WAVE REPORT

The Forrester Wave™: Managed Detection And Response, Q2 2023

The 13 Providers That Matter Most And How They Stack Up

May 17, 2023

Jeff Pollard

with Joseph Blankenship, Lok Sze Sung, Michael Belden

Summary

In our 23-criterion evaluation of managed detection and response providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals select the right one for their needs.

Topics

- Collaborative Response And Comprehensive Hunting Divide Good From Great
- Evaluation Summary
- Vendor Offerings
- Vendor Profiles
- Evaluation Overview
- Supplemental Material

Collaborative Response And Comprehensive Hunting Divide Good From Great

Managed detection and response (MDR) brought much needed disruption to the managed security services market over the last decade, but now as the providers enter the next stage of maturity, they

confront the beast that slew many energized, upstart providers: going from hundreds to thousands of customers and from a few services to many. For some providers, the cracks are already starting to show, while others managed to stay the course and keep close to what got them where they are: a stable of services that deliver superior detection, comprehensive investigations, thorough response, and extraordinary customer engagement. MDR providers in this Forrester Wave™ maintain exceptionally high rates of customer satisfaction, retain existing customers at unprecedented levels, and have growth rates that any maturing companies — and startups — would envy. Providers must maintain this commitment to customer obsession in a market with more competition, savvy buyers, budget constraints, and shareholder expectations.

As a result of these trends, MDR customers should look for providers that:

- Perform actual response without requiring automation. Some MDR providers now require automation for any vendor-performed response action. These providers will "assist" customers in taking nonautomated actions but no longer perform them. For security teams, automation requires: 1) comprehensive playbooks, 2) strong situational awareness of assets and impact, and 3) understanding of the threat. MDR providers can assist with the first, often depend on the customer for the second, and bring enormous expertise to the third. Restricting response to automated actions does help reduce the cost of delivering the service to customers but lets down customers that are unable — or unready — to automate.
- Conduct threat hunts with clear success criteria across a wide range of data sources. Real threat hunting requires a human-led, hypothesis-driven approach with defined success criteria. Some providers stress "automated threat hunting," but a name for that already exists: analytics. Real threat hunting requires a systematic approach to creating a hypothesis with clear success criteria and establishing a threshold at which the hunt is complete. Many MDR providers offer threat hunting within their service but give less clarity on the motives behind hunts, the hypothesis being validated, and when the hunt is deemed complete. Threat hunting tries to find attackers that evade security controls, which requires MDR providers that offer hunting to do so with a systematic, formal methodology.
- Expect data ingest but request data federation. Interacting with data that MDR providers never ingest is the newest innovation driving detection and investigations in MDR. From our earliest MDR research, Forrester believed that ingest was necessary but not sufficient, and the providers in this Forrester Wave ingest from many different data sources. Today the difference comes when providers use data without needing to ingest it. Using data wherever it's stored, without ingesting it, on demand, is one of the recent innovations shaking up the MDR market today and not something every provider supports. Customers save money because they avoid paying for multiple points of ingest, and providers get more data they can use during investigations.

Forrester receives significant interest from clients about Microsoft, and the vendor maintains extensive partner relationships with many of the MDR providers evaluated in this Forrester Wave. In 2022,

Microsoft introduced its own set of MDR services. Its generally available services currently do not meet the completeness-of-offering inclusion criterion for this Forrester Wave. Therefore, Forrester elected not to include Microsoft in this evaluation.

Evaluation Summary

The Forrester Wave evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in our report The Managed Detection And Response Landscape, Q1 2023.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 1

Forrester Wave™: Managed Detection And Response, Q2 2023

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: Managed Detection And Response Scorecard, Q2 2023

	Forrester's weighting	Arctic Wolf	Binary Defense	BlueVoyant	CrowdStrike	Deepwatch	eSentire	Expel
Current offering	50%	2.36	3.02	2.64	3.68	1.56	3.04	4.60
Time to value	7%	3.00	5.00	3.00	3.00	1.00	5.00	5.00
Threat hunting	7%	3.00	5.00	3.00	5.00	3.00	3.00	5.00
Threat intelligence	7%	3.00	3.00	5.00	5.00	1.00	5.00	3.00
Case management	7%	3.00	1.00	5.00	3.00	3.00	3.00	5.00
Analyst experience (AX)	7%	1.00	3.00	1.00	3.00	1.00	3.00	5.00
Analytics	7%	3.00	1.00	3.00	3.00	1.00	1.00	5.00
Extended detection and response (XDR)	7%	3.00	3.00	3.00	3.00	1.00	3.00	5.00
Managed detection	7%	3.00	3.00	3.00	5.00	1.00	3.00	5.00
Managed investigations	7%	3.00	5.00	1.00	3.00	3.00	3.00	3.00
Managed response	7%	1.00	3.00	3.00	5.00	3.00	5.00	5.00
Dashboards and reporting	6%	3.00	1.00	1.00	5.00	1.00	3.00	3.00
Metrics	6%	3.00	1.00	1.00	3.00	1.00	3.00	5.00
Scripting engine	6%	1.00	5.00	1.00	1.00	1.00	1.00	5.00
Product security	6%	1.00	5.00	3.00	3.00	1.00	3.00	5.00
Platform capabilities	6%	1.00	1.00	3.00	5.00	1.00	1.00	5.00
Strategy	50%	3.34	2.62	2.02	4.32	2.32	2.36	3.72
Product vision	17%	3.00	1.00	1.00	5.00	3.00	1.00	5.00
Market approach	17%	3.00	3.00	3.00	5.00	3.00	3.00	5.00
Adoption	17%	5.00	3.00	1.00	5.00	3.00	5.00	5.00
Planned enhancements	17%	3.00	1.00	3.00	3.00	1.00	1.00	5.00
Partner ecosystem	17%	3.00	3.00	3.00	3.00	1.00	3.00	1.00
Commercial model	15%	3.00	5.00	1.00	5.00	3.00	1.00	1.00
Market presence	0%	5.00	1.00	2.00	5.00	2.00	4.00	2.00
Revenue	50%	5.00	1.00	1.00	5.00	3.00	4.00	2.00
Number of customers	50%	5.00	1.00	3.00	5.00	1.00	4.00	2.00

	Forrester's weighting	IBM	Rapid7	Red Canary	ReliaQuest	Secureworks	SentinelOne
Current offering	50%	1.70	3.28	3.96	2.58	3.94	2.44
Time to value	7%	1.00	3.00	5.00	1.00	5.00	5.00
Threat hunting	7%	1.00	5.00	5.00	1.00	5.00	1.00
Threat intelligence	7%	1.00	3.00	5.00	3.00	3.00	3.00
Case management	7%	3.00	3.00	3.00	5.00	3.00	1.00
Analyst experience (AX)	7%	3.00	3.00	5.00	1.00	3.00	1.00
Analytics	7%	3.00	3.00	3.00	1.00	5.00	1.00
Extended detection and response (XDR)	7%	3.00	3.00	5.00	5.00	3.00	3.00
Managed detection	7%	1.00	3.00	5.00	3.00	5.00	3.00
Managed investigations	7%	3.00	5.00	3.00	1.00	3.00	3.00
Managed response	7%	1.00	3.00	3.00	3.00	5.00	1.00
Dashboards and reporting	6%	1.00	3.00	3.00	3.00	3.00	3.00
Metrics	6%	1.00	3.00	3.00	3.00	3.00	1.00
Scripting engine	6%	1.00	3.00	3.00	1.00	5.00	3.00
Product security	6%	1.00	1.00	3.00	3.00	3.00	5.00
Platform capabilities	6%	1.00	5.00	5.00	5.00	5.00	3.00
Strategy	50%	1.68	2.66	3.68	2.32	2.32	3.00
Product vision	17%	3.00	3.00	5.00	3.00	3.00	3.00
Market approach	17%	1.00	3.00	3.00	1.00	1.00	3.00
Adoption	17%	3.00	3.00	5.00	3.00	3.00	3.00
Planned enhancements	17%	1.00	1.00	3.00	3.00	3.00	1.00
Partner ecosystem	17%	1.00	3.00	3.00	1.00	1.00	5.00
Commercial model	15%	1.00	3.00	3.00	3.00	3.00	3.00
Market presence	0%	1.50	3.50	3.00	3.00	5.00	3.50
Revenue	50%	2.00	4.00	3.00	4.00	5.00	3.00
Number of customers	50%	1.00	3.00	3.00	2.00	5.00	4.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Figure 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
Arctic Wolf	Managed Detection and Response
Binary Defense	Binary Defense Managed Detection & Response
BlueVoyant	BlueVoyant MDR Services
CrowdStrike	Falcon Complete
Deepwatch	Deepwatch MDR
eSentire	eSentire Managed Detection and Response
Expel	Expel Managed Detection & Response
IBM	Managed Detection and Response
Rapid7	Managed Threat Complete
Red Canary	Red Canary MDR
ReliaQuest	ReliaQuest GreyMatter
Secureworks	Taegis ManagedXDR
SentinelOne	SentinelOne Vigilance Respond Pro

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **Expel** understands security operations in ways few in the industry can match. Expel continues its history of flawless roadmap execution and maintains its place as one of the vendors with the clearest vision of where security operations and MDR will go in the future. The provider's vision and planned enhancements recognize that security practitioners want to work directly with their data and the platforms of their MDR provider. Competitors embraced the channel ecosystem long before Expel, and the provider faces immense competition as it tries to catch up. In addition, Expel's competitors go to market with bigger budgets and more reach, which will add pressure as the company tries to maintain its rapid growth.

Expel brings a customer-obsessed service to market that delights practitioners. Customers can deploy within hours via its simple onboarding process and then find themselves in a platform that works for them regardless of their skill levels. Everything about the user interface reminds customers that the service is designed to help them make better decisions and improve their operational workflows. Of course, all of that comes with a price, and Expel is one of the more expensive providers. Reference customers mention the consistent delivery of feature enhancements as promised and consistent service delivery experiences as strengths. Reference customers confirmed that Expel is one of the more expensive providers. Organizations that want their teams to work with a stellar security operations platform and hope to uplevel their skill sets by working with exceptional practitioners — and have some budget headroom — should turn to Expel.

- **CrowdStrike** blends products, platforms, and services seamlessly for customers. Few companies can boast a string of successes like CrowdStrike. The vendor became a preeminent incident response firm and a dominant player in the endpoint security space. It delivers an exceptional MDR service and taught cybersecurity firms how software-as-a-service (SaaS) businesses work. A commitment to analyst experience, extended detection and response that keeps endpoint at its center, and an emphasis on adding its acquisitions to its MDR portfolio rapidly all indicate the provider will avoid major mistakes that would rob it of its momentum.

  CrowdStrike's extensive view of threat landscape and incident response services give it an advantage when it comes to threat intelligence and managed detection. CrowdStrike's innovative approach to service delivery includes eliminating the tiered security operations center (SOC) model other providers use, which reduces the likelihood that customer experiences will vary from one interaction to the next. CrowdStrike's limited API access is a notable deficit, and CrowdStrike depends on integrations for technologies outside the Falcon ecosystem. Reference customers second CrowdStrike's extensive knowledge of threat actor behavior as a key area of strength. References noted that gaps in cloud capabilities are a weakness of CrowdStrike. For companies that are looking to source products, platforms, and services from one provider and that want superior threat intelligence added in, CrowdStrike is the right choice.

- **Red Canary** proves the value of turning threat intelligence into meaningful detections. If Red Canary possessed the same skill at marketing and business development as it has at service delivery, then it would be one of the best-known names in cybersecurity. While that isn't the case — for now — Red Canary is positioned to continue its success and lengthen its reach in the market. Red Canary's vision and planned enhancements include offering comprehensive adversary profiles and tools like atomic red team to help its MDR customers better prepare for cybersecurity incidents, rather than solely helping customers react to them.

  If the cybersecurity industry needs one example of how to make threat intelligence useful and drive detection-engineering efforts via threat hunting, look no further than Red Canary. The provider possesses laudable expertise in going well beyond the limits of what customer-supported technologies can detect in its platform. Customer references highlight these factors, calling out a superior detection library and high-fidelity detections as strengths. Red Canary does

need to catch up on helping customers understand what changes to make to improve their overall security posture, something customer references also noted as a weakness. Security leaders looking for superior threat-hunting and detection engineering capabilities should evaluate Red Canary.

Strong Performers

- Secureworks' service and platform shine, but it has yet to prove its relevance in channel. In a market where everything eventually becomes a service and product vendors and services providers went from partners to competitors, Secureworks stands out as the company that made the biggest successful pivot to blend platforms, products, and services. But that pivot took place in the past, and the future is where Secureworks will encounter headwinds. Secureworks plans to pivot its go-to-market and take an all-channel approach, but it remains uncertain whether it can replicate its direct sales success in an indirect sales world. Its competitors have a head start and a longer history of supporting channel programs, questions remain as to whether the provider will stay committed to channel after the current macroeconomic challenges end.

  Secureworks recognizes that time to value can make or break an MDR relationship, and it comes prepared to make that process as simple and transparent as possible. Secureworks builds a RACI matrix for customers that explains ownership of the activities necessary to get the service up and running. Secureworks is a provider with multiple decades delivering security services, and customer references highlight that as a strength. Dashboards and reporting are not as comprehensive as others, and reference customers note that some of the fields from the interface are not available as customizable options when creating reports. Companies seeking rapid, clear time to value and a provider with a history of delivering security services should seek out Secureworks.

- **Rapid7** understands today's MDR customer needs, but its future vision needs work. Rapid7 understood the value in offering security services on top of its intellectual property well before many other providers. Its InsightIDR product and MDR service offering benefit as a result of that foresight. Unfortunately, Rapid7's view of the future is unremarkable today in comparison to the past. Planned enhancements include incorporating additional data sources like Sysmon, expanding cloud detection and response, and adding additional security orchestration, automation, and response (SOAR) capabilities to increase the amount of automation available to customers. It's a roadmap that isn't wrong based on where the provider is today, but it's also one that isn't putting Rapid7 ahead of competitors in the future.

  Rapid7 does stand out in the amount of threat hunts it performs and the comprehensive number of hypotheses and techniques it uses to threat hunt for adversaries. Rapid7 also offers detailed forensics during the investigative process to assist customers and accelerate potential incident response efforts if the customer requires boots-on-the-ground support. Reference customers echo these sentiments with mentions of responsive personnel and proactive alerts as strengths. The roadmap cracks also are visible to reference customers, who mention slow integrations and limited support for other security tools as weaknesses. Businesses that want skilled practitioners that engage in frequent, varied threat hunts to find adversaries should seek out Rapid7.

- **Arctic Wolf** delights with concierge security, but portfolio sprawl risks its progress. Arctic Wolf was an early entrant into MDR and a pioneer of high-touch service delivery in the MDR space. The nature of the customer experience also serves the provider well in terms of its future plans; the vendor features a customer's security journey and plans to add gamification elements to help incentivize customers to improve their security posture. While not resting on its laurels when it comes to customer service, much of the rest of the Arctic Wolf roadmap does not meaningfully differentiate it from its competitors. More integrations, improvements to managed detection and managed response, and an improvement to a recently launched two-way integration with ServiceNow feature in a cluttered roadmap that also tries to satisfy non-MDR use cases like vulnerability management.

  With its current offering Arctic Wolf stands out when customers interact with the concierge security team, but not so much when they interact with the provider's platform. Arctic Wolf activates customers reasonably quickly and creates quick time to value and performs thorough threat hunts, but it struggles with analyst experience and case management. Reference customers mention a lightweight EDR agent and threat intelligence as strengths. Reference customers note case management and resolution of issues as areas of weakness. Security teams looking for a comprehensive offering that want to be hands-off and rely on their service provider to carry more of the load should consider Arctic Wolf.

- **Binary Defense** brings unsurpassed technical chops, but its platform needs work. Given that Dave Kennedy founded Binary Defense, it's not surprising that the provider brings strong technical expertise to service delivery. As it enters the next stage of its growth, it also recently added new leaders to its team who have a history of developing and scaling strong service delivery organizations. Binary Defense is still a practitioner-focused service, but its roadmap does indicate it is aware of its shortcomings. Items the provider is actively addressing include additional ingest capabilities via extended detection and response (XDR), advanced forensics capabilities, a ServiceNow build-out to enhance integration with the case management platform, and identity-based detection capabilities.

  Binary Defense brings a solid set of capabilities to market today with rapid time to value, threat-hunting expertise, and a scripting engine built into its platform that enables customers to use Jupyter notebooks to interact with their data in the provider's platform. Binary Defense offers strong threat hunting but falls short when it comes to metrics and reporting. Reference customers confirm the vendor's detection reliability as an area of strength but mention metrics and event notification gaps as weaknesses. Buyers that want a strong technical provider that is on a trajectory to become an enterprise partner should consider Binary Defense.

- **SentinelOne** leans into its channel successes, but its service delivery falls behind. SentinelOne sustained much of the momentum it gained in prior years and moved early to channel, which will benefit the provider as almost every other provider makes the same shift. Unfortunately, as SentinelOne continued to add portfolio and product features, the planned enhancements to its service have fallen behind. The provider's roadmap and future vision stress its commitment to its go-to-market efforts. One interesting area of innovation includes predictive threat analytics and the now standard "expanding XDR" roadmap item. Others, such as preprogrammed playbooks

and incident prioritization, are already available from most competitors.

Storyline Active Response (STAR) and the agent's ability to autonomously gather artifacts and incident-relevant activity are standout features of the provider — but these benefits come from its product, not its service. Like most MDR providers SentinelOne continues to add additional features via acquisition, and it does integrate those into its service quickly. Reference customers say that the ease of management of the agent and overall product effectiveness are strengths, while reporting the need for a stronger user community and that its acquisitions have a lower overall feature maturity level as weaknesses. Customers looking for an MDR provider with excellent managed security services provider (MSSP) relationships and a strong platform should think about SentinelOne.

- **eSentire** needs to make its service delivery and platform as relevant as its messaging. eSentire understands its customer base exceptionally well and mixes business-relevant messaging with technical explanations of what it brings to market. eSentire's vision includes a balanced plan for growth with a mix of marketplaces, managed service providers, and distributors to scale downmarket. eSentire's roadmap and planned enhancements include improvements in self-service capabilities, incident response, and enhanced cloud detection. Successfully executing on those items will still leave eSentire well behind competitors as the provider lacks its own intellectual property, giving competitors a sizable head start.

  eSentire's current offering includes a dated interface that stands out — not in a good way — when compared to the sleek, functional user interfaces of competitors. eSentire offers comprehensive response actions and does not make automation mandatory. This is a refreshing change, considering many other MDR providers now rely on automation to reduce analyst involvement in alerts. Reference customers confirm that response is an area of strength, mentioning that eSentire interacts with customer environments like their own, but also state that dashboards, reporting, and the current user interface are areas of weakness. eSentire is a strong potential partner for security leaders looking for a provider with a history of delivering a wide service portfolio that needs help articulating the business value of MDR during the purchase process.

Contenders

- **ReliaQuest** nails the platform part of MDR, but inconsistent service delivery holds it back. ReliaQuest is probably one of the oldest providers you recently heard about for the first time. This is largely due to the provider's struggles in how it messages its GreyMatter platform. This is also a challenge for ReliaQuest because, at present, GreyMatter is far better as an SOC platform than ReliaQuest is as an MDR service provider. ReliaQuest built its business on a direct sales model in the large enterprise. Like virtually every other MDR provider, it is now turning to channel, which is not an easy pivot to make. Its roadmap and planned enhancements include scaling out its platform capabilities, increasing use of automation, innovating in incident response, and increasing customer engagement.

  ReliaQuest recognized that interacting with federated data via APIs worked far better than depending on data ingest, and this continues to pay dividends for the provider in its MDR

service. The acquisition of Digital Shadows augmented the provider's threat intelligence capabilities, and it clearly spent time and attention on case management. ReliaQuest brings a feature-rich platform to market in the MDR space, and reference customers mention the platform and continuous innovation as areas of strength. References note that tuning rules, reporting, and speed of response are areas of weakness. Companies that want to be at the leading edge of SOC platform development and can accept a service that doesn't quite measure up should think about ReliaQuest.

- **BlueVoyant** excels at Microsoft Sentinel but lags in pure-play MDR capabilities. BlueVoyant debuted with an emphasis on its threat intelligence, but Microsoft's launch of Sentinel and a timely acquisition helped the vendor establish itself as a capable partner for managed Sentinel. BlueVoyant's roadmap and planned enhancements lean into its source of strength, emphasizing Microsoft Sentinel, security operations, and security information and event management (SIEM) use cases. Planned enhancements for more of a pure-play MDR service exist but seem to be a lower priority for the provider, with a more holistic approach to improving security operations and upskilling customer personnel in its roadmap.

  One area where BlueVoyant does innovate compared to its peers is in its focus on supply chain and third-party risk services. At the moment, those services stand apart from MDR, but given that these are common entry points for breaches, these services can play a role in managed detection and investigation. BlueVoyant stands out in generating and curating threat intelligence, and its focus on case management shines compared to other providers. Reference customers echo these strengths, identifying responsiveness and processes as strengths of the provider. However, reference customers also note that dashboarding, identity-based investigations, and cloud visibility are weaknesses. Organizations that need to solve Microsoft Sentinel related problems that also want MDR capabilities should consider BlueVoyant.

- **Deepwatch** rules over Splunk deployments but lags if EDR is the focus. Deepwatch continues to prove its mastery of Splunk as a platform. This doesn't, however, translate to the dominant MDR use cases in ways that Deepwatch hopes for. Deepwatch does not depend solely on Splunk, but its non-Splunk capabilities don't match what it can do when the SIEM solution is present. Deepwatch does innovate outside of Splunk, and the provider's roadmap and vision include improving analyst experience, extending its existing maturity models, and focusing on the continuation of its already successful channel program.

  Deepwatch emphasizes system criticality as an important aspect of detection. One specific innovation involves Threat Probability Value (TPV), which handles correlation, entity relationships, and identities. TPV brings in valuable context during detection, triage, investigation, and response. Deepwatch's service delivery features aspects of MDR and SOCaaS but leans more toward SOCaaS. Reference customers confirm that Deepwatch's overall approach to service delivery and integration with customer teams are strengths. References also indicated inconsistent service delivery and overly generic threat intelligence as weaknesses. Enterprise organizations looking for a provider with strong Splunk capabilities that can also handle MDR-related use cases should consider Deepwatch.

Challengers

- **IBM** hopes Resilient will make its MDR offering relevant. IBM entered the MDR market later than many competitors as it maintained a focus on its core MSSP offering, and it shows. IBM's acquisitive nature enabled it to acquire aspects of its offering and launch MDR, but it's unclear if those acquisitions will coalesce as the backbone of a quality service. IBM stresses the breadth of its portfolio of products and services in its roadmap. The provider's planned enhancements include identity detection, analytics, and reducing the need to ingest log data to perform detection.

  IBM's current MDR offering falls short of others. It comes together as a bit of a jumbled set of capabilities spanning multiple offerings: IBM QRadar, ReaQta, Resilient, and IBM partnerships. The siloed nature of the technologies also extends to service delivery. IBM matches other providers in areas like extended detection and response and analyst experience but fails to stand out in any specific aspect of MDR. Reference customers mention its broad service portfolio and global thought leadership as strengths. References echo the siloed nature of product and service delivery, expertise gaps with service delivery personnel, and inconsistent communication as weaknesses. Existing IBM customers or those looking for an established provider with global reach should evaluate IBM's MDR service.

Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include time to value, threat hunting, threat intelligence, case management, analyst experience (AX), analytics, extended detection and response (XDR), managed detection, managed investigations, managed response, dashboards and reporting, metrics, scripting engine, product security, and platform capabilities.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, market approach, adoption, planned enhancements, partner ecosystem, and commercial model.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's revenue and number of customers.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Forrester mindshare.** To ensure relevance to Forrester clients and the quality of the references being provided, Forrester considers the level of interest from our clients based on inquiries, advisories, consulting engagements, and other interactions.
- **Service revenue.** The provider must have at least $20 million in MDR revenue.

- **Core service delivery capabilities.** The provider must offer MDR with EDR, XDR, and SOAR capabilities with human-led, hypothesis-driven threat hunting and consider those core use cases.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by March 3, 2023 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.