Managed Detection and Response

Selective Outsourcing for Understaffed SOCs and the Platforms That Enable MDR Services

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
Research Report

By Paula Musich
May 2020

SPONSORED BY:

Secureworks®

EMA™

Table of Contents

A TINY MARKET WITH BIG POTENTIAL

The MDR market has only been in existence for about four years. Market penetration at this point in its lifecycle is still quite small, with some estimates suggesting it at less than 10%.[1] However, interest in MDR services is strong, and it has fueled a gold rush of sorts by service providers of different stripes looking to get a foothold before demand takes off. EMA sought to measure that interest among those not already using an MDR service. Respondents validated the strength of that interest. For the roughly three-quarters of all respondents not already using an MDR service, only 6% indicated that their organizations were not looking into it. At 46%, just under half of all those not using an MDR service said their organizations were currently evaluating an MDR service. Another 33% said their organizations were considering adopting an MDR service, and another 15% indicated that their organizations planned to evaluate MDR services in the next 12 to 18 months.

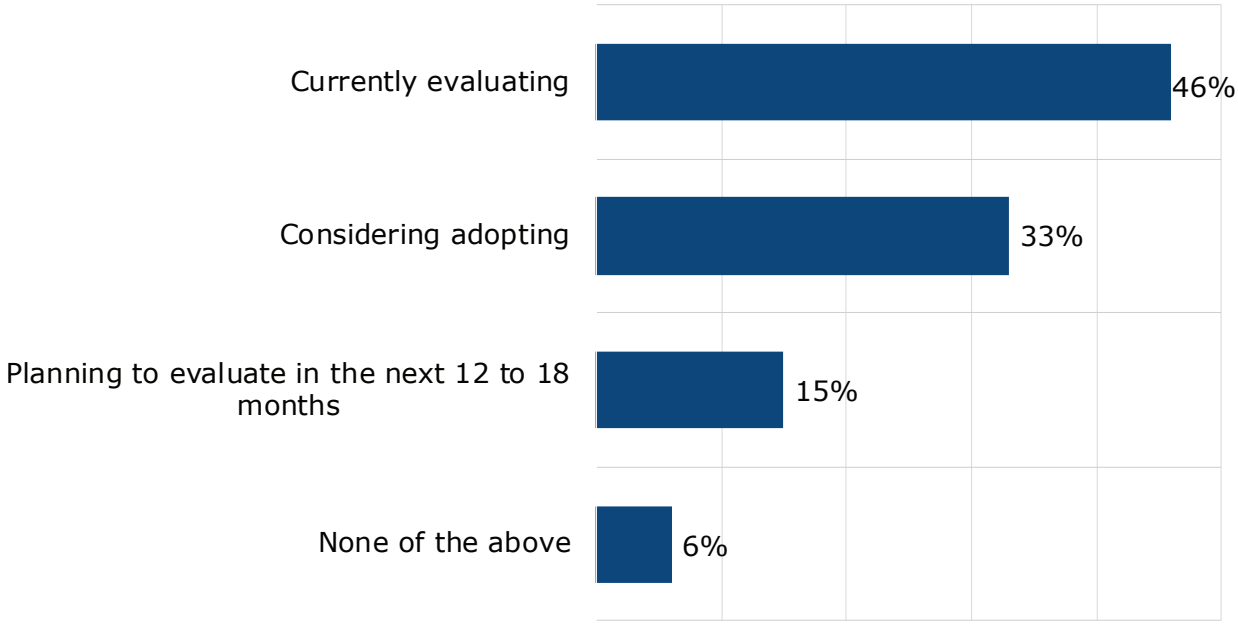


Figure 1: Is your organization currently evaluating an MDR service, considering adopting an MDR service, or planning to evaluate an MDR service in the next 12 to 18 months?

To put a finer point on it, the research attempted to dive deeper into that market interest. Near-term, the strongest interest in MDR services is driven primarily by midmarket organizations, with 67% reporting that their organizations are currently evaluating MDR services. Among SMEs, 43% of their organizations are currently evaluating MDR services and another 40% are considering adopting an MDR service. Of particular note is the fact that among those organizations interested in MDR services, the lion's share are actively looking to adopt such services in the near term, rather than 12 to 18 months from now. It's clear from the research that the need for such services is imminent, which suggests that providers should be actively educating the market on their unique advantages—especially those that benefit smaller organizations. These organizations tend to make acquisition decisions much faster than large enterprises, which should give marketers a sense of urgency.

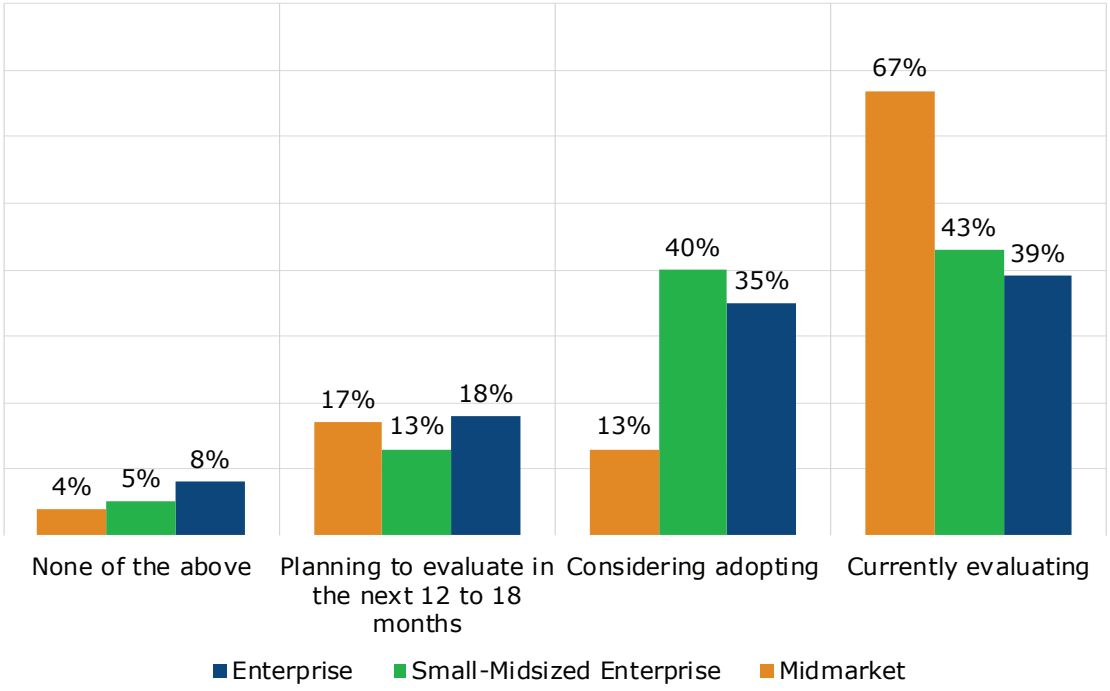
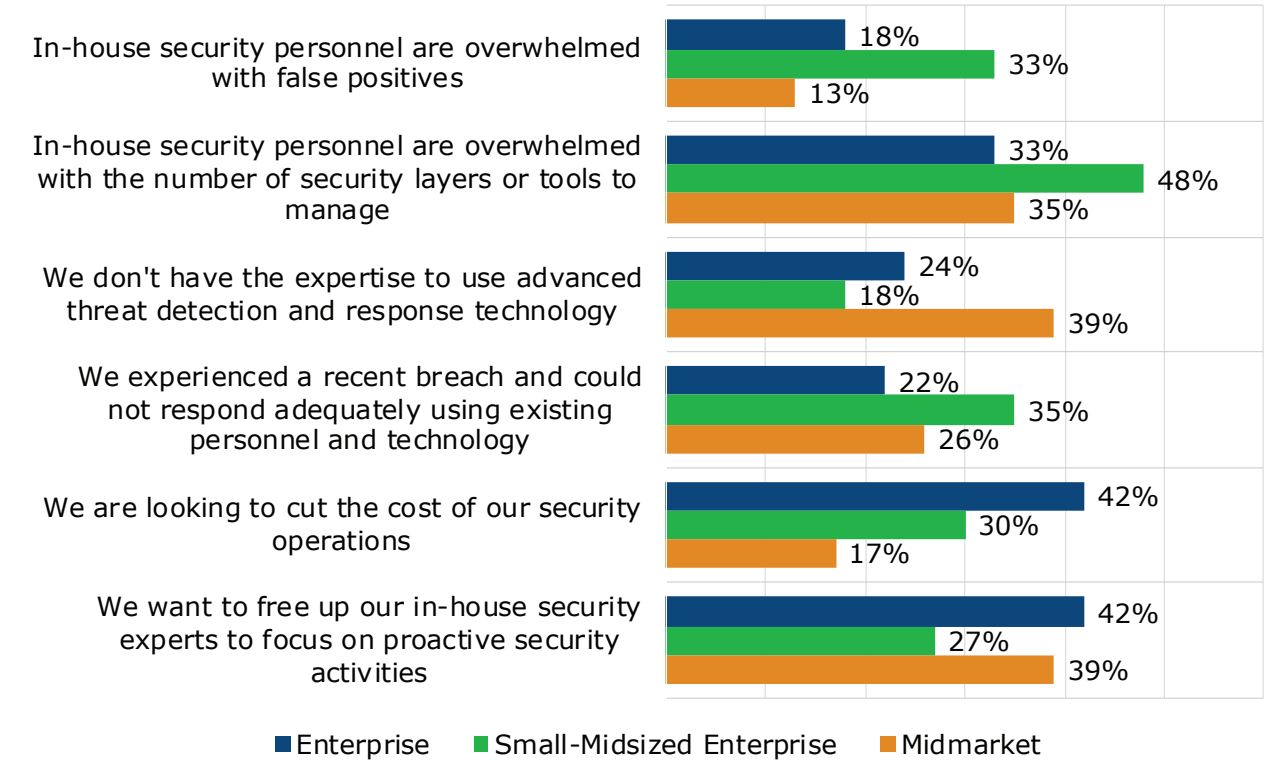


Figure 2: Midmarket demonstrates the strongest interest in MDR service adoption

What's Driving Interest in MDR Adoption?

Behind this strong interest in adding MDR services to their information security arsenals, respondents indicated a variety of reasons spurring their interest. Beyond the top-level issue of addressing the IT security skills gap are several drivers. Among all respondents interested in MDR services, the top drivers include the fact that their in-house security personnel are overwhelmed with the number of security layers or tools to manage at 41%, organizations want to free up in-house security experts to focus on proactive security activities at 34%, others are looking to cut the cost of security operations at 32%, and 29% experienced a recent breach and could not respond adequately using existing personnel and technology. Interestingly, on the other end of the spectrum of drivers, only 11% of respondents said their organizations had no skilled threat hunters on staff. However, priorities fueling this interest vary once again by company size. It's no surprise that the largest percentage of midmarket companies don't have the expertise to use advanced threat detection and response technology at 39%. At the same time, 39% of those same midmarket companies also want to free up their in-house experts to focus on more proactive security activities. Clearly, these organizations are ready to move beyond firefighting mode and into more strategic use of a precious resource. For nearly half of SMEs looking into MDR services, their in-house security personnel are overwhelmed with the number of security layers or tools they have to manage, while another 35% experienced a recent breach and could not respond adequately with existing resources. Behind the interest in reducing the cost of security operations are large enterprises, which suggests that the spending pendulum that has spurred the multi-year growth in security budgets is now starting to swing back in the other direction. It's likely those organizations believe they are not getting the full return on their investments in security tools and are looking to optimize and improve the efficiency of their security operations. Forty-two percent of respondents representing large enterprises indicated cost cutting as a top driver, along with another 42% that expressed a desire to free in-house experts to work on more strategic security tasks.



Top 3 most frequently selected responses out of 11 possible responses

Figure 3: What are the primary reasons your organization is evaluating, considering adopting, or planning to evaluate an MDR service in the next 12 to 18 months?

In looking at the top vertical industries represented in the sample, interest in adding MDR services to their security operations is very near-term. Those industries include manufacturing, finance/banking/insurance, healthcare/medical/pharmaceutical, high technology software, and retail/wholesale for consumer goods. The strongest near-term interest came from healthcare, with 58% of respondents reporting that their organizations were currently evaluating an MDR service, followed by manufacturing at 52%. Both of these verticals are not typically in the vanguard of new technology adoption, but at the same time are increasingly relying on IoT devices to advance their own digital transformation initiatives. They likely see the increasing threat posed by this larger attack surface and wish to shore up their defenses as quickly as possible by outsourcing threat detection and response capabilities. One other vertical—financial services—indicated strong near-term interest in MDR services, with half of those respondents that were interested in MDR services indicating their organizations were currently evaluating an MDR service. It's also interesting to note that while high technology software and retail respondents demonstrated their organizations were not as far along in their adoption journey, their interest seems to be extended across a longer timeframe.

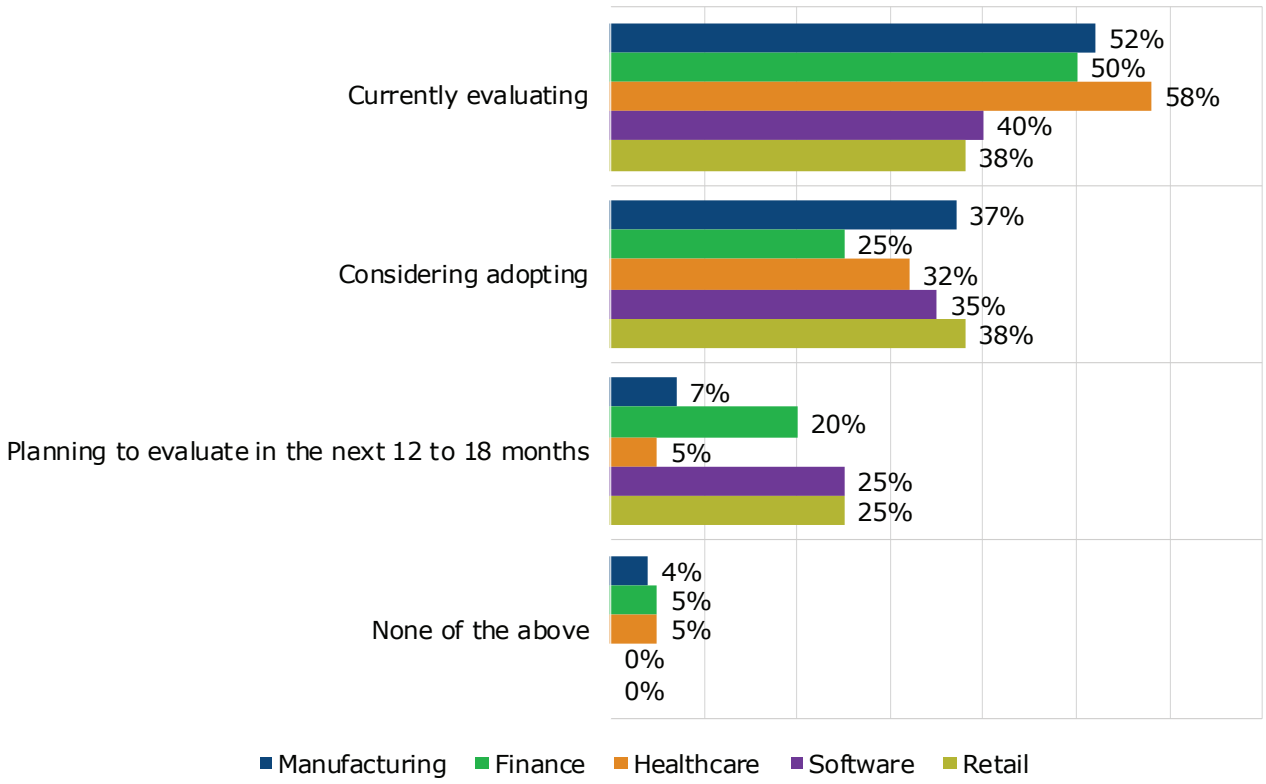


Figure 4: Vertical industry interest in MDR adoption

Service Type, Interest, and Approach

Those interested in adopting MDR services have a couple of choices in the types of services they can adopt. Although managed endpoint detection and response (EDR) comes to mind most often when thinking about MDR services, other options exist. Prospects can also elect to procure a managed SIEM service or a combination of both managed EDR and SIEM. In truth, for such services to effectively provide high fidelity threat detection and rapid response, they must rely on a combination of technologies most often customized and integrated by the service provider to optimize efficiency in threat hunting, analysis, and response once a suspected threat is validated. While pure-play MDR providers may rely on their own collection of integrated tools to deliver their service, others with an MSSP orientation may rely instead on a specific one of the customer's existing security tools.

Among respondents looking into acquiring MDR services, EMA first sought to gauge interest in the broad categories of service available in the market. Were their organizations most interested in a managed EDR service, a managed SIEM service, or both? Across the three different organization sizes represented in the survey sample, the resounding answer for all three is *both*. Seventy percent of midmarket respondents indicated both, while 65% of SMEs said the same and 49% of large enterprise respondents indicated both. However, it does make sense that large enterprises are also interested in one or the other, with 31% of those expressing interest in just a managed SIEM service and 33% indicating interest in just a managed EDR service. These organizations are more likely to selectively outsource specific functions because of existing holes in their internal coverage.

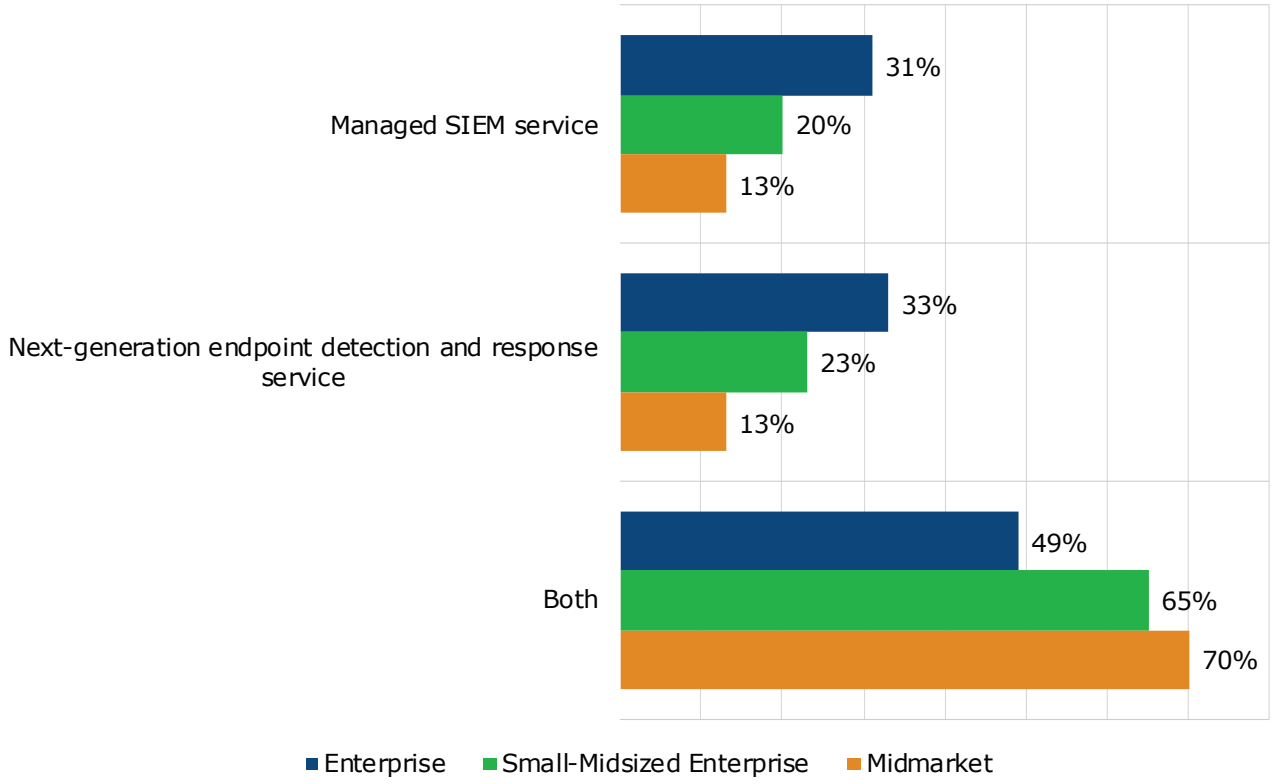


Figure 5: Level of interest in different types of MDR services varies by company size

For existing internal security operations, it's not unusual for organizations to rely on multiple endpoint protection tools. This defense-in-depth approach to securing endpoints was only bolstered by the failure of legacy AV tools to stop more advanced threats, which gave rise to the addition of EDR tools intended to find and eliminate the threats that bypassed the legacy AV defenses. As organizations consider outsourcing their threat detection and response capabilities, do they intend to continue the practice of using multiple next-generation EDR/EPP tools, or standardize on a single tool? According to respondents, the answer depends in part on the size of the organization. A strong majority of SMEs and slightly smaller majority of enterprises intend to continue the practice of using multiple EPP/ERD tools at 77% and 65%, respectively. Smaller midmarket respondents appeared to be more evenly split on that decision, with 53% indicating a desire to standardize on a single tool, while another 47% intend to use multiple tools. The adoption of secondary EDR tools that back up an existing EPP defenses among small to medium-sized businesses was fairly scant, given the expertise needed to use EDR tools. This is likely reflected in the larger percentage of midmarket respondents that wish to standardize on a single EDR/EPP tool.

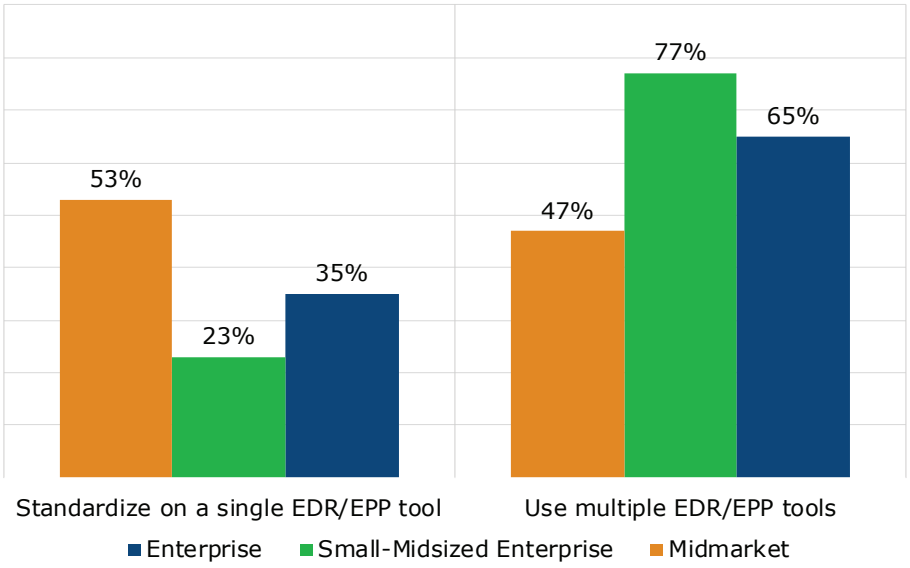


Figure 6: Does your organization intend to use multiple EDR/EPP tools in your potential MDR services engagement, or will your organization standardize on a single EDR/EPP tool?

EARLY CUSTOMER EXPERIENCE WITH MDR SERVICES

Early adopters of any new technology solution benefit from the innovation but struggle with the lack of extensive field experience in using newly minted solutions. Still, with MDR, many solution providers tout strong renewal rates among those early customers. In the earliest days of the market, as organizations sought to introduce MDR services into their security operations programs, what were their priorities in finding the right fit with a potential MDR solution provider? Given the new market and its growing field of competitors, which MDR services providers were these new prospects familiar with and learning about? What functions did early prospects want to offload to the MDR provider's experts?

Selecting an MDR Provider

As enterprises of different sizes and industries journey through their digital transformations and continue to move more and more workloads to the cloud to gain greater flexibility, lower cost, and improved time to market, their security leaders recognize the need to defend an increasingly dispersed attack surface. At the same time, new and unfamiliar environments, such as public clouds, industrial control systems, smart devices of various stripes, and more, challenge these leaders to learn new ways to defend their organization's digital assets. As would-be MDR services consumers seek to outsource detection and response capabilities against this backdrop, how important was it that their potential MDR providers would be up to the challenge of protecting these environments? Respondents whose organizations were already using an MDR service were asked to rate the importance of these issues in their selection criteria. Specifically, they were asked on a five-point scale (very important to not at all important) to rate the importance of having expertise in the vertical markets their firms represented, the importance of coverage for cloud-based workloads and applications, and the importance of (at the very least) having a plan to provide coverage for industrial IoT or other IoT devices. All three of these factors were rated very important in selecting their MDR provider by a healthy majority of respondents using MDR services. In addition, 44% of MDR users reported that it was very important that their chosen MDR services provider could integrate easily with their existing security infrastructure.

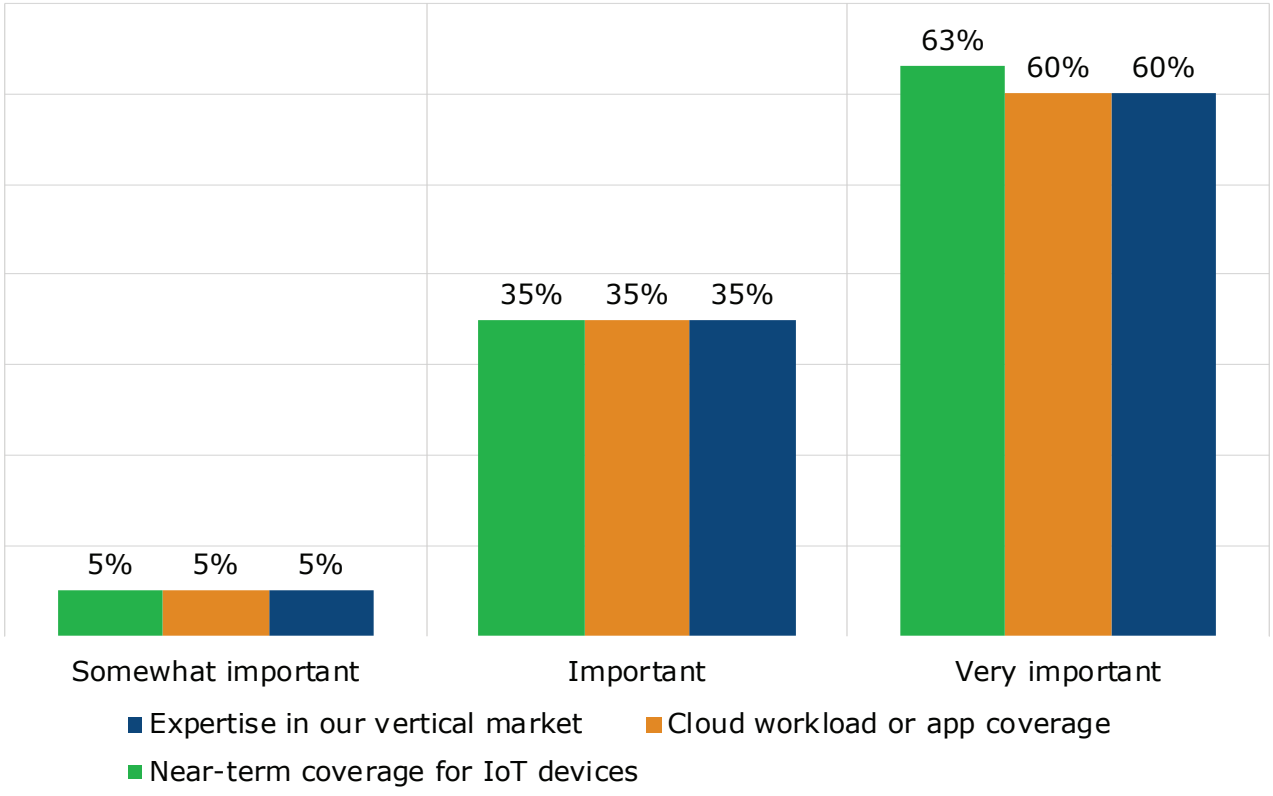


Figure 7: Key criteria in MDR provider selection

As part of their mission to provide faster and higher fidelity threat detection and response on behalf of their clients, MDR providers carry out a variety of tasks. Those can include network monitoring and threat analytics; endpoint monitoring to detect, analyze, and respond to suspicious activity; forensics; active threat investigation; and incident management and response. However, in which of these activities do MDR users find the greatest value? Put another way, what activities do MDR providers carry out that customers can't do well enough for themselves? The answer more often depends on the size of the organization. For large enterprises tasked with securing a large population of endpoints, many of which are likely to be mobile, the overwhelming answer is endpoint detection and response. Seventy-five percent of respondents using MDR solutions selected that option. Over half of those organizations expect their MDR provider to manage the health and reporting status of endpoint sensors, while a slightly smaller percentage expect their MDR provider to install EDR/EPP sensors on the customer's behalf. For SMEs, however, just over half indicated that they valued their MDR provider's ability to perform network analytics. Conversely, none of the SME respondents using MDR services indicated that they valued incident response activities, which was the same percentage given by large enterprises. These larger organizations most likely invested time and effort into developing and maturing their own IR capabilities after multiple waves of attacks and saw no need to put further resources into it. For midmarket MDR users, 17% indicated that they put a high value on IR activities, although the highest percentage of those users indicated that network threat analytics offered the greatest-value activity for their requirements.

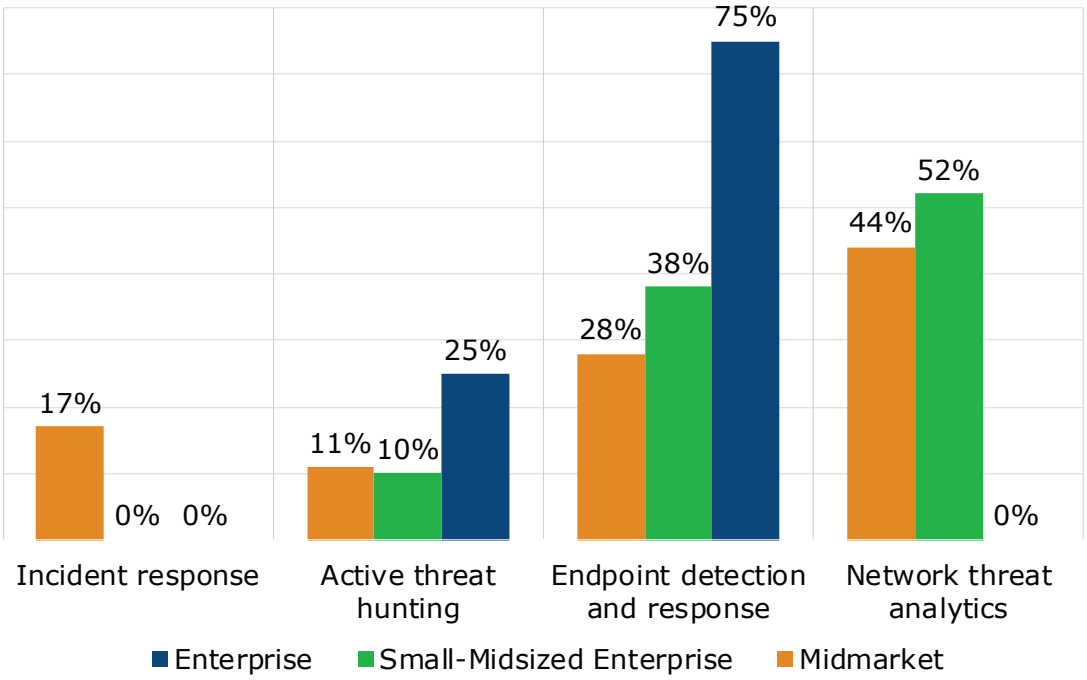


Figure 8: Of the following capabilities most often associated with MDR service providers, which does your organization see as offering the greatest value? by How many employees are in your company worldwide?

One other important note about selecting an MDR provider: The underlying tools and platform used by MDR providers are critical components of the overall service. Many providers often start with open-source security tools and create significant integrations and customization for their own use cases. Multi-tenancy is a must for scalability and privacy, and automation is key in enabling faster detection and response. MDR users understand this and place great weight on these platforms as part of their MDR provider selection criteria.

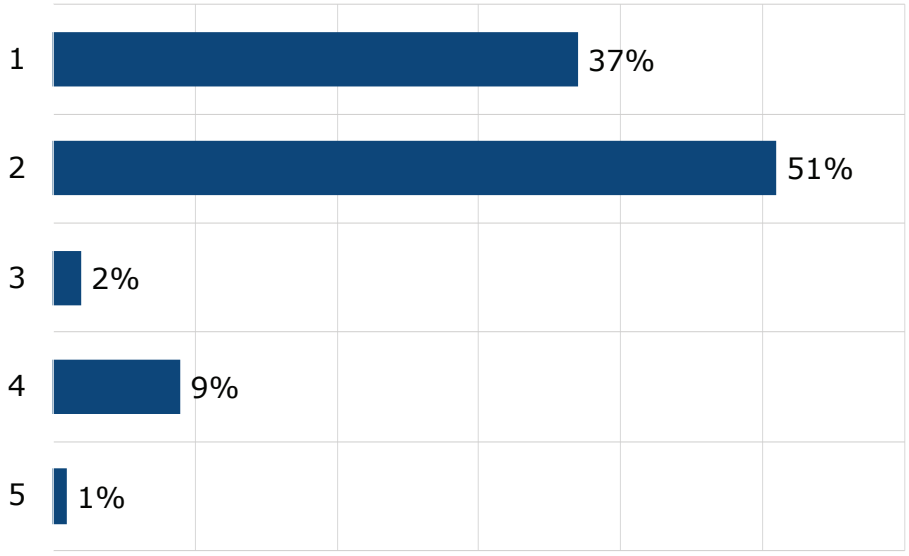


Figure 9: On a scale of 1 to 5, with 1 being most important and 5 being least important, please rate the importance of your MDR provider's underlying tools and technologies in your selection process.

GETTING RESULTS, PROVING VALUE

Whatever the cost concerns some organizations have around contracting with MDR services providers, there is no doubt that users are seeing results in the drive to more quickly discover and vanquish advanced threats already operating within organizations' networks and infrastructure. MDR user respondents indicated that as a result of their MDR providers' efforts, they have significantly reduced mean time to resolution (MTTR) of attacks. For the largest percentage of MDR users (35%), that reduction was between 25% and 49%. Only 5% of MDR users reported an MTTR reduction of less than 10%.

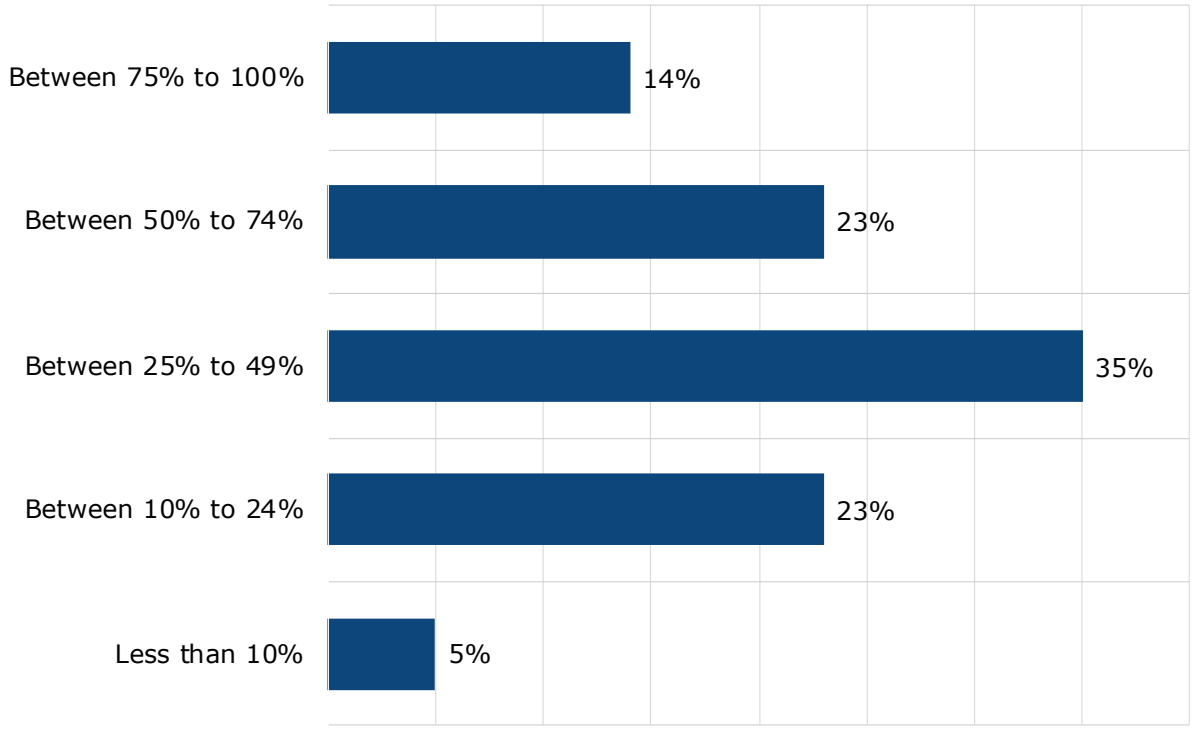


Figure 10: Since your MDR provider began monitoring your organization's network, how much, if at all, have they reduced the mean time to resolution of attacks?

How long it takes MDR providers to respond once a threat has been confirmed may play a role in those MTTR reduction numbers. For all MDR users, the largest percentage reported that their MDR providers typically respond within 16 to 30 minutes at 53%, with another 30% reporting typical response times of 31 to 45 minutes. However, for large enterprises, typical response times for the majority of those organizations are less than 15 minutes. Seventy-five percent of those respondents indicated that quick turnaround. For 67% of midsized organizations and 48% of SMEs, the typical response time was 16 to 30 minutes. It's possible that large enterprises see a faster MTTR because they contract for a full array of capabilities offered by their MDR providers. If true, this suggests that midmarket and SME customers are not getting the full benefit of MDR services by limiting what they contract for.

MDR providers typically report good satisfaction levels with their service, as measured by customer turnover. EMA sought to understand what satisfaction levels were among MDR user respondents across several measures, including overall service level, level of expertise applied to the customer's environment, overall availability of the provider's professionals, and the level of context provided in threat reports. Respondents across the board expressed very high levels of satisfaction. Over half of MDR respondents said their organizations were extremely satisfied with their overall service level and level of expertise available from their providers. Just under half said they were extremely satisfied with the availability of their provider's professionals and the level of context provided in periodic threat report.

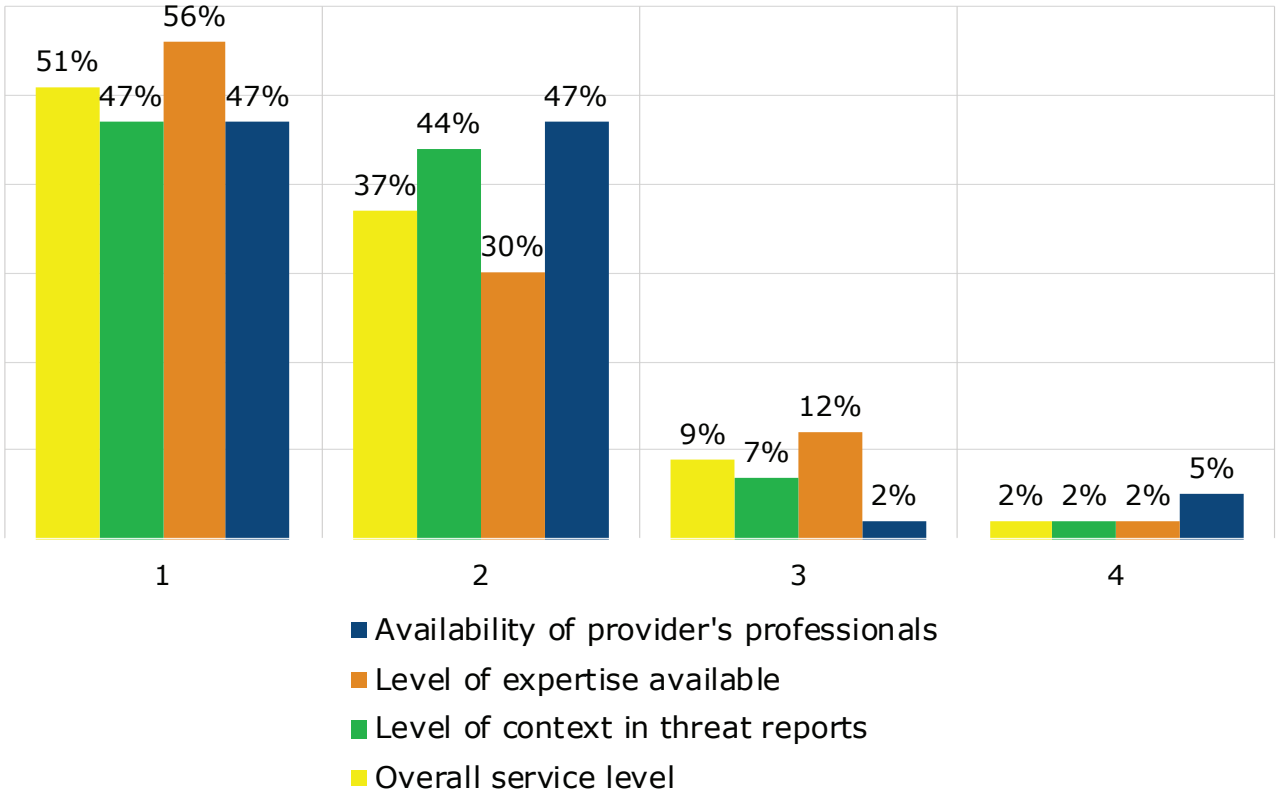


Figure 11: On a scale from 1 to 5, with 1 being extremely satisfied and 5 being not at all satisfied, how satisfied is your organization with…

Given the relatively high satisfaction levels expressed across the board by MDR users, it's likely that they would opt to offload additional tasks to their MDR providers that they view as less strategic, or seek to add capabilities they view as missing in their security operations. The research sought to assess what additional capabilities MDR users would like to procure from their providers that are not currently available to them. The top options selected include penetration and risk assessment at 17% each, followed by automation playbook recommendations, risk reporting, and vulnerability remediation/management at 16% each. Out of seven possible choices, only 4% of MDR users selected none of the above. Clearly, there are additional opportunities for MDR providers to expand their portfolio of services and share of customer wallet.

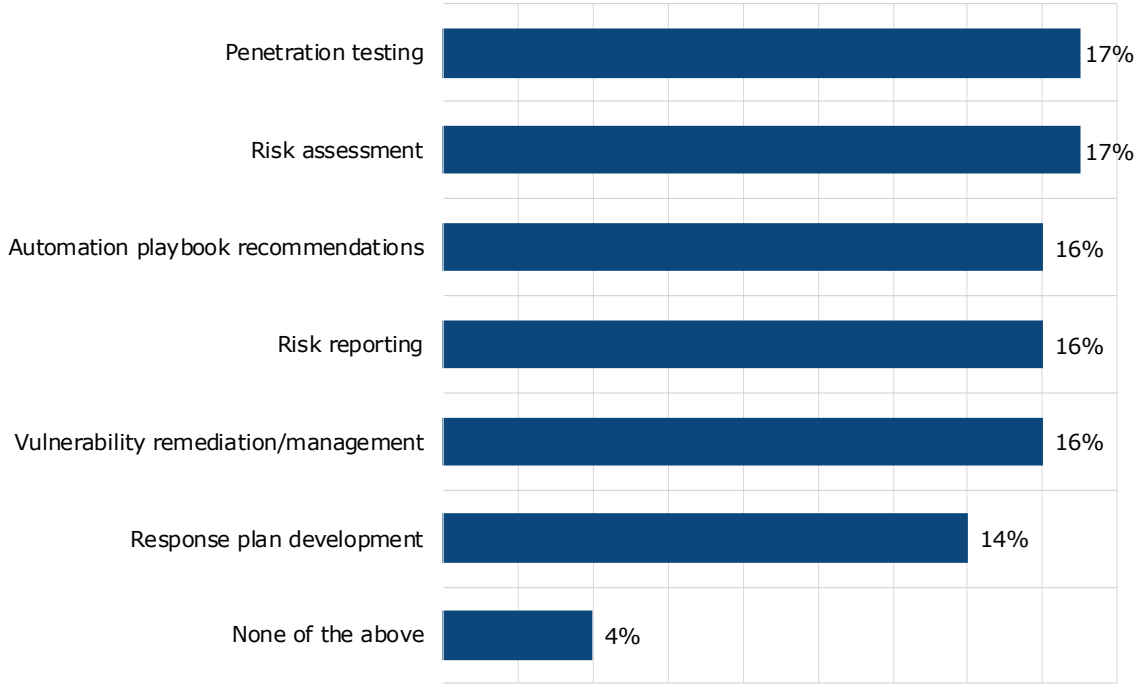


Figure 12: Which of the following services, if any, would you like to receive from your MDR provider that they don't currently offer?

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

3961.04082020