Market Guide for Managed Detection and Response Services

10 May 2016 | ID:G00294325

Analyst(s): Toby Bussa, Craig Lawson, Kelly M. Kavanagh

Summary

New service providers have emerged to support organizations seeking to improve their threat detection and incident response capabilities. Security leaders should use this research to understand the MDR services market and its fit for their security monitoring and incident response requirements.

Overview

Key Findings

- Organizations struggle to deploy, manage and use an effective combination of expertise and tools to detect threats, especially targeted advanced threats and insider threats.
- A growing number of providers are offering outcome-based services that differ from traditional managed security services (MSSs) offerings, because they are focused on detecting previously undetected threats that have breached an organization's perimeter and are moving laterally through the IT environment.
- MDR services are not delivered by the majority of MSSPs today, but this is changing.
- MDR services are still focused at the enterprise and upper-midmarket customer, but new entrants are targeting smaller midsize organizations.
- Many MDR service providers are new to the market, and there are limited means available to validate the effectiveness of the tools and methods employed.

Recommendations

IT security leaders should:

- Use MDR services to augment existing security monitoring capabilities to address gaps in advanced threat detection and incident response before investing in more security monitoring tools (e.g., security information and event management [SIEM], network, and host-threat detection), and associated staff and expertise.
- Consider managed security service providers (MSSPs) that offer MDR-like services when device management and compliance use cases are required. Data residency requirements may also drive consideration of an MSSP over an MDR service provider.
- Conduct a detailed analysis of MDR service provider offerings relative to your specific use cases. Look

for MDR providers who can incorporate your existing security controls in the scope of their services to improve context and coverage.

Strategic Planning Assumptions

By 2020, 15% of midsize and enterprise organizations (see Note 1) will be using services like MDR, up from less than 1% today.

By 2020, 50% of worldwide MSSPs will offer MDR-type services.

Market Definition

Managed detection and response (MDR) services are an emerging group of security monitoring providers with approaches that do not fit the traditional MSS model (see "Magic Quadrant for Managed Security Services, Worldwide"). These services aim to remove the burden from clients of having to figure out "what method or device to use" for a security monitoring and response capability. MDR services focus on specific outcomes — threat detection, with 24/7 monitoring and alerting, and remote incident investigation and response (see Note 2) included in the end-to-end service.

MDR providers are often providing this service using one or more of the five styles of advanced threat defense. They are also responding to increasing customer demand for the need to improve basic incident response capabilities, which are important. However, both are expensive and difficult to obtain for many organizations, especially midsize ones. Monitoring is not focused on only ingress-egress traffic at the perimeter, but also lateral movement (east-west) once an attacker is inside an organization. Additionally, monitoring can be provided to public and private cloud environments.

MDR services are characterized by the following attributes, many that specifically differentiate them from traditional MSSPs:

- A focus on threat detection use cases, especially advanced or targeted attacks that have bypassed existing perimeter controls (e.g., next-generation firewalls [NGFWs], secure web gateways [SWGs], network intrusion detection systems [NIDSs], endpoint security). Compliance use cases are not a focus and commonly not addressed at all.
- Delivery of services usually using a vendor-provided stack of network- and host-based controls (e.g., commercial, open source or provider-developed). These tools are not only positioned at the traditional internet gateways, but are also inward-facing to detect the threats not typically discovered by traditional perimeter security technologies. These tools, where deployed, are managed and monitored by the provider to improve an organization's ability to detect threats. The types of tools and detection methods used by the providers vary in the use of logs, network flows and traffic, and endpoint activity. For example, some vendors rely solely on network security monitoring while others only on endpoint agents to generate logs or detect threats, and others rely solely on the logs generated by a customer's existing security tools.
- Security event management and analysis technology that utilizes threat intelligence and advanced data analytics is commonly, but not exclusively, at the core of these services. It is fed events from the stack of vendor-supplied controls, customer log and event sources, or some combination of the three.
-

24/7 monitoring, analysis and customer alerting of security events with preliminary triage performed by a person (e.g., not relying just on automation to add some context to an event).

- Incident validation and remote response services, such as hunting for additional hits on indicators of compromise (IOCs), reverse malware engineering, and consulting on containment and remediation are included in the service, without the need for an incident response (IR)-specific retainer or agreement. Retainers are reserved for on-site breach response services.
- Assistance with remediation actions in bringing the environment back to some form of "known good" is sometimes included or available as an additional service.

Market Direction

MDR services is an emerging market. There are few vendors relative to the overall MSS market, and most offerings have come to market within the last two years (although several vendors have had various offerings for upward of at least five years). There has been little visibility outside of organizations looking to augment or expand their existing security operations centers (SOCs), or organizations standing up a new SOC and wanting to accelerate their advanced threat detection capabilities through buying an end-to-end service.

The market is focused on threat detection and response, and targets customers with budgets to spend in this area. Gartner has seen many new entrants over the past 12 months. Gartner anticipates an increasing number of entrants to the MDR service market over the next two to three years, including startups and existing MSSPs who will reshape their existing offerings or introduce new offerings based on customer demand. Gartner expects to see the larger, worldwide MSSPs adopt and deliver capabilities and services similar to the MDR market, blurring the line between these two markets over the next five years.

Market Analysis

There are three elements of the MDR market that best define its current state. First, this is a dynamic market that is witnessing new vendors entering and trying to differentiate themselves against existing vendors, who themselves are adjusting their branding and offerings. Second, while the outcomes are usually the same (e.g., detect threats), the methods to deliver the service to customers, the level of IR services provided and the target customers all vary. Third, there is some overlap with MSSPs, with an expectation that the MSSPs will react to these new providers by adjusting their offerings and adding new ones.

The MDR services market is still immature, lacks broad visibility and does not yet have the battle scars other security monitoring approaches (i.e., SIEMs and MSSs) have collected as part of the assessment, use and validation by customers for nearly 20 years. Additionally, MDR providers are also relying on a variety of big data platforms (e.g., Hadoop, NoSQL) to deliver the service and on advanced analytics to detect threats. Both approaches are meant to help providers be more agile while keeping costs lower (e.g., no need to purchase a commercial, multitenant SIEM). Adding to the dynamic nature of the market are the multitude of approaches and methods being used by providers to deliver the service. The providers leverage different means of collecting the necessary data (e.g., logs, net flow, packet captures) from customers.

Many MDR providers' delivery approach looks similar to those used by MSS — get logs and events from relevant sources, ingest into a platform for analysis that generates events that are triaged by an analyst 24/7 from an SOC, and notify the customer. However, what's "under the hood" (e.g., the tools, analysis platform, people, processes) is sufficiently different from traditional MSSs.

Some MDR providers take a device- and host-agnostic approach, and place the responsibility on the customer to identify and send events from relevant log sources to the MDR provider's log management and analysis platform. Other MDR service providers have a technology stack that is deployed on the customer's premises. The technology stack is usually composed of a network-monitoring appliance and a host-based agent to detect events of interest, provide context for incident response activities, or both. Some providers rely on a single-tool approach — network or host.

It is common for an MDR service to focus on leveraging big data tools to collect and store logs for analysis. The use of big data platforms allows the service providers to ingest a wider variety of log sources and a great volume of events. Logs are not parsed and normalized, but left in their raw, machine state. This also influences the licensing approach used by some of the providers; services are not priced on the specific types and size of the sources generating logs, but rather on the number of users or entities that could generate events and logs.

One of the key differentiators is the reliance on threat intelligence and advanced analytics, like statistical modeling and machine learning, to detect incidents rather than relying on traditional methods, like signatures and rule-based detection that are augmented by a team of Tier 1 SOC analysts. This often means that customers have little input on refining the detection methods used by the MDR providers, which, for many customers, is acceptable as they want to rely on the provider's expertise to detect threats. The value proposition of the MDRs is the use of security analytics to reduce the need for the traditional, three-tiered SOC analyst model. Instead, the MDR providers favor investing in a smaller team of experienced analysts focused on incident response. Threat intelligence is commonly part of the analytics platform, providing an additional source of context to be analyzed along with customer generated events. Several of the MDR providers are also threat intelligence providers, so they are not relying on open-source or other commercial threat intelligence services.

MDR providers are differentiating themselves from MSSs in other ways, too:

- MSSs have operated over the last 15 years with a focus on their ability to address both compliance and threat detection use cases. MDR providers focus only on threat detection, some specifically on advanced threats, and very rarely are any compliance use cases addressed. Most MDR providers do not do device management, although there are some providers who do this in order to extend the reach of remote incident response services to a customer (e.g., updating network and host firewalls to block threats).
- MDR providers do not offer device management for customer-owned equipment, such as firewalls, IDS/IPS or web gateways. The MDR may provide technology deployed on the customer network, but this is owned and managed by the MDR service provider to deliver the service.
- Many MSSPs offer basic detection and alerting services, and it is the responsibility of the customer's security team to provide additional incident, analysis and associated response activities. MDR services include "lightweight," remote incident response services as part of the offering. As noted earlier, many MDR providers employ dedicated incident response experts to validate potential incidents, assemble the appropriate context, investigate as much as is feasible about the scope and severity given the

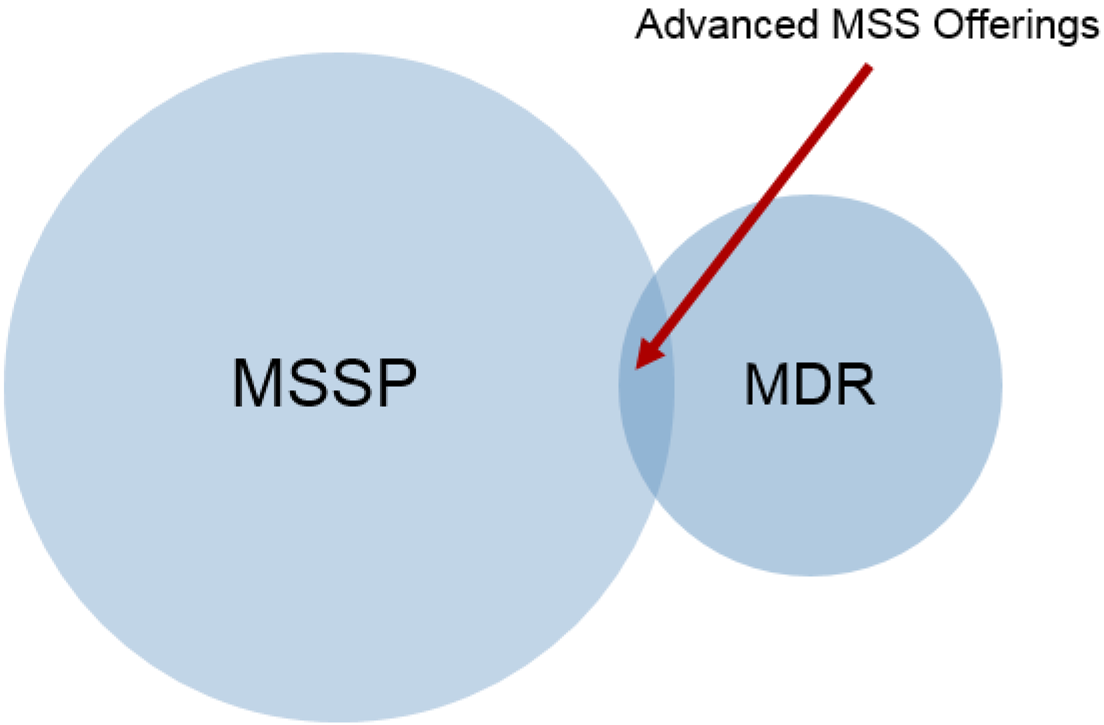
information and tools available, and make recommendations so the customer can quickly start containment and remediation activities. Many vendors also actively hunt through their customers' logs and data looking for indicators of compromise, such that threat detection occurs from both reactive and proactive methods. Gartner clients report they want a more comprehensive service than is typically reported with many MSSPs, where customers receive an alert of a suspected incident, which has minimal information, and are left to fend for themselves using the MSSP's portal and tools.

- MDR services focus on detecting threats once they bypass traditional perimeter security controls, regardless of whether they are in a customer's data center or public cloud services provider. Most MSSPs focus on monitoring a customer's internet perimeter security controls (e.g., firewall, unified threat management [UTM], identity proofing service [IDPS], SWG).The more skilled, or advanced, attackers are able to compromise an organization and establish a foothold without being detected by these perimeter controls. MDR services are focusing on detecting the foothold (or installation phase in the cyber kill chain model — see "Addressing the Cyber Kill Chain"), communications (command-and-control phase), lateral movement during the action on objectives, and what may have been exfiltrated by an attacker. These services aim to better-detect the delivery to action on objectives phases of the kill chain.
- Most MSSPs traditionally only monitor a customer's perimeter. Increasingly, however, organizations are budgeting to include other log sources like host, application, user directories, and identity and access management tools. The traditional MSSP model is a Catch-22, as it works against both parties. That's because a variety and volume of log sources are necessary to better-detect threats, but MSSPs charge by the volume of logs and number of devices. This forces customers to make tough risk-versus-budget decisions (e.g., "Do I increase my MSSP budget and reduce spend on other security controls?"). The MSSP also loses as it doesn't have enough log sources to better-detect and prioritize threats, and provide the necessary context. This leads to the perception that MSSPs can't detect threats well and, if they do, the alerts lack sufficient detail and context for the customer to properly analyze and take action. MDR service providers, by virtue of building their technology stacks and delivery platforms to leverage open-source tools, big data platforms and advanced analytics, aim to remove this constraint, because they remove the limits on the types and number of log sources feeding the analysis platform.
- Most MDR providers do not offer SLAs to customers, as they believe it constrains them from providing their services. Many providers prefer to give their customers more in-depth analysis and actionable advice specific to the threat detected rather than being tied to a response metric. Some offer service-level objectives (SLOs) that are best efforts rather than something they are contractually bound to measure and achieve.

MDR services are positioned across a variety of industry verticals and operational security maturity levels. Many MDR providers focus their services on mature, enterprise-level customers today (see Note 1). Many vendors are currently targeting their services at the enterprise customer who has a mature security monitoring capability (either using an SIEM and an SOC, or by partnering with an MSSP). These MDR providers are providing their services to augment these existing monitoring capabilities specifically to detect advanced attack use cases. At the opposite end of the spectrum, albeit with fewer options, some MDR providers are targeting midsize customers (on average, 500 staff and above) that lack a formal security team and dedicated security monitoring function, thus wanting to help customers implement a threat-detection-focused monitoring capability.

The above analysis suggests that there is a gap between MSSPs and MDR providers, as MSSPs have not traditionally delivered well to the small and midsize market. Several worldwide MSSPs (see "Magic Quadrant for Managed Security Services, Worldwide") are also updating their delivery platforms to incorporate the big data and security analytics capabilities commonly utilized by MDR providers (see Figure 1).

Figure 1. Where MDR Service Providers Sit in Relation to Traditional MSSPs



Source: Gartner (May 2016)

However, the overlap between MSSPs and MDR providers is still limited. Clients should be wary of claims from traditional MSSPs on their ability to deliver MDR-like services. Delivering these services requires technologies not traditionally in scope for MSS, such as endpoint threat detection/response, or network behavior analysis or forensic tools. Those exploring MSSPs for these services should understand the MSSPs' expertise in running the technologies, and in using them to effectively identify and respond to breaches.

Several MSSPs are developing services based on one or more of the five styles of advanced threat defense (see "Technology Overview for MSSP Advanced Threat Defense"). There are examples where overlap between the markets currently exists, such as BAE Systems Advanced Threat Detection service, BT Assure Cyber, CGI's Advanced Threat Investigation (ATI), and SecureWorks' Advanced Endpoint Threat Detection (AETD) service.

Gartner expects that the MDR vendors will, in response to customer demand for services that also address monitoring of their existing security controls, add more MSS-like services (at least for security monitoring; device management is less likely to be in scope for MDRs). For similar reasons, MSSPs will continue to expand the scope of their services to include more MDR capabilities. Evidence of this trend, in addition to the example cited, includes the ongoing development of big data storage capabilities and advanced analytics use cases in most of the MSSPs covered in the "Magic Quadrant for Managed Security Services, Worldwide."

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.

Arctic Wolf Networks

Arctic Wolf Networks' (AWN') Cyber-SOC service is focused on midmarket organizations that have dedicated IT staff, but lack a dedicated security team. The service leverages a proprietary network appliance that collects logs from customer sources and sends those logs to their Amazon Web Services (AWS) cloud-based, big data platform where they are correlated with threat intelligence and advanced analysis is performed. The appliance can also be leveraged to provide other services, such as network security monitoring and vulnerability scanning, if a customer lacks their own tools. Alerts are monitored and actioned from 24/7, dedicated SOCs located in Canada and the U.S. Customers have access to alerts, basic event data and reports via a web-based portal. SOC analysts provide remote incident response services based on detected threats including specific remediation advice. Arctic Wolf assigns SOC staff to a group of customers, positioning analysts as virtual security monitoring and incident response experts. The service targets the small and midsize business (SMB) market. It is licensed based on number of seats in an organization, and can be consumed as a monthly or annual subscription.

Alert Logic

Alert Logic's flagship solution is Cloud Defender, which integrates network intrusion detection, web application firewall, vulnerability scanning, and central log management and analysis. The suite consists of several Alert Logic solutions, including Log Manager, Threat Manager, Web Security Manager, ActiveAnalytics, ActiveIntelligence and ActiveWatch. Data is collected using a combination of the solutions (e.g., logs, packets and application), which is then aggregated, and stored in the ActiveAnalytics platform. Products are deployed through any combination of physical and virtual appliances, and agents. Threat intelligence and security content are provided by two dedicated, in-house teams. Alerts are monitored 24/7 from dedicated SOCs located in the U.S. and U.K. Basic incident response is provided remotely as part of the services. Alert Logic also has a focus on monitoring public cloud services, like AWS and Microsoft Azure. The service is subscription-based, which is licensed based on the amount of data collected and stored.

Cisco

Cisco's Active Threat Analytics (ATA) is part of Cisco's Managed Security Services offerings. The service has three service tiers (Essential, Enhanced and Premier) that all provide log and event collection, correlation against Cisco threat intelligence, and 24/7 monitoring from one of Cisco's dedicated SOCs located in the U.S, Poland and Japan. Enhanced and Premier services include options like the application of advanced analytics, network security monitoring capabilities and proactive hunting. Active Threat Analytics leverages security knowledge from Cisco Talos Security Intelligence and Research Group and Cisco Collective Security Intelligence for Premier-level customers. Premier customers also receive additional services like proactive threat hunting, full packet capture and big data storage that are delivered using a technology stack of Cisco equipment deployed on the customer's premise. Cisco's target customer with ATA is the larger enterprise in verticals dealing with targeted, advanced threats. The service is delivered as a subscription, even with the Cisco technology stack, and is priced by service tier and the analyzed volume of data.

CrowdStrike

CrowdStrike's Falcon Overwatch is a managed service delivered using the Falcon Host and Platform (which are also available stand-alone in a SaaS model without 24/7 monitoring). Customers deploy the Falcon Host agent to their endpoints and servers (Windows, Linux and Mac) as the primary event monitoring, detection and prevention tool. Events are captured at the endpoints and sent back to the Falcon Platform for analysis. The Falcon Platform, powered by CrowdStrike Threat Graph, uses advanced analytics and machine learning, along with the Falcon Intelligence service, to detect, prioritize and remediate threats. Threats are monitored and reviewed 24/7 by dedicated intrusion analysts. CrowdStrike's intrusion analysts also proactively hunt for threats across all customer data. Customer's benefit from the capabilities in the Falcon Host, which allows threats to be blocked based on IOCs and other threat detection methods. Falcon Overwatch can be used in tandem with CrowdStrike Services' Incident Response team, which provides on-the-ground support if needed to deal with any major incidents or breaches.

eSentire

eSentire's Active Threat Protection service is composed of several technologies — IDPS with full packet capture and behavior-based threat detection, SIEM, and vulnerability scanning — to gather data. Real time, 24/7 analysis is performed centrally by analysts in its Canada and U.K.-based SOCs to identify, hunt and respond to advanced attacks that have bypassed the customer's existing perimeter and signature-based defenses. eSentire applies its own threat intelligence and third-party feeds against collected customer data, which is then processed by its analytics platform for indications of attacks. eSentire uses a hybrid architecture that keeps the sensitive packet data inside the customer network rather than sending it to an externally hosted log management and analysis platform. As a threat is investigated in real time, a SOC analyst securely connects to the Network Interceptor IDPS sensor and evaluates the threat using all of the available event and forensic data. Remote incident response services are provided as part of the alert investigation before presentation to the customer. The service is licensed based on hardware and implementation costs, annual device maintenance, and service fee based on the number of end users. eSentire customers range from small to midsize enterprises.

FireEye

FireEye offers several managed solutions primarily based around the FireEye product suite (network, host, sandbox) and its Threat Analytics Platform (TAP), which is augmented with threat intelligence provided by its Mandiant and iSIGHT Partners divisions. FireEye has deployed seven Advanced Threat Response Centers (ATRC) around the globe, providing 24/7, follow-the-sun coverage for customers. Customers purchase, or bring to the service, one or more FireEye products that can be leveraged remotely by the FireEye ATRCs to deliver three levels of service — detection, investigation and proactive hunting. Threats are detected and investigated by SOC analysts using these tools along with threat intelligence and advanced analytics. They provide a detailed assessment of the incident, a timeline of events and recommended actions to customers when alerted, and over the course of any active threat activity until it is contained and remediated. TAP can be leveraged with the above services to expand visibility and enhance investigations. Pricing is a four-step process based on the selected threat coverage, platform coverage, service level and number of nodes monitored. Target customers range from midsize organizations with limited security resources to large enterprises looking to augment their existing internal SOCs.

Mnemonic

Mnemonic is a service provider based in Norway that leverages a proprietary platform called Argus that is used to deliver its Managed Defence service. It provides 24/7 monitoring services from European-based SOCs staffed with incident responders and handlers. Argus is leveraged against customer security logs to apply threat intelligence and advanced analytics to detect threats with as much automation as possible. Customer logs are analyzed on their premises using the Argus Networks Analyzer appliance that integrates multiple network security monitoring functions. SOC analysts leverage the Argus platform and sensor to investigate threats and perform remote incident response. Mnemonic also has a special version of its network appliance (Argus ICS Defender) for monitoring threats against industrial control systems (ICS), and supervisory control and data acquisition (SCADA) environments. Mnemonic serves large enterprises and the SMB market. Service pricing is based on the number of users in an organization and the amount of data (i.e., throughput) monitored.

Morphick

Morphick, based in the U.S., provides MDR services to upper-midsize and enterprise customers using a combination of network, endpoint, email and DNS monitoring to detect threats. Network monitoring is achieved using a dedicated out-of-band appliance deployed on a customer's network. The appliance provides multiple types of network security monitoring (NSM), full packet capture and agentless endpoint threat-hunting capabilities. Email and DNS threat monitoring are offered as additional services. All events are aggregated on the Morphick Defense Platform that applies multiple methods (signature, reputation, behavior and advanced analytics) to detect and help prioritize incidents to remediate. Events are monitored and validated 24/7 from Morphick's SOC by a dedicated staff of incident response analysts who also perform proactive threat hunting. Customers can leverage Morphick's Incident Response services for breach response support and Threat Intelligence for deep intelligence gathering and analysis, and other incident response services (like malware reverse engineering and customer signature development) as needed. The service is targeted at midsize to large enterprises, and licensed based on the services selected, size of the organization, sensors deployed and amount of data monitored.

Netswitch

Netswitch's offering is based on the Securli Advanced Threat Protection offering and the SecurliXF threat intelligence platform, which are fed security event logs from customer-managed sources. A curated list of commercial security controls is available to customers to extend the security monitoring, and incident response and remediation capabilities of the monitoring service to, for example, monitor public cloud services, endpoints and networks. Netswitch will manage the monitoring tools selected by the customer. The service is delivered using three partner SOCs — two in the U.S. and one in Hong Kong. The SOCs provide 24/7 monitoring, incident investigation, alerting and remediation services if selected by the customer. A 15-minute response SLA is available to customers. Netswitch is predominantly used by midsize organizations, but is also targeting enterprises with its MDR service. The service is priced on the number of log sources and the security monitoring tools selected from the Netswitch technology portfolio.

Rapid7

Rapid7 Analytic Response is a managed service based on the company's InsightIDR product. Customer security events and logs are forwarded to the cloud-based InsightIDR platform, where threat intelligence and analytics (e.g., machine learning, user behavior) are applied. Monitoring of cloud and SaaS offerings, like AWS, Box and Office 365, is supported. An endpoint detection and response (EDR) agent is deployed to extend monitoring capabilities down to the host for the purpose of threat validation and incident response. The service is delivered from a U.S.-based, 24/7 SOC staffed with analysts who are primarily focused on threat hunting across a customer environment, in addition to investigating and validating threats detected using analytics analysis. Threat validation is conducted by analysts to provide context before notifying customers with remediation recommendations. An administrative platform is available to customers in addition to a dedicated threat assessment manager to assist customers. Service onboarding starts with a compromise assessment, then traditional monitoring and remote incident response services are turned up. The service is targeted at organizations with a lack of in-house expertise and organizations with an existing SOC that need augmented support for advanced, targeted attack detection. Pricing is based on the number of assets monitored.

Raytheon Foreground Security

Raytheon Foreground Security's Virtual Security Operations Center (V-SOC) service provides MDR services to the U.S. federal government, and commercial and international customers. Threat intelligence, advanced analytics and hunting techniques (both automated and manual) are applied against customer-generated security logs, event data and network traffic, with all customer data being retained on their premises. Automated hunting is performed using the Automated Threat Intelligence Platform (ATIP) appliance deployed at the customer's site. The ATIP also acts as the customer portal. The Raytheon Foreground Security delivery platform leverages a virtual desktop infrastructure (VDI), so analyst's from the 24/7 U.S.- or EMEA-based SOCs are able to remotely investigate and perform incident response activities. Remote incident response investigation is performed on alerts and actionable advice is provided to customers. There are two levels of service, both primarily based on automated threat intelligence and active analytics, with differences in monitoring coverage and additional incident response activities like forensic and malware analysis. Pricing is based on a combination of the service level required, number of users and other available service options.

Rook Security

Rook Security's Managed Threat Response (MTR) program is an on-premises or cloud-based platform. It consumes logs and security events from customer-owned tools or Rook's proprietary network analysis sensor and EDR agent deployed in a client's environment. The MTR platform is leveraged by analysts in its 24/7 U.S. SOC to perform monitoring, analysis, event detection and automatic context enrichment. When a threat is suspected, the Rook SOC analysts work incidents in the War Room (a stand-alone application that can be used with the MTR platform) to perform further analysis and incident response activities. Customers are notified and can participate in the incident response activities using the War Room app. Customers are provided context and actionable advice by the SOC staff for each incident. Rook offers various service options, including full remote security operations that could include remote incident remediation depending on the tools deployed by the customer. Clients can also choose whether they do the investigation or rely on Rook's SOC analysts. The MTR platform is priced based on daily log volume, storage and computing resources needed to deliver service. Rook's managed service overlay for MTR platform customers is priced based on log reporting, analysis frequency, number of nodes and number of tickets. Rook customers range from large enterprises to midmarket organizations.

Market Recommendations

- Choose a vendor based on specific requirements and existing threat detection and response capabilities, as all MDR services are not the same. There is sufficient variability in offerings, delivery models, target customer market and vertical, and pricing that makes direct comparisons more challenging. Having a strong set of requirements at the beginning will ease the analysis and selection process.
- Evaluate providers based on existing tools and expertise in your organization, looking for those vendors who best meet requirements while filling the gaps in tool and expertise coverage.
- Don't go it alone when implementing an SOC capability. Look to an MDR service provider as a partner who can augment your SOC. This allows you to quickly implement mature threat detection and response capabilities rather than having to build from scratch. This can mean an SOC is operating at a greater maturity level in several months rather than several years.
- Focus on cloud environment and SaaS monitoring needs, which will reduce the field of potential providers. Only a few MDR service vendors are currently capable of meeting these requirements.
- Use proof of concepts to your advantage to validate claims and fit for purpose with your organization's requirements. Most MDR providers lack the vetting and decades of competition that MSSPs have faced. Therefore, there is an increased burden on the customer to perform sufficient due diligence on the MDR providers before signing a contract.
- If you have data residency requirements, look to MDR service providers that operate within your geographic region or those that utilize a decentralized data collection architecture where your data remains on-premises, and only metadata or event data is sent back to a central SOC.

Note 1
Organization Size Definitions

Gartner defines an enterprise business as one that has over 1,000 employees and greater than $1 billion in annual revenue. Gartner defines a midsize business as "[a] business which, due to its size, has different IT requirements — and often faces different IT challenges — than do large enterprises, and whose IT resources (usually budget and staff) are often highly constrained." Midsize enterprises have 100 to 999 employees, with $50 million to $1 billion in annual revenue.

Note 2
Incident Response

In the context of MDR service providers, incident response is investigation and analysis activities that can be conducted remotely to validate an incident; for example, collecting malware samples and performing analysis using a sandbox or manual reverse engineering methods to extract indicators of compromise and other contextual information that can then be used to perform additional investigation across a customer's logs to determine the scope and potential severity of an incident. Other activities might include leveraging network packet capture tools and EDR tools to perform more in-depth investigation. Not considered part of these remote incident response activities are breach response activities that involve execution of a retainer to deploy experts on-site for deeper and wider data collection and forensic activities, and working with various parts of a business and even third parties to notify customers.