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
April 2020

SPONSORED BY:

IBM Security

red canary

Secureworks

EMA™

Table of Contents

EXECUTIVE SUMMARY

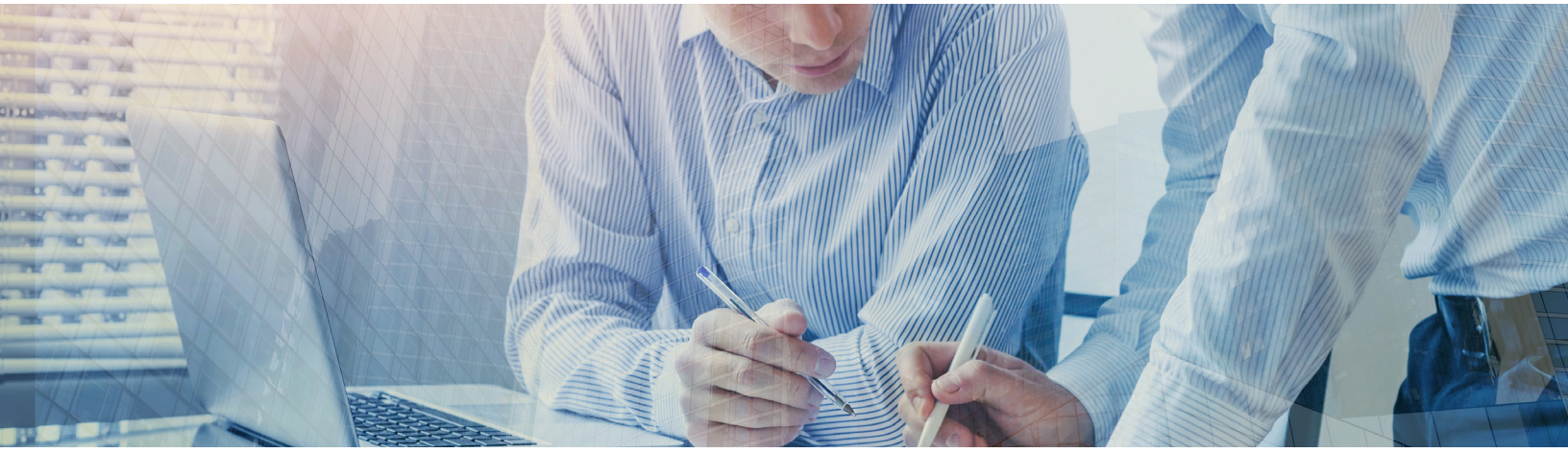
Although small now, the market for managed threat detection and response services commands great interest. Organizations of different sizes actively investigate adding such services to either offload that function from overburdened in-house staff or fill in gaps that exist in their current information security operations. In EMA's research, those not already using an MDR service overwhelmingly indicated that they are actively looking into it or plan to do so in the next 12 to 18 months. Only 6% of those not using an MDR service were not looking into it.

For large enterprises, MDR providers offer the opportunity to augment existing security operations outside of normal business hours. For smaller organizations, those service providers most often completely outsource the threat detection and response function. However, several issues drive interest in MDR services. Those issues include the fact that in-house security personnel are overwhelmed with the number of security layers or tools they have to manage and organizations want to free up in-house security experts to focus on proactive security activities, as reported respectively by 41% and 34% of those looking into MDR services.

Of the different activities MDR providers carry out on behalf of their clients, the ones the customers value the most will often depend on the size of the organization. Large enterprises, for the most part, see the greatest value in endpoint detection and response activities. Meanwhile, small to medium sized enterprises (with between 1,000 and 5,000 employees) greatly value their MDR providers' network analytics capabilities.

When it comes to making full use of their MDR providers' services, large enterprises typically sign up for the whole enchilada, while smaller organizations more often opt for less. For 33% of MDR user respondents representing midmarket organizations (with 500 to 1,000 employees), detection-only services are the option they choose. This may account for the difference in response times reported by respondents at differently sized organizations. Seventy-five percent of large enterprise MDR users report response times to security incidents of under 15 minutes, while 67% of SMEs report response times of 16 to 30 minutes.

Despite these different experiences, all MDR users expressed high satisfaction with the services they buy. Greater than half of MDR respondents said their organizations were extremely satisfied with their overall service level. Although EMA does not view MDR services as a panacea for all the issues faced by information security operations, it appears to be easing some big pain points in more quickly detecting threats and shutting them down before they can cause great harm.



INTRODUCTION

Managed detection and response services are an outgrowth of several trends in the cybersecurity market. At their foundation, they represent broad recognition among IT security practitioners that determined attackers are going to find their way around existing cyber threat defenses and work to carry out their subversive aims. Thanks to the shortage of skilled cybersecurity professionals and the complexity of managing sophisticated detection and response tools—whether endpoint focused, network focused, or SIEM focused—a growing number of organizations find themselves outgunned by a potent array of adversaries. As a result, more and more organizations are turning to outside service providers to take over the function of actively looking for signs of bad actors moving about within their IT infrastructure and managing the response when those attackers are uncovered.

Although market penetration of MDR services is still in its infancy, interest in such services is growing rapidly. In response, the field of service providers that market outsourced MDR services is expanding at a fast clip. These service providers range from more traditional managed security services providers that have pivoted to add MDR services, such as IBM and SecureWorks, to pure play startups focused specifically on MDR services, such as Red Canary. EDR tools providers, such as CrowdStrike, have added MDR service options to their product portfolios.

The services MDR providers offer include active threat hunting, alert investigation, validating actual security incidents, remotely responding to validated threats, and reporting on threat activity. Remote responses can include isolating an infected host, blocking an IP address on a perimeter device, and more. What MDR service providers don't often do includes compliance reporting, vulnerability management, and onsite incident response (although in some cases that can be an optional add-on).

Most MDR service providers work from their own technology stack or platform, often crafted on open-source security tools and their own collection of threat intelligence feeds to look for indicators of compromise. They typically either install their own sensors and monitors or use the customer's existing sensors and monitoring infrastructure. While some emphasize expertise and a white-glove approach in which each customer works with a dedicated threat hunter, others rely on automation to allow them to serve more clients. Key to these platforms is the ability to scale their services, support multi-tenancy, and use machine learning and other analytics to more quickly detect threats and shut them down before they can do serious damage.

In this research project, EMA sought to better understand the attitudes among IT professionals about MDR's value and place in their security program, as well as gain a deeper understanding about what prompts organizations to build out their own detection and response operation rather than outsource it, which selection criteria are most critical in choosing a provider, and how much control customers are willing to give up in outsourcing that function.

METHODOLOGY AND DEMOGRAPHIC OVERVIEW

In early 2020, EMA surveyed 179 IT executives and contributors whose organizations primarily service customers or constituents in North America. The largest percentage of respondents held IT Director-related roles in their organizations at 36%, 23% held IT Manager-related positions, 17% represented IT security/risk management functions, and another 17% were IT executives.

Breaking Down the Basics

In terms of organization size, the research focused on organizations with at least 500 employees. Small businesses were excluded because MDR services are not a good fit for their security requirements. Instead, the research emphasized midmarket companies with between 500 and 999 employees, small to medium sized enterprises (SME) with between 1,000 and 4,999 employees, and large enterprises with over 5,000 employees. SMEs represented just under half of all respondents in the sample, followed by large enterprises at 30%. Very large enterprises with at least 20,000 employees represented 8% of all respondents. In terms of annual revenue, just over half of all respondents represented companies with between $100 million and just under $1 billion in annual revenue. Although respondents were spread out across at least 17 different vertical industries, the best-represented vertical industries among respondents included manufacturing at 19%, followed by finance/banking/insurance at 15%.

Company Size (Employees)	Revenue	Industry
23% Midmarket (500-999)	5% $5M - <$20M	19% Manufacturing
47% SME* (1000-4999)	8% $20M - <$100M	15% Finance
30% Enterprise (5000+)	51% $100M - <$1B	13% Healthcare
	35% $1B+	12% Software
		8% Retail

*Small to midsized enterprise

Figure 1: Enterprise highlights

In terms of annual IT budgets, just under one-quarter of all respondents reported annual IT budgets in the range of $10 million to just under $25 million, while another 20% reported annual IT budgets in the range of $25 million to just under $50 million. Relative to annual total IT spending, the largest percentage of respondents indicated their organizations spend between 10% and 14% of their IT budget on security at 28%, while another 20% reported spending between 15% and 20% of their total IT budget on security. This reflects a multi-year trend in spending increases on IT security relative to the overall IT budget in response to an increase in the frequency of successful attacks that have done significant damage to organizations' bottom lines.

Total Annual IT Budget	IT Security Spending as Percentage of IT Budget
2% <$1M	3% less than 5%
8% $1M - <$5M	7% between 5%-9%
17% $5 - <$10M	28% between 10%-14%
24% $10 - <$25M	20% between 15%-19%
20% $25M - <$50M	17% between 20%-24%
17% $50M - >$100M	16% between 25%-29%
11% $100M+	6% at 30%+

Figure 2: Budget highlights

While the trend in the growth of information security or cybersecurity budgets relative to the overall IT budget has been documented over the last six or seven years in several EMA studies, more recent EMA research suggests that this growth is moderating. In early 2020, this research project uncovered a renewed increase in the size of overall IT budget compared to the size of the information security budget at respondent organizations. Figure 3 demonstrates that the largest budget increase year over year went to the overall IT budget, rather than the information security budget, while a larger percentage of cybersecurity budgets stayed the same. It is increasingly evident that more organizations, after several years of building up insufficient cybersecurity budgets, have reached the level of spending they deem necessary to deal with the current threat landscape.

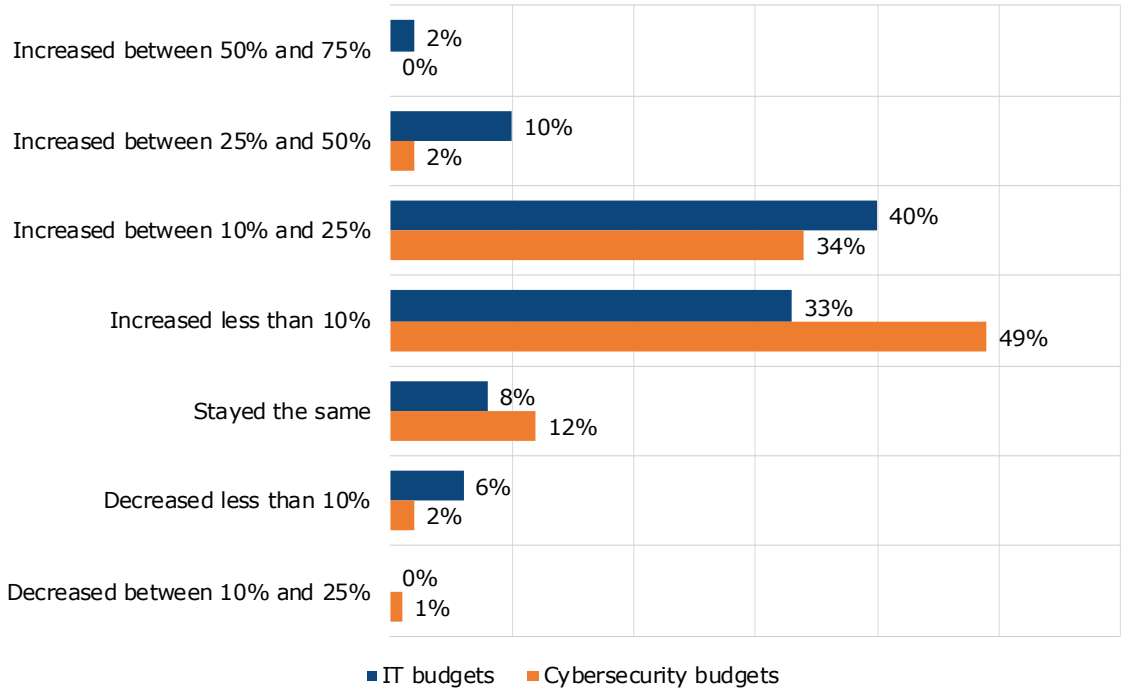


Figure 3: IT vs. cybersecurity budget changes (increase/decrease from last year to this year)

Managed Security Service Provider (MSSP)

– Outsources management of traditional security technologies including event monitoring, alert handling, and threat detection to maintain a basic level of security for clients.

Managed Detection and Response (MDR)

– A service that provides advanced threat detection and response, as well as threat hunting by skilled experts. The service includes elimination of discovered threats and often includes the use of sophisticated forensics technology.

MDR in the Context of Existing Teams and Approaches

Managed detection and response services are available from a growing range of providers with different backgrounds. To ensure that all respondents answered questions based on a common understanding, the survey provided definitions of the two major types of providers.

Managed Security Service Provider (MSSP) – Outsources management of traditional security technologies including event monitoring, alert handling, and threat detection to maintain a basic level of security for clients.

Managed Detection and Response (MDR) – A service that provides advanced threat detection and response, as well as threat hunting by skilled experts. The service includes elimination of discovered threats and often includes the use of sophisticated forensics technology.

To ensure the best possible responses based on experience with the selection and use of threat detection and response solutions, EMA sought to include respondents who had some level of involvement with the solutions their organizations employ or plan to employ. The following chart illustrates respondents' involvement with cyber threat detection and response solutions in their organization. It's important to note respondents could select multiple responses.

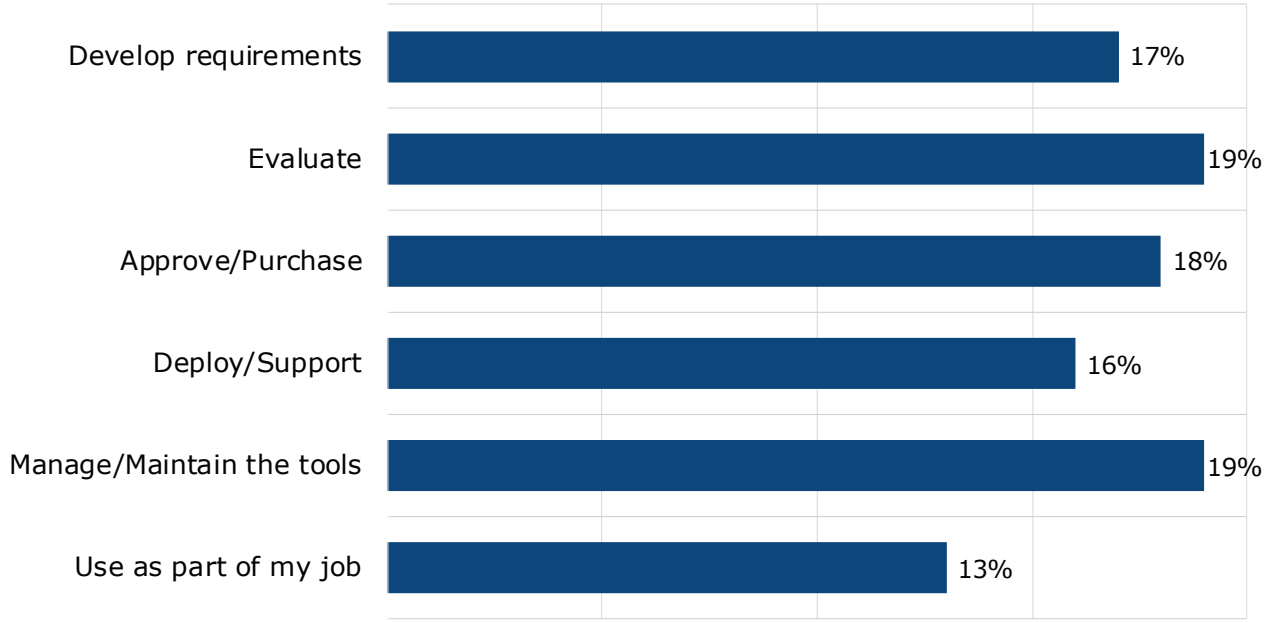


Figure 4: Respondent involvement in threat detection and response solutions

EMA also sought to understand the size of respondent security teams and the number of members holding the title of "security analyst." The average number of information or IT security team members among all survey respondents was 466, while the average number of security analysts was 277. The average was skewed by respondents representing very large enterprises that reported security team sizes in the thousands, and security analyst roles in the hundreds or even low thousands. To gain more granular insight into team sizes across the survey sample, answers were plotted across seven different group sizes. Those ranged from 0 to 100 up to 4,000 or more. For a clear majority of respondents, both security team size and security analyst roles fell in the 0 to 100 category: 60% for security team sizes and 75% for total number of security analysts. Given that half of all respondents represent organizations with less than 2,500 employees, this lines up with the survey sample. It also reflects the ongoing battle that is especially pitched for small and midsized organizations in attracting and retaining experienced security professionals.

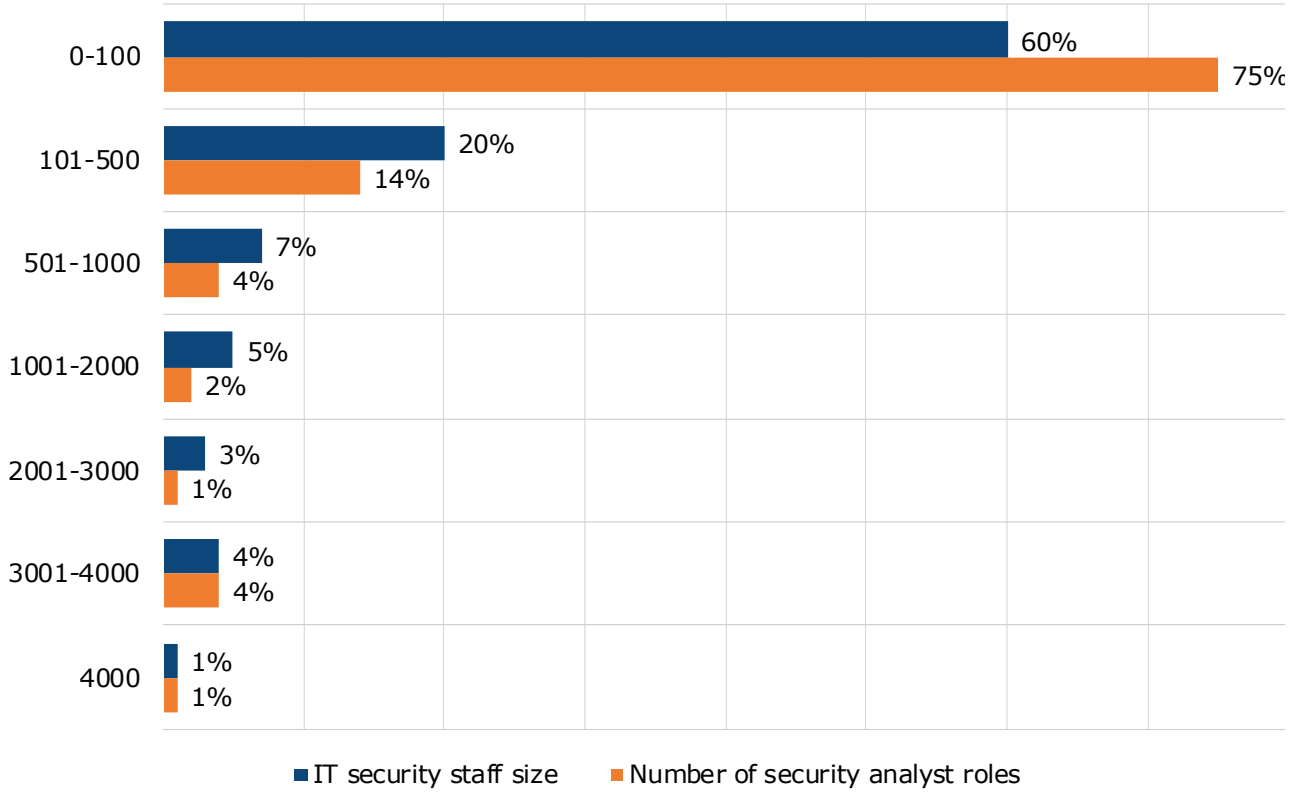


Figure 5: IT security staff size vs. number of security analyst roles

Early in the survey, EMA sought to establish a baseline understanding of how respondents' organizations approach the management of cyber threat detection and response as a day-to-day activity. Do most organizations handle it themselves? Outsource the whole function? Or augment internal staff with a service provider outside of regular business hours? How does that vary across organizations of different sizes? Across all respondent organizations, 36% manage threat detection and response themselves with commercial tools, 24% manage it themselves using open-source tools that their organizations customized, 2% do it themselves using their own homegrown tools, 13% use services to augment their staff outside of normal business hours, 11% work with an MSSP, and 13% use an MDR provider.

Not surprisingly, large enterprises with more than 5,000 employees are most likely to manage the function internally. Forty percent of those enterprises do that internally using commercial tools, and 30% handle it themselves using open-source tools customized for their own usage. If they turn to an MDR provider, they are much more likely to use those services to augment their internal handling of threat detection and response outside of normal business hours. Nineteen percent of those representing large enterprises indicated using that approach, compared to only 2% that indicated they outsourced that function to an MDR provider. That contrasts with midmarket organizations with 500 to 1,000 employees, where 42% of respondents indicated their employers outsource the function to either MDR providers or MSSPs that offer an MDR service. However, given that the market is still in its infancy, it's not unusual that 31% of those midsized enterprises still manage the function internally using commercial tools. It's likely that as these smaller organizations struggle to maintain their information security staff in the face of increasing competition for their skills, they will drive the expansion of the market in the next several years.

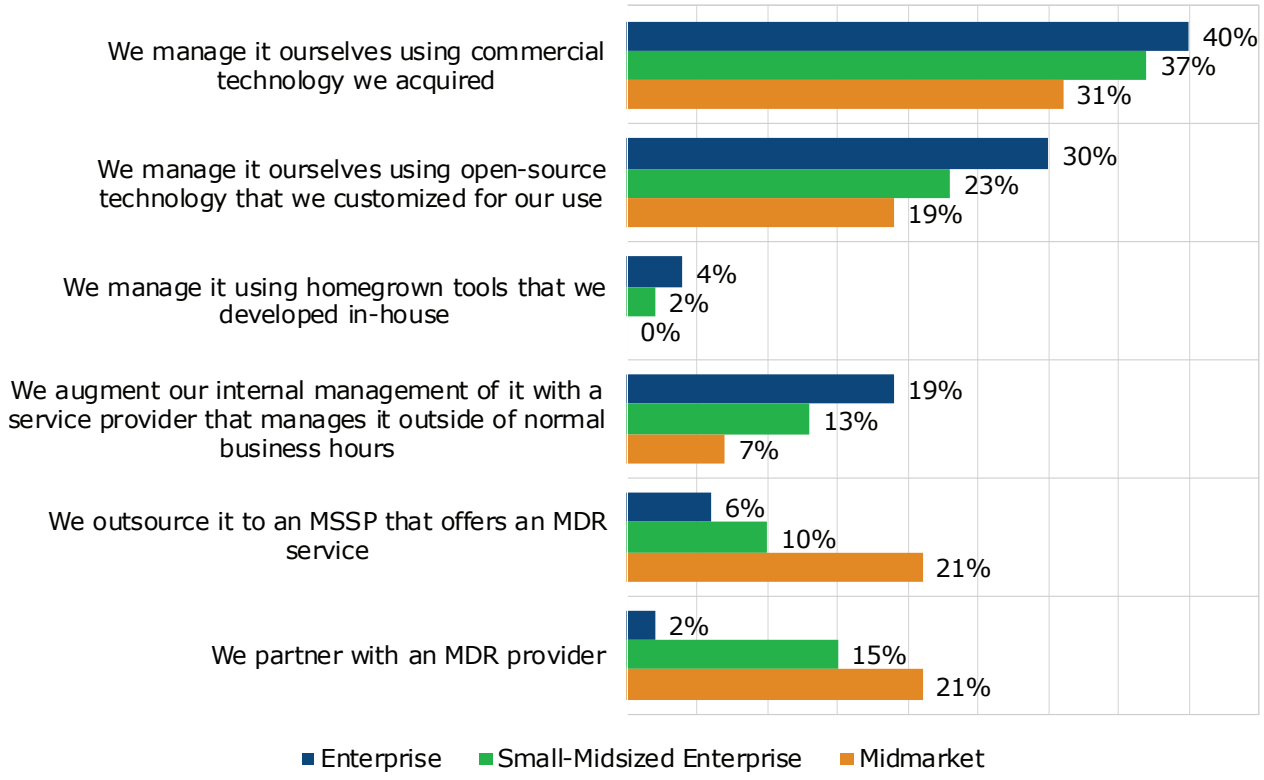


Figure 6: How different sizes of organizations manage threat detection and response

Given the complexity of the tools used to perform threat detection and the struggle (as well as cost) to maintain the required expertise to adequately perform threat detection and response, EMA's research sought to better understand the factors that lead organizations to choose to internally manage the function. Respondents were asked to rank eight different drivers for internally managing threat detection and response according to the level of influence each had on the decision. The top choice for all respondents was that the respondents' organizations had the budget and expertise to manage the function internally, with 32% giving that driver the top ranking.

That answer was given by 35% of large enterprise respondents, while only 26% of respondents at midsized organizations gave it that ranking. Meanwhile, 31% of all respondents indicated that the top driver for internally managed TDR was because of data privacy concerns that kept their organizations from working with an outside service provider. Those data privacy concerns were shared by both large enterprises and midsized companies, while it was less of an issue for SMEs with between 1,000 and just under 5,000 employees.

Twelve percent of respondents indicated that the biggest factor in the decision to internally manage TDR was the desire to avoid service provider lock-in, with slightly more midmarket and SMEs indicating that as a top reason than large enterprise respondents. Factors that had the least influence on the decision to internally manage TDR varied by organization size. For respondents at midmarket companies, the least concern they expressed about outsourcing MDR services included trusting that service providers would respond fast enough to a serious breach and potentially not enough risk reduction to justify the cost of an outsourced threat detection and response service. Clearly, among those midmarket respondent organizations not already outsourcing TDR functions, they nevertheless see value in those services.

Not surprisingly, respondents representing large enterprises ranked a fear of being a lower priority to larger customers dead last. This was also not a big concern for SMEs, nor did SME respondent organizations worry that outside service providers would not understand which of their applications are mission-critical.

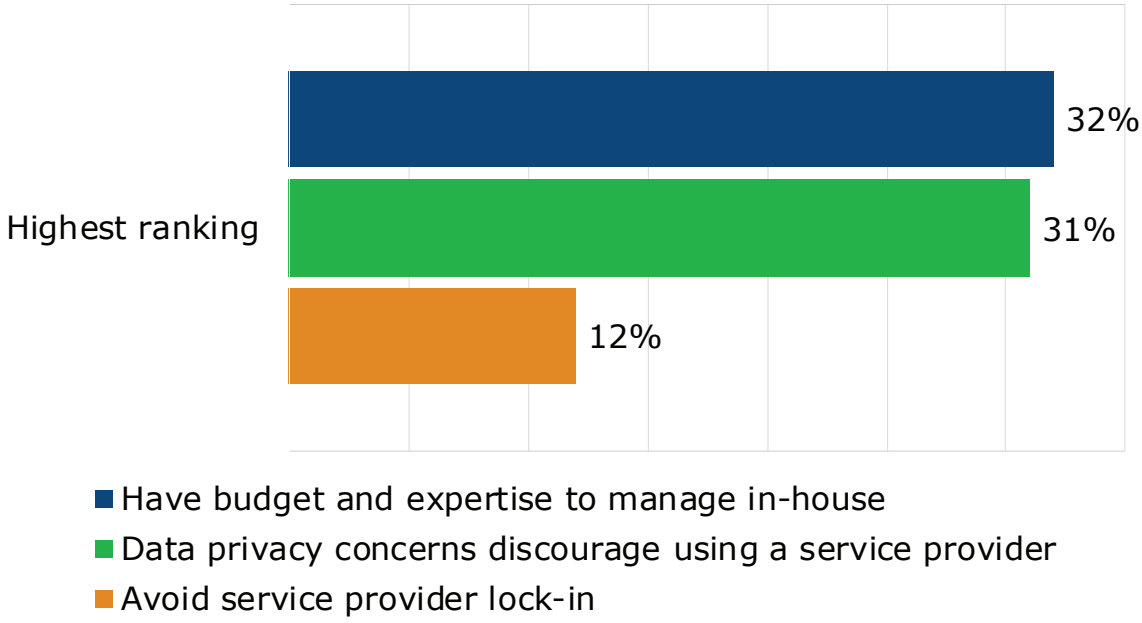


Figure 7: Why manage threat detection and response internally?

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.

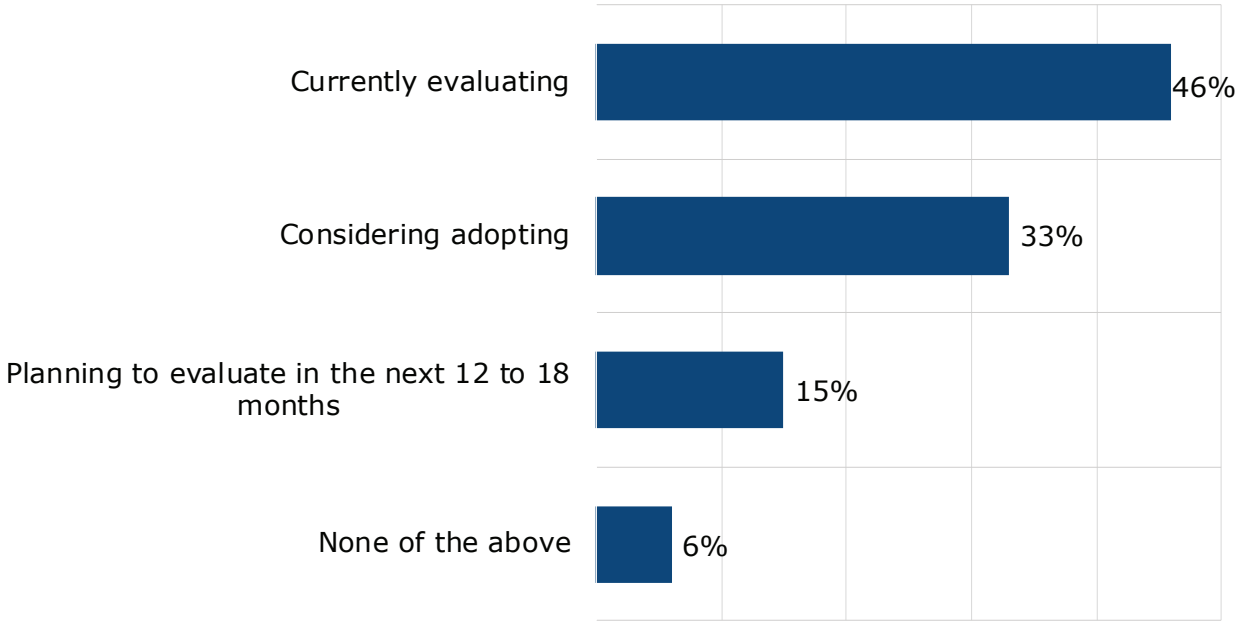


Figure 8: Is your organization currently evaluating an MDR service, considering adopting an MDR service, or planning to evaluate an MDR service in the next 12 to 18 months?

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.

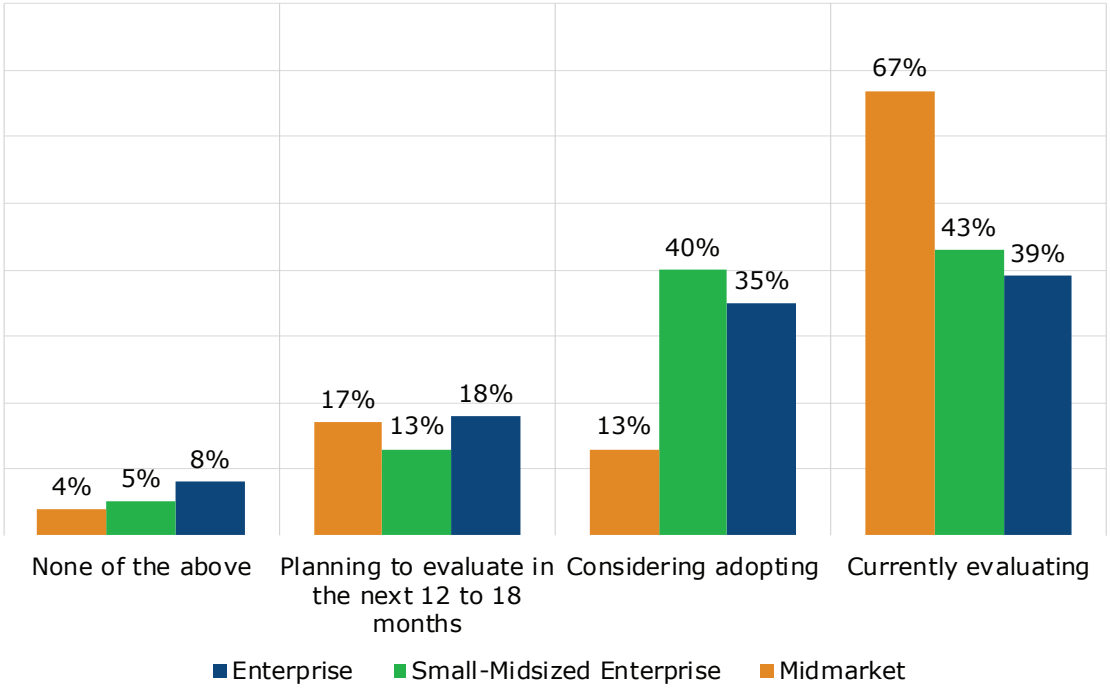
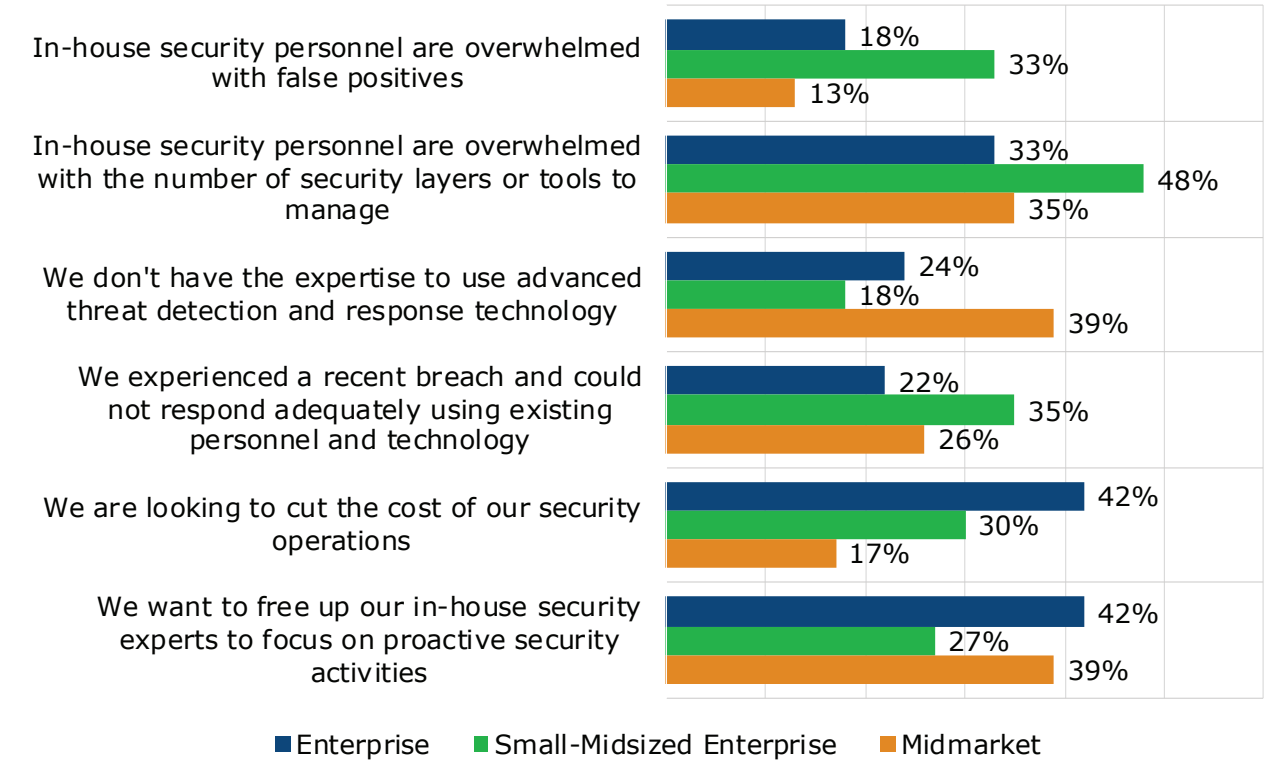


Figure 9: Midmarket demonstrates the strongest interest in MDR service adoption

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 10: 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.

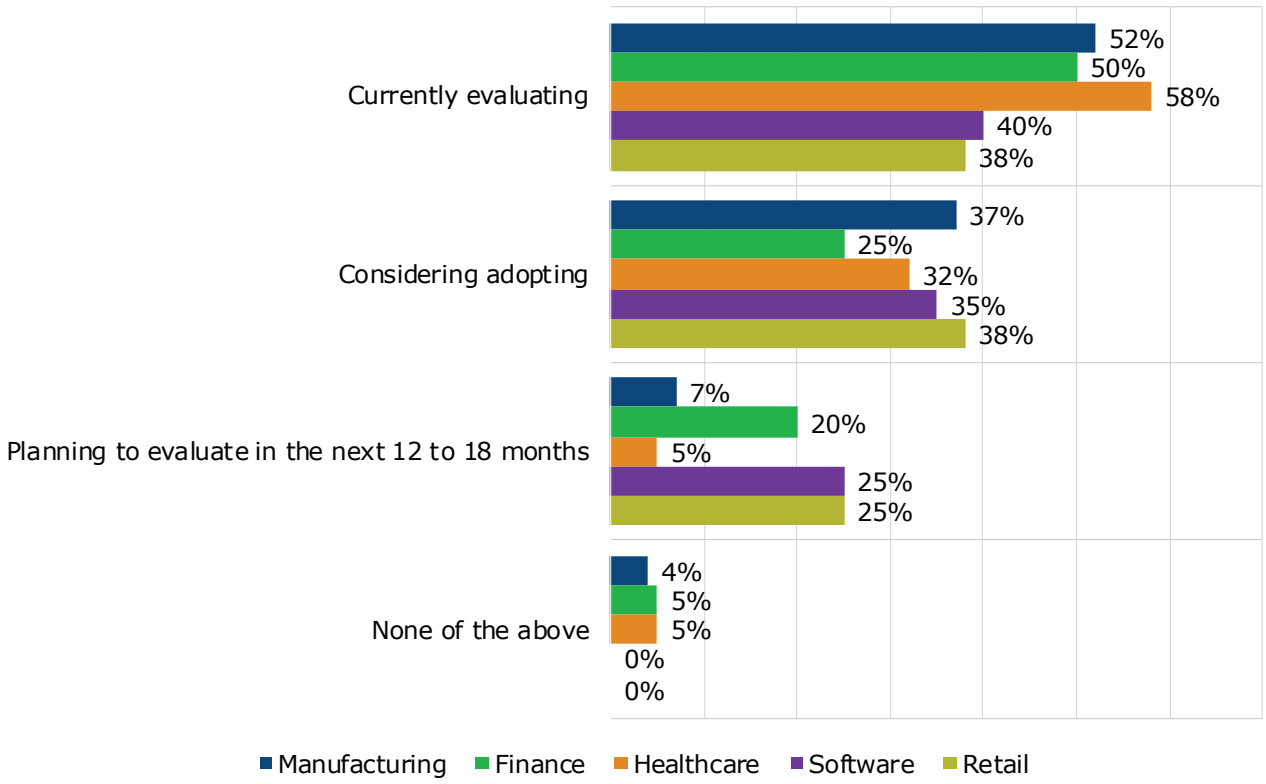


Figure 11: Vertical industry interest in MDR adoption

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.

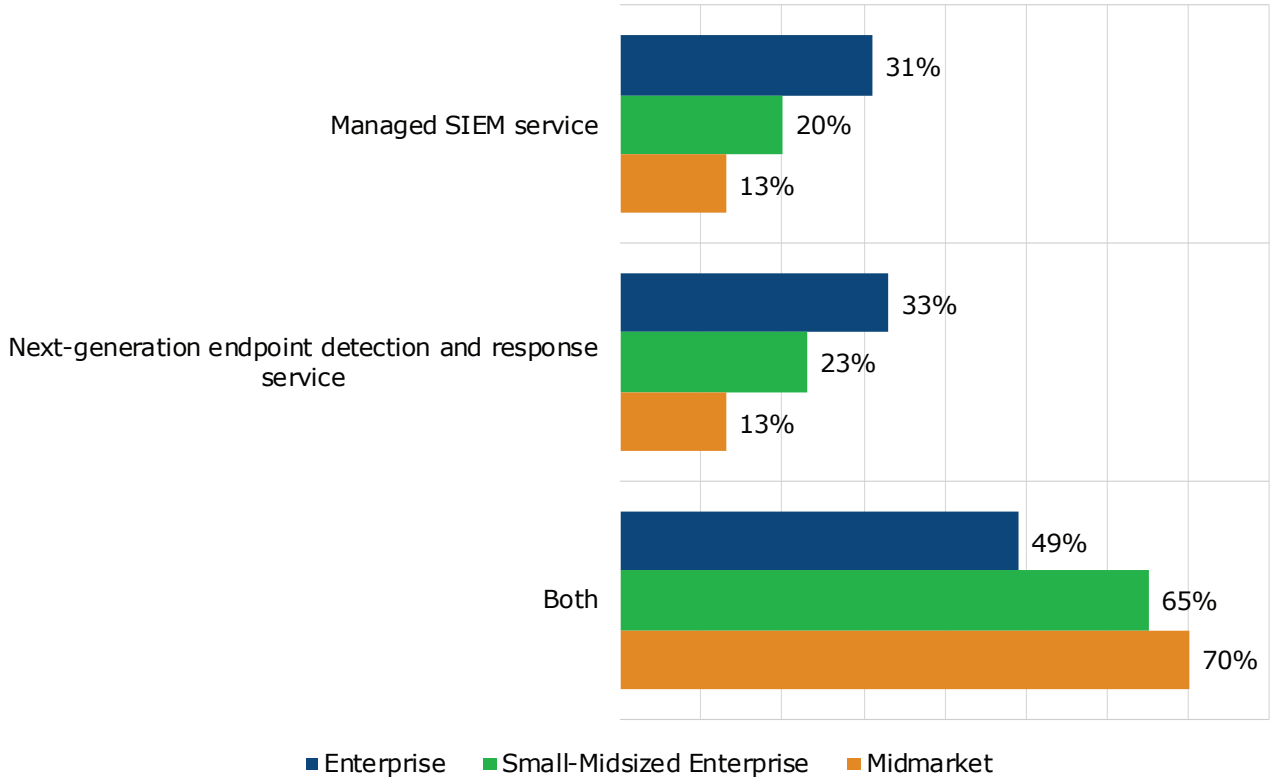


Figure 12: Level of interest in different types of MDR services varies by company size

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.

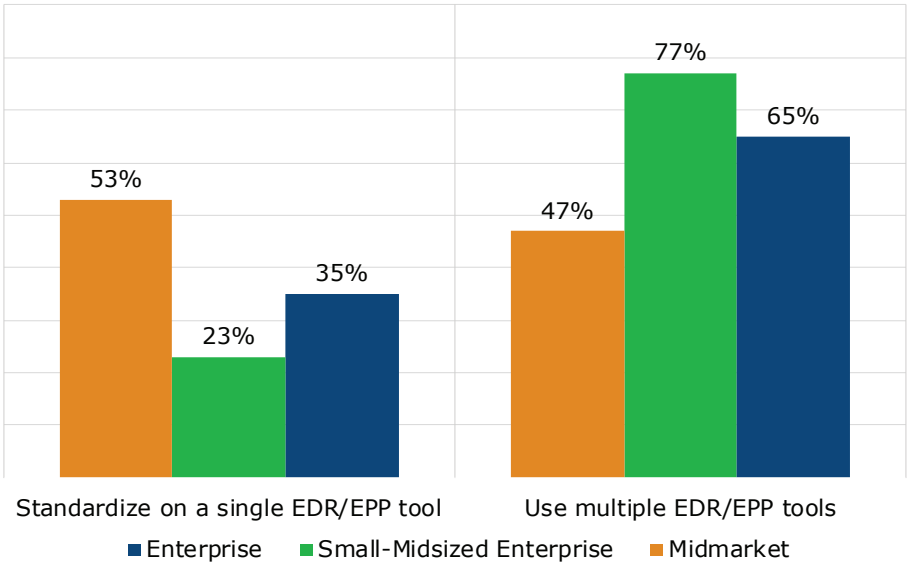


Figure 13: Does your organization intend to use multiple EDR/EPP tools in your potential MDR services engagement, or will your organization standardize on a single EDR/EPP tool?

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.

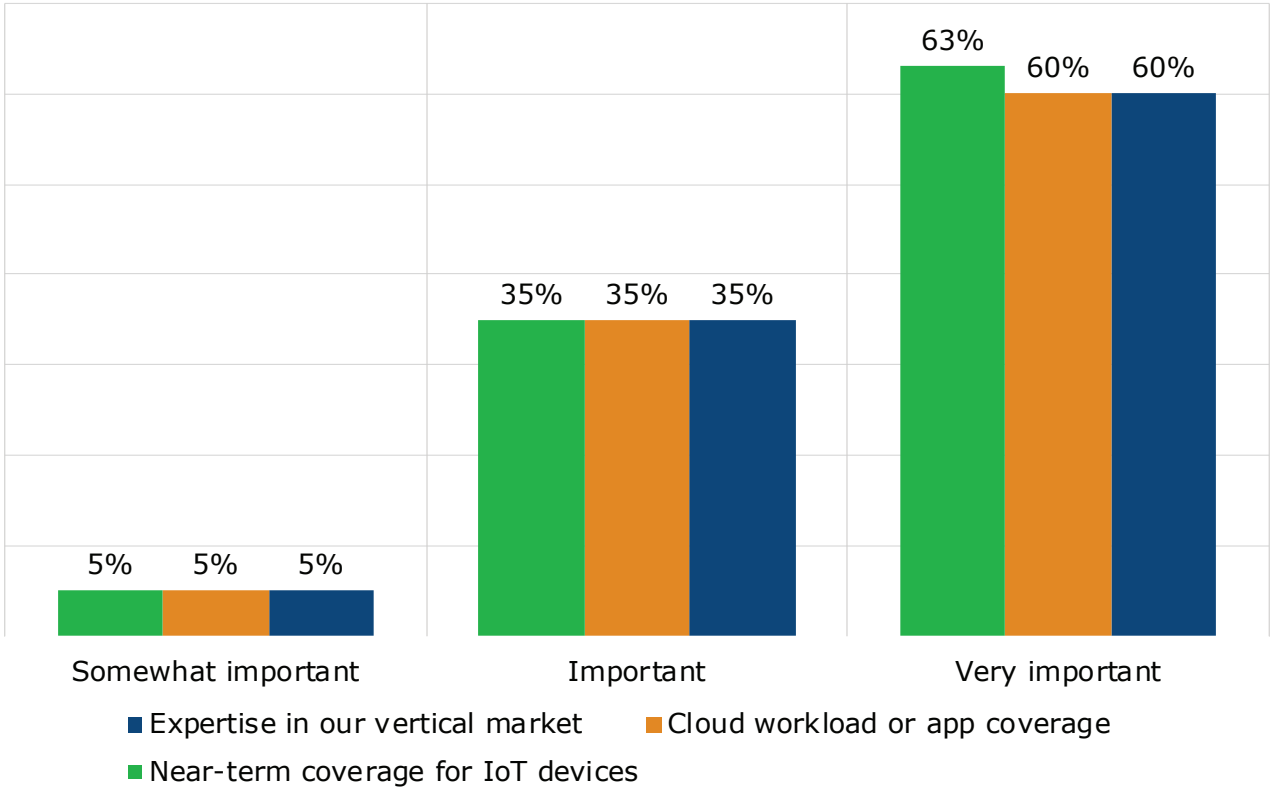


Figure 14: Key criteria in MDR provider selection

The market for MDR services is populated by a growing variety of different solution providers, ranging from well-known security services providers, such as IBM and Secureworks, to dedicated MDR startups, such as Arctic Wolf and Red Canary, to newcomers, such as Cisco Systems. The latter only introduced its managed threat detection and response service in early 2020. To gauge how familiar respondents using MDR solutions were with the field of providers in the market, EMA presented them with a list of 16 recognized MDR providers. IBM and Cisco both benefitted from their broad brand awareness across a wide range of market segments. Smaller, more focused MDR providers have a much bigger education task ahead of them to raise awareness in an increasingly crowded market.

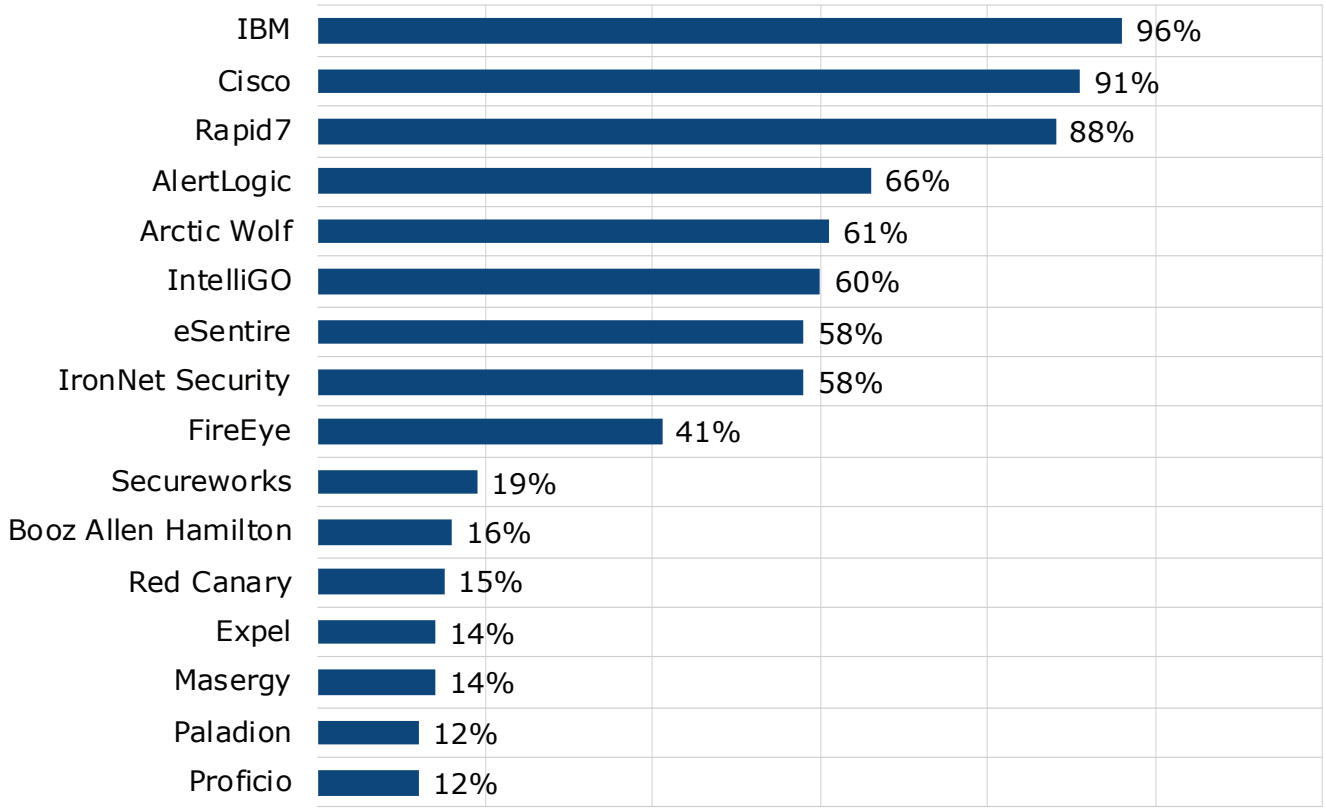


Figure 15: MDR research respondent brand familiarity

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.

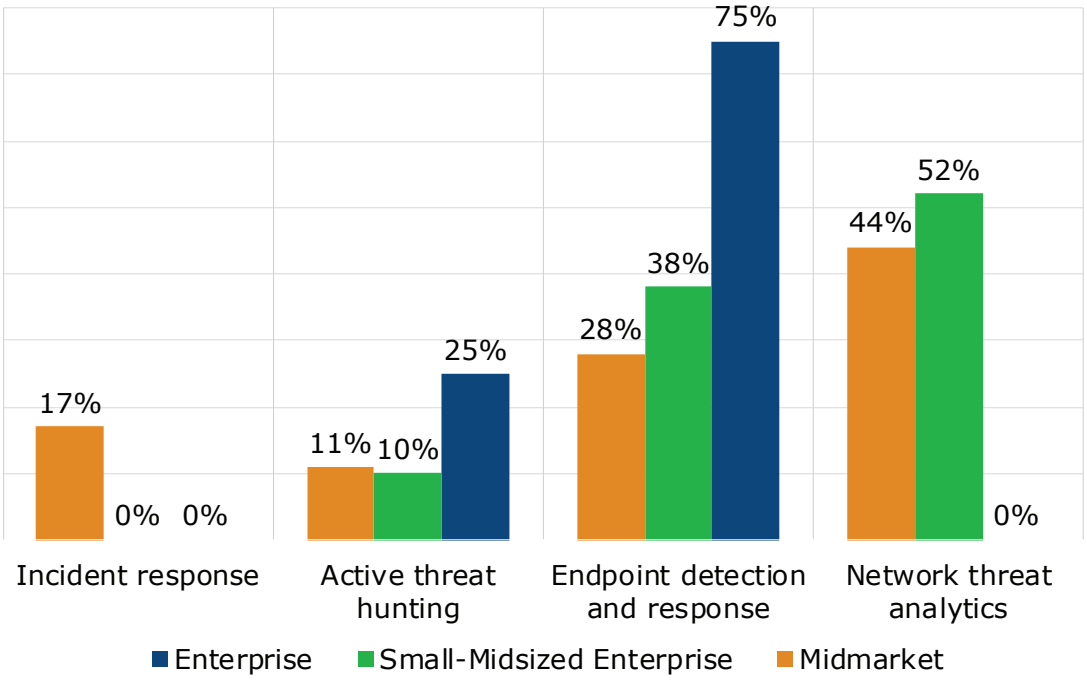


Figure 16: Of the following capabilities most often associated with MDR service providers, which does your organization see as offering the greatest value? by How many employees are in your company worldwide?

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.

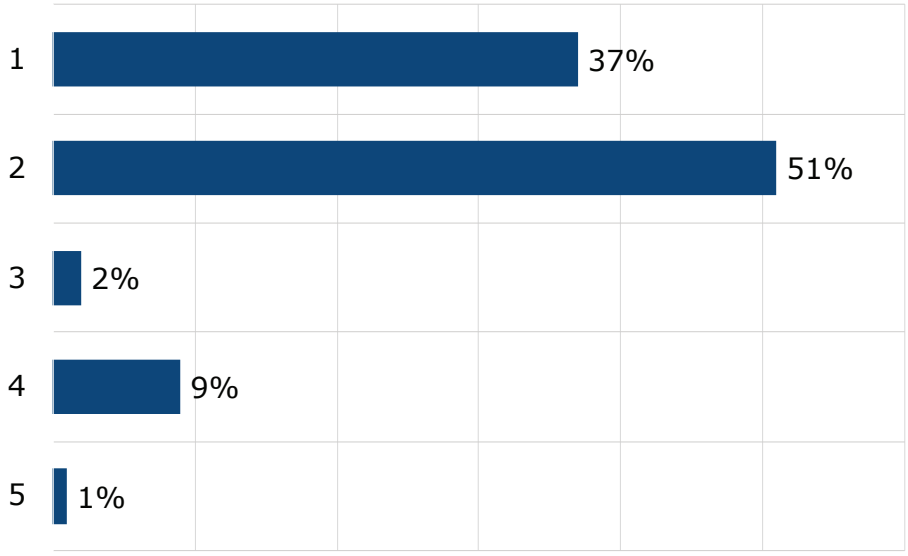


Figure 17: On a scale of 1 to 5, with 1 being most important and 5 being least important, please rate the importance of your MDR provider's underlying tools and technologies in your selection process.

Operationalizing MDR Services

Once a service provider is selected, the process of onboarding customers and establishing the rules of engagement can take anywhere from less than a day to up to three months, depending on how extensive the service offering is, how much if any integration is required with the customer's existing security infrastructure, and other considerations. EMA asked MDR users how long it took their provider to make the service fully operational for their organization. The largest percentage of respondents indicated that it took one week at 44%, with another 28% indicating it took one to two weeks. At the same time, a healthy majority of MDR users indicated that it was relatively easy for their MDR provider to operationalize their service. When asked to rate the ease of onboarding on a scale from one to five with one being the easiest, 58% gave their provider's effort a two, while 21% gave it a one. This is encouraging, but it's important to note that, just like fuel economy, mileage may vary from one provider to another. Some MDR providers report taking as long as five weeks to fully operationalize their service. As providers gain more experience and apply greater levels of automation in onboarding more clients, these timeframes are likely to decrease.

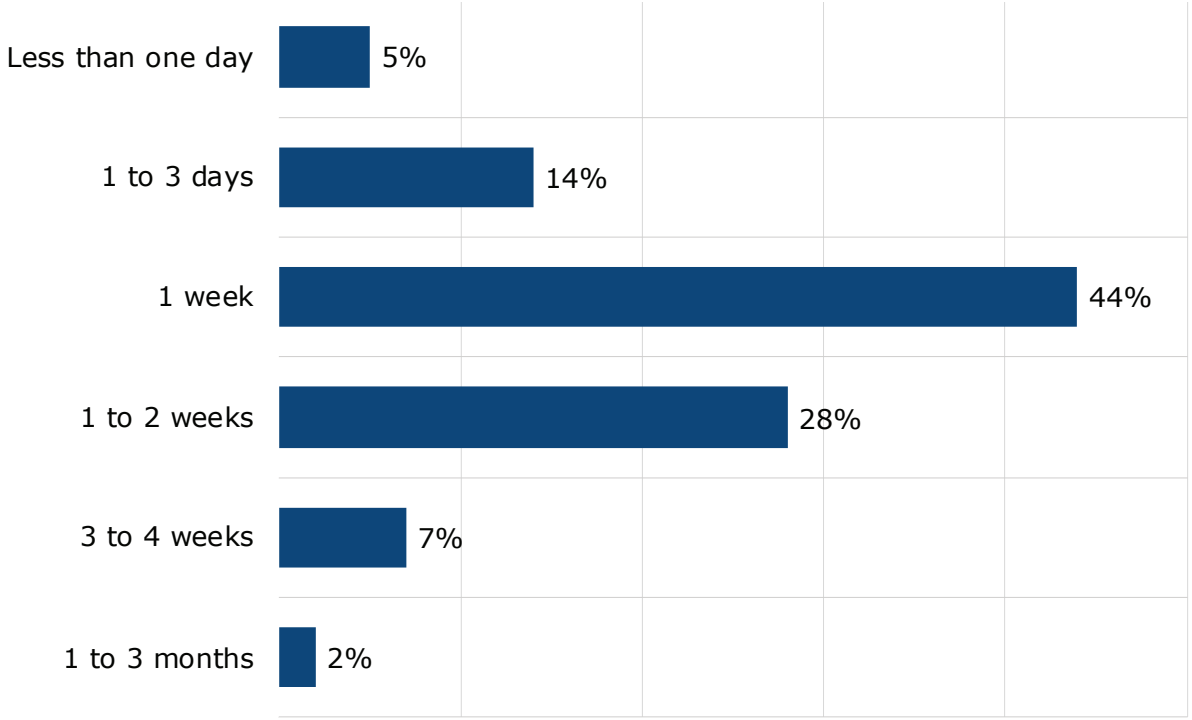


Figure 18: Once your organization selected your MDR provider, how quickly were they able to make the service fully operational for your organization?

As a part of the onboarding process, it is critical for MDR providers to ensure that their own security tools integrate well with a customer's existing defenses to guarantee that providers can move quickly to shut down threats once they are detected and validated. Whether the action is to block an IP address at the firewall, close down spear phishing attempts, or execute another response, speeding such actions is a key component of the MDR provider's value proposition. EMA asked respondents to rank the security tools their organizations were using according to how critical it was for MDR providers to integrate with them in order to initiate and expedite incident response processes. The list included 11 different security or security-related products. Surprisingly for this set of MDR users, the top-ranked tool indicated is their security orchestration and automation response system, with 53% of respondents ranking it as the most critical for integration. Commercial SOAR tools are not yet widely deployed in the still-early market, although growth forecasts are generally robust. It's likely that the research's emphasis on gathering responses from organizations with larger security teams resulted in a larger number of SOAR users than the overall market. Another 35% of MDR user respondents ranked integration with their organization's vulnerability management system as a top priority. This is interesting, and it could suggest that organizations are looking to their MDR providers for help with more quickly remediating the vulnerabilities that are actively being targeted within their organizations. Another 29% reported that SIEM integration was a top priority.

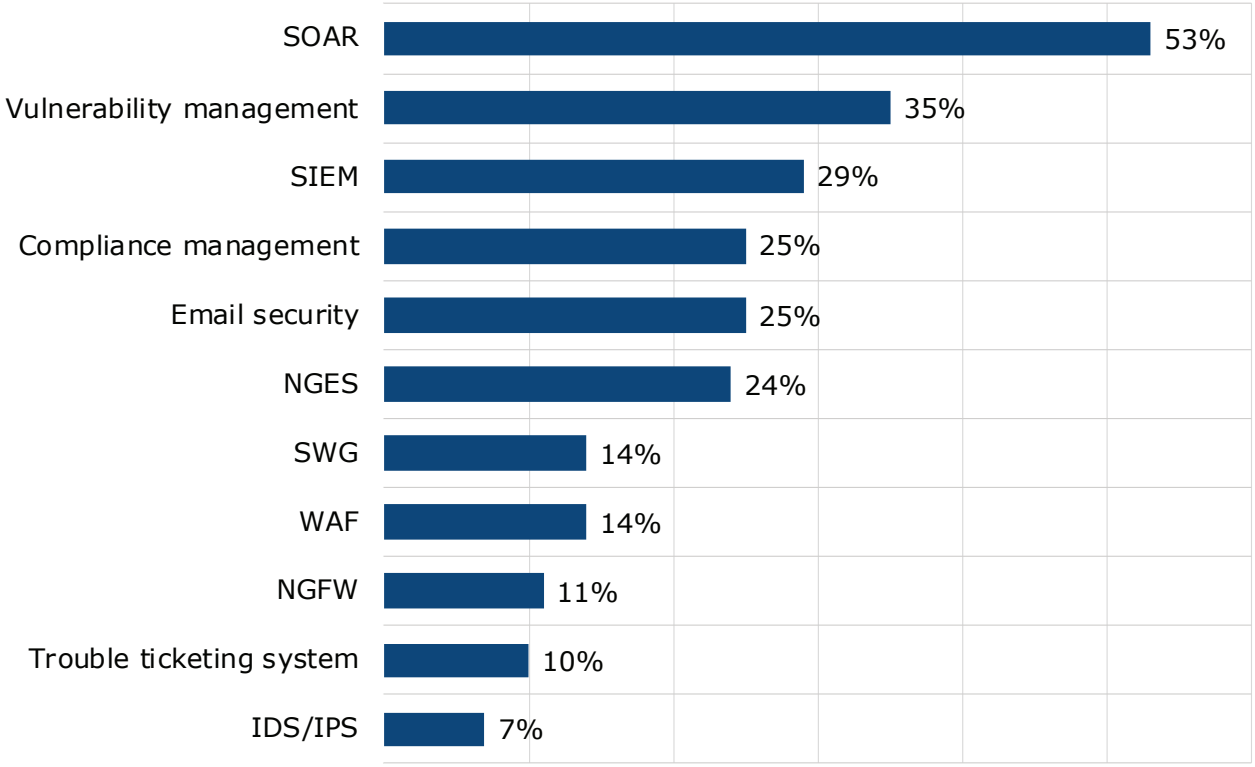


Figure 19: Security tools most critical for MDR providers to integrate with to expedite incident response – top ranking

Some of the primary drivers behind the broad and growing interest in procuring the help of skilled threat detection and response professionals are the complexity and cost associated with establishing and maintaining such operations internally. Skilled threat hunters are in high demand and can command exceptional salaries, and the security tools and infrastructure needed to carry out such activities come with a high price tag—both from capital outlay and operational overhead perspectives. Organizations see the value in it, but they are eager to find less costly and less risky paths to achieve it. Thus, it's no surprise that for a significant majority of MDR respondents, MDR providers are hired to augment, rather than replace, in-house security practitioners. Sixty-seven percent of MDR users indicated this, compared to 33% who are using MDR service providers to replace in-house IT security staff. The latter point speaks to the severity of the security skills shortage. Even for large enterprises with over 5,000 employees, one-quarter of those respondents indicated their organizations were replacing in-house staff. This could be a reflection of the fact that the driver for some organizations to adopt MDR services is to cut the cost of their IT security operation.

For those augmenting their existing security function, just under half of MDR users report interacting with their MDR provider's professionals on a weekly basis, with another 28% interacting on a monthly basis. Only 12% meet daily, and that 12% is dominated by larger enterprises, with 75% of those respondents indicating daily interaction with their MDR service provider professionals. That's no surprise, given the large attack surface those larger enterprises possess and the fact that the greater value of their assets draws more frequent attacks.

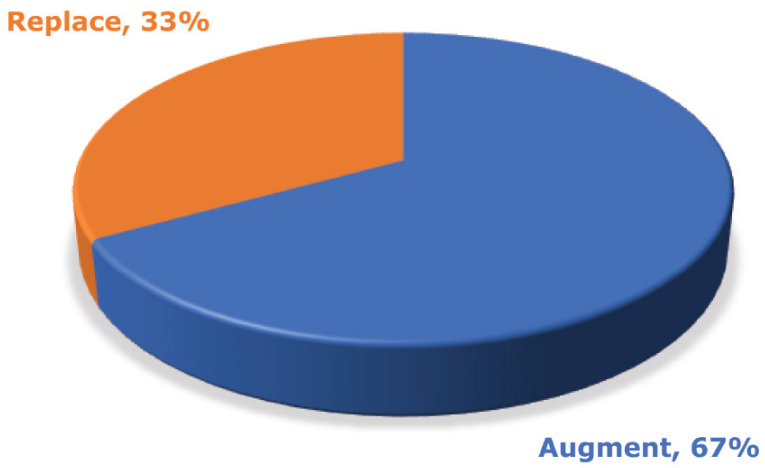


Figure 20: Do MDR service providers augment or replace existing IT security staff?

Although one of the hallmarks and sources of pride for MDR service providers is their ability to provide 24x7 coverage for their clients, not all organizations seeking such services are willing to pay the price tag associated with that extensive coverage. It's not unusual that large enterprises with potentially global operations are more willing to contract for 24x7x365 coverage. The research found that 75% of MDR respondent organizations contract for that level of coverage, while only 25% contract for 24x7 coverage minus holidays. Meanwhile, just over half of SMEs contract for 24x7 coverage minus holidays, with 29% opting for full coverage and 19% opting for just 8x7 (extended business hours). It's no surprise that the smaller the customer, the less frequently they pony up for full coverage.

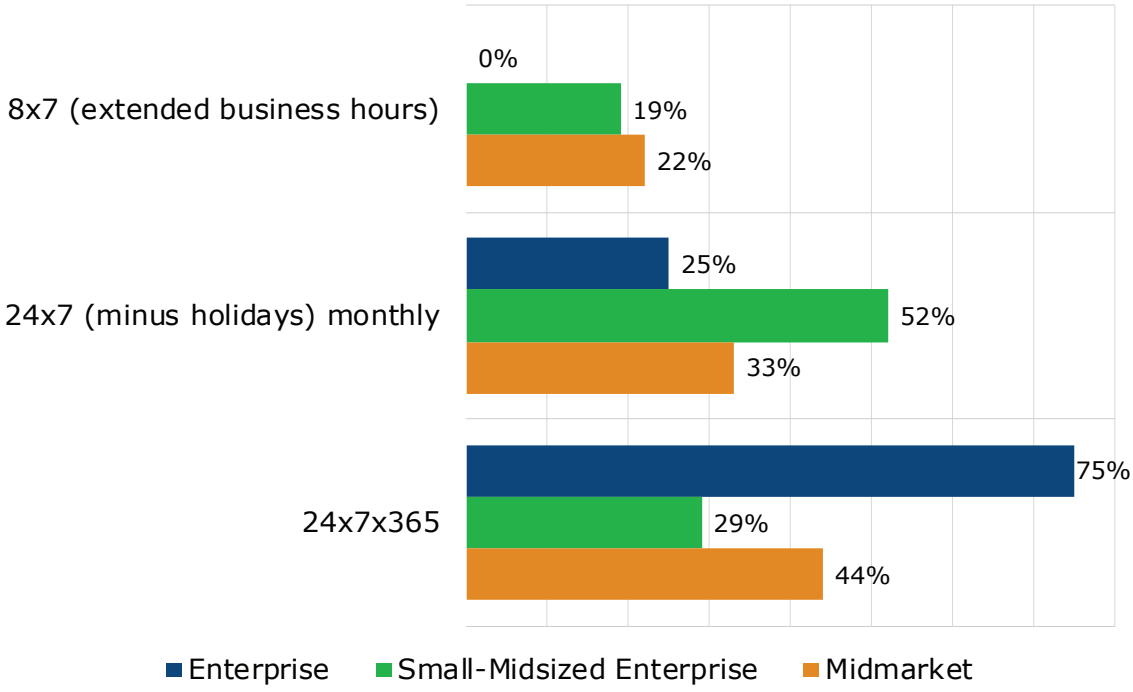


Figure 21: What is the extent of coverage your MDR contract specifies?

Two other data points concerning the operationalization of MDR services are useful to note. Those using MDR services are more likely than not to require that their MDR provider customizes their services to meet specific use cases or other requirements. When asked to rate the importance of that capability on a 1-5 scale, with 1 being the most important, 53% of MDR users gave it a 2, while 37% gave it a 1. This requirement is likely to extend to integration with industry frameworks, such as Mitre ATT&CK. Just under half of MDR respondents indicated that was most important.

ROLLING UP THEIR SLEEVES AND PROVING THEIR WORTH

The range of activities carried out by MDR services providers extends from threat hunting to validation, alert triage, threat remediation, and reporting. The extent of activities offered varies from one MDR provider to the next, and in many cases customers can select increasing levels of capabilities offered by the MDR provider. To better understand what services MDR customers are including in their contracts, the research provided MDR respondents with a list of 10 different activities and asked which of those were included in their contract with their provider. In comparing answers across differently sized organizations, it is clear that large enterprises consistently sign up for more functions by a wide margin. Those functions include not only threats, but also vulnerability hunting, threat and vulnerability remediation, and direct (internal) access to the detection software used by the MDR provider. Given that vulnerability management is not often an option from pure-play MDR providers, this group of users is more likely using MSSPs that have added MDR services to their services portfolio. Virtually all large enterprise respondent organizations include threat validation in their contracts, and 75% include seven other functions. No large enterprises sign up for detection-only services, while 33% of respondents representing midmarket companies do so. SMEs sit somewhere in the middle, with the largest percentages including detection and response, vulnerability remediation, and threat validation at 62%, 62%, and 57%, respectively.

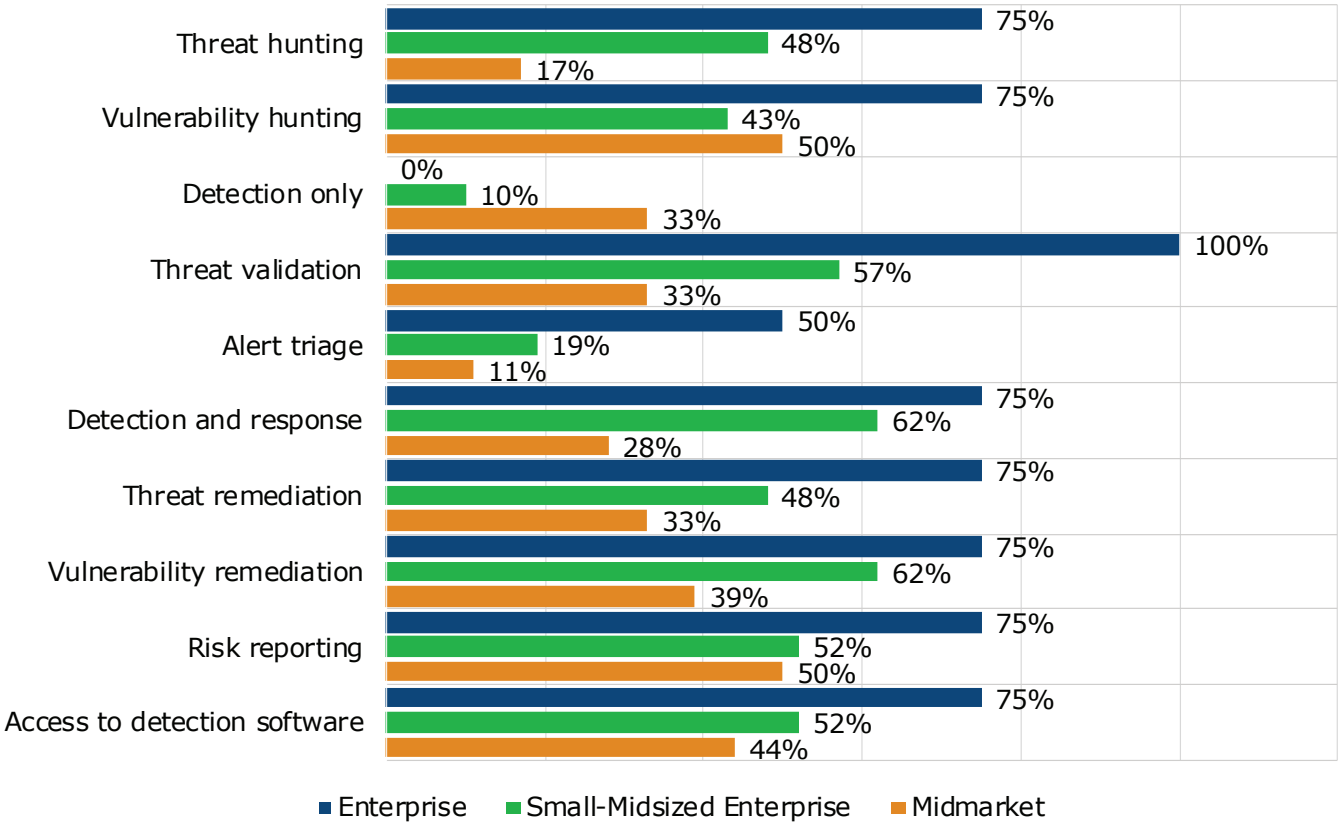


Figure 22: Which of the following services are included in your contract with your MDR provider?

Searching for the Needle in the Haystack

In carrying out their threat hunting activities on behalf of clients, MDR providers monitor a wide swath of the attack surface, including IoT devices and cloud workloads. Across eight possible entry points for attackers, the largest percentage of respondents indicated that their MDR providers monitor IoT devices, cloud workloads, network devices, and servers. IT elements least likely to be included in their MDR provider's monitoring activities include mobile devices, containers, and serverless. For the largest percentage of MDR users, the type of telemetry relied on most often by their MDR providers includes threat intelligence, network, and endpoint activity. Logs are the least-used telemetry for threat monitoring.

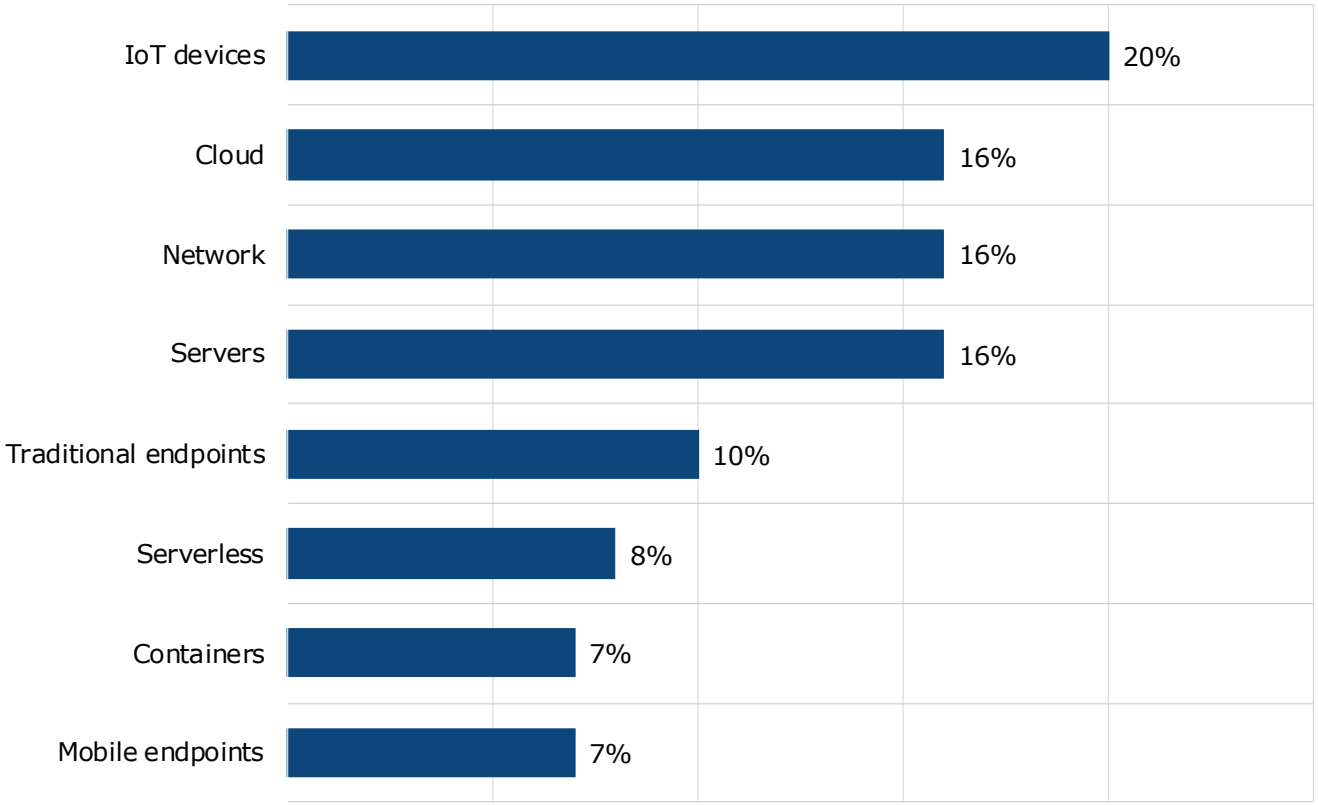


Figure 23: IT elements MDR providers monitor

To better understand how well their services are working to uncover the stealthy threats that bypass existing client defenses, MDR users were asked to identify the types of threats their MDR providers uncovered as part of their service. Out of a list of 12 major categories of attack types, the largest percentage of MDR respondents reported that their providers uncovered SQL injection attacks, command and control activity, and business email compromise/phishing attacks at 12%, 12%, and 11%, respectively. Activities that are harder to detect, such as lateral movement within the customer's network and credential theft, were the least reported attacker activities. This suggests that MDR providers are still largely uncovering attacker activity that is easier to detect, more so than activity that is harder to detect, further along the kill chain and closer to success.

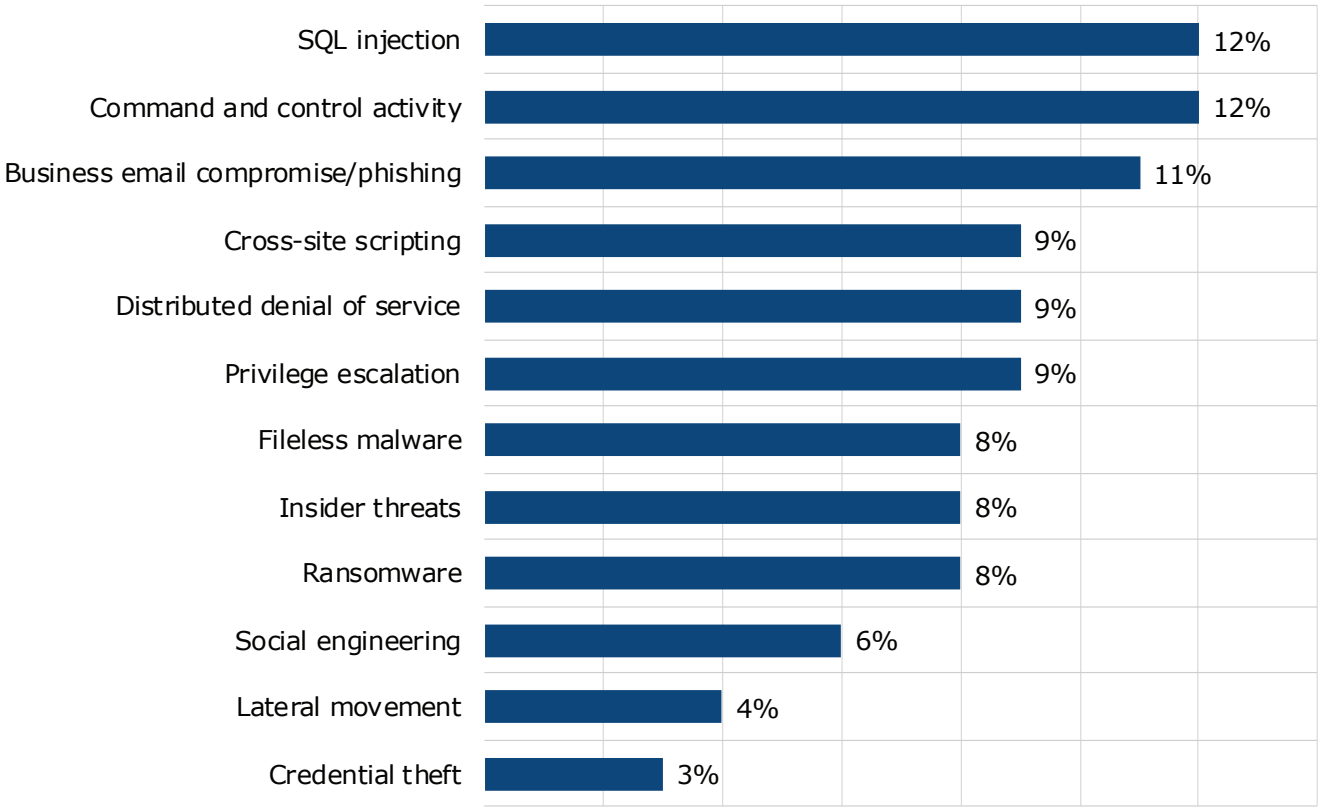


Figure 24: Which, if any, of the following types of threats has your MDR provider found so far that managed to bypass your organization's existing defenses?

Once a security alert or incident has been validated as a real threat, MDR security analysts can execute a range of different threat mitigation activities. For the largest percentage of MDR users, that may start with capturing malicious files for additional analysis, but then extends to such activities as collecting additional forensics from an infected device, blocking specific network traffic using a legacy IDS/IPS device, using DNS to block threats at other TCP/IP layers, quarantining an endpoint, and more. For the smallest percentage of MDR users, providers are free to delete registry keys, perform TCP reset, and disable user accounts. According to 36% of MDR users, response activities for validated threats are automated via machine learning, with 35% indicating such automation is achieved using API integration. Only 1% of respondents reported that their MDR providers manually handle threat response.

Such high levels of automation are key to scalability (and profitability) for MDR providers, but they could find resistance to such automation depending on how it is executed. Fully automatic remediation means that no humans are involved in the decision to execute a remediation step, which could spell disaster if it is not accurate. Automated responses that involve checking with a human operator before executing a response is generally more acceptable. The survey asked MDR users about their comfort levels with the automated remediation capabilities of their providers. Specifically, they were asked to rate their comfort level, on a scale from 1 to 5 with 1 being the most comfortable, in allowing their MDR provider's platform or system to take automated remediation actions without human involvement based on established playbooks. Seventy-five percent of large enterprises expressed the highest level of comfort, while 50% of midmarket customers and 43% of SMEs expressed the second-highest level of comfort with such automation. It's likely that large enterprises have had a greater amount of exposure to automated remediation and had the opportunity to develop greater trust in such capabilities.

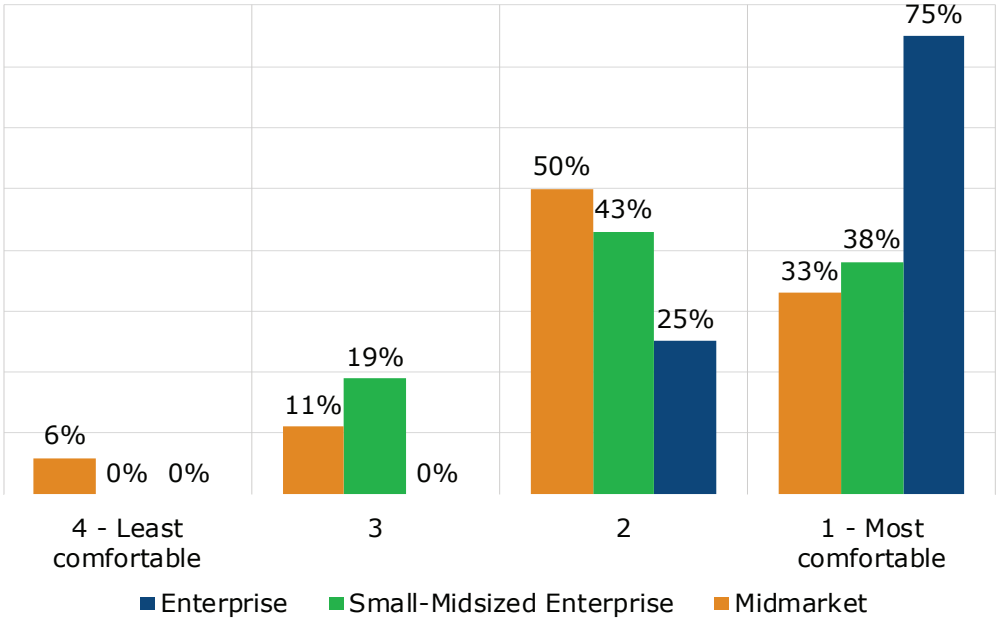


Figure 25: Large enterprises more comfortable with automated remediation

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%.

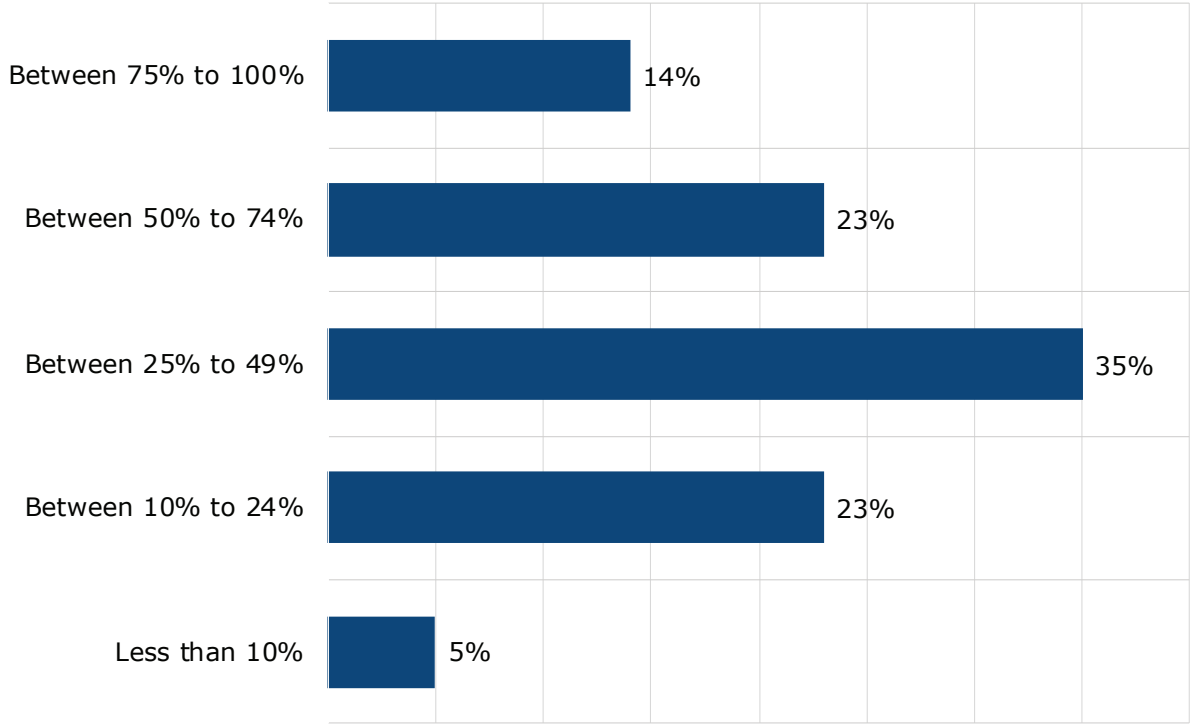


Figure 26: Since your MDR provider began monitoring your organization's network, how much, if at all, have they reduced the mean time to resolution of attacks?

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.

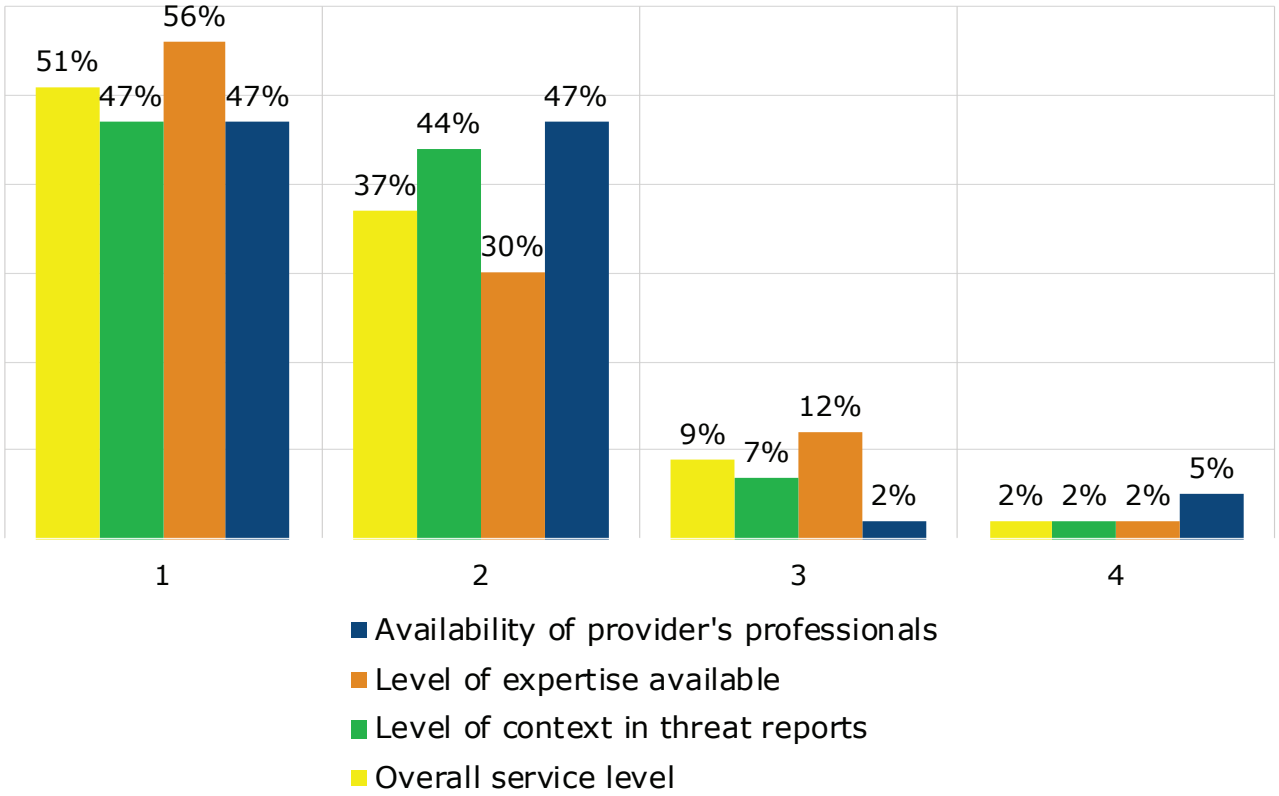


Figure 27: On a scale from 1 to 5, with 1 being extremely satisfied and 5 being not at all satisfied, how satisfied is your organization with…

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.

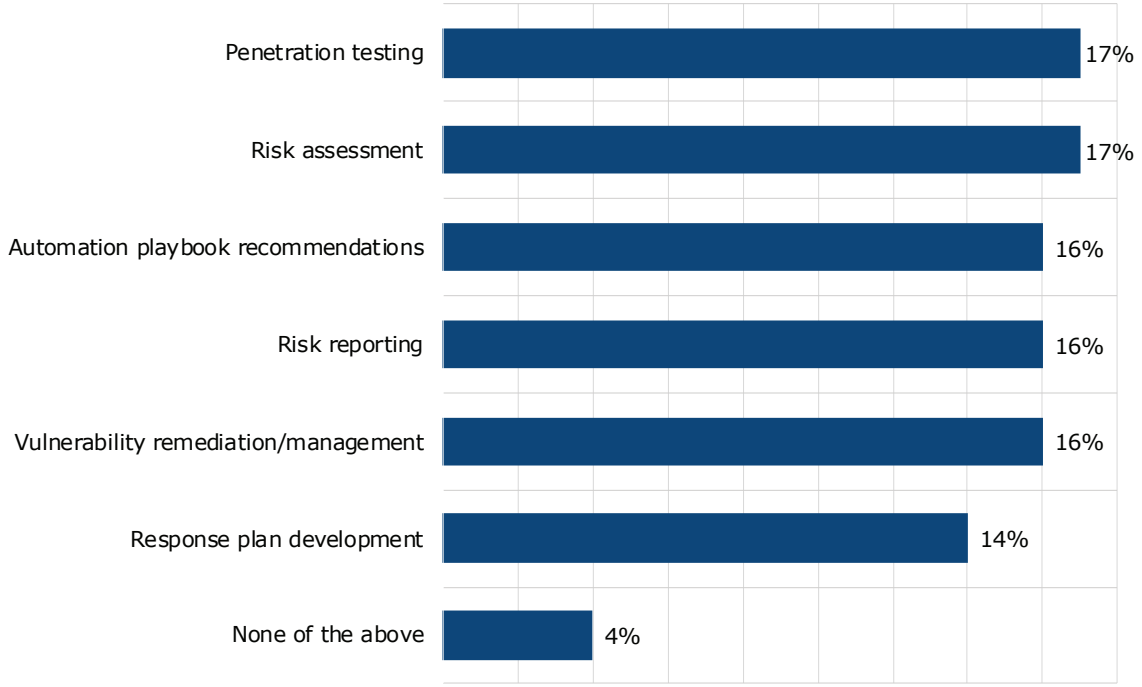


Figure 28: Which of the following services, if any, would you like to receive from your MDR provider that they don't currently offer?

CONCLUSION

The success bad actors are seeing in bypassing existing defenses, along with the complexity and overhead associated with hunting down threats within enterprise infrastructure, are spurring the fast growth of the managed detection and response market. Although it's still early days, interest in these selectively outsourced managed threat detection and mitigation services is quite high, also owing in part to the broad gulf in available information security talent. As CISOs and other IT security executives seek to move protections to new attack surfaces, such as cloud-based workloads and IoT endpoints, they are learning that existing security practices don't translate well to these new environments and are struggling to understand how to best protect those assets against exploitation by cyber criminals. Pure-play MDR providers, MSSPs adding new MDR services, and others can marshal the right talent, create the most efficient processes through automated workflows and design the right security stack to underpin those services. This can help organizations solve a big pain point that will only get larger with time.

There are a few caveats, however. These services must prove to be less costly than the alternative of performing that function in-house, especially as large enterprises seek to reduce the cost of their security operations. At the same time, speed is vital in catching and shutting down attackers once threats are discovered and validated. It only takes one significant breach to lose the customer's trust, and so it is vital that MDR providers detect and mitigate threats early in their lifecycle—before they can do significant damage. The good news is that MDR providers appear to be achieving those aims, given the relatively high satisfaction levels reported by MDR users. Their success is opening up new opportunities to extend the array of services they provide to those satisfied customers.

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