MDR providers to perform more elements of the incident response function. In North America, but less so in Europe, the Asia/Pacific (APAC) region or Latin America, Gartner clients increasingly state that they want their MDR service providers to deliver active responses.

When customers are uncomfortable with the providers performing the actions, they want easy mechanisms to initiate any threat containment or disruption actions themselves. MDR service providers indicate that it takes 90 days, on average, for a customer to gain confidence and trust in the service delivery before they allow providers to take active responses for them.

Threat remediation is rarely performed by MDR providers; however, security leaders should be demanding threat containment. Once a threat has established itself in an environment, usually on an endpoint or server, or within the control plane of a cloud service provider, fully remediating a threat, such as removing a binary and backing out all the changes made or doing a system rebuild, is done by the customer. This is after their MDR providers have contained or disrupted threats. Where EDR is deployed, the ability to remove an attacker from an endpoint is feasible, but will depend on the risk appetite of the customer (e.g., do I trust that attackers and their tools have been entirely cleaned). Customers also want to know whether this will fit in existing policies and procedures, and whether it will impact any regulatory concerns for managing IT systems. Some MDR providers that offer incident response retainers may also assist with the recover phase. If this is not an option (or the customer has other options), then it's the customer's responsibility to manage.

Security Processes Are Still Owned by You

MDR can be a compelling offering, but it is not all encompassing. Security leaders are advised to focus on the "process" piece here and finding the best way to integrate an MDR service provider's capabilities into your incident response processes (see "Develop a Comprehensive Incident Response Process"). Fine-tuning your security processes is critical if you hope to improve your overall outcomes. It is also important to allow internal resources to work with your providers. This will improve outcomes and maintain good working relationships with providers (see "Success With Security Service Providers Requires Open Communication").

Some example processes include:

- Vulnerability management
- Security of specialized environments (OT/ICS)
- Technical testing (e.g., penetration testing and red/purple team)

The MDR Service Market Continues to Evolve

Some areas during the past 12 months highlight how the market is evolving and maturing. There is an expansion of threat detection and response services for cloud environments, which is steadily becoming more visible, as MDR services providers mature and expand their offerings. However, it's still early. Coverage for popular SaaS applications such as Microsoft 365, Google G Suite and Box is increasing, but broad coverage for SaaS, such as via a CASB solution in the provider's technology stack, is still rare. Comprehensive coverage for infrastructure as a service (IaaS) is still in the early stage. Some providers have invested in monitoring IaaS and platform as a service (PaaS) via proprietary approaches, using proprietary technology solutions or via adding solutions to their tech stacks and service offerings.

Some providers are using proprietary or commercial security orchestration, automation and response (SOAR) tools, particularly to improve their internal SOC efficiency, while assisting clients by reducing dwell time. Some providers are starting to expose these orchestration and automation capabilities to their customers, which may require more interaction and work with the provider. This may not appeal to buyers that just want to lean on providers as the experts, but it will appeal to buyers looking for more flexibility in interacting and customizing their MDR experiences.

As some MDR providers target more-mature buyers, the scope of log sources is expanding, based on the realization that turnkey services that require a set of technologies from the provider are not optimal for organizations with existing investments in security tools. Some providers are even expanding into log-agnostic analytics to detect threats. However, this approach starts to look closer to traditional SOC services from MSSPs, but with a stronger emphasis on incident response activities (not just alerting and notification).

The challenges of accommodating any log or alerting source the customer wants may be difficult for the customer and the provider. For example: Are the logs going to require customization to analyze? Do the logs and alerts have the right type of data and level of detail to be useful and generate high fidelity detections or support threat hunting activities? Are they going to support the provider's incident response activities? Who will monitor that the logs are being sent? Can they also perform meaningful security analytics on this telemetry to help with the core mission of MDR, aiding in the detection and response to threats?

Many customers fail with their threat monitoring, detection and response initiatives, because of the focus on monitoring avariety of log sources from whatever technologies they have deployed, instead of having the right sources generating telemetry and alerts, at the right time, in the right format, in the right locations. Buyers considering MDR services need to closely evaluate and confirm the capabilities of the MDR service provider to answer these questions.

The MDR Market Continues to Experience Merger and Acquisition Activity

During the past 12 months, there have been several acquisitions in this market:

- August 2019 — GoSecure acquired EdgeWave.

- January 2020 — IntelliGO Networks was acquired by ActZero.
- January 2020 — Skyview Capital acquired Fidelis Cybersecurity.
- May 2020 — Ankura acquired the MDR business from UnitedLex.
- June 2020 — Atos announced its intent to acquire Paladion.

Security leaders need to be prepared for the fact that, in a rapidly growing market, providers continue to be acquired. They will need a plan that addresses this situation if it occurs (see "Protect Yourself as Your MDR Is Merged or Acquired").

Representative Vendors

Market Introduction

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 (see Note 1).

Table 1: Representative Vendors

Provider	Service Name	Headquarters
Alert Logic	Managed Detection and Response	Houston, Texas, U.S.
Arctic Wolf	Managed Detection and Response	Sunnyvale, California, U.S.
Armor	Armor Anywhere	Richardson, Texas, U.S.
Binary Defense	Managed Detection & Response	Stow, Ohio, U.S.
Blackpoint Cyber	Managed Detection and Response	Ellicott City, Maryland, U.S.
BlueVoyant	Managed Detection and Response	New York, New York, U.S.
Booz Allen Hamilton	Managed Detection and Response, and Managed Threat Services	McLean, Virginia, U.S.
CI Security	Managed Detection & Response	Seattle, Washington, U.S.

Cisco	Managed Detection and Response	San Jose, California, U.S.
ControlScan	Managed Detection and Response	Alpharetta, Georgia, U.S.
CRITICALSTART	Managed Detection & Response	Plano, Texas, U.S.
CrowdStrike	Falcon Complete	Sunnyvale, California, U.S.
CSIS	Managed Detection and Response	Copenhagen, Denmark
Cysiv	Cysiv SOC-as-a-Service	Dallas, Texas, U.S. and Ottawa, Canada
Datashield	Managed Detection & Response	Scottsdale, Arizona, U.S.
eSentire	Managed Detection and Response	Waterloo, Ontario, Canada
Expel	Expel	Herndon, Virginia, U.S.
F-Secure	F-Secure Countercept and Rapid Detection & Response Service	Helsinki, Finland
Fidelis Cybersecurity	Fidelis Managed Detection and Response	Bethesda, Maryland, U.S.
FireEye-Mandiant	Managed Defense	Milpitas, California, U.S.
Fishtech CYDERES	Managed Detection and Response (MDR)	Kansas City, Missouri, U.S.
GoSecure	Managed Detection and Response	La Jolla, California, U.S., and Montreal, Quebec, Canada

IntelliGO Networks	Managed Detection & Response	Toronto, Ontario, Canada
Kudelski Security	Managed Security Services, and Managed Detection and Response	Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, U.S.
LMNTRIX	Adaptive Threat Response	Orange, California, U.S.
Masergy	Managed Security	Plano, Texas, U.S.
mnemonic	Argus Managed Defence	Oslo, Norway
Open Systems	Managed Detection & Response	Zurich, Switzerland
Orange Cyberdefense	Managed Threat Detection	Paris, France
Paladion	Managed Detection and Response Service	Reston, Virginia, U.S.
Ponduranc e	Managed Detection and Response	Indianapolis, Indiana, U.S.
Proficio	Managed Detection and Response Service	Carlsbad, California, U.S.
Rapid7	Managed Detection and Response Services	Boston, Massachusetts, U.S.
Red Canary	Managed Detection and Response	Denver, Colorado, U.S.
Redscan	ThreatDetect MDR Service	London, U.K.
Securework s	Managed Detection & Response, and Advanced Endpoint Threat Detection	Atlanta, Georgia, U.S.
Sophos	Managed Threat Response	Abingdon, United Kingdom
Trustwave	Managed Threat Detection and Response	Chicago, Illinois, U.S.

Verizon	Managed Detection and Response	Basking Ridge, New Jersey, U.S.

Source: Gartner (August 2020)

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 Recommendations

- MDR services are not for every organization. As discussed in the Market Analysis section, a variety of delivery styles for MDR services align with different types of buyers. See "Ask These Critical Questions and Consider These Risks When Selecting an MDR Provider" for a set of questions that can be used to determine whether MDR services are right for your organization.
- It is important to have clearly defined outcomes and goals that address defined use cases and a solid understanding of what the future steady state looks like once engaged with an MDR provider. As with any outsourcing initiative, if they are not defined, regardless of what service provider is used, the chance of success will be lessened (see "Toolkit: Communicating Effective Security Use Cases to Your MSSP" and "Get the Foundational Elements Right When Selecting a Detection and Response Service Provider").
- Purchasing MDR services is not a replacement for having the foundations for incident response in place. Incident response policies and procedures are still required (although some MDR providers are positioned to help their customers develop these if they don't exist or require updating). Other internal departments, such as HR and legal, may need to be involved, which an MDR is not going to be able to replace. Organizations should add an incident response retainer, either from their MDR provider or a third party, to deal with major incidents, investigations and breaches that go beyond what the MDR provider is prepared to support (see "Prepare for the Inevitable With an Effective Security Incident Response Plan" and "Market Guide for Digital Forensics and Incident Response Services."
- Most MDR providers lack the vetting and decades of competition that MSSPs have faced. You must perform sufficient due diligence on the MDR providers before signing a contract. Use a proof of concept (PoC), and ask for sample deliverables, to validate claims and fit for purpose with your organization's requirements, as well as other sources, 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.

Note 1
Representative 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 100 providers in this market claim to offer MDR services. Listed here are those that are visible to Gartner clients based on inquiries, have differentiators representative of the dynamic nature of the MDR market, and represent future capabilities and offerings that may drive the direction of the market.

Recommended by the Authors

The Managed Security Services Landscape Is Changing

Ask These Critical Questions and Consider These Risks When Selecting an MDR Provider

Midsize Enterprises Should Embrace MDR Providers

Protect Yourself as Your MDR Is Merged or Acquired

5 Things You Must Absolutely Get Right for Secure IaaS and PaaS

Market Guide for Endpoint Detection and Response Solutions

Market Guide for Network Detection and Response

Market Guide for Digital Forensics and Incident Response Services

Recommended For You

Balancing Your Approach to IT Centralization, Decentralization and Federation

Summary Translation: CIO Strategies to Improve Cash Flow in a Downturn

Summary Translation: Toolkit: Enterprise Internet of Things Maturity

Summary Translation: The Managed Security Services Landscape Is Changing

Summary Translation: Case Study: Internal Data Science Team Development (Eastman)

any third party. For further information, see "Guiding Principles on Independence and Objectivity."