

Publication date:

June 2021

Author:

Jeff Wilson

Managed Security Service Opportunities in a Transforming World



Commissioned by:



Brought to you by Informa Tech

Contents

The state of managed security services	3
MSSPs and enterprises agree on the power of MDR	9
Managed security in the era of distributed secure networking	12
Conclusion: It's all because of the cloud	17
Appendix	18

Table of figures

Figure 1: Enterprise: Managed security investment drivers	4
Figure 2: Enterprise: Increasing use of MSS	5
Figure 3: Enterprise: Drivers for increased use of MSS	6
Figure 4: MSSP: What services are important to customers?	7
Figure 5: Enterprise: Drivers for increased use of MSS	8
Figure 6: Enterprise: Benefits of buying MDR from an MSSP	10
Figure 7: MSSP: Is MDR strategic to your business?	11
Figure 8: Enterprise: Thoughts on SASE and managed services	13
Figure 9: Enterprise: Choosing a security solution provider	14
Figure 10: MSSP: Will enterprises move to SASE?	15
Figure 11: MSSP: Competition from cloud-delivered security vendors	16
Figure 12: MSSP respondent region	18
Figure 13: SMB and enterprise respondent region	19
Figure 14: MSSP respondent role	20
Figure 15: SMB and enterprise respondent role	20

The state of managed security services

Since the birth of managed security in the mid-to-late 1990s, managed security service providers (MSSPs) have been making dependable, high-margin revenue managing on-premises security devices. Twenty-five years and one pandemic later, the world has changed, and MSSPs need to look at new service and revenue opportunities, and emerging technologies and architectures such as managed detection and response (MDR) and secure access service edge (SASE) represent two key ends of the new managed security spectrum. Most MSSPs are already on the path to delivering MDR as an evolution of endpoint detection and response (EDR) in addition to their traditional device management and monitoring services, but few have comprehensive MDR offerings. Regardless of their progress, the drivers for purchasing MDR are really focused on improved security efficacy. Customers are looking at SASE because they want a unified architecture for securely accessing resources (data, applications, and infrastructure) from any device at any location. SASE is less about security and more about a unified IT architecture that includes on-premises deployments as well as private and public cloud rollouts, but it is forcing most enterprises to reevaluate the role of virtual private networks (VPNs), another key revenue stream in a traditional managed security service (MSS) offering.

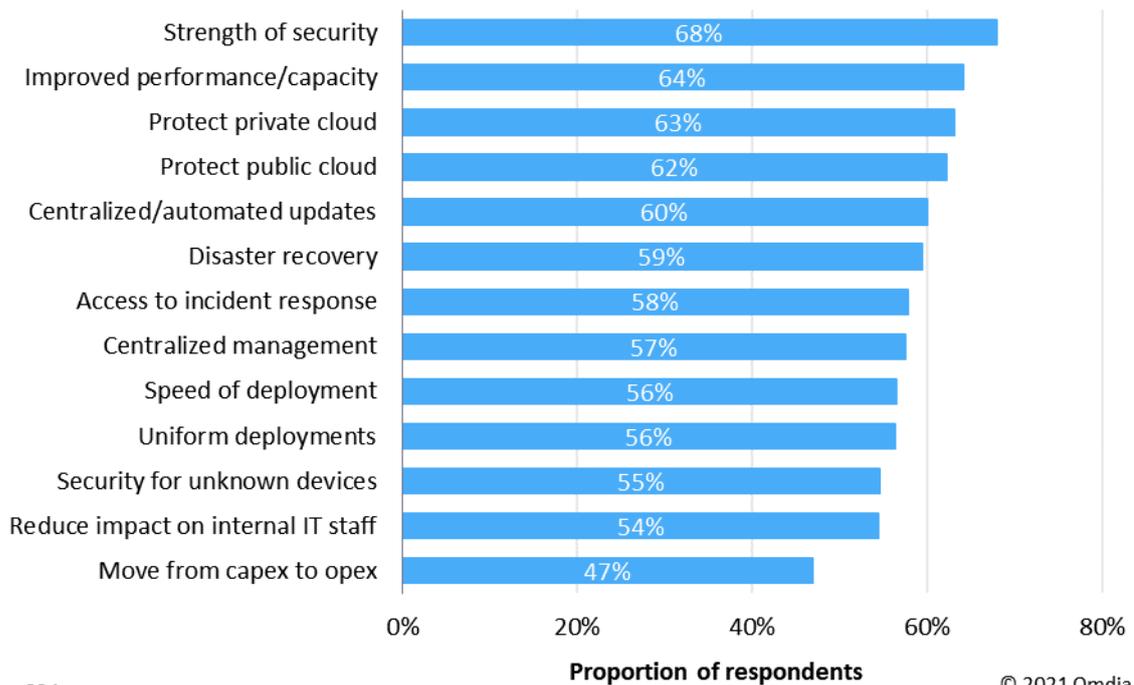
In December 2020 Omdia surveyed 162 purchase decision makers at MSSPs and 834 purchase decision makers at small, medium-sized, and enterprise managed security service buyers around the globe in order to understand how their MSS deployments and purchases were changing in the new, distributed multicloud world.

The first question we asked enterprises is what drives them to make new security investments. We gave respondents a list of common drivers for investing in managed security and asked them to rate each driver on a scale of 1–7 (where 1 was “not a driver” and 7 is a “strong driver”). The chart shows the percentage of respondents that considered each factor an important driver, meaning they rated it 6 or 7.

“Strength of security” tops the list: buyers simply believe service providers help them achieve better protection than they achieve by going it alone, often as a result of preintegration of security solutions, dedicated monitoring capability, and the availability of incident response services. A majority of respondents found nearly all of these factors to be key drivers of the purchase of managed security. Managed security services exist to help mitigate the complexity of deploying and managing security, complexity that rears its head in many places, including scaling up security performance, managing security for public or private cloud, handling patching, and updating solutions.

Figure 1: Enterprise: Managed security investment drivers

On a scale of 1 to 7, please rate the following factors in your decision to deploy managed security services.



Note: n=834

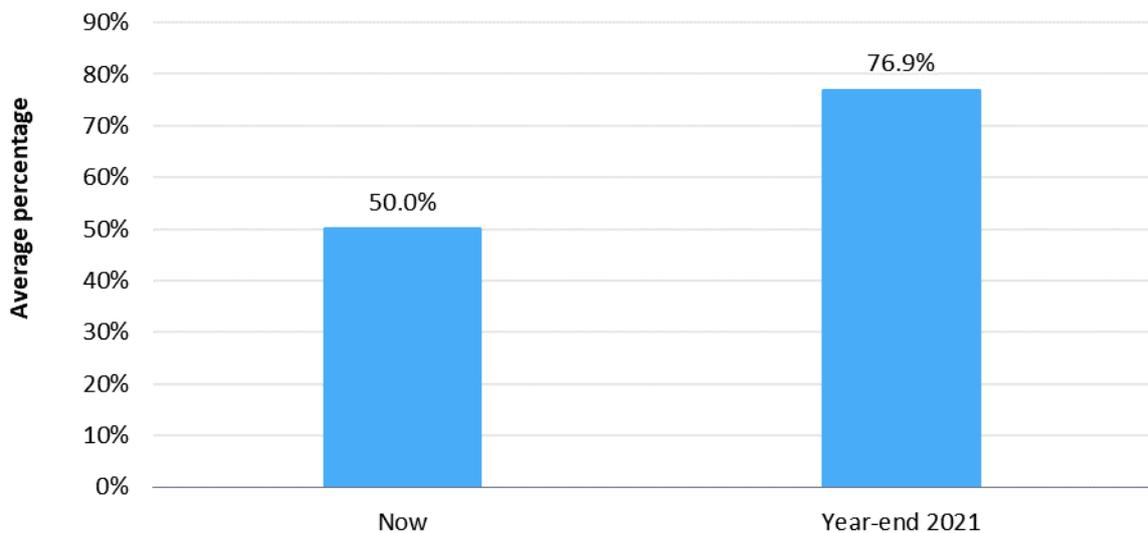
© 2021 Omdia

Source: Omdia

We then asked our enterprise respondents how pervasive use of managed security services is in their organizations, and at the time of the survey, an average of 50% of users were already protected by MSS, growing to 77% of users by the end of 2021, which is a significant increase.

Figure 2: Enterprise: Increasing use of MSS

What percentage of your total users/seats are protected by managed security services now, and what percentage do you expect by the end of 2021?



Note: n=834

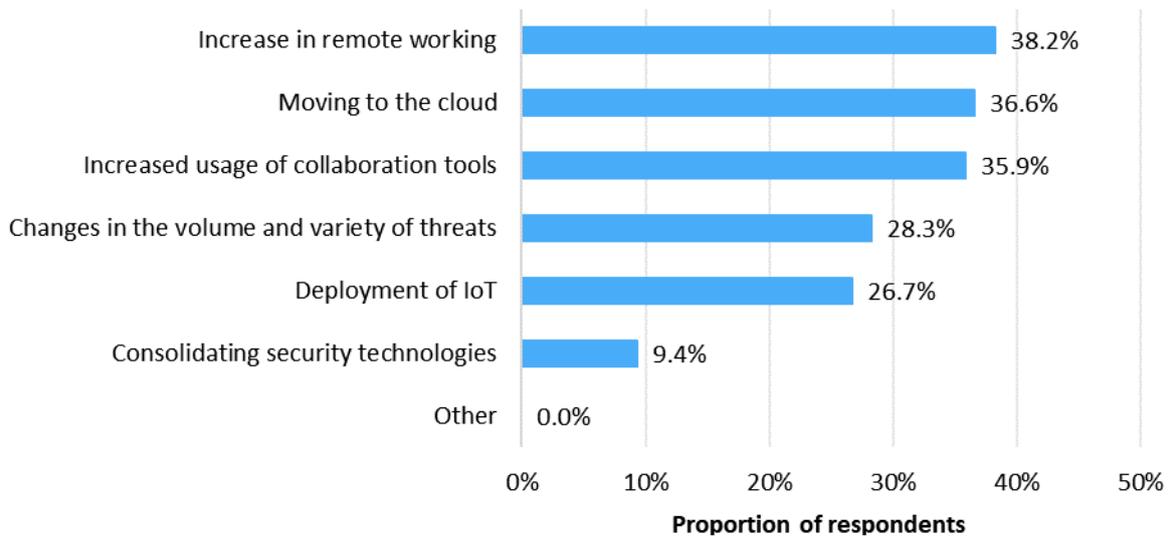
© 2021 Omdia

Source: Omdia

When we asked about key drivers for increased use of MSS, three related drivers hinted at the need for SASE (mobility, cloud, and collaboration), and one was squarely focused on efficacy (changes in volume and variety of threats). While the cloud is named in only one of the top four drivers, if no cloud existed there would not be such a significant move to remote working or such a sharp increase in the use of (cloud-delivered) collaboration tools. Increasing use of the cloud is a key underlying driver for almost every purchase decision in security today.

Figure 3: Enterprise: Drivers for increased use of MSS

Which of the following drivers are causing the most changes to your consumption of managed security services?



Note: n=834

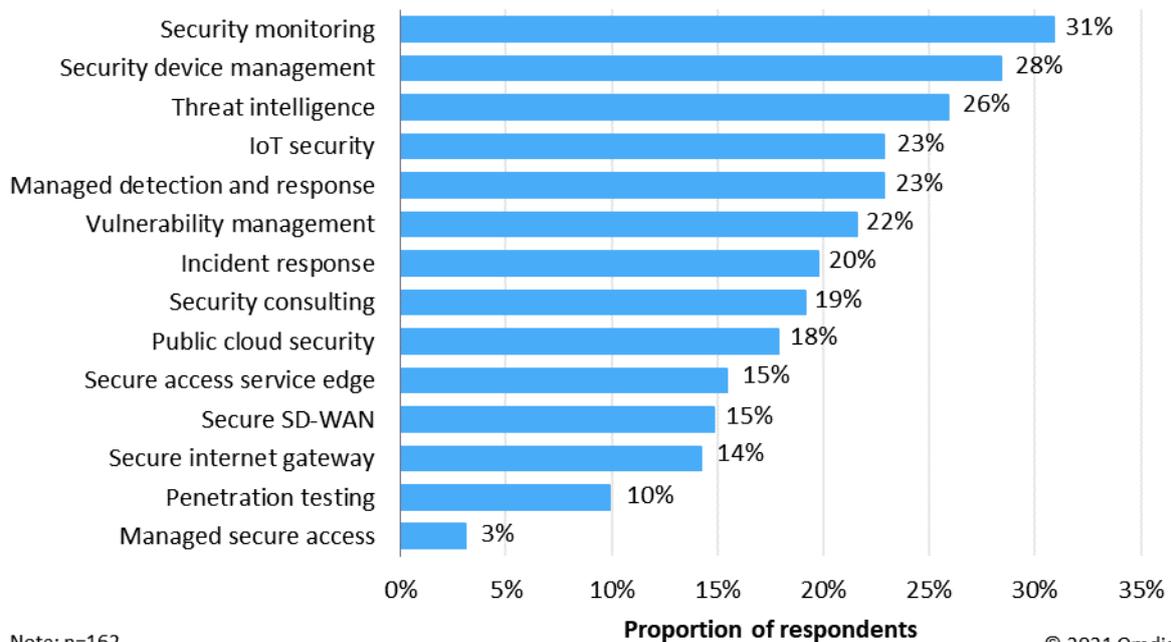
© 2021 Omdia

Source: Omdia

Today, monitoring services and traditional device management services are the most commonly used services and generate the bulk of MSS revenue. We asked MSSPs to get out a crystal ball and identify which services would be most important to customers in 2023. Respondents had to make choices here: they could only choose up to three answers. While the traditional monitoring and management services still lead their thinking in 2023, the answers are reasonably well distributed. Many MSSPs are preparing for a world in which they will have to provide a much more diverse set of security services.

Figure 4: MSSP: What services are important to customers?

Which three of the following types of services do expect will be most important to your customers by the end of 2023?



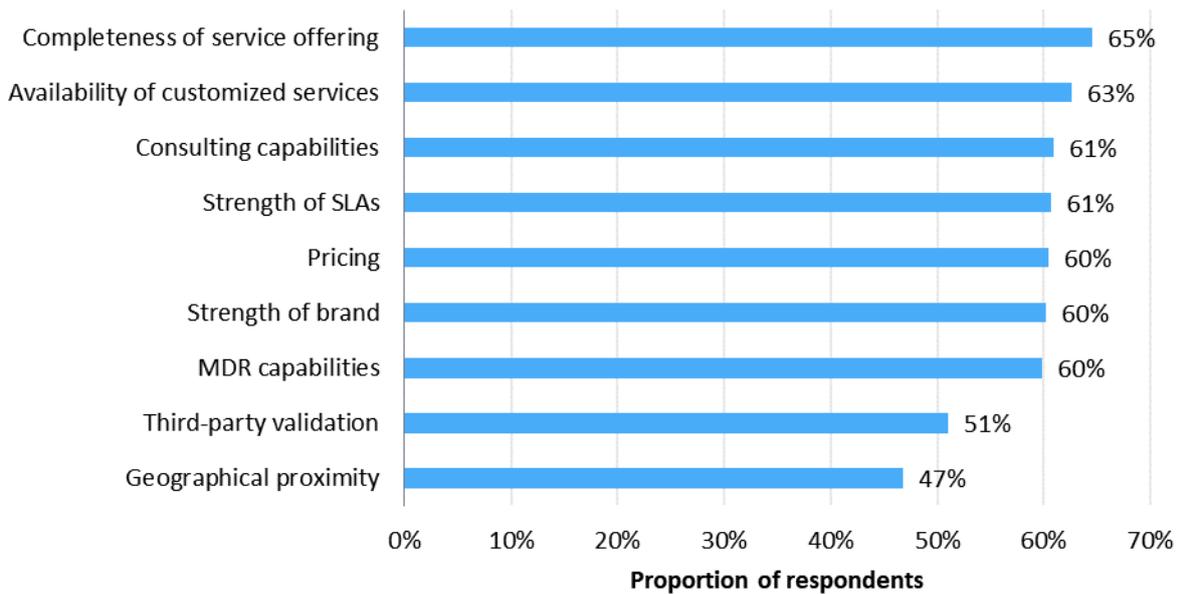
Source: Omdia

Finally for this state of managed security services snapshot, we asked the enterprise respondents how they select the MSSPs they use. We gave respondents a list of common factors for selecting an MSSP and asked them to rate each factor on a scale of 1 to 7, where 1 was “not a driver” and 7 is a “strong driver.” **Figure 5** shows the percentage of respondents that consider each factor an important driver (meaning they rated it 6 or 7).

As with drivers for investing in managed services, respondents have high expectations for their chosen MSSPs. They are looking for a single provider that has a complete offering with the ability to customize and do consulting as needed. Geographical proximity was the least important on the list here, but with many large service providers and MSSPs building their edge networks and getting physically closer to many customer locations, proximity and its impact on performance are likely to become more important.

Figure 5: Enterprise: Drivers for increased use of MSS

On a scale of 1 to 7, please rate the following factors in your decision when selecting a managed security service provider.



Note: n=834

© 2021 Omdia

Source: Omdia

In a separate question, we asked what would cause respondents to switch MSSPs, and three cases topped the list at about 50% of respondents: a breach, cost, or access to new technology. The massive digital/cloud transformation presents IT organizations with an opportunity to reevaluate how they do everything, including selecting MSSPs and using managed security services.

We have hinted that customers and MSSPs may not be exactly in sync, so we asked a series of follow-up questions to both groups about a variety of topics, including two that are absolutely critical today: SASE and MDR.

MSSPs and enterprises agree on the power of MDR

The concept of managed security services came to life in the mid-to-late 90s as many new and already overburdened IT organizations struggled with the rollout of distributed security tools, namely firewalls. As companies rolled internet access out to more sites and locations, they typically discovered they needed protection at every location: the LAN was safe, but it needed to be protected from intruders riding the internet into their offices. Firewall rollouts often also included site-to-site VPNs to further leverage the internet for cheap business connectivity. There was, however, a serious skills shortage, and many customers looked to their ISPs/connectivity providers to deploy and maintain firewalls. The first managed security services were essentially device management, with some light response if there was malicious activity discovered by or related to the firewall.

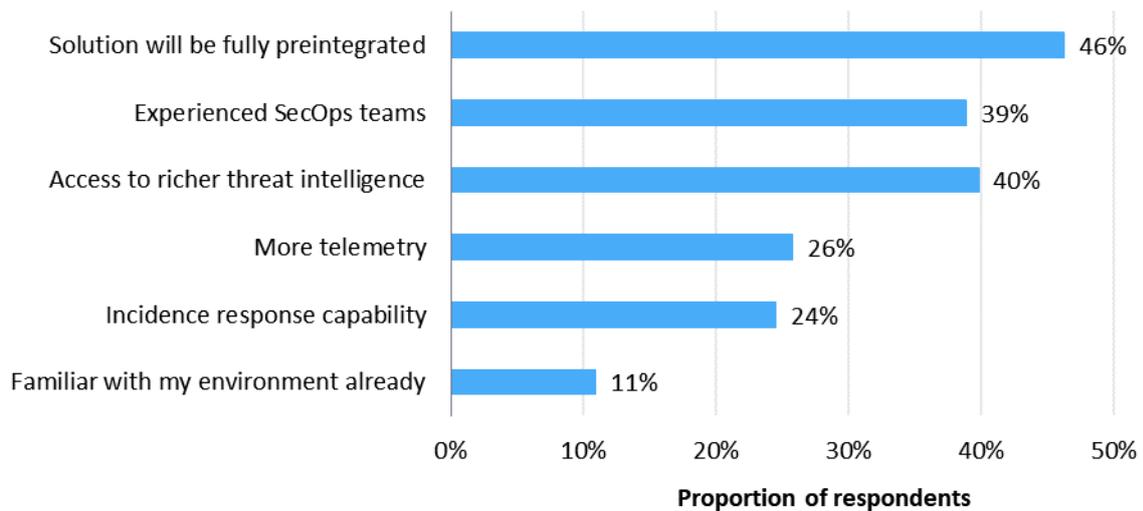
Skip forward nearly 30 years, and most MSSPs have evolved their roles to include much more event detection, correlation, and incident response. Most build security operations centers (SOCs) and use a combination of home-brewed and commercial tools to aid them in helping protect their customers. Along the way, technology vendors innovated endpoint, network, and cloud security tools into what are generally categorized as *detection and response* tools. These tools use a variety of sensors to detect security events in progress and then respond in whatever way is most appropriate (sometimes in an automated fashion) to protect customers quickly and completely. Providers have already started integrating detection and response tools into their arsenal, but they face a new issue: since many MDR tools greatly simplify the detection and response process, many enterprises can now cut services providers out of the deal and handle detection and response on their own or buy MDR solutions directly from the technology vendors. Omdia wanted to see to what degree both enterprises and MSSPs understood this issue and how it was affecting deployments.

We asked our enterprise respondents how many were already buying MDR from an MSSP: 51% already have, and 54% plan to by the end of 2021. The MSSPs' base of MDR customers is not growing the way it should be given how much the overall MDR market is growing right now. Sixty percent of respondents said that MDR capabilities were one of the key drivers in the overall selection process for MSSPs, so it appears many MSSPs need to look (or relook) at the MDR solutions they are (or are not) offering.

In a follow-up question, we asked them what the benefits of buying MDR from their MSSP were.

Figure 6: Enterprise: Benefits of buying MDR from an MSSP

Which of the following are key benefits of buying MDR from a managed security service provider?



Note: n=450

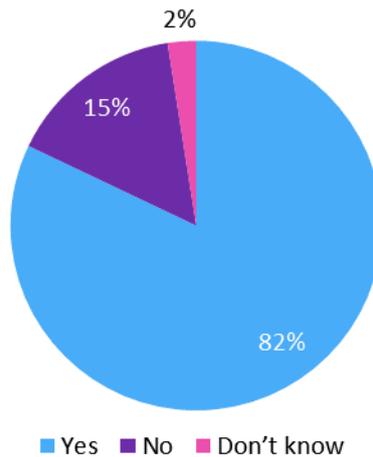
© 2021 Omdia

Source: Omdia

In many cases staff, resource, and skills shortages are behind MSS purchases, and that seems to be the case for MDR as well. Buyers are looking for preintegration to save time and optimize performance of the technology, and they want access to the SecOps teams and larger pool of threat intelligence that MSSPs sit on. Those are the messages that MSSPs should focus on when it comes to MDR. MSSPs are on the same page as customers: 82% believe that MDR solutions are strategic to their business.

Figure 7: MSSP: Is MDR strategic to your business?

Do you think managed detection and response services (MDR) are strategic for your business?



Note: n=162

© 2021 Omdia

Source: Omdia

We followed up by asking respondents how they are building MDR services. Forty percent buy and resell an existing MDR solution, 29% are building their service from the ground up, and 25% plan to do a mix of the two. Since a significant portion of what many MSSPs will be offering as MDR will be repackaged technology from an MDR vendor that also sells to enterprises, it will be critical for MSSPs to clearly explain what value they add in addition. Do they provide access to a larger SOC team? More threat intel? Correlation across multiple customers? MSSPs can also integrate MDR with other security services they are offering to create a more complete and more secure overall solution. In addition, since MDR is still leading-edge technology, customers are still picky about what technology powers an MSSP's MDR service. Providers need to understand which vendors and brands are leading the market and resonating best with customers, because brand could actually drive purchase decisions.

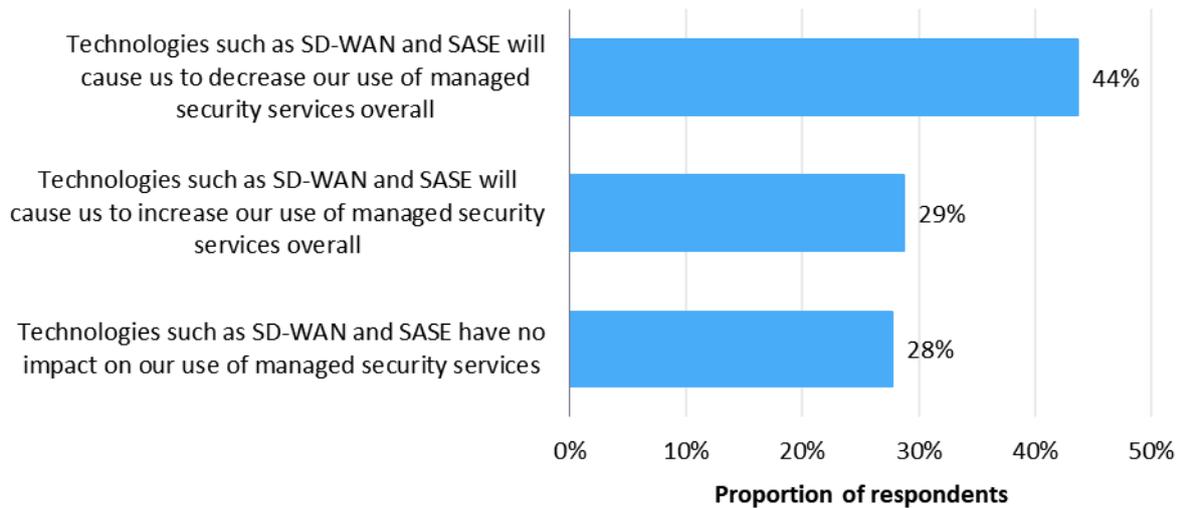
Managed security in the era of distributed secure networking

As with MDR, many MSSPs are already in the secure connectivity business, since VPNs for much of their life were a feature in the firewalls they were managing already. The arrival of SASE, which pairs very popular software-defined WAN (SD-WAN) capabilities with cloud-delivered security (firewall, secure web gateway, cloud access security broker, data loss prevention, etc.), will likely have a huge impact on VPNs and secure connectivity/access in general. The popularity of both SD-WAN and cloud-delivered security grew wildly during the pandemic, and they both make it much easier to deliver IT services to users regardless of location, network, or device. SD-WAN product vendors and cloud-delivered security providers saw massive growth in their business, and an architecture that marries the benefits of both shows great promise for a growing pool of buyers.

Unlike with MDR though, MSSPs are a little less sure of their role in or plans for SASE. Providers going down a pure security route are going all-in on MDR, but many have mixed thoughts about SASE. Omdia asked enterprise respondents whether SD-WAN, cloud-delivered security, and SASE were in their future, and 52% had either already deployed or had plans to deploy soon. Any of these technologies can be purchased from standalone product and software-as-a-service (SaaS) vendors or from an MSSP, so we wanted to understand whether enterprises thought that using them would affect their use of managed services. Forty-four percent thought they would actually decrease their use of managed services as a result.

Figure 8: Enterprise: Thoughts on SASE and managed services

Which of the following statements do you most agree with?



Note: n=834

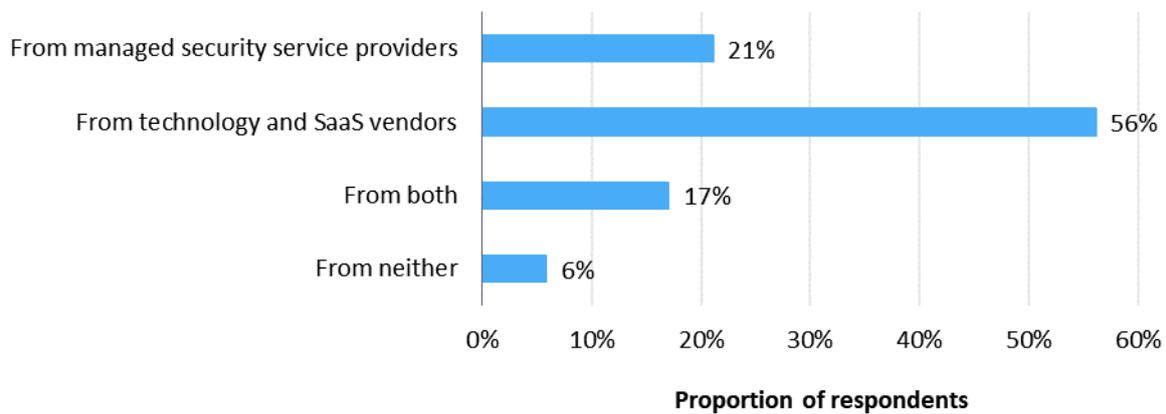
© 2021 Omdia

Source: Omdia

Once deployed, SASE solutions should greatly reduce the cost and complexity of deploying unified secure access while improving their security posture at the same time. The time savings and increased security posture might be enough for enterprises to move away from their MSSP for secure connectivity. We asked respondents outright who they would buy cloud-delivered security or SASE from, and the answer does not look great for MSSPs.

Figure 9: Enterprise: Choosing a security solution provider

How would you buy cloud-delivered security solutions (e.g., SIG and SASE)?



Note: n=834

© 2021 Omdia

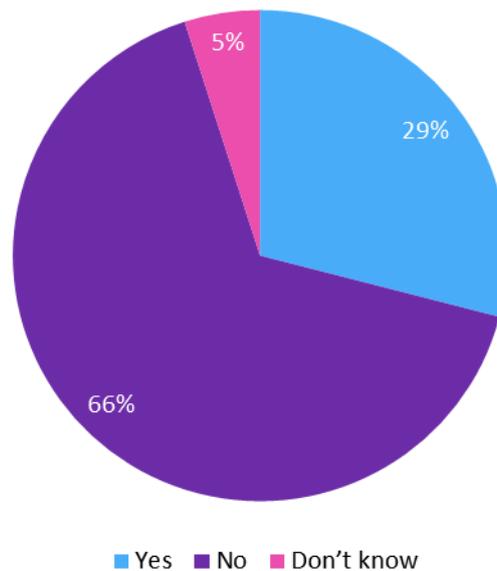
Source: Omdia

Most enterprise respondents expect to buy directly from the technology vendors or service providers. The question is, is this a supply issue or a demand issue? Omdia asked enterprises whether they would buy from an MSSP if it was offered, and an encouraging 41% said they would.

So we turned to MSSPs and asked a similar set of questions, and the results were very different from the results for MDR. A staggering 66% do not believe that buyers will move away from traditional WAN and VPN solutions to SASE by 2023, which is very different from what enterprises told us. Additionally, a move to SASE does not just affect potential revenue for managed VPNs: the cloud-delivered security portion of SASE will in many cases have an impact on managed firewall, managed web security gateway, and a wide variety of other security services that MSSPs rely on for core revenue, because customers that deploy cloud-delivered security do not have boxes on their premises for providers to manage.

Figure 10: MSSP: Will enterprises move to SASE?

Do you believe that most enterprises will migrate away from traditional WAN and remote access VPN solutions to SASE by the end of 2023?



Note: n=162

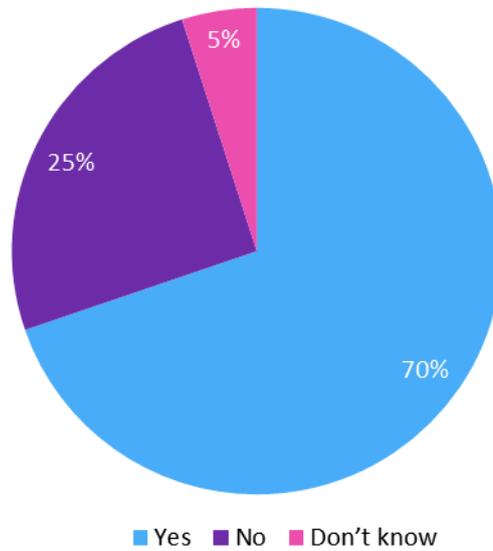
© 2021 Omdia

Source: Omdia

The primary inhibitor for providers not investigating SASE solutions appears to be the SD-WAN/networking side of the business: 40% of MSSP respondents said they plan to focus purely on security services. Another issue is that MSSPs are afraid of cannibalization of revenue: 48% believe that if they deployed SASE services it would cannibalize existing revenue. If MSSPs deploy SASE services, it may cannibalize legacy revenue, but at least they can collect that revenue. If they do not offer SASE solutions, 100% of the revenue generated by customers moving to SASE will end up in someone else's pocket. There is a disconnect though, because Omdia asked MSSP respondents outright whether they believe the vendors offering cloud-delivered security are competitors, and most do. The 30% that answered "no" or "don't know" may want to take a look at how some of the vendors in this space performed in 2020; it might be eye opening.

Figure 11: MSSP: Competition from cloud-delivered security vendors

Do you consider cloud-delivered security companies (e.g., Zscaler) and cloud-delivered security technology solutions (e.g., Palo Alto Networks Prisma Access and Cisco Umbrella) to be competitors to your managed security service business?



Note: n=162

Source: Omdia

© 2021 Omdia

Conclusion: It's all because of the cloud

The cloud is at the heart of the IT transformation that enterprises and service providers are going through right now. Significant portions of infrastructure, critical applications, and data are moving to the cloud. The need for security for cloud applications will be met in many cases by cloud-delivered security services. Cloud technology is at the heart of new security solutions, solutions that can be deployed anywhere and scaled nearly infinitely. In many cases cloud-based data lakes drive the analytics capabilities of MDR/XDR solutions. SASE as an architecture exists because increased use of the cloud eroded traditional perimeters, and the solutions themselves will be powered by and delivered over the cloud in many cases.

Pointing out the role that cloud services and technology play is critical, because at their core, MSS are useful because they preintegrate a complex web of technology and allow customers to focus on their businesses' core competency. In the first 10 years of serious business use of the cloud one thing is clear: the cloud makes security more complex, not less. MSSPs have a unique opportunity to weave cloud-native and cloud-delivered security into their traditional device management services. MSSPs that do not focus on the cloud and new cloud-enabled and cloud-delivered security solutions are simply handing customers to the competition, whether that competition is other MSSPs, security technology companies with cloud security offerings, or pure-play security SaaS vendors.

MDR/XDR and SASE/cloud-delivered security are in high demand today because of two critical drivers for security purchases: the need to significantly improve security efficacy and radical changes in IT architecture driven by development around the cloud. Both solutions will be purchased and deployed by a wide range of enterprise and small and medium-sized (SMB) customers because they simply make sense, and they will buy them whether MSSPs offer them or not. Omdia believes that for MSSPs to be viable moving forward, they need to invest in and greatly bulk up their value propositions around both MDR/XDR and SASE/cloud-delivered security.

Appendix

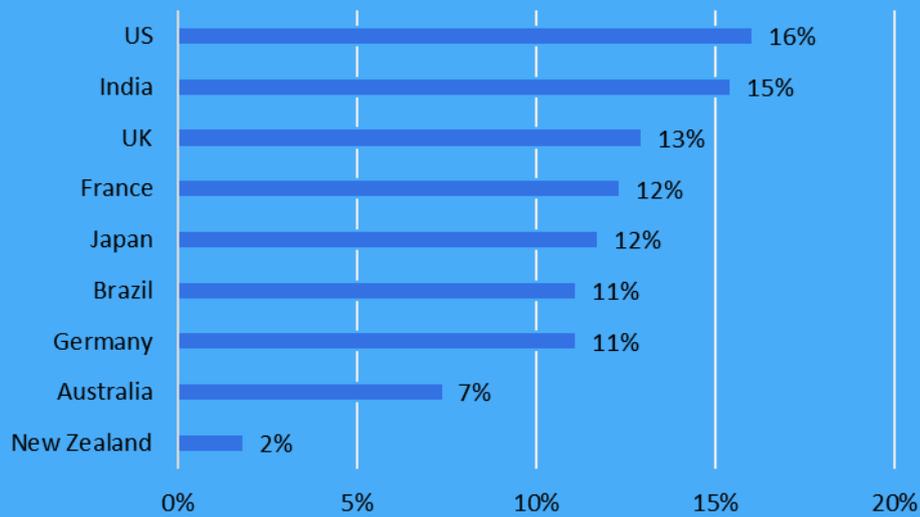
Methodology

Using a panel of qualified security technology decision makers, Omdia conducted a web survey in December 2020 with

- 162 respondents at managed security service providers

- 834 SMB and enterprise managed security service customers

Countries

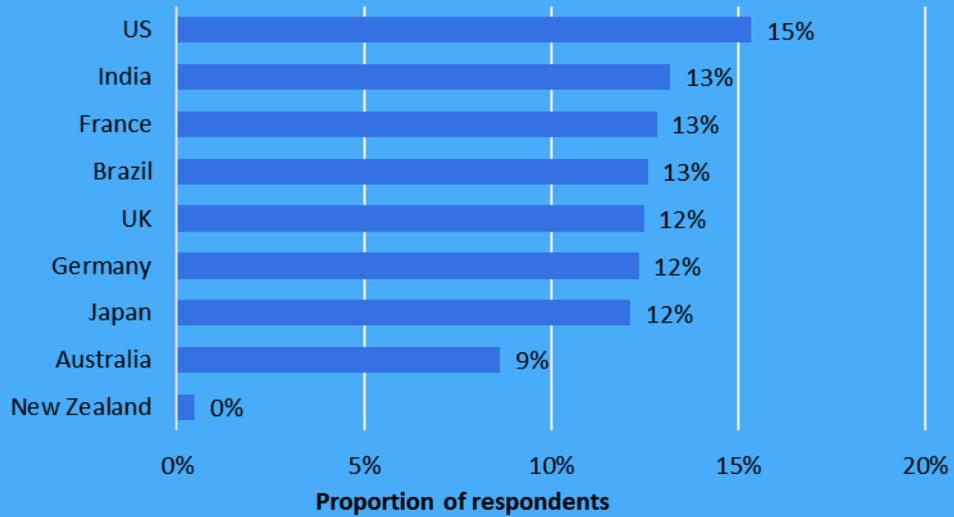


Note: n=162

© 2021 Omdia

Source: Omdia

Countries



Note: n=834

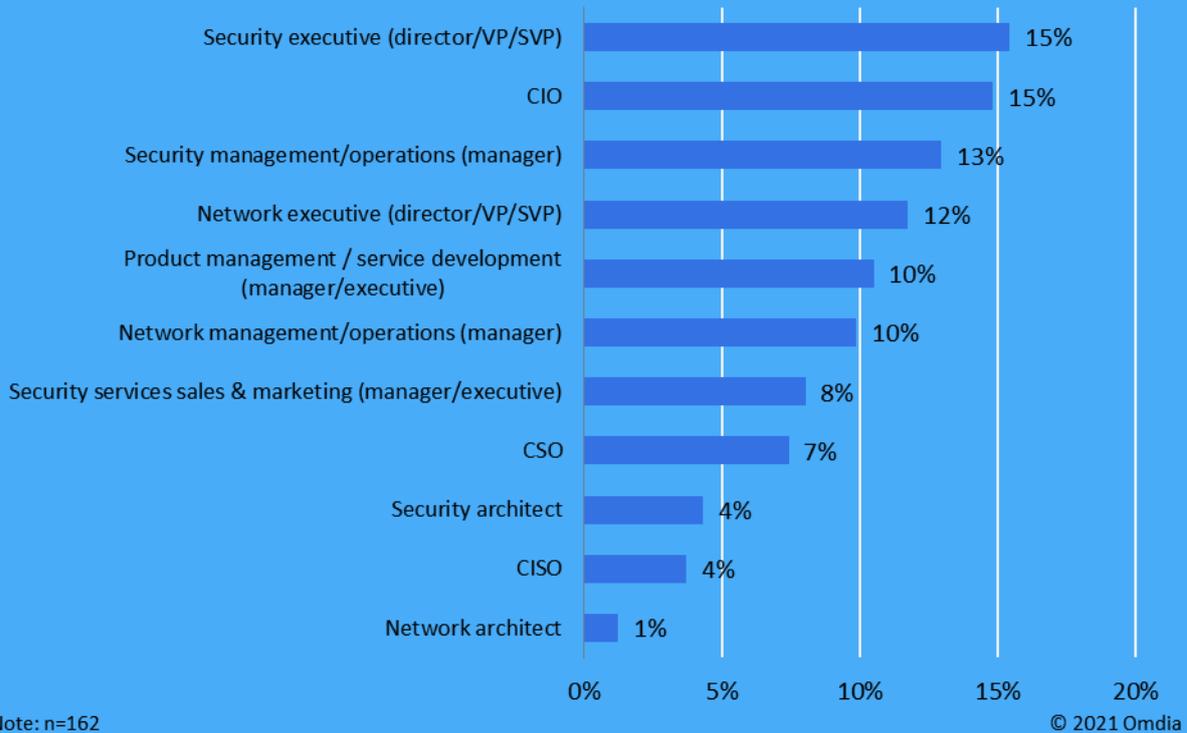
© 2021 Omdia

Source: Omdia

To qualify, respondents needed to be responsible for deploying (MSSP) or purchasing (SMB/enterprise) managed security services at their organizations. They also needed to have detailed knowledge of and purchase decision influence over their organization’s managed security services. This was a key part of the screening process to ensure that we received responses from the knowledgeable decision makers who influence the buying process.

Respondents had to have at least manager-level positions in security or networking, with 64% of respondents having director (or higher) titles; 31% of respondents had architect or C-level titles. Respondents were given no incentives for completing the survey.

What is your role/level within your organization?



Source: Omdia

What is your role/level within your organization?



Source: Omdia

Author

Jeff Wilson

Chief Analyst, Cybersecurity Technology
customersuccess@omdia.com

Get in touch

www.omnia.com
customersuccess@omnia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Fortinet

Fortinet delivers the Fortinet Security Fabric which continuously assesses the risks and automatically adjusts to provide comprehensive real-time protection across the digital attack surface and cycle. Powered by FortiOS, the Fabric is the industry's highest-performing integrated cybersecurity platform with a rich ecosystem. The Fabric enables consistent security across the extended digital attack surface. Seamless interoperability, complete visibility, and granular control are now possible for hybrid deployments including hardware, software, and x-as-a-service across networks, endpoints, and clouds.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, and agents disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.