IDC MarketScape

IDC MarketScape: U.S. Managed Detection and Response Services 2021 Vendor Assessment

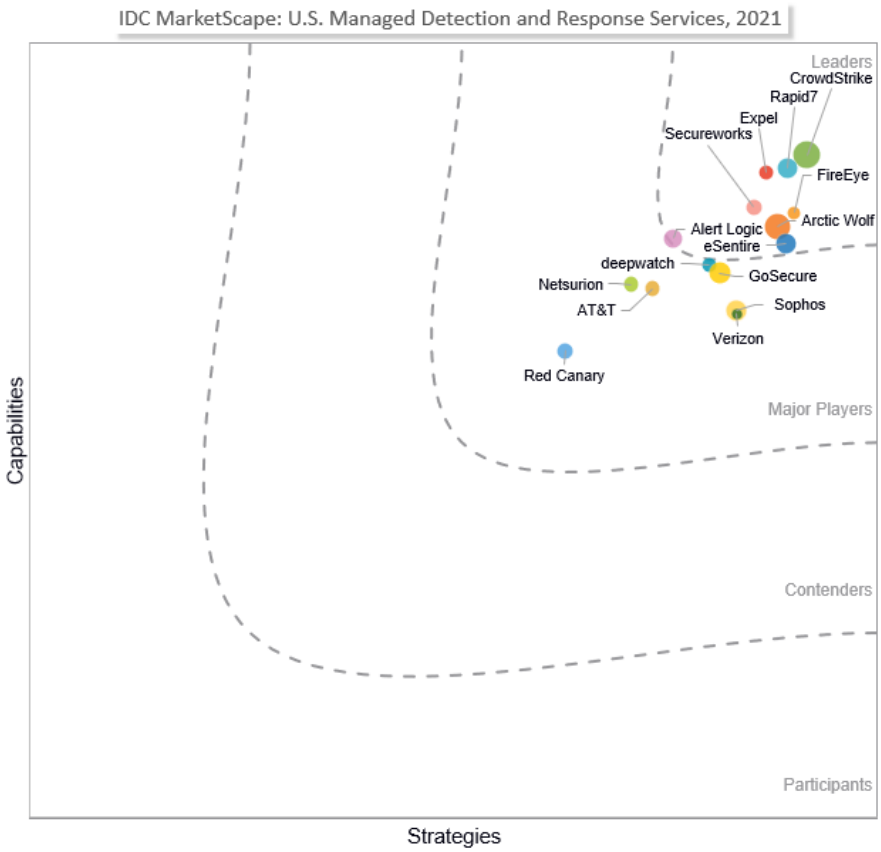
Christina Richmond Craig Robinson

THIS IDC MARKETSCAPE EXCERPT FEATURES ARCTIC WOLF

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape U.S. Managed Detection and Response Services Vendor Assessment



Source: IDC, 2021

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

August 2021, IDC #US48129921e

IDC OPINION

Buyers of cybersecurity are evolving and driving vendors and security services providers to deliver more robust prevention, detection, and rapid response actions in the fight against cyberattacks. As the managed security services (MSS) market evolves to meet customer expectations, managed security service providers (MSSPs), consultancies, and other providers are serving up managed detection and response (MDR) services to meet the demand. IDC recognizes MDR as the third maturity level of MSS, which now encompasses more efficient advanced detection and response capabilities.

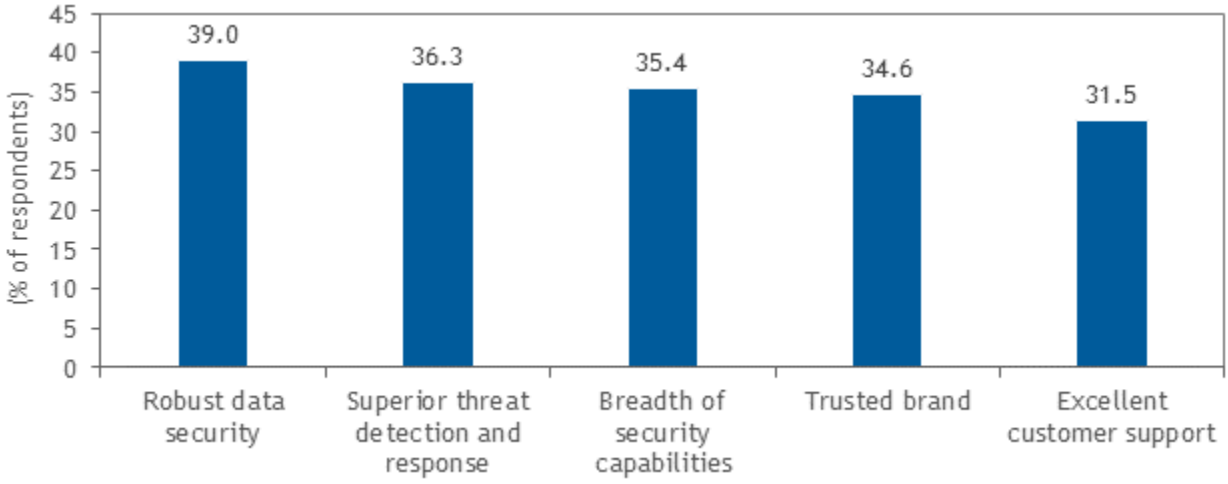
Some security leaders are beginning to examine security from a strategic, business, and industry viewpoint — the right direction and context — to understand how they can be proactive and better prepared for attacks. A cybersecurity buyer priority is shortening detection and response times, but organizations also want to elevate their cybersecurity maturity and reduce risk. Many struggle to understand their current state and are unclear how to proceed. MDR providers are stepping up to help organizations solve these challenges.

In IDC's 2020 *MSSP and MDR Survey,* organizations were asked about attributes of managed security SPs and MDR providers used during evaluations. Respondents noted the five most important MDR provider attributes: robust data security, superior threat detection and response, breadth of security capabilities, trusted brand, and excellent customer support (see Figure 2).

FIGURE 2

Attributes Evaluated for MDR Services

Q. What five attributes are most important when evaluating a managed security services provider (MSSP) and managed detection and response (MDR) providers?



n = 410

Source: IDC's *MSSP and MDR Survey,* May 2020

Additional research and the findings in this IDC MarketScape study lead IDC to believe that the following capabilities align with the attributes most valued by buyers and will drive the MDR market forward while providing vendors with the opportunity to home in on a differentiated proposition:

- **Onboarding.** MDR provider onboarding timelines vary from hours to weeks. Ideally, customized onboarding processes contribute to risk reduction through elements such as threat modeling exercises, security health checks, and/or security program reviews. Day 1 of being "live" on an MDR service will not typically offer the same protection levels that will exist when a customer is weeks or months into an engagement. Reaching a more fully protected, mature stance takes time, especially for organizations that have not used a SIEM or other collection system to gather the historical data that is crucial for machine learning (ML) algorithms to ingest. Over time, the MDR service is able to better determine what is normal activity versus abnormal activity. Nevertheless, reducing time to onboard is a key differentiator.
- **24 x 7 x 365 monitoring.** Not all organizations operate around the clock, but attackers do. Full-time monitoring and the support of security operations centers (SOCs) are rapidly becoming necessities.
- **Curated threat intelligence.** The expansion of the risk surface, fueled by the rush to the cloud, has increased the number of indicators of compromise (IoCs) that SOC teams are tasked with investigating. Curated threat intelligence helps reduce the number of false-positive alerts by focusing on the threats that are more likely to be launched against an organization and cause harm.
- **Encryption.** A few MDR providers include some form of encryption in their services or offer it as a separate product. Encryption will be another essential layer of protection.
- **Threat hunting expertise.** Reactive threat hunting, targeted threat hunting, and proactive threat hunting all are important in helping organizations improve security maturity and strengthen their defenses. Another key differentiator is continuous proactive threat hunting, which is an optimal preventive strategy.
- **Endpoint detection and response (EDR).** All types of endpoints, including Internet of Things (IoT), industrial Internet of Things (IIoT), and Internet of Medical Things (IoMT), need to be monitored and secured. A robust EDR system is often the go-to tool used to deal with attacks that land on an endpoint.
- **Security orchestration, automation, and response (SOAR).** SOAR levels vary across areas such as onboarding, SIEM systems, detection, investigations, analytics, alerts, workflows, and response and remediation actions. A few MDR providers use bots for triage, investigation, and analysis.
- **Incident detection and response times.** Speed is of the essence in detecting and stopping threats. As reported by study participants, mean time to detect (MTTD) varies significantly, although the numbers must be understood in context of the provider's definitions and measurements. Mean time to respond (MTTR) also is a key metric that should be explored with providers. Certain providers measure other actions, such as mean time to validate and mean time to remediate.

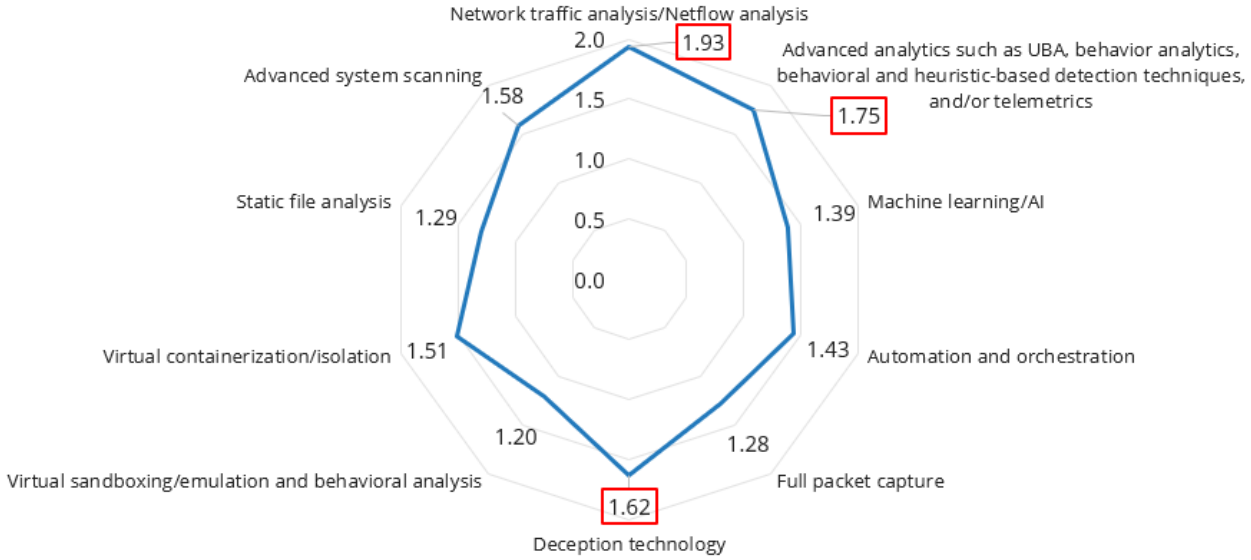
In addition, cybersecurity buyers believe network traffic analysis, user behavior analytics (UBA), and deception technologies are core to detection and response. These areas represent opportunities for MDR providers to broaden and distinguish their services (see Figure 3).

In this 2021 U.S. IDC MarketScape for MDR services study, IDC explored how MDR providers are evolving their businesses, technologies, and offerings to detect and respond to modern cyberattacks. MDR providers were asked to demonstrate advanced capabilities that provide detection, not only from the endpoint but also from broader sources of telemetry, and deliver rapid, effective response actions.

FIGURE 3

Technologies Core to Detection and Response

Q. Which five core advanced detection and response technologies do you consider most important in an MDR offering?



n = 410

Source: IDC's *MSSP and MDR Survey,* May 2020

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied 15 vendors that provide MDR in the United States and surveyed providers' customers that utilize their services. Because MDR is considered a subset of MSS, many MDR providers could be evaluated. The vendors included in the study had to meet certain criteria to qualify for this vendor assessment:

- **Geographic presence.** Each vendor was required to have a minimum of 70% of its MDR revenue within the United States.
- **Customer base.** In 2020, vendors had to have a presence within the midsize to enterprise segment, with 100+ customers.
- **MDR capability**. The MDR service providers must have a well-trained cybersecurity staff in a 24 x 7 x 365 remote SOC. Each vendor is required to have detection and response capabilities across at least three points of telemetry as well as a minimum of three additional integrated

services such as threat intelligence, threat hunting, forensics, response, orchestration, and remote incident response (containment, isolation, removal, and/or remediation).

ADVICE FOR TECHNOLOGY BUYERS

IDC believes MDR is powerful and effective because it integrates technologies and services into a holistic detection and response capability. Optimally, MDR services enable organizations to maintain a consistent level of awareness and protection, along with the flexibility to reprioritize, reassess, and reconfigure their risk as well as detection and response tolerances and activities. Increasingly, security leaders view MDR as a necessity to help mature their cybersecurity programs.

The most complete MDR portfolios include the following capabilities:

- 24 x 7 x 365 monitoring (including log monitoring)
- Endpoint detection and response
- SIEM and/or SIEM integration
- Extended detection and response (XDR), which expands "X" telemetry collection to network, packet capture, cloud, email, messaging, IoT/IIoT/IoMT devices, and all edges and includes automated correlation, machine learning, and threat intelligence, as well as provides an integrated platform on which policy and controls are monitored and managed
- Multiple intelligence feeds from endpoints, the dark web, open and commercial sources, and industry-specific sources to better reveal tactics, techniques, and procedures (TTPs) (Many providers map TTPs with the MITRE ATT&CK framework, which IDC believes is a differentiator.)
- Curated, contextualized threat intelligence
- Vulnerability management, vulnerability scanning, and vulnerability assessments
- Human-led reactive and proactive threat hunting based on risk analysis and integrated threat intelligence feeds to augment indicators of compromise
- On-premises and remote incident response capabilities
- Incident analysis and forensic investigations capabilities
- Remediation services to return customers to a normal state
- Integration of incident response IP into threat intelligence
- A single, easy-to-use, configurable portal/dashboard that includes advanced capabilities such as real-time updating; integration with third-party service desk and ticketing tools; ability for customers to create, update, and close tickets if they choose to do so; visibility of workflow tasks between providers and customers; and ability for customers to follow analyst actions and collaborate if they choose to do so
- A mobile app that can be utilized to gain summary and drill down access to current alerts, message the appropriate provider and internal support staff, and quickly approve and escalate relevant issues as needed

The Market Definition section in the Appendix provides a description of what IDC believes is the minimum set of capabilities an MDR provider should offer.

MDR and XDR Are Not the Same

Early versions of MDR were more endpoint focused. They did not ingest and correlate the broad telemetry that can be utilized to shorten time to detect attacks. The development of XDR was in part

due to the need for detection and response platforms to have the ability to look at a variety of telemetry beyond the endpoint. Examples include the hybrid cloud data that organizations are increasingly generating, network telemetry, and the various flavors of IoT data such as IoMT and IIoT.

Buyers looking to improve their detection and response capabilities will likely see an improvement in these capabilities if they purchase an XDR platform or subscribe to an MDR service. Note the difference in language: XDR in its purest form is a platform that offers detection and response capabilities utilizing e(X)tended telemetry sources that is managed by the purchasing entity.

MDR in its purest form is an elevated managed service that utilizes the same features and functionality that an XDR platform offers. MDR providers either natively have the IP to look at various telemetry or utilize an XDR platform. Additional services, such as – but not limited to – 24 x 7 eyes-on-glass monitoring, detection and response services by a third-party managed security SP or MDR provider, human-led and automated threat hunting, and incident response capabilities, are added to improve detection and response capabilities.

IDC recognizes that the market is fluid, and confusion is inevitable as some XDR providers start to layer additional services onto their XDR platforms, blurring the difference between an XDR platform and an MDR service. Conversely, not every MDR provider has the capability or IP to ingest and correlate the types of telemetry that XDR platforms typically utilize. Potential buyers of a detection and response platform like XDR, or a service like MDR, need to clarify their current capabilities and desired business outcomes before evaluating MDR or XDR providers.

MDR Purchase Considerations

Prior to evaluating MDR providers and making investment decisions, IDC urges security leaders to identify their most valuable assets, determine their needs for continuous monitoring, and identify the levels of protection required for different areas of the business and types of data.

The following information provides context for security leaders to better understand and evaluate MDR capabilities:

- **Managed detection.** MTTD varies by provider, but average MTTD from MDR providers typically is shorter than the MTTD from traditional MSSPs. Shorter detection times can assist in lowering time to respond. The use of automation and workflow processes improves detection, particularly in a provider's ability to normalize, enrich, and analyze the data coming in from various sources.

  Ideally, a provider's technologies and processes work with an organization's existing technology stack, so organizations are not required to rip-and-replace technology to eliminate blind spots and strengthen their defenses. This synergistic approach may begin with the discovery and profiling of assets to augment the collection of data and security event observations from multiple sources. Advanced MDR providers integrate and map events to the MITRE ATT&CK framework to enrich threat intelligence with TTPs.
- **Managed response.** MDR providers demonstrate various types of response mechanisms across a spectrum of security services. However, not all response motions are equally effective nor are they defined in the same way by providers. Consider EDR. Depending on how deep the integration is with each vendor/partner, the allowed actions can vary. Buyers should ask about the specific response actions that a provider can take on their behalf. Which response actions can be taken by either the customer or the provider? Can the provider contain, isolate, and eliminate the incident? Is remediation to normal state offered, and if yes,

who owns it — MDR provider or partner? Some MDR providers offer only remediation guidance to customers that are responsible for taking action. This approach potentially extends MTTR, and security teams must be prepared to set aside other tasks or priorities and address an incident immediately.

Providers are investing in their managed response mechanisms and automating them to various degrees. Buyers will want to understand what is and is not automated, what will be automated in future, which response actions can be predefined and approved by customers, and how to determine the extent to which they want or need manual triggering of response actions.

IDC notes in this study that although MDR providers may be able to provide automation of various response capabilities, these rapid response functions can be hamstrung when a customer refuses to allow response measures to be applied automatically. CISOs, CIOs, and other technology leaders need to work with their MDR provider to identify the appropriate, allowable automated response actions based on the unique factors that apply. These include the who, what, and where of a particular attack. Failure to proactively identify and allow automated and scripted response actions will lead to unnecessary response delays and potential harm to the organization.

- **Incident response support.** Buyers will want to explore the limits of incident response support, the availability of onsite and/or remote incident response, and the option for emergency incident response and built-in retainer hours which several of the providers in the study offer, although hours and terms vary.

  MDR providers may offer incident response capabilities as part of their core offering or for an additional price. It is not uncommon for MDR providers to utilize third-party partners to provide their incident response capabilities. Buyers will want to fully flush out how the MDR provider transfers part or all of the ownership of an incident response campaign to a partner.

  Use of an incident response retainer, to allow for expedited response, is another feature that buyers will want to explore. Find out if and how much of the incident response retainer can be utilized for proactive services should the need for incident response be less than anticipated during a contract period.
- **Cloud support.** Determine which cloud service providers an MDR provider supports and if there are detection and response strategies unique to each cloud SP. Cloud response capabilities may include forensic log analysis, root cause analysis, and correlation to MITRE ATT&CK. Some providers have automated cloud response actions.
- **Threat intelligence.** Threat intelligence should feed into threat hunting abilities. Buyers of MDR will want to understand the type of feeds, number of sources, whether the threat data is ingested in real time, and how automation and ML/AI are used across different telemetry to enable rapid, actionable threat intelligence. Threat intelligence is core to the ability of providers to finding threats efficiently within a customer's environment. Advanced providers conduct adversary research and understand what the attackers are doing and the types of campaigns the attackers are running.
- **Customer service.** Some MDR providers offer a "white-glove approach" to customer experience and support. A dedicated customer support person or concierge team assists customers with onboarding and with building and executing a security journey. Advanced providers can help organizations meet their security goals and objectives while identifying opportunities to strengthen their security posture over time and reduce risk.
- **Service-level agreements (SLAs).** Service-level agreements are not offered by all MDR providers. Buyers can expect a range of SLA types from providers that offer them:
  - Standard SLAs that are the same for all customers

    - SLAs unique to each customer
    - Different SLAs based on alert type
    - An uptime SLA
- **Continued technology investments.** To remain competitive, MDR providers must continue to invest in their people, processes, and technologies. Areas for buyer scrutiny include:
    - Development of tiers of MDR offerings to accommodate the needs of diverse customer segments and sizes
    - Customization of communication, workflows, and escalations (e.g., portal enhancements that allow customers to interact and/or collaborate with a provider in diverse ways and/or customize dashboards, fields, and reports)
    - Remediation capabilities and how they are delivered
    - Integration with EDR vendors and business systems such as IT service management
    - XDR platform enhancements and telemetry collection
    - Availability of consulting services, security assessments, and other tools or expertise centered on cybersecurity maturity

In addition, buyers may want to consider cyberinsurance, which is nascent in the MDR market, and only a few providers offer it through partners.

IDC encourages buyers to evaluate MDR providers based on the outcomes they want to achieve related to day-to-day detection and response and cybersecurity maturity.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Arctic Wolf

Arctic Wolf is positioned in the Leaders category in the 2021 IDC MarketScape for U.S. managed detection and response services.

Arctic Wolf Networks, which was founded in 2012 and initially offered SOC as a service, is headquartered in Eden Prairie, Minnesota. The company's stated mission is to end cyber-risk by helping its customers switch their thinking from a tools focus to an operational mindset. This switches the paradigm to focus on the business outcomes that an MDR service can enable.

Three priorities support the switch: optimize existing technology stacks and send them to the cloud, focus on a complete security operations framework that covers attack types and attack surfaces, and build resilience with expert guidance and 24 x 7 protection (storage, enrichment, correlation, analysis, and investigation) and implementation of tactics and strategies. Arctic Wolf owns security outcomes that align with identify, protect, detect, respond, and recover.

The company aims to provide simple, easy, personalized consumption that hides complexity and doesn't require a rip-and-replace approach. To this end, a concierge engagement model defines roles and responsibilities for Arctic Wolf and customers in areas such as activation, deployment, customization, service delivery, ad hoc requests, and scheduled interactions.

The cloud-native Arctic Wolf Platform supports solutions including MDR, managed risk, managed cloud monitoring, and managed security awareness. Telemetry ingestion, detection, investigation, and ticketing are automated through the platform, which leverages a combination of the Arctic Wolf Platform with the customers' technology stacks to provide visibility across endpoint, network, cloud, identity, and users. A dedicated triage team investigates alerts, and the team provides tactical support and guidance to customers and the concierge team during security events.

Strengths

Arctic Wolf has well-developed road maps in areas of managed service, managed detection, and managed response. The breadth of visibility is excellent, and the company expects to invest in orchestration and automation and to develop an enhanced MDR tier and offerings for specific customer segments.

The four current United States–based SOCs will be supplemented in the near future, with SOCs in Germany, APAC, and North America to expand Arctic Wolf's capabilities to address customers in these geographies, both with the Arctic Wolf Platform and with its triage and concierge teams. Having a team that is closer to the customer is a benefit, as the company does not send an incident to a customer until it has been looked at by a human during what Arctic Wolf calls the "the last human mile of triage."

The concierge team, which provides unlimited support, works with each customer to build and execute a security journey aligned with organizational goals and objectives. A customer commented that the level of service is "off the charts."

Challenges

The customer portal, which is designed with operational staff in mind, offers interactivity in areas such as configurations, endpoint health, and gaps in monitoring but not in-depth investigative capabilities. In addition, customers aren't able to create, update, or close tickets or edit or customize reports themselves, although they can request any number of reports.

Threat hunting is not continuous; however, Arctic Wolf intends to add staff to this function. And while the company aspires to provide response "across everything," a few areas, including identity and access management (IAM), do not yet have a response beyond alerting.

A customer noted that the company's rapid growth has resulted in growing pains in areas such as new service deployments and quality assurance.

Consider Arctic Wolf When

SMB and midmarket companies – generally without SIEM systems – that prefer a concierge approach, a robust sales/support structure, and the advantages of SaaS consumption should consider engaging Arctic Wolf.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

MDR, as a subset of MSS, combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity detection and response capabilities for an organization. Service providers can deploy MDR services utilizing a mixture of customers' existing capabilities, along with partner-supplied tools or services and private intellectual property. MDR services are typically supplied by a provider's well-trained cybersecurity staff that works in one or more 24 x 7 x 365 remote SOCs.

Figure 4 depicts the MDR elements of greatest importance to delivering value, impact, and desired outcomes. IDC recognizes the following capabilities as a minimum set of MDR capabilities:

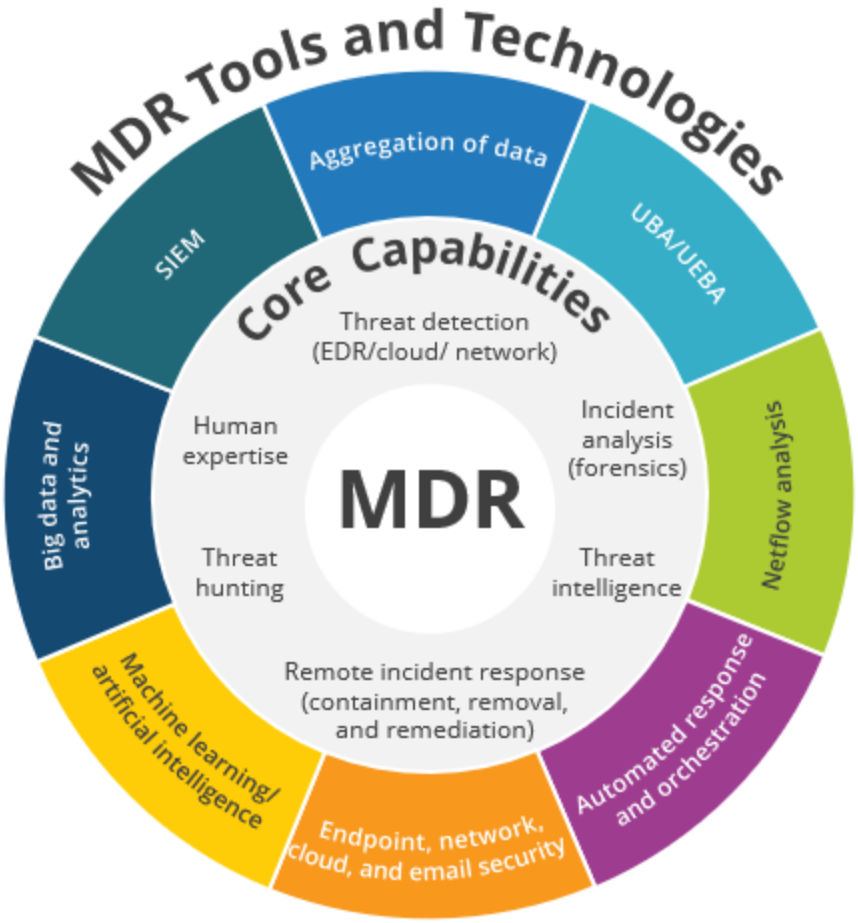
- **Utilization of endpoint protection capabilities as embodied in an EDR system.** XDR, with its access to "X" telemetry data such as the network, cloud, or messaging systems, can be used in place of an EDR system.
- **The integration of multiple threat intelligence feeds to provide timely information into the MDR service.** The objective is to enable organizations to understand what systems are being targeted, who is doing the targeting, and the tactics, techniques, and procedures that are vital in moving cybersecurity from a reactive stance to a proactive stance.
- **Regular use of human-led threat hunting to supplement threats uncovered by IoCs to be based on risk analysis and/or integrated threat intelligence feeds.** The processes and playbooks that are created in the human-led threat hunting activities should be included into the equally important automated threat hunting activity.
- **Remote incident response (little R) services including containment and removal of adversaries, incidents, or breaches where data is suspected or known to have been exfiltrated, destroyed, or manipulated.** IDC believes that a core part of the MDR service must

go beyond offering guidance and recommendations and should include a component that can automate a response for a customer when malware is downloaded but no other collateral damage occurs.

- **Comprehensive remote incident response (big R) services (at an additional charge) for the serious breaches that require a coordinated response, remediation, and forensic capability.**
- **Web-based dashboards that allow for the monitoring, updating, and reporting of all IoCs and/or tickets that are created from the service.**

FIGURE 4

An Effective Managed Detection and Response Solution



Note: For more information, see *MDR: The Next Generation of Managed Security Services* (IDC #US46427920, June 2020).

Source: IDC, 2021

Strategies and Capabilities Criteria

The importance of a firm's characteristics to project success and relevance of the security detection and response challenge combined with IDC's opinion about the impact those elements have on selection of

firms implies a unique weighting of these elements when evaluating a firm's overall strategies and capabilities to address market opportunity and realizing market success (see Tables 1 and 2).

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment* (IDC #US46235320, September 2020)
- *MDR: The Next Generation of Managed Security Services* (IDC #US46427920, June 2020)

Synopsis

This IDC study presents a vendor assessment of U.S. providers offering managed detection and response (MDR) services through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for MDR. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the MDR market over the short term and the long term.

"Security leaders are shifting their stance on cybersecurity to examine it through a strategic, business, and industry lens, which IDC believes is the right approach. Efficient, effective security for the entire enterprise is a necessity at a time when networks are evaporating and endpoints are proliferating — and relentless adversaries continually adapt their tactics, techniques, and procedures. Organizations are looking for comprehensive threat detection and response as well as assistance with elevating cybersecurity maturity. Managed detection and response providers are stepping up to this challenge and differentiating themselves in areas such as XDR, automation and orchestration, threat intelligence, and threat hunting and assisting customers with building and executing their security journeys." — Craig Robinson, program director, Security Services at IDC

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com