IDC MarketScape

IDC MarketScape: Worldwide Managed Detection and Response 2024 Vendor Assessment

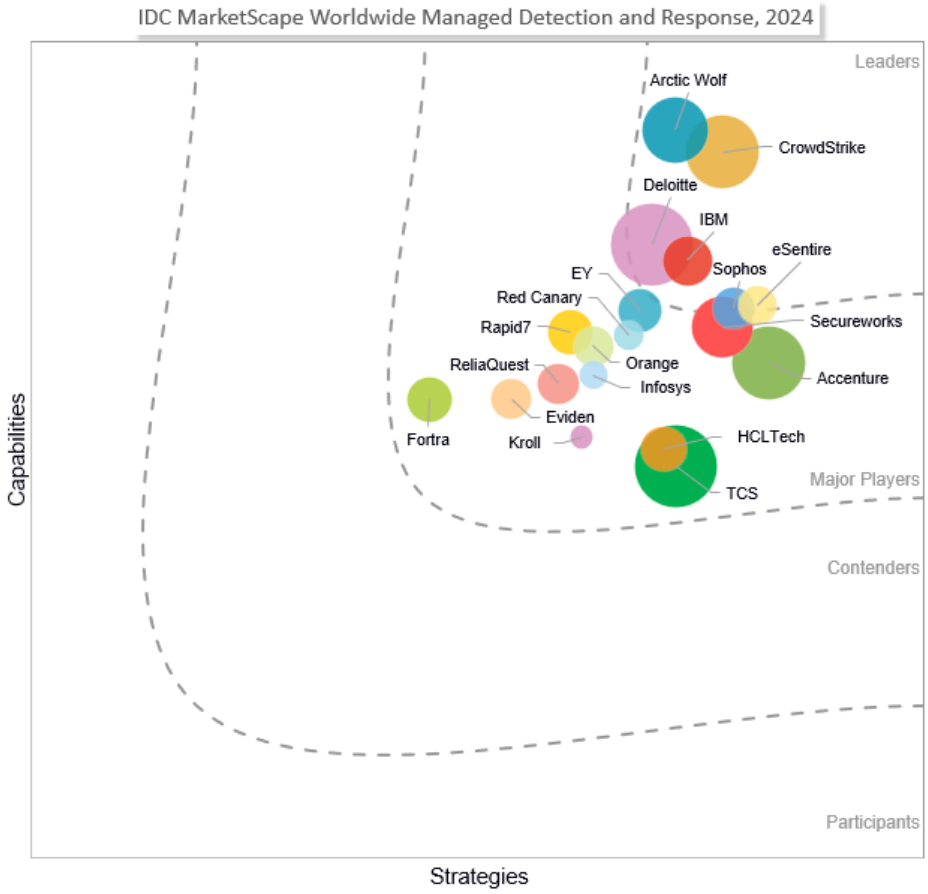
Craig Robinson

IDC MARKETSCAPE ARCTIC WOLF

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Detection and Response Vendor Assessment



Source: IDC, 2024

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

April 2024, IDC #US49006922e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Managed Detection and Response 2024 Vendor Assessment (Doc # US49006922e). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The managed detection and response (MDR) market has evolved extensively over the past couple of years. This should be seen as a positive movement as MDR providers have had to evolve to meet the growing threat landscape and heightened customer expectations. Some notable changes are discussed in the sections that follow.

Response

Prior years saw MDR providers touting their ability to do full response, as opposed to just throwing a ticket into their customers' IT ticketing system. Fast forward to the present day and now almost all MDR vendors provide full response cycles up until the time that a full-blown incident is discovered. When a normal detection turns into a full-blown incident response (IR) situation, the level of support is now a differentiator.

Some vendors provide a block of hours per incident or over the lifetime of a contract. Other vendors tout unlimited incident response hours. Some provide monetary compensation toward different categories of reimbursable expenses. The saying that "the devil is in the details" applies as similar sounding promises of support and compensation can actually widely differ based on the fine language.

Visibility

Transparency is a sought-after trait in many areas outside of cybersecurity, but in the realm of utilizing a managed security service (MSS) like MDR, it is increasingly being desired by buyers of MDR. Many providers reviewed in this study demonstrated that the information that their customers see in the portal is exactly what their security operations center (SOC) analysts see.

The ability to view statistics concerning the MDR provider's performance is another visibility change that IDC is observing. This ties back to many of the performance SLAs that are being included in MDR contracts. Guarantees such as the MDR vendor's performance for mean time to detect (MTTD) and mean time to respond (MTTR) are and have been table stake measurements for a number of years. What has changed more recently is the visibility into exactly the when, what, where, and how when it comes to detecting, stopping, and applying remedial action for an attack.

Outsource, Comanage, or In-House Options

There are definitive trends to note around *how* MDR is being utilized based on the size of the organization. The quick ability of MDR to elevate a fledging cybersecurity program makes it a very attractive service to consume for the SMB market. The ability to get 24 x 7 x 365 coverage for much if not all of an organization's IT and/or OT assets is compelling. The math is not that hard, and to make things even more inviting, some MDR providers even offer up an ROI calculator to justify the cost.

For the SMB market, the operating model is largely one where the MDR provider provides the detection and response services while the consuming organization can stay out of the picture for many

day-to-day operations. Of course, organizations still have to work with their MDR provider on proactive work such as refining the playbooks, runbooks, and use cases that are specific to their operations. There are also times where the institutional knowledge that consumers of MDR possess is needed to resolve some cases, and at other times, they need to get engaged for remediation issues. This is not an all-encompassing list of the intersection between the MDR provider's operations and the consuming organization, but rather an acknowledgement that MDR for the SMB market shifts most, but not all, of the day-to-day tactical work to the vendor, but the MDR buyer still has many moments where it needs to be a willing partner.

As organizations grow, so too does the complexity of their IT operations. MDR is increasingly being used by organizations on the larger end of the spectrum, but usually in a different manner than smaller organizations. The ownership of who does what can shift. For some organizations that lack experienced threat hunters or higher-tiered SOC analysts, they might choose to do tier 1, or tier 1 and tier 2 operations, using in-house SOC analysts, and then shift or comanage tier 3 activities to their MDR provider. Another scenario reviewed in this study occurs when the MDR provider handles tier 1 and tier 2 activities, and then the client's security team handles tier 3 and other elevated activity on their own or as a comanaged model.

Reducing Cost and Complexity

The number of security leaders who are being asked to reduce the rate of growth of their respective budgets, and/or reduce their budgets, is growing. The growth in managed security services, with MDR being the high-growth leader within this market, is partially driven by the cost savings that organizations can often realize by shifting their tactical security operations to an MDR provider.

One of the many comments that IDC noted in this research when talking to the security leaders that utilize MDR is how the employees of the MDR provider feel like an extension of their team. One of the takeaways that this shows is the level of familiarity that these providers attain with their clients. This intimacy of operations is not readily gained. It takes time and effort.

Organizations that readily consume other managed or professional security services have to invest in these relationships. Besides the hard dollar costs, many organizations are recognizing the soft costs associated with engaging in what can feel like endless relationships to obtain the needed expertise and capabilities that managed security service providers (SPs) and other security service providers offer.

MDR providers that have robust adjacent capabilities will be able to add additional stickiness to their relationships by simplifying their customers' vendor portfolio. The risk to buyers of having "'too many eggs"' in fewer baskets is a legitimate concern, but many will see that the hard and soft costs of consolidating the number of different cybersecurity firms that they work with will be worth the risk.

The MDR Versus MXDR Difference

The lines blur when trying to differentiate between a managed extended detection and response (MXDR) platform-based service and a managed service like MDR. Generally speaking, an MDR service wraps services around the customer's current cybersecurity tooling stack. Tools like endpoint detection and response (EDR) and security information and event management (SIEM) were the workhorses of early MDR services. As MDR matured, security orchestration, automation, and response (SOAR) capabilities were add-on options, usually at an extra cost, for their customers.

Today, SOAR capabilities are a given, and the capabilities that these tools provide are almost always embedded into the MDR service.

The evolution of the extended detection and response (XDR) market has provided new opportunities for enhanced detection and response. Building upon its roots as an extension of EDR, XDR is now the platform for which detection and response actions can occur beyond the endpoint. Initial iterations of XDR added on additional telemetry that traditional EDR did not provide, such as cloud, messaging, and application telemetry ingestion and correlation. More recent iterations of XDR are more cognizant of the value of network telemetry and usually provide internal network detection and response (NDR) capabilities, or they work with third-party NDR providers to provide this capability. Like other major security tools, XDR is often offered up as a managed service by managed security SPs or systems integrators and consultancies as a MXDR service.

The different flavors of XDR can vary for MXDR providers. Some vendors have their own XDR platform that is largely built around their own set of security tooling. Others take a more best-of-breed approach with a more limited set of third-party tools tightly integrated into their XDR platform. Another interesting model occurs when a provider is willing to take on new clients with its existing set of security tools, and then transition them on to their XDR platform over time.

The inevitable question that buyers and prognosticators ask is this: Is MXDR better than MDR? They each have their own strengths and weaknesses.

A provider that offers an MXDR service utilizing its own native tools and IP is compelling. The engineering effort to integrate all of the different components is less as the underlying software has been bult in-house. IDC has a belief that complexity is the enemy of cybersecurity, so the less engineering required to bridge various third-party security tools, the better.

The costs go down for that provider since it owns the underlying components that make up the XDR platform. On paper, this makes for a more seamless and higher-margin opportunity for the MXDR provider. Less friction from an engineering and architecture perspective usually leads to better results such as quicker detection and response times.

This all sounds good. What are the downsides? Well one first has to recognize that even if an MXDR provider owns most if not all of the components of its XDR platform, not all natively owned tools have organic roots. Oftentimes, these additional capabilities have been acquired from a third party, and then it has to be integrated into the underlying XDR platform. If a groundbreaking new capability comes up — like an AI-powered capability — from a third party, if it is compelling enough, then it needs to be acquired or integrated into the XDR platform.

As for traditional MDR services, they are still a compelling option for organizations with deep, customized security tooling. Muttering the words "rip and replace" will not bring about positive vibes from the CFO. Investing into an MXDR provider should occur with an extra dose of due diligence, as the road to switch out of that service is filled with more potholes than it would take to switch off of a traditional MDR service.

MDR services that are not provided on an XDR platform have different challenges and opportunities. The MDR provider has to do the engineering work to stitch together the necessary integrations between the toolsets that make up their service. This raises the operating costs of the platform and requires extra effort to understand the road maps of the different vendors that they work with. The

upside is that these providers don't have to have a "'rip and replace"' philosophy as they can usually work with their customers' existing security tools.

Another type of provider has to be noted here. There are some MDR providers that wrap services around a third-party XDR platform. This gives them an opportunity to specialize around one platform while adding on some of their own IP that they have from other security services (usually MSS or incident response related). Some will even offer up MDR that can support multiple XDR platforms.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the worldwide managed detection and response 2024 vendor assessment, providers had to meet the following criteria:

- **Portfolio of MDR services:** The security service provider must offer 24 x 7 managed services for detection and response. These could include any or all the following:
  - Pure-play MDR/MXDR service
  - Managed EDR service
  - Managed threat hunting service
  - Managed SIEM
- **Revenue:** The worldwide MDR revenue of the service provider should be greater than $60 million for the year 2021.
- **Multiregion footprint:** The MDR service provider should have customers in more than one of the following regions: North America, LATAM, EMEA, and APAC.

ADVICE FOR TECHNOLOGY BUYERS

Buyers that choose to utilize an MDR service have many motivating factors that can drive this decision. Lack of in-house talent, desires for cost savings, a need to elevate current capabilities, and a desire to expand coverage of a dispersed attack surface are easily top reasons to consider.

In addition to reviewing the capabilities listed for each studied provider in this study, other foundational questions need to be considered:

- **How complicated are the IT and security systems that are in place?** Highly complicated systems might benefit from an MDR provider that invests heavily into gaining telemetry from a wide swath of sources, and also by having the ability to manage specific point products as necessary.
- **Geographic presence.** How dispersed is the MDR provider's operations? Do they have local language capabilities in the countries that you operate? What about their local presence?
- **Digital sovereignty**. Is the MDR provider fully prepared to honor the digital sovereignty requirements that you operate in, or that you might operate in over the length of time of the MDR contract (usually three years).
- **Best of breed or platform?** Your IT strategy in this regard might influence a potential change in this fundamental question. There is no question that the momentum in the market is toward platform-centric operations, but every organization needs to make this decision based on what works best for them.

- **Adjacent capabilities.** Gaining a managed vulnerability service is a common next step that first-time buyers of MDR often pursue, but what other capabilities would you like to consolidate on? Keep in mind that while vendor and tool rationalization is a growing trend, most buyers of MDR prefer to have a separate provider to handle offensive security testing like red team engagements.
- **Cost certainty.** There are multiple consumption-driven options to consider. Pricing can be done by data ingestion, number of endpoints (and the definition of endpoints can widely vary), numbers of tickets, number of events, and other hybrid ways.
- **Incident response**. Incident response is a critical function that most MDR providers offer. Some providers offer up blocks of hours as a standard offering for incident response before any additional cost is incurred for their response activity. Other providers offer up unlimited response and/or offer some financial compensation if incident response is needed. Buyers need to balance the IR capabilities and potential costs incurred against internal financial capabilities to pay for all of the related costs (compliance, media, operational downtime, remediation, legal, forensic, etc.) that go into a full-fledged IR situation.

  Remember all the fine print associated with a cyberinsurance policy that you might have? The fine print around how any IR service is provided, along with any potential financial reimbursement, should likely be reviewed by the organization's legal counsel.
- **Historical data.** Most buyers of MDR feel more confident in their provider over time. IDC recognizes that part of this increased confidence tracks back to the fact that the ingestion of data over the time that the contracted service has started allows for normal versus abnormal behavior to be identified. IDC strongly encourages buyers of MDR to work with providers that can ingest historical data.

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 2024 IDC MarketScape for worldwide managed detection and response services.

Quick facts about Arctic Wolf include:

- **Years in business:** Founded in 2012
- **Employees:** Over 600 employees involved in detect and respond roles
- **Presence:** Significant presence in North America and EMEA

Arctic Wolf's MDR service is centered around its investment in its open-XDR Arctic Wolf Platform, which allows it to offer a vendor-neutral approach to ingesting telemetry from the entirety of its customers' attack surfaces and existing stack of security tooling. The strategy is to leverage its customers' existing technology stack to gain broad visibility across the endpoint, network, cloud, identity, and even the human element.

Taking a vendor and technology-neutral approach, Arctic Wolf's customers have the flexibility to swap out tools and technologies (and therefore vendors), as well, preventing vendor lock-in without

sacrificing their security efficacy. The Arctic Wolf platform extracts security insights from over 5.2 trillion events per week across multiple industries, organization sizes, and attack surfaces.

IDC notes that SOCs have been overwhelmed with tickets that often end up being false positives. Arctic Wolf fights this trend by distilling the telemetry that it ingests down to less than actionable one ticket per day per customer. Early visibility is obtained and analyzed whenever possible at the source.

Arctic Wolf Labs' threat research team uses the power of machine learning (ML) and AI to discover novel indicators of compromise (IoCs) within its data. Detection logic built into the threat detection pipeline improves the efficacy of the platform. Threat research informs the security posture assessment work that the Concierge Security Teams perform with customers on a programmatic and regular basis to harden its security posture, reducing the likelihood that it will experience a cyberevent in the first place.

Arctic Wolf recognizes that its customers struggle with the evolving security demands of their organizations and the growth of their vulnerable attack surfaces. To help mitigate this risk, it created a program called Security Journey. As the name implies, the program designs a custom security journey for every customer to streamline the process of proactively mitigating risk and minimizing attack surface exposure. The Security Journey is delivered in incremental, actionable steps via what it calls Security Posture in-depth Reviews (SPiDRs).

The Concierge Security Team will build a program of SPiDRs to address threat mapping (aligned to NIST and MITRE) and reduce the exposed attack surface through short, actionable, and encapsulated activities. These activities can be focused on technology (e.g., firewall) or environmental (e.g., policy) audits, change management aids (e.g., insider threat risk mitigation), and security assessment (e.g., Microsoft attack surface reduction)–related activities to reduce the risk to their environment. Arctic Wolf has developed a library of over 100 highly valued SPiDRs that align with compliance frameworks, insurability needs, and specific threats.

The Concierge Security Team proactively hardens environments by learning the business context of every customer. It then leverages this context to further develop the Security Journey and to help optimize the detection and response guidelines for each customer.

Strengths

Arctic Wolf offers up its IR Plan Builder to guide organizations through a process that collects the critical information needed to kick off an IR investigation. The IR plans include five categories of information: Response Team, IT Providers, Network Information, Incident Escalation, and Systems and Data. When completed, Arctic Wolf will review a client's IR plan to identify gaps and missing information that will cause delays. The IR plan is safely stored off-network and accessible to customers as well as the Arctic Wolf Incident Response team during cyberattacks.

Challenges

While Jira and ServiceNow are top-of-mind tools that are utilized for handling IT- and cybersecurity-related tickets, one customer noted it was awaiting an integration with a different ticketing system that would be beneficial for its team.

Consider Arctic Wolf When

Organizations that are looking for a high-touch partner for their cybersecurity needs should consider utilizing Arctic Wolf. Organizations looking for an MDR partner that offers up a warranty in exchange for a broader relationship beyond MDR should also consider 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

Managed detection and response (MDR), as a subset of managed security services (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 and 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.

IDC recognizes the following capabilities as a minimum set of MDR capabilities for this study:

- **There should be utilization of endpoint protection capabilities as embodied in an endpoint detection and response (EDR) system.** The greying of lines between EDR and XDR is resulting in the recognition that an XDR platform that contains EDR functionality in it can take the place of a traditional EDR system.
- **MDR systems must ingest telemetry from endpoint, identity, cloud, network, UBA and/or UEBA, and SIEM data to be considered a complete MDR service.** IoT, OT, email/messaging, and mobile telemetry feeds are beneficial but not always captured.

- **Use of big data analytics and machine learning (ML) algorithms that correlates and then detects likely attacks that require further investigation and possible response action.**
- **The integration of multiple threat intelligence feeds provides 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 include containment and removal of adversaries.** 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) is for the serious breaches that require a coordinated response, remediation, and forensic capability.** Some firms will choose to utilize a partner for the actual incident response work. In addition. some MDR providers might choose to utilize a partner for any required forensics.
- **Web-based dashboards allow for the monitoring, updating, and reporting of all IoCs and/or tickets that are created from the service.**

LEARN MORE

Related Research

- *Worldwide and U.S. Comprehensive Security Services Forecast, 2024-2028* (IDC #US50635924, April 2024)
- *IDC MarketScape: Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment* (IDC #US50463223, March 2024)
- *Abundance in Tools, Shortages in Talent – Security Service Providers Addressing Feast and Famine in 2023* (IDC #US51842423, February 2024)
- *Market Analysis Perspective: Worldwide Security Services, 2023 and Beyond* (IDC #US51228723, September 2023)

Synopsis

This IDC study provides an in-depth analysis of the evolving managed detection and response/managed extended detection and response (MDR/MXDR) market, highlighting the importance of full response capabilities, key adjacent capabilities, transparency, and various service models tailored to organizational size and complexity. It emphasizes the growing need for MDR services due to increasing threats and budget constraints, differentiating between MDR and MXDR services while offering strategic advice for technology buyers. The document also includes vendor evaluations, focusing on their strengths, challenges, and unique offerings.

"In an era where cybersecurity threats evolve daily, MDR services have become a beacon of hope, offering a compelling managed service tailored to meet the growing threat landscape and customer expectations," says Craig Robinson, research VP, IDC's Worldwide Security Services. "Resource-

constrained CIOs and CISOs now have an option to elevate their cybersecurity program in an affordable manner that is personalized to meet their unique security and risk needs."

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

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