The Forrester Wave™: Managed Detection And Response, Q1 2021

The 15 Providers That Matter Most And How They Stack Up

by Jeff Pollard and Claire O'Malley

March 24, 2021

Why Read This Report

In our 19-criterion evaluation of managed detection and response providers, we identified the 15 most significant ones — Arctic Wolf, Binary Defense, CrowdStrike, Cybereason, deepwatch, eSentire, Expel, FireEye, Kudelski Security, NCC Group, Rapid7, Red Canary, Secureworks, SentinelOne, and Trustwave — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

The Forrester Wave™: Managed Detection And Response, Q1 2021

The 15 Providers That Matter Most And How They Stack Up

by Jeff Pollard and Claire O'Malley
with Joseph Blankenship, Shannon Fish, and Peggy Dostie

March 24, 2021

The Threat Hunting-To-Analytics Pipeline Is A Difference Maker In MDR

Forrester's 2021 evaluation of the managed detection and response (MDR) market showed sophisticated use cases, educated customers, and high expectations. Good MDR vendors have definitively avoided becoming the alert factories their MSS cousins became. Innovation in the segment is fast and furious as providers rolled out cloud detection and response capabilities and prioritized support for multiple endpoint agents — in particular, Microsoft Defender, which every vendor mentioned. The use of other telemetry — sources beyond the endpoint to augment and add context to alerts — varied immensely by provider, and response actions were often limited to what the endpoint detection and response software the vendor supported. Client references wanted specific benefits from their MDR vendors: 1) better detection than the customer could achieve on their own; 2) rapid investigation to provide context as input into decision-making; and 3) expertise available to make faster, more accurate decisions on which response actions to choose.

Organizations evaluating MDR should look for providers that:

- **Deliver via squad models for vertical expertise and cultural fit.** Many MDR vendors offer the squad model for a customized delivery experience — a dedicated team of analysts, responders, and customer support specialists that work within a given vertical and geography. The strongest MDR vendors work with customers while building each squad to ensure the team members are the best fit for personality, team culture, and desired capabilities. Customers noted the importance of the customized squad approach and appreciated that they were able to swap out team members during the early stages to get the most out of their MDR provider.
- **Use detection as their superpower.** Clients sought MDR services for their ability to combine strong hunting methodologies with organic threat intelligence capabilities that take indicators from an active incident in one client and apply that to endpoints at scale. Finding potential intrusions quickly and coupling those findings with customized, prescriptive, action-oriented alerts is what makes buyers love their MDR service. The happiest MDR customers found vendors that could easily scale detection, customize alerts, and offer response actions intimately tailored to the client environment.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

- **Provide skilled practitioners, that are just as smart as (or smarter than) they are.** The MDR customers we spoke with were highly educated, seasoned, and had clear use cases for why they selected their MDR provider. They needed their MDR provider to sync with their security technology stack, specialize in specific types of detection and response activity, and act as a complement to the existing security team. When deciding on an MDR provider, prospective customers should create success criteria with this level of detail and select providers that can prove they match it.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our report "Now Tech: Managed Detection And Response Services Providers, Q4 2020."

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 Figure 1 and see Figure 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, Q1 2021

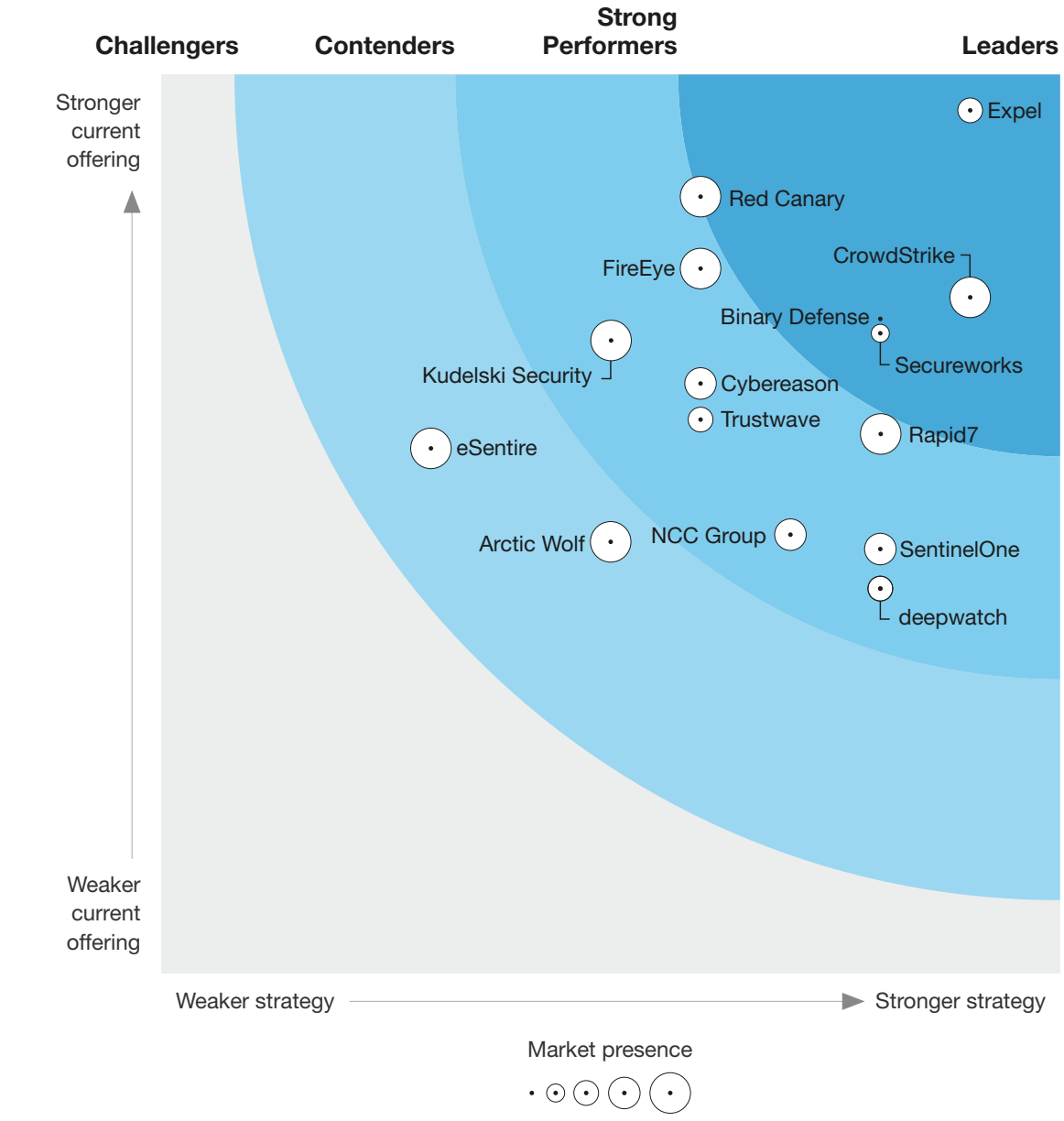

FIGURE 2 Forrester Wave™: Managed Detection And Response Scorecard, Q1 2021

	Forrester's weighting	Arctic Wolf	Binary Defense	CrowdStrike	Cybereason	deepwatch	eSentire	Expel	FireEye
Current offering	50%	2.40	3.64	3.76	3.28	2.14	2.92	4.80	3.92
Time-to-value	6%	3.00	3.00	5.00	3.00	3.00	3.00	5.00	3.00
Threat hunting	10%	3.00	5.00	5.00	5.00	1.00	3.00	5.00	5.00
Threat intelligence	6%	1.00	5.00	5.00	3.00	1.00	3.00	3.00	5.00
Collaboration	10%	3.00	3.00	3.00	3.00	3.00	1.00	5.00	3.00
User interface	6%	3.00	3.00	5.00	3.00	3.00	3.00	5.00	3.00
ML/AI	6%	3.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00
MITRE ATT&CK framework mapping and use	10%	3.00	5.00	5.00	5.00	0.00	3.00	5.00	5.00
Managed detection	12%	1.00	5.00	5.00	3.00	3.00	3.00	5.00	5.00
Managed response	12%	3.00	3.00	3.00	3.00	1.00	3.00	5.00	5.00
XDR collection, correlation, and APIs	6%	3.00	1.00	1.00	3.00	3.00	5.00	5.00	3.00
Automation and orchestration	6%	1.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00
System criticality	4%	3.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Metrics	6%	1.00	3.00	3.00	1.00	3.00	3.00	5.00	3.00
Strategy	50%	2.50	4.00	4.50	3.00	4.00	1.50	4.50	3.00
Performance	25%	5.00	3.00	5.00	3.00	5.00	1.00	5.00	5.00
Product vision	25%	1.00	5.00	5.00	3.00	3.00	1.00	3.00	1.00
Roadmap	25%	1.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00
Vision and milestones	25%	3.00	5.00	5.00	3.00	5.00	1.00	5.00	3.00
Market presence	0%	5.00	1.00	5.00	4.00	3.00	5.00	3.00	5.00
Product revenue	50%	5.00	1.00	5.00	3.00	3.00	5.00	3.00	5.00
Enterprise clients	50%	5.00	1.00	5.00	5.00	3.00	5.00	3.00	5.00

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

FIGURE 2 Forrester Wave™: Managed Detection And Response Scorecard, Q1 2021 (Cont.)

	Forrester's weighting	Kudelski Security	NCC Group	Rapid7	Red Canary	Secureworks	SentinelOne	Trustwave
Current offering	50%	3.52	2.44	3.00	4.32	3.56	2.36	3.08
Time-to-value	6%	5.00	1.00	3.00	3.00	5.00	3.00	1.00
Threat hunting	10%	3.00	3.00	5.00	5.00	3.00	1.00	3.00
Threat intelligence	6%	3.00	5.00	3.00	3.00	3.00	1.00	5.00
Collaboration	10%	5.00	3.00	3.00	5.00	5.00	1.00	5.00
User interface	6%	3.00	1.00	3.00	5.00	3.00	5.00	3.00
ML/AI	6%	3.00	5.00	3.00	3.00	3.00	5.00	3.00
MITRE ATT&CK framework mapping and use	10%	5.00	1.00	1.00	5.00	3.00	3.00	3.00
Managed detection	12%	3.00	3.00	3.00	5.00	3.00	3.00	1.00
Managed response	12%	3.00	1.00	3.00	5.00	5.00	1.00	3.00
XDR collection, correlation, and APIs	6%	3.00	3.00	3.00	3.00	3.00	1.00	5.00
Automation and orchestration	6%	3.00	1.00	3.00	5.00	3.00	3.00	3.00
System criticality	4%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Metrics	6%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Strategy	50%	2.50	3.50	4.00	3.00	4.00	4.00	3.00
Performance	25%	3.00	5.00	5.00	3.00	3.00	5.00	3.00
Product vision	25%	3.00	3.00	5.00	3.00	5.00	3.00	3.00
Roadmap	25%	3.00	3.00	3.00	3.00	5.00	5.00	3.00
Vision and milestones	25%	1.00	3.00	3.00	3.00	3.00	3.00	3.00
Market presence	0%	5.00	4.00	5.00	5.00	2.00	4.00	3.00
Product revenue	50%	5.00	5.00	5.00	5.00	3.00	3.00	3.00
Enterprise clients	50%	5.00	3.00	5.00	5.00	1.00	5.00	3.00

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

Vendor Offerings

Forrester included 15 vendors in this assessment: Arctic Wolf, Binary Defense, CrowdStrike, Cybereason, deepwatch, eSentire, Expel, FireEye, Kudelski Security, NCC Group, Rapid7, Red Canary, Secureworks, SentinelOne, and Trustwave.

Vendor Profiles

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

Leaders

- **Expel proves elite practitioners, strong platforms, and collaboration can coexist.** Expel's outstanding user interface proves that some security vendors understand user experience. The vendor provides a clean, easy-to-navigate user interface with compelling metrics but couples it with phenomenal practitioner expertise in service delivery. The company's blogs include topics ranging from cloud detection techniques to SOC metrics to employee burnout, transcending what most other security vendors share with clients. These blogs are available outside the paywall, proving Expel's dedication to better the security community. Transparency is omnipresent in Expel's service delivery to clients. Expel exhibits robust threat hunting methodologies, with a more sophisticated approach to detection via cloud API telemetry as compared to other providers in this assessment.

  Client references note the technical competence of Expel's personnel involved in MDR service delivery and product management as major areas of strength. Expel's references offered that sometimes remediation recommendations were a bit aggressive and that its capabilities came at a premium price compared to competitors. Security leaders looking for innovative startups with experienced founder teams, focused on MDR, and that take a collaborative and transparent approach to service delivery should put Expel at the top of their list.

- **CrowdStrike links its superlative incident response pedigree to its strong EDR tool.** CrowdStrike's financial performance and excellent attach rates of services to endpoint sales already make competitors jealous, but its clean, easy-to-navigate user interface should also cause them envy. CrowdStrike capitalizes on threat intelligence it gathers via incident response and the Falcon endpoint platform, embedding the organic threat intelligence captured from those sources throughout its approach to MDR service delivery and providing substantial value to clients. CrowdStrike's threat hunting capabilities also stand out, with hypothesis-driven, behavioral, analytic, and adversary-based threat hunts happening on a consistent basis. These are tailored and customized to clients' environments as needed.

  CrowdStrike client references highlight the speed with which the vendor responds to both detected security incidents and to support issues in general and the process-driven nature of investigations as major strengths. References indicated they could only get full administrative access to the Falcon endpoint agent by special request, and the integration process for other sources of

instrumentation was not as intuitive as it should be as weaknesses. Companies looking for a vendor that owns the intellectual property for a strong EDR tool, along with the capability to couple skilled practitioner-led MDR delivery MDR should put CrowdStrike on their shortlist.

- **Binary Defense exhibits its defense mission belief through its MDR service.** The vendor combines strong practitioner leadership, exceptional cybersecurity research, and a strong consulting sister company to bring a comprehensive MDR service to market. While most MDR vendors think like defenders, Binary Defense differentiates by starting with the attackers' perspective as the foundation for its MDR offering. Collaboration and partnership stand out as key elements behind its service delivery to ensure that security practitioners have what they need to detect, investigate, and respond to security incidents. Binary Defense's emphasis on cybersecurity research leads to sophisticated threat hunting capabilities.

  Client references mention rapid detection of innovative threat actor techniques and the skills of service delivery personnel when assisting clients as strengths. Weaknesses client references discussed include challenges with the general pricing structure and a noticeable drop-off between the skill of junior analysts versus more experienced personnel. Security buyers looking for a rapidly growing MDR-focused provider with a clear emphasis on security research and threat detection should evaluate Binary Defense.

- **Secureworks' MSS legacy helps, but its MDR platform is the real star.** Secureworks is one of the largest MSSPs, with a history spanning multiple decades. Swinging an old services vendor to a platform-centric approach to MDR via Red Cloak (now named Taegis Managed XDR) is no small feat, but Secureworks is making it happen. While the emphasis on the product and endpoint agent are there, Secureworks has not abandoned its flagship delivery personnel and Counter Threat Unit threat intelligence as part of its MDR service offering. Not surprisingly, its flexibility in managed response actions is a clear differentiator, proving its experience delivering MSS serves Secureworks well for MDR.

  Client references mentioned speed and quality of response support, along with rapid iteration and innovation on the MDR platform, as strengths. More integration with other security products and the need for more-configurable dynamic reporting were weaknesses noted by client references. Buyers with existing MSS relationships that want to begin the conversion to MDR, as well as those soured by the traditional MSSP delivery approach, should consider Secureworks' version of MDR as a fresh alternative.

- **Red Canary operates as a security ally for its clients.** Red Canary is one of the earliest MDR players. In spite of the vast number of newcomers that have entered the market, it remains a vendor that truly understands what its MDR clients need and want from a provider. The vendor offers outstanding integration and use of the MITRE ATT&CK framework, which are primary differentiators for Red Canary. The vendor provides comprehensive details and data so that clients can enhance their own detection engineering profile. Red Canary offers highly collaborative delivery

as part of its MDR service, along with a wide range of technical integrations to provide context for EDR-generated alerts. The vendor also allows clients flexibility with configurable ad hoc response actions through its portal or automated playbooks clients can customize as needed.

Red Canary client references mentioned well-vetted, high-quality detection alerts and a strong customer-centric approach to service delivery as major strengths. They named lightweight network, cloud, API integrations to add more context to detection events, and cost as weaknesses. Companies looking for an experienced, customer-focused MDR provider with vetted alerts and expert use of MITRE ATT&CK with a budget for a premium MDR service should research Red Canary's approach.

Strong Performers

- **Rapid7 emphasizes behavioral detection coupled with broad tech integrations.** Rapid7 expands insider threat detection into MDR. This makes sense, as most intrusions result in credential capture and reuse. However, MDR represents a growing set of MSS capabilities from Rapid7 as it continues its expansion security portfolio vendor. The vendor delivers a solid user interface that encompasses the range of services delivered for clients, although the high-touch nature of the service means that clients aren't required to use it. Security professionals with extensive incident response and threat hunting experience head up the MDR offering, thereby instilling those philosophies into the service. Rapid7's security research and consulting legacy also adds substantial value to its MDR offering.

  Rapid7's client references mention the context and value across multiple services and partnerships as strengths. References noted that the speed of growth is obvious and has led to some service challenges. They also expressed a desire for Rapid7 to do a better job of announcing and communicating feature enhancements. Security leaders looking for a white-glove, behavioral detection-inspired approach to MDR should consider Rapid7.

- **FireEye steps outside of its own product ecosystem in its MDR service.** Mandiant Managed Defense — and its various iterations — is considered one of the first, if not the first, iterations of MDR that existed. That legacy remains in the service and for good reason. FireEye's MDR offering is one aimed at more sophisticated practitioners, with mature investigative methodologies and strong threat hunting capabilities as one would expect given the company's reputation for incident response. FireEye's MDR service does not require client sophistication in order to receive benefits, but more-mature clients and more-skilled practitioners with IR and threat intelligence experience will definitely maximize the value inherent in it.

  FireEye client references mentioned the in-depth research provided in alerts and the ability to quickly pivot to and engage IR personnel in the event of a serious incident as strengths. References noted that the service feels highly fragmented, with five different services delivered by five different platforms, and until the announcements expanding device support to include non-FireEye

technology in mid-2020, restrictions to an all FireEye technology ecosystem are a severe limitation. Mature security teams and those with heavy investments in the FireEye ecosystem should think about the vendor for MDR services.

- **Cybereason centers its MDR service on its deep threat hunting expertise.** Cybereason has long made malicious operations, "malops," in its terms, a core part of its messaging and approach to service delivery. This emphasis is reflected in its strong threat hunting capability along with its outstanding service delivery personnel. Extensive use of the MITRE ATT&CK framework throughout the entirety of its service allows clients to understand incidents and events in a common, relevant external framework. This helps clients improve their approach to detection engineering in their security programs. On the downside, Cybereason provides limited metrics for clients, and its user interface is not as impressive as other vendors in this evaluation.

  Strengths client references mention include standout endpoint visibility and ability to detect intruder activity. References, however, cited support for cloud detection use cases and needed improvements to the UX as weaknesses Cybereason needs to address. Security buyers that want a company with strong cybersecurity practitioners, deep threat hunting expertise, and high endpoint visibility in a toolset the vendor controls should connect with Cybereason.

- **SentinelOne allows its user interface to attract clients, but service tiers hook them.** While a tiered approach can sometimes lead to complexity for buyers, SentinelOne does a good job of articulating what is available in each tier, which contrasts with other vendors that are using a more one-size-fits-all model. SentinelOne touts an impressive user interface as one of its key differentiators for its EDR product. Fortunately for the vendor, this remains true for its MDR service as well. The vendor's comprehensive and detailed explanation of how analytics and machine learning were applied to the service to improve managed detection capabilities is an added bonus for clients.

  According to client references, SentinelOne's service delivery strengths include strong detection and clear annotations and explanations of detections in ways that are easy for users to comprehend. Reference customers noted a lack of transparency for the work effort and activities performed by SentinelOne as a weakness. They also stated that better support for enterprise ticketing and case management solutions is needed. Companies looking for strong managed detection and flexible service tiers to satisfy budget concerns should take a long look at what SentinelOne brings to market.

- **Deepwatch features Splunk heavily in its MDR approach as it expands.** Deepwatch is a relatively new cybersecurity vendor. That newness requires the vendor to play catch-up, but it hasn't shackled the company's plans. Substantial growth in its client base plus quick iteration on its platform and services with an impressive release cadence have elevated deepwatch as a vendor in the cybersecurity space. As a startup emerging from an integrator of SIEM technologies, a reliance on Managed Splunk for the core of its MDR service is not surprising, but a solid roadmap of release

plans and service expansions indicate that will change in the future. As a relatively new vendor, deepwatch lags behind other providers in its ability to generate organic threat intelligence and its incident response experience.

Client references listed its service delivery personnel's ability to communicate and explain alerts and incidents and deepwatch's proactive eyes on where the cybersecurity market is headed in its strategy as strengths. References mention that threat hunting, executive dashboards, and reporting need to mature. Organizations looking for vendors that can couple managed SIEM with MDR should consider deepwatch.

- **Trustwave blends its MSS legacy and SpiderLabs expertise as it turns to MDR.** Rapid geographic expansion and well-timed internal platform investments demonstrate Trustwave's capabilities as an MDR vendor. Threat intelligence and security research led by SpiderLabs, and a strong spirit of collaboration that started in its MSS practice, make Trustwave's MDR compelling as a service offering. Expanded platform capabilities and better support for cloud infrastructure and APIs help Trustwave obtain extensive visibility beyond EDR tools, providing valuable context in the execution of detection and response workflow for clients.

  Client references note the vendor's global delivery footprint and a portfolio that includes MDR and MSS services from a single provider as strengths. Trustwave's weaknesses include the slow and challenging speed of client onboarding and the lack of clarity and enrichment of alerts. Security teams requiring a blended offering of MSS and MDR services, as well as multinational companies that want expanded global service delivery capabilities, should add Trustwave to their vendor mix.

- **Kudelski Security customizes its MDR approach based on what clients want.** Kudelski Security has a background as a high-touch MSSP. The customized approach used in its MSS delivery is echoed in the design of its MDR service. This allows Kudelski Security to tailor its service to clients. The vendor can optionally act as the entirety of the clients' detection and response team or engage as a first responder for security incidents before handing them off and collaborating with client teams. Kudelski Security's degree of personalization differentiates it from other vendors in this evaluation. Clients benefit from this approach, as they can onboard rapidly then customize the service as they go when necessary. Kudelski Security's extensive collaboration capability helps clients understand and resolve incidents more effectively. The downside to this approach is that Kudelski Security is behind other vendors in its use of automation, and the client experience can be inconsistent.

  Client references indicate their robust trust in the Kudelski Security teams working with them, as well as the overall cybersecurity knowledge of the practitioners they work with, as strengths of the service. They also said, however, that the Kudelski Security teams could be too technical at times and that response documentation needed improvements. Security leaders needing a high-touch, customized version of MDR and a vendor that blends MSS and MDR together seamlessly should engage with Kudelski Security.

- **NCC Group approaches MDR with an attacker's mindset.** Thinking like an attacker is a valuable skillset for defenders, which NCC Group injects into its MDR offering in a unique way. It combines this approach with threat intelligence, native offensive and defensive security research, and its 2015 acquisition of Fox-IT, which all allow NCC Group to meaningfully deliver MDR. The vendor provides rich, detailed explanations of how it applies its offensive and defensive security research combined with its threat intelligence to advance detection efforts through analytics and machine learning. Its use of the MITRE ATT&CK framework in its presales process also stands out as a positive. NCC Group's user interface falls short of other vendors in this evaluation, and it needs to use MITRE ATT&CK more consistently throughout its MDR service.

  Reference customers cited the high quality of MDR service delivery personnel and awareness of adversary tools, techniques, and procedures (TTPs) as strengths. Client references stated that implementation and onboarding challenges, along with less-than-adequate reporting and user interface issues, as areas that need improvement. Security leaders seeking an international MDR vendor with a rich history in cybersecurity that understands attackers' techniques should evaluate NCC Group for fit.

Contenders

- **Arctic Wolf mixes its as-a-service platform with white-glove MDR service.** Arctic Wolf has sustained strong growth and demonstrates a clear understanding of how to build a platform for MSS delivery. The vendor has now pivoted toward MDR with a focus on high-touch client interaction. Arctic Wolf's history as an MSSP also helps it offer a broad set of services and intake data to provide context for MDR-based alerts. Its organic generation of threat intelligence, threat hunting, and investigative methodologies falls behind other vendors in this evaluation. However, given Arctic Wolf's history and trajectory, those shortcomings are symptoms of it being a rapidly growing vendor and will likely be overcome.

  Client references for Arctic Wolf indicate rapid addition of features to its platform and customer service and support as areas of strength. Reference customers mention growing pains and low process maturity leading to inconsistency in service delivery as weaknesses. Security buyers looking for a high-touch, innovative MDR provider willing to tolerate the occasional delivery hiccup that comes with innovation should factor in Arctic Wolf as a serious option.

- **eSentire investors provided substantial funding to drive its MDR execution.** eSentire has a long history as an MSSP but now focuses on its MDR service as the crown jewel of its service delivery. Machine learning and artificial intelligence help fuel managed detection, and frontline detection and response consultants aren't the only personnel available 24/7. IR consultants are also available on-demand 24/7, so clients can call if they need additional expertise to handle incidents or provide guidance on response choices. eSentire has received substantial funding from investors in recent years, using that investment to build out its leadership and service delivery teams to continue its expansion into MDR with positive results. The vendor's primary challenge is that the MDR market is rife with innovation and well-funded competitors, which does limit the advantage this confers.

Client references rave about eSentire's client support and its ability to educate security practitioners during incident investigation as strengths. Reference customers stated that communications regarding service and platform improvements need to improve. They also commented that the vendor needs better integration with expanded MDR use cases for cloud environments. Security leaders looking for a mature service delivery organization with excellent client support for MDR should get to know eSentire.

Evaluation Overview

We evaluated vendors against 19 criteria, which we grouped 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 intel, collaboration, user interface, ML/AI, MITRE ATT&CK framework mapping and use, managed detection, managed response, XDR collection, correlation, APIs, automation and orchestration, system criticality, and metrics.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated performance, product vision, roadmap, and vision and milestones.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's service revenue and enterprise clients (with 1,000+ employees).

Vendor Inclusion Criteria

Forrester included 15 vendors in the assessment: Arctic Wolf, Binary Defense, CrowdStrike, Cybereason, deepwatch, eSentire, Expel, FireEye, Kudelski Security, NCC Group, Rapid7, Red Canary, Secureworks, SentinelOne, and Trustwave. Each of these vendors has:

- **Significant interest from Forrester customers.** To select the most relevant vendors to evaluate, Forrester also considered the level of interest from our clients based on inquiries, advisories, consulting engagements, and other interactions.
- **Offered MDR service since at least 2017.** We included vendors that demonstrated a multiyear commitment to offering MDR services.
- **Had at least 70 clients, 75,000 endpoints, and $15 million in revenue in MDR.** These vendors demonstrated clear MDR revenue. We eliminated vendors attempting to convert or represent software licensing transitions to as-a-service models, managed security service providers converting to clients to MDR, and others rebranding to MDR. All vendors included proved specific, dedicated MDR revenue as a service line.
- **Leveraged an EDR tool that participated in a prior MITRE ATT&CK evaluation.** It did not matter if a vendor supported commonly deployed EDR tools or used its own IP, as long as the vendor actively supported an EDR tool with results in a MITRE ATT&CK evaluation prior to the invite window.

- **Supported multiple nonproprietary sources of non-EDR telemetry.** Extended detection and response (XDR) has always been a required feature of an MDR offering, going back to our earliest MDR research in 2016 and 2017. Therefore, providers have included support XDR as a component of MDR and do not require proprietary tools and licenses to do so.
- **Provided detailed descriptions of threat hunting methodologies.** Unfortunately, most MDR service providers mistake threat hunting for standard detection or analytics. The vendors included in the assessment provided detailed explanations of their threat hunting methodologies that did not conflate hunting with standard detection or analytics.

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 Guide 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 December 14, 2020 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 The Forrester Wave™ and New Wave™ 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 The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor 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.

We help business and technology leaders use customer obsession to accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.