SOPHOS

MSP Perspectives 2024

Insights into cybersecurity tools, risks, challenges, and business opportunities from 350 MSPs.

A Sophos Whitepaper. May 2024

Introduction

The **MSP Perspectives 2024** report provides insights into five key areas of MSP business:

- RMM and PSA tools
- Cybersecurity management
- MDR services
- Challenges and risks facing MSPs and their customers
- Impact of cyber insurance

Findings are based on learnings from an independent, vendor-agnostic survey of 350 MSPs across the U.S. (200), U.K. (50), Germany (50) and Australia (50). The survey was commissioned by Sophos and conducted by research house Vanson Bourne in March 2024.

350 MSPs
across four countries

U.S.
200 respondents

UK
50 respondents

Germany
50 respondents

Australia
50 respondents

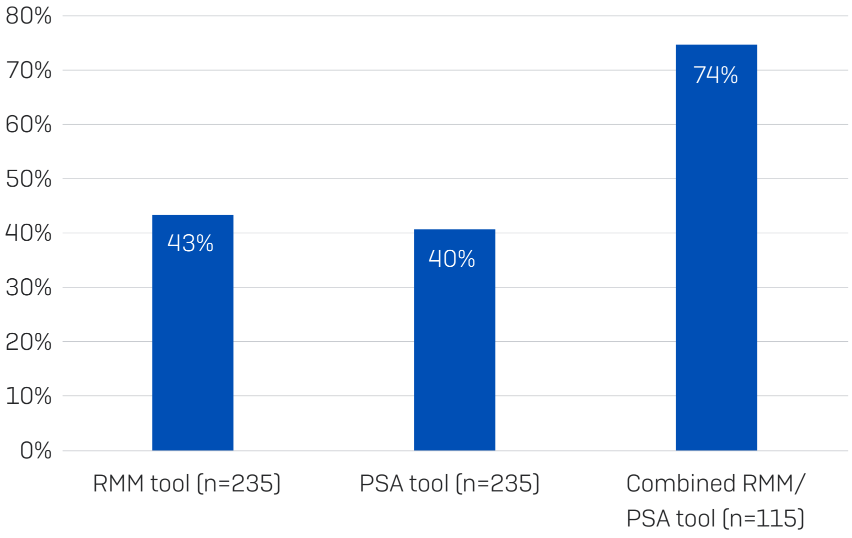
RMM and PSA Tools

Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) tools empower the efficient and effective delivery of MSP services while streamlining operational overheads. The survey revealed two notable insights in relation to these foundational MSP technologies.

Combined RMM/PSA tools deliver much higher levels of satisfaction than standalone tools

Almost three quarters (74%) of MSPs that use a combined RMM/PSA tool are "very satisfied" with their solution, compared to just 43% of MSPs using standalone RMM tools and 40% of those using standalone PSA tools.

Respondents that are 'very satisfied' with their existing RMM and PSA tools

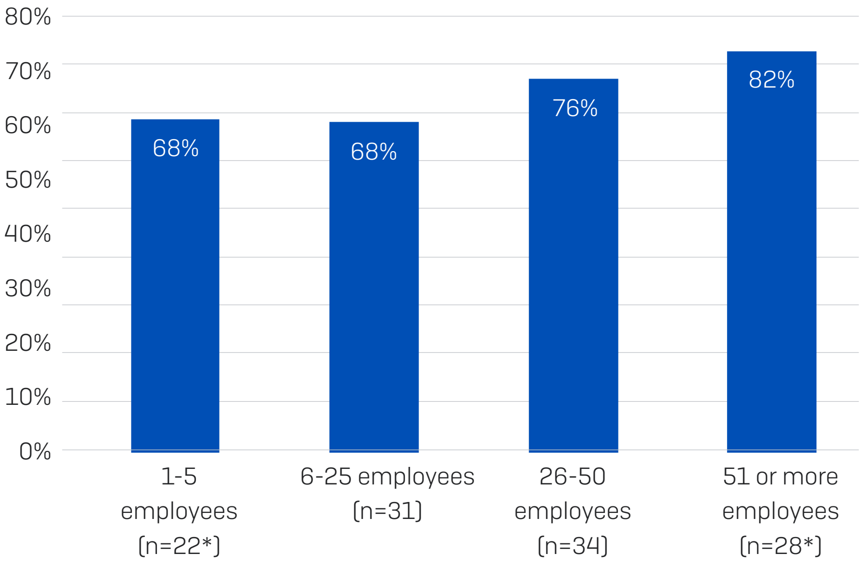


How satisfied is your organization with its existing RMM and PSA tools? Base numbers in chart

Satisfaction with joint RMM/PSA tools increases with MSP size

Just over two thirds (68%) of MSPs with up to 25 employees are very satisfied with their joint RMM/PSA tool, rising to 76% of those with 26-50 employees, and 82% of MSPs with 51 or more employees. With larger MSPs likely supporting a greater number of customers, the findings suggest that the more customers you have, the greater the benefit gained from joint RMM/PSA tools.

Respondents that are 'very happy' with their joint RMM/PSA tool



How satisfied is your organization with its existing RMM and PSA tools? Base numbers in chart.
* The number of respondents in this segment is low so findings should be considered indicative rather than statistically significant.

Recommendation: MSPs using standalone RMM/PSA tools may wish to consider moving to a joint RMM/PSA solution to increase satisfaction, particularly if they are planning to expand their customer base.

Cybersecurity management

Cybersecurity vendor partnerships

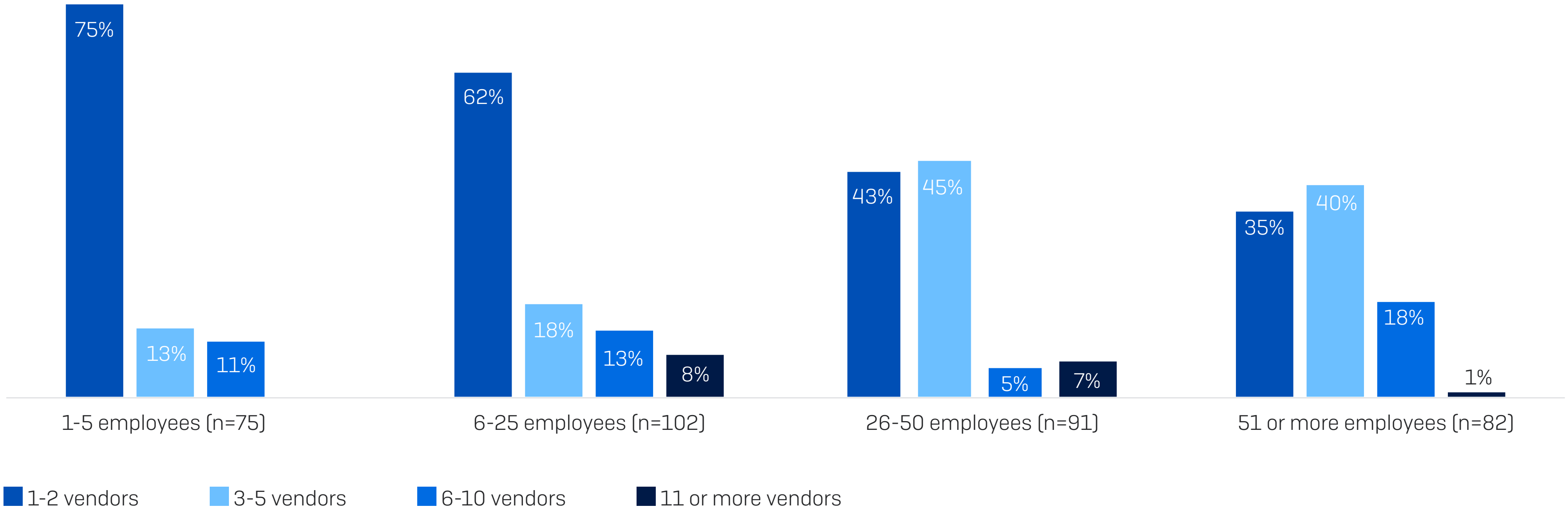
Cybersecurity is a core offering for most MSPs. The study revealed that MSPs typically work with a small number of cybersecurity vendors to protect their customers:

- 53% work with one or two cybersecurity vendors
- 83% work with between one and five cybersecurity vendors
- 4% work with 11 or more cybersecurity vendors

The data also shows that the number of cybersecurity vendors used generally increases with the size of the MSP organization. 75% of the smallest MSPs (1-5 employees) work with one or two cybersecurity vendors, compared to just 35% of MSPs with 51 or more employees.

Conversely, the largest MSPs are almost twice as likely to work with six or more cybersecurity vendors than the smallest (20% with rounding vs. 11%). While working with more cybersecurity vendors may increase the range of services that can be offered, it also likely increases vendor management overheads and the challenges of integrating disparate technologies.

Number of cybersecurity vendors used to protect customers



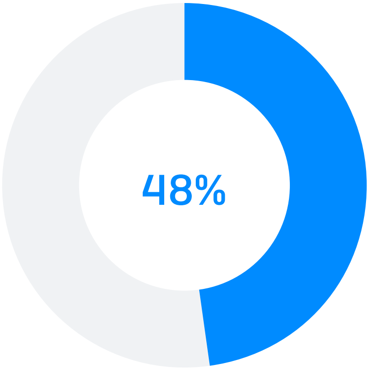
How many cybersecurity vendors does your organization currently use to protect its customers? n=350. Base number in chart. Excludes 'don't know' responses.

Cybersecurity platform consolidation

The survey reveals that there is huge potential for MSPs to increase efficiency and reduce overheads through cybersecurity platform consolidation.

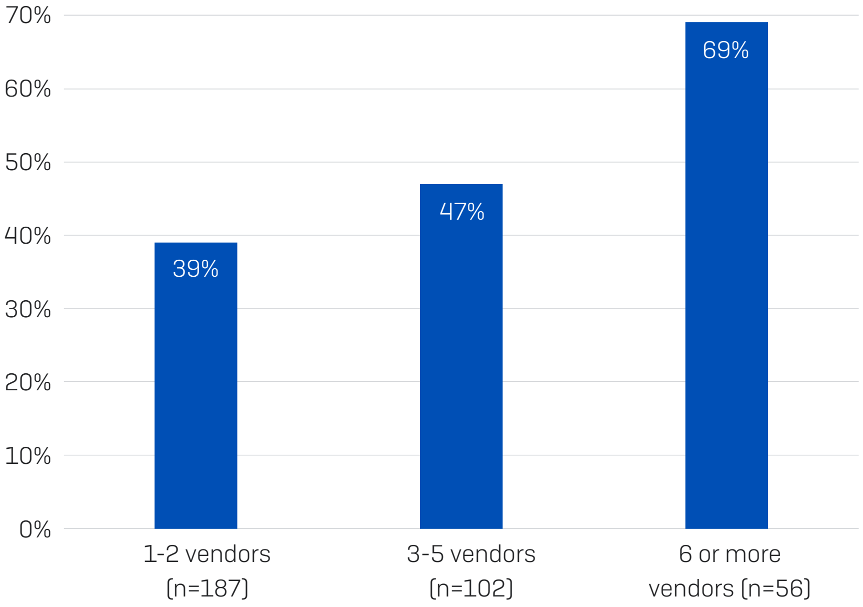
MSPs that are currently using multiple platforms estimate they would save, on average, 48% of their day-to-day management time if they could manage all their cybersecurity tools from a single platform.

Estimated day-to-day management time saving from consolidating on a single cybersecurity platform



Potential management time savings increases with the number of cybersecurity vendors currently used. MSPs that work with six or more cybersecurity vendors anticipate they would cut their day-to-day management time by over two-thirds (69%) if they could manage all their cybersecurity tools from a single platform. Management overhead reductions of this magnitude would make a material difference to profitability while also freeing up team members for revenue-generating activities.

Average estimated day-to-day management time saving from consolidating on a single cybersecurity platform - split by number of vendors used



Please estimate how much management time your organization could save on a day-to-day basis if it could manage all of its cybersecurity tools in a single platform, if any? Base numbers in chart.

Recommendation: MSPs using multiple cybersecurity platforms should explore consolidation options and the TCO savings they could gain by managing all their cybersecurity tools through a single platform.

MDR services

Adoption of MDR services

Demand for managed detection and response (MDR) services is growing fast, driven by the increased complexity of both cyberthreats and the tools and technologies that stop them. Recent Gartner data indicates a total market value of $7.5 billion together with a compound annual growth rate (CAGR) of 25.8%.

With this level of demand and growth, it's not surprising that the majority (81%) of MSPs already offer some level of MDR service, with most others planning to add MDR to their offerings in the near and mid-term. However, the survey did reveal considerable variation in the maturity of MDR service adoption across the four countries surveyed.

MSPs in the U.S. lead the way with almost all (94%) already offering an MDR service, compared to 70% in Germany, 62% in the U.K., and 58% in Australia. Globally, among the MSPs that do not currently offer MDR, almost all plan to add it to their portfolio in the coming years, with almost a third (32%) of U.K. MSPs planning to add MDR in 2024.

	🇺🇸	🇬🇧	🇩🇪	🇦🇺
Currently offer MDR services	**94%**	**62%**	**70%**	**58%**
Plan to add MDR in 2024	5%	32%	20%	18%
Plan to add MDR in 2025 or later	2%	6%	10%	22%

Does your organization currently provide a managed detection and response (MDR) service for its customers? n=350 (U.S, 200, UK 50, Germany 50, Australia 50), excludes some answer options.

Delivery of MDR services

There are three primary models for MSP delivery of MDR services: through the MSP's own security operations center (SOC), via a third-party vendor, and jointly by the MSP SOC and third-party vendor.

The survey reveals that 66% use a third-party vendor to deliver their MDR service, 20% use their own SOC, and 15% use a third-party vendor in tandem with their own SOC. Overall, 80% (with rounding) of MSPs work with a third-party vendor in some capacity to deliver their MDR service.

34% (with rounding) of MSPs have an in-house SOC that delivers MDR services – either standalone or jointly with a third-party vendor. In-house provisioning is remarkably consistent across all organization sizes, with just four percentage points difference between the highest propensity to have an in-house SOC (37% - 26-50 employees) and the lowest (33% - all other bands).

Delivery method of MDR services

MSP's own SOC	3rd party MDR vendor	MSP's SOC and 3rd party MDR vendor
20%	66%	15%

Does your organization currently provide a managed detection and response (MDR) service for its customers? n=282 that provide an MDR service. Excludes some answer options.

Required capabilities from MDR providers

As we've seen, four in five MSPs use third-party vendors to deliver their MDR service. Given the significant and growing demand for MDR services, it's vital that MSPs choose the right provider for them and their clients.

MDR providers act as an extension of the MSP, so their caliber and competence reflect directly on the MSP. Furthermore, the MDR vendor's capabilities impact the range of services the MSP can provide to their clients and the level of work and input the MSP needs to deliver.

24/7 incident response service tops the list of must-have capabilities, with 36% saying it is "essential", rising to 49% in MSPs with 1-5 employees. With 91% of ransomware attacks starting outside standard business hours[1], having round-the-clock coverage is vital to effectively defend an organization. Working with an MDR provider that offers full 24/7 coverage gives MSPs peace of mind that their clients are always protected without the burden of standing up this level of expert provision in-house.

In second place is *Ability to detect account takeover threats in Microsoft 365 and/ or Google Workspace*, with one third (33%) of MSPs saying it is an "essential" requirement and 43% rating it "very important".

The *ability to get additional security tools – in particular firewalls/network security and endpoint protection – from the MDR provider* is also highly requested, with three quarters of respondents rating it "essential or very important". Having the option to work with a single provider for cybersecurity tools and MDR services reduces admin overheads while streamlining operations.

At the same time, the study makes clear that MSPs require flexibility and do not want to be limited in the tools they can use nor obligated to buy cybersecurity tools from their MDR provider. 71% say it is "essential or very important" that the vendor can *use telemetry from their existing security tools for threat detection and response.*

24/7 Incident Response Service is the #1 requirement in an MDR provider

CAPABILITY	"ESSENTIAL"	"ESSENTIAL" OR "VERY IMPORTANT"
24/7 incident response service	36%	74%
Ability to detect account takeover threats in **Microsoft 365 and/ or Google Workspace**	33%	77%
Ability to get **firewall/network security** from the MDR provider	31%	74%
Ability to get **endpoint protection** from the MDR provider	28%	75%
Single console for MDR and other security solutions	28%	74%
Breach **warranty** provision	26%	70%
Ability to use telemetry from **existing security tools** for threat detection and response	25%	71%

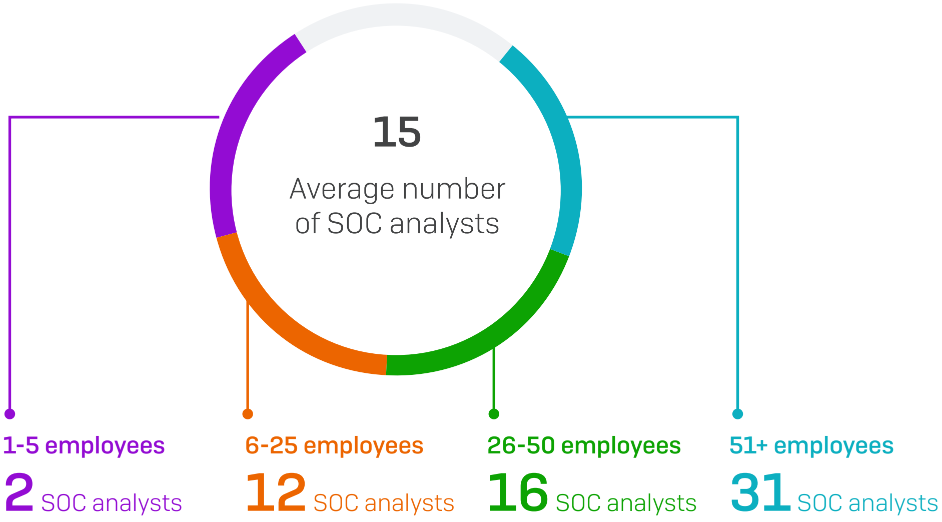
If your organization needs to select an MDR provider, how important is it that the MDR provider offers the following capabilities? n=350 (U.S, 200, UK 50, Germany 50, Australia 50), excludes some answer options.

In-house SOC analysts

34% of MSPs that provide an MDR service have an in-house SOC, which necessitates in-house specialist analysts. The research reveals that a typical MSP SOC has, on average, 15 analysts. However, this number masks considerable variation by organization size.

MSPs with 1-5 employees have, on average, two analysts monitoring their customers' environments and detecting and responding to threats. The number of analysts rises steadily with organization size, with the largest MSPs reporting an average of 31 SOC analysts. Note, the number of respondents in each individual segment is quite low so these findings should be considered indicative rather than statistically significant.

With adversaries deliberately timing their attacks for evenings, weekends, and holidays, 24/7 coverage is essential for an effective MDR service. For smaller MSPs with fewer SOC analysts, in-house-only delivery likely puts huge pressure on their limited resources.



Thinking about your organization's SOC, how many analysts does your organization have monitoring and responding to suspicious events in your customers' environments?

Recommendation: MSPs that do not currently offer MDR services should consider adding it to their portfolio sooner rather than later to avoid being left behind. When selecting a third-party MDR vendor, be sure to identify the capabilities that are important to you and assess providers' abilities to deliver on them.

Challenges and cyber risks

Top challenges facing MSPs today

The MSP world does not stand still. Threats continue to evolve, driving changes and advancements to cybersecurity controls and client needs.

The survey reveals that *keeping up with the latest cybersecurity solutions/ technologies* is the biggest challenge facing MSPs today – both in terms of their single biggest challenge and their top three challenges.

Given the speed of innovation in this space, it is unsurprising that many MSPs are struggling to keep up. As threats evolve, so do the cyber controls that stop them. Existing technologies gain new capabilities while brand new products are regularly released to the market. Keeping on top of all these developments is both difficult and time consuming.

Difficulty securing sufficient cybersecurity analyst resources is at the heart of the second biggest challenge facing MSPs today:

- *Providing out-of-hours coverage (including evening and weekends)* is MSPs' #2 single biggest challenge
- *Adding new cybersecurity analysts to keep pace with growth* is #2 on the top-three challenges list

Specialist cybersecurity analysts are in short supply and command high salaries. Compounding the challenge, full 24/7 coverage requires a minimum of 5-6 analysts, which is a tall ask for many MSPs.

Single Biggest Challenge

#1	Keeping up with the latest cybersecurity solutions/ technologies
#2	Providing out-of-hours coverage (inc. evenings, weekends and holidays)
#3	Winning new customers

Top-Three Challenges

#1	Keeping up with the latest cybersecurity solutions/ technologies
#2	Adding new cybersecurity analysts to keep pace with customer growth
#3	Keeping up with the latest cyberthreats

Thinking about your organization, what are the top challenges your organization is facing day-to-day? Please rank your top three. n=350

Cyber risks

The survey explored what MSPs perceive to be the biggest cyber risks to both their own organizations and to their clients. The results reveal both areas of commonality and of difference.

Two factors topped the list for both MSPs and their clients:

- Stolen access data and credentials
- Shortage of in-house cybersecurity skills/expertise

Adversaries don't break into organizations – they log in. Using stolen access data and credentials, often purchased on the dark web from an initial access broker (IAB), they impersonate legitimate employees to penetrate their target. As evidenced in Sophos' State of Ransomware 2024 report, 29% of ransomware attacks last year started with compromised credentials, indicating the scale of the challenge.

MSPs

Single Biggest Risk		Top-Three Risks	
#1=	Shortage of in-house cybersecurity skills/ expertise	#1	Stolen access data and credentials
#1=	Insecure wireless networking	#2	Security tool misconfiguration
#3	Shortage of cybersecurity tools	#3	Insecure wireless networking

MSP Clients

Single Biggest Risk		Top-Three Risks	
#1	Shortage of in-house cybersecurity skills/ expertise	#1	Stolen access data and credentials
#2	Unpatched vulnerabilities	#2	Shortage of cybersecurity tools
#3	Remote access tools	#3	Unpatched vulnerabilities

Who or what do you consider to be the biggest cybersecurity risks for your organization/your organization's clients? n=350

Despite continual advances in cybersecurity technology and artificial intelligence, humans remain central to effective cybersecurity. Skilled professionals need to configure, deploy, manage, respond to, and update technology solutions. And technology alone cannot automatically stop every cyberthreat. The shortage of skilled professionals is well-known, and organizations are increasingly turning to MSPs to fill the gaps, exacerbating the challenge.

While the top perceived risks are common for both MSPs and their clients, when we move down the rating differences emerge.

Insecure wireless networking is a leading perceived cyber risk for MSPs (joint #1 "single biggest risk", #3 of the "top three risks"). Using insecure networks can lead to several dangers, including data being intercepted and used to extract login and password information that enables adversaries to access personal and business accounts.

Security tool misconfiguration is also a top perceived risk for MSPs. Firewalls, endpoint protection, and other tools only work if they are correctly configured.

Unpatched vulnerabilities are one of the top perceived risks for MSP clients (#2 "single biggest risk", #3 of the "top-three risks"). With 32% of ransomware attacks in the last year starting with the exploitation of an unpatched vulnerability, MSPs are wise to consider this a major danger to their clients.

Recommendation: To minimize vendor and day-to-day management overheads in the face of this broad range of risks and challenges, MSPs should look for cybersecurity partners that offer a full range of services and tools. Deploying solutions that combine robust, adaptive protection from evolving threats without the need for complex configuration and deployments will make it easier to keep up. Furthermore, MSPs should take advantage of MDR providers to expand and extend their in-house cybersecurity skills and expertise, with a focus on partners that support their business model and can adapt to their needs as they change and grow.

Impact of cyber insurance

The use of cyber insurance to transfer cyber risk has increased steadily, with 90% of mid-sized organizations now having some form of coverage according to Sophos research. 50% have a standalone cyber insurance policy while 40% have cyber coverage as part of a wider business insurance policy, such as a general liability policy.

The widespread adoption of cyber insurance is driving high levels of channel engagement, with 99% of MSPs reporting an increase in demand for support and solutions to meet cyber insurance requirements.

Globally, the most common request (47%) is from clients looking to implement an MDR service to improve their insurability, followed closely by customers needing help completing their insurance application (45%). Both these requirements provide major revenue-generating opportunities for MSPs by way of MDR delivery and professional services billings.

CUSTOMER NEED	GLOBAL	🇺🇸	🇬🇧	🇩🇪	🇦🇺
To **get MDR** to improve insurability	**47%**	49%	38%	56%	36%
Help completing insurance **application**	**45%**	49%	46%	30%	42%
To get **EDR** to improve insurability	**34%**	31%	32%	28%	52%
To get **non-EDR/MDR** technologies and services to improve their insurability	**33%**	31%	22%	48%	40%

Has your organization seen an increased need for support and solutions to meet cybersecurity requirements from your customers? n=350 (U.S, 200, UK 50, Germany 50, Australia 50).

One third (34%) of MSPs report clients looking to add endpoint detection and response (EDR) to their security stacks to improve insurability. It is interesting to note that, outside Australia, insurance-driven demand for MDR is considerably greater than demand for EDR, reflecting the greater risk reduction a specialist 24/7 MDR service can deliver over a stretched in-house team.

One third (33%) of respondents reported that they had seen increased demand for non-EDR/MDR technologies and services from clients wanting to improve their insurability. While the study didn't explore this further, requirements are likely to include multi-factor authentication (MFA) tools, email, and network security – all commonly required/desired by insurance providers.

Recommendation: The provision of services and technologies that improve insurability is a major opportunity for MSPs, and organizations should look to optimize their support in this area to maximize revenue potential.

Conclusion

In the face of inevitable cyberattacks, MSPs have many opportunities to grow their businesses and improve profitability. From reducing day-to-day overheads through management platform consolidation, to optimizing engagement with third-party MDR vendors to expand their service offerings, to aligning activities to cyber insurance needs, MSPs can advance their businesses while elevating their clients' protection against ransomware and breaches.

The MSP market can be a competitive environment. Leveraging these insights to accelerate and grow, MSPs can take full advantage of the opportunities ahead.

Sophos MSP Program

Sophos helps MSPs grow their businesses and increase profitability. Innovative, adaptive defenses and a complete MSP cybersecurity system deliver cyber confidence that empowers success.

- With a complete portfolio of cybersecurity services and products at your fingertips, you can be sure to your clients' current and future needs
- Minimize day-to-day management overhead and free-up billable hours with the Sophos Central security platform that enables you to manage all your clients' security in a single console
- Enjoy attractive margins, lucrative incentives, and aggregate billing with the Sophos MSP Program

To learn more about the Sophos MSP program, visit sophos.com/MSP and to explore Sophos MDR, visit sophos.com/MDR

Sophos MDR: 24/7 Incident Response as standard

Sophos MDR is the world's most trusted managed detection and response service, used by more organizations than any other provider. With 24/7 detection and hands-on response included as standard, MSPs and their clients enjoy the peace of mind that Sophos experts are on hand to stop attacks at any time of the day or night. Highlights include:

- 24/7 hands-on-keyboard remediation
- Comprehensive incident response
- 24/7 direct call-in support
- Dedicated incident response lead
- Choice of response modes
- Breach warranty provision
- Proactive threat hunting
- Works with Sophos and non-Sophos endpoint protection
- Detects account takeovers in Microsoft 365 and Google Workspace
- And much more.

Whether you're looking for a fully outsourced service, or a flexible extension to your in-house SOC, Sophos MDR can help you grow your business.

> *"Sophos MDR saved several clients from potentially catastrophic business failures. Our margins have increased 100%, while revenue has seen a 300% increase."*
>
> James Wagner, President, The ITeam

[1] Active Adversary Report for Business Leaders, Sophos, 2023

2024-05-21 (WP-NP)