THE MSP HORIZONS REPORT 2025

Future IT insights
to take action today

N-ABLE™

Table of Contents

A note on quotes:

All quotes referenced in these pages were taken directly from live interviews conducted with IT professionals for the purpose of creating this report.

Securing the Future

Welcome to the 2025 N-able MSP Horizons Report.

This annual report aims to provide MSPs with key insights—both from a technology and go-to-market perspective—on where to invest over the next three to five years to drive sustained growth.

A central theme of this year's report is cyber resilience. As cyber threats grow more complex, compliance requirements tighten, and data breach liabilities increase for both MSPs and their customers, a constant trend remains: cybersecurity is a key revenue driver. In fact, 90% of survey respondents expect cybersecurity services to grow, up from 80% last year.

Conversations with MSPs worldwide make it clear that the line between IT operations and security operations has blurred. A strong security offering is no longer optional – it's essential. The leading MSPs differentiate themselves by addressing security across the entire attack lifecycle: from protection and detection to response and recovery.

When it comes to cybersecurity: "good enough" is no longer good enough.

MSPs need the right tools to stay ahead of threat actors—not only securing their customers' environments but also meeting increasing compliance demands that impact both their customers and their own businesses.

That's why we are committed to an end-to-end approach to cyber resilience. Our vision is reflected in strategic moves like our recent acquisition of XDR/MDR provider Adlumin, continued investment in Cove Data Protection, and broader innovations designed to strengthen our leading security posture.

Beyond security, MSPs face operational complexity when deploying third-party solutions. Unfortunately, technologies from different vendors don't always integrate smoothly, leading to inefficiencies. That's why we embrace an open ecosystem philosophy—to help ensure our products integrate seamlessly with the tools MSPs rely on most. This gives you the flexibility to build the right tech stack and maintain control over your business's success.

A central theme of this year's report is cyber resilience.

Despite constant change, the MSP industry continues to prove its value as a critical force in keeping everyday businesses secure. You are the essential partner in the global business landscape.

We are excited to support you at every stage of your growth journey. We hope this report provides valuable insights to help guide your business to its next level of success.

Forward Together,

John Pagliuca

John Pagliuca, CEO, N-able

Executive Summary

As the second annual MSP Horizons Report reveals, change continues to be a consistent theme for managed services providers. However, they are rising to the challenge to provide an increasingly valuable array of both IT management and security services, which are helping to build resilience for the small and medium enterprises they serve across the globe.

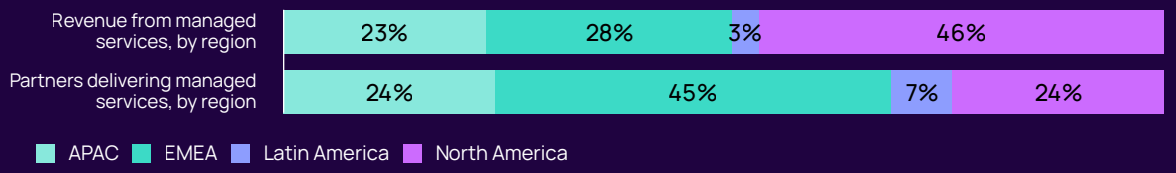
If we take a broader look at how the industry has performed, in 2024 Canalys estimates managed services revenue globally grew just under 11% year-on-year. While macro-economic and political volatility may have had a significant influence on customer spending levels, there have been pockets of success. For example, AI has been everywhere, and managed services partners are still exploring a wide range of both internal and external use cases that could bring real-time cost savings for themselves and their customers. Overall, there's no denying 2024 was a more difficult year than 2023 globally for managed services (and IT in general), however, the outlook for 2025 is more positive, with 39% of MSP respondents projecting managed services revenue growth at 20%.

338,717
the number of channel partners that are delivering IT managed services.

+11% from 2023

$525 billion
the value (in USD) of managed IT services delivered by channel partners globally.

Managed Services at a glance



What's driving MSP optimism and where are the challenges?

Endpoint and cybersecurity are star growth levers

While network services may be the top driver for managed services revenue today, over the next three years the industry is expecting to see this drop significantly in favor of endpoint services, with managed endpoint services (PC, smartphone, device as a service) and endpoint security topping the list of services MSPs will be looking to offer. Indeed, cybersecurity in general continues to be key to managed services growth for the foreseeable future, and opportunities also continue to grow for cloud infrastructure, and SaaS and AI-powered backup.

The hidden opportunities in compliance

In the past 12 months, regulation and compliance have really started to make their mark on everyone involved in IT; becoming more difficult to manage across the board. However, there are also more vendors offering compliance-as-

Nearly 40% project **managed services revenue growth** at 20%

Top tech growth areas
for managed services in 3 years

- Managed endpoint services
- Endpoint security
- Managed BDR
- Network security

showed interest in **M&A**, significantly up from last year

+10% YoY

Cybersecurity managed services sales growth expected, rising from **80% to 90% of partners**

+17 points

Co-managed go-to-market models working alongside customers expected to rise (+17 points) in 2025

+6 points

More **MDR** (+6 points) to be delivered via third-party

Top two challenges

New Customer Aquisition

Staff Upskilling

service tools, too. This is creating a trade-off between tool sprawl and exploiting the growing demand for compliance consulting and managed services, one of which is complicated further by the growing number of insurance companies competing with channel partners to offer their own risk management and compliance services. There is no denying, though, that this is going to be a big area for MSPs over the coming years.

Change isn't just good. It's necessary.

Elsewhere, the co-managed IT model is expected to see even higher adoption (+17 pts from 2024), with co-partnering dropping (-14 pts) in 2025, and M&A is back on the agenda after a fallow year in 2024. But the risks are also increasing and MSPs are struggling with new customer acquisition, skills, compliance, and cost controls. In a time when the barrier to entry to being an MSP is as low as ever, being a good MSP has never been harder. Being a great MSP means resolving challenges by strategically embracing change.

It's about long-term investment vs. shortcuts

Over the course of this report, we'll dive into what's driving the changes in the industry and what MSPs need to be focusing on in order to continue to drive growth in the short to medium term, as well as what technologies they need to be investing in to stay relevant to the needs of their customers.

As we move further ahead, partners must understand how their customers want to buy. Over the past five years, MSPs have been trying to achieve the simplified, single offering service stacks that were deemed to be best practice for building a profitable MSP. But with the advent of younger IT buyers, and cloud SaaS marketplaces, many want to pick and choose what they want from their MSP, tailoring it to fit their exact IT needs. This means it will be even more important for MSPs to understand the profit margins of every element of their stacks, as well as ensuring that they are adding tools that integrate well together. There is, and always will be, a trade-off between offering bespoke IT managed services and a simplified IT stack with a cybersecurity wrap.

There will almost certainly be strong growth in 2025 for MSPs, and as long as partners continue to invest in internal AI capabilities and cyber risk offerings for customers – as well as understanding three things: their customer, their profit model, and their risk exposure – they can stay ahead of the curve.

The data in this report has been gathered through an extensive global survey of managed services providers as well as in-depth interviews.

SECTION 1

Managed Services Business

How to Go from Surviving to Thriving

Introduction

The evolving MSP landscape is characterized by several factors including cybersecurity, collaboration, upskilling, and strategic consolidation. Most MSPs are prioritizing in-house resources to deliver services, yet there is a rise in co-managed services highlighting a shift toward collaborative models. To sustain growth, MSPs must overcome hurdles like acquiring new customers in a competitive market, bridging skills gaps, and addressing customers' cybersecurity vulnerabilities. To navigate present challenges, MSPs are eyeing mergers and acquisitions (M&A) as a way to access new customers, technical expertise, and geographic expansion while enabling broader service delivery.

Key Takeaways

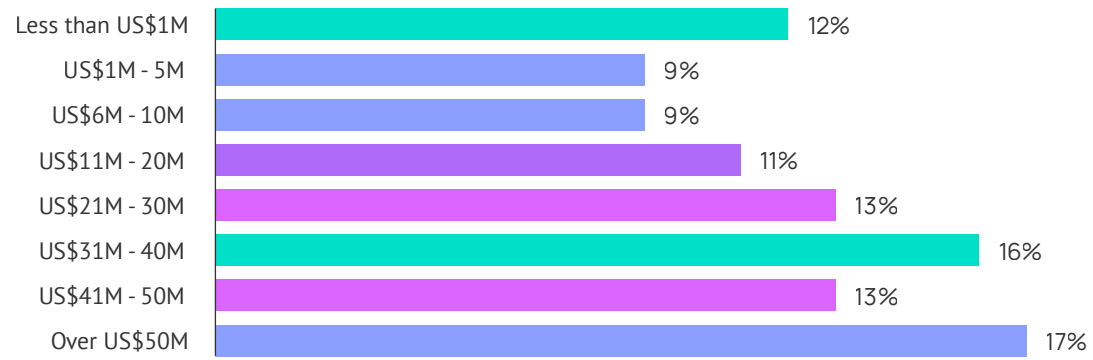
- 90% of MSPs surveyed are expecting growth in their managed security services revenue over the next three years (up from 80% in last year's report).
- 59% believe their revenue will grow more than 20% year on year in 2025.
- Some of the fastest growing areas of investment for MSPs are in automation, as they explore every avenue to minimize administrative and low-level management overheads.
- Product commoditization and standardization of IT support services have put pressure on MSPs to master a broad ecosystem today that is only going to become more complex.
- The co-management model is growing and can act as a launch pad, opening the door for MSPs to enter new markets and verticals.
- MSPs must invest in their current staff by providing them with the proper upskilling, training, certifications and development programs, so they avoid becoming obsolete.
- M&A is back on the table. When asked if they were looking to acquire any other MSPs within the next three years, a resounding 90% (up from 44% last year) stated they were.

OBSERVATION

MSPs expect strong growth revenue in 2025. Here's why.

FIGURE 1

How much overall revenue will you make in 2025?



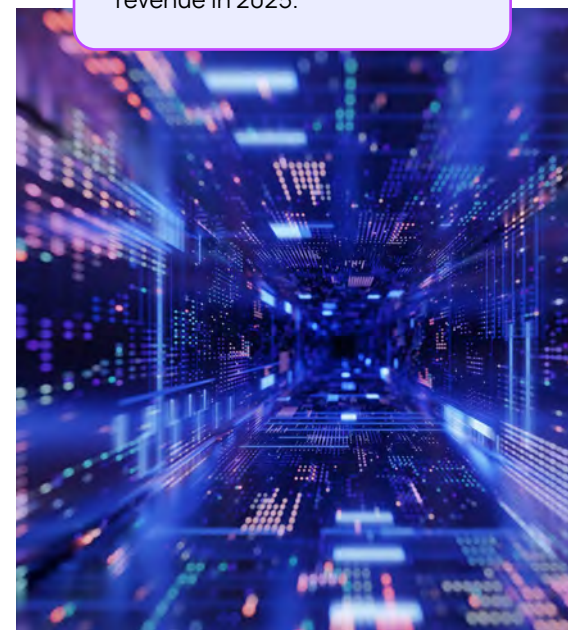
Source: Canalys, Candefero survey, 449 respondents, October 2024 to November 2024

59%
of partners said their revenue would grow more than 20% year on year in 2025.

Canalys estimates 96% of all channel partners globally make less than US $5m from IT managed services. However, respondents in this survey were fairly evenly distributed across the revenue bands, as only 21% said they fell into this category. Another 20% of partners said they made between US $5M and US $20M, with 59% of respondents saying they made more than US $20M from managed services.

When comparing growth expectations for the following year with the previous MSP Horizons Report (released at the beginning of 2024), the numbers are very encouraging. In last year's report, 77% of partners said they would see their revenue grow up to 20%, with respondents split evenly between 1-10% and 11-20% growth. This year only 37% believe their revenue will grow below 20%, while 59% of partners said their revenue would grow more than 20% year on year in 2025.

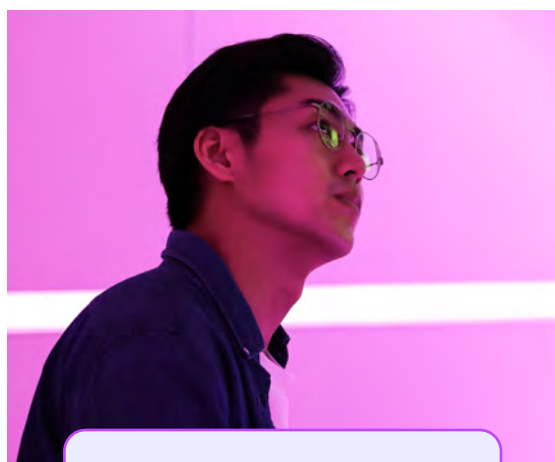
49%
of channel partners in this survey expect growth greater than 20% in managed services revenue in 2025.



The picture is similar for managed services revenue, only 12% expected growth to be over 20% in managed services revenue. In 2025, that number has grown significantly — 49% of channel partners in this survey expect growth greater than 20% in managed services revenue in 2025. The word is out, and the picture is clear: 2025 will be a strong year for the IT channel, and partners selling managed services will be front and center of that growth.

It is also important that partners grow profitably. In any given quarter approximately 20% of all MSPs are not regularly profitable, and in key areas such as cybersecurity services only 24% of partners are hitting the industry standard watermark of 40% service gross margin (which is a key step in producing that net profitability) according to the latest Canalys data.

It is encouraging, therefore, to see 52% of partners in this study saying they will grow gross profit by more than 20% in 2025, with 40% seeing the same growth in managed services profitability.



52%
of partners in this study saying they will grow gross profit by more than 20% in 2025

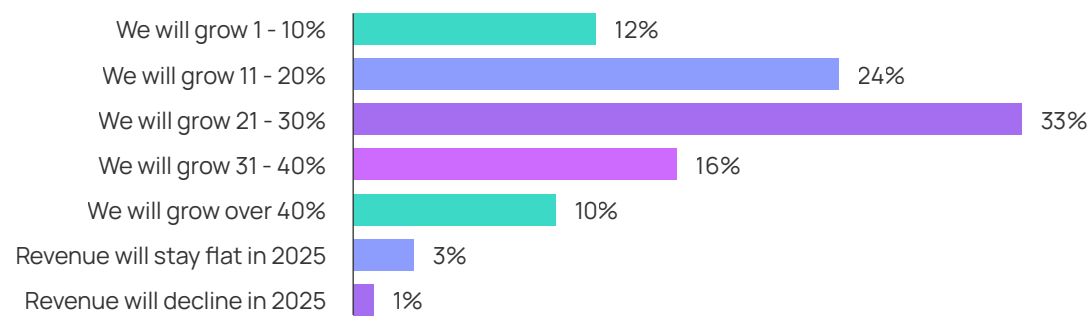
The managed services model is in constant evolution, and there is an acceleration towards tech and services stack rationalization. Some of the fastest growing areas of investment for MSPs are in automation, as they explore every avenue to minimize administrative and low-level management overheads. Partners are not yet at the point of replacing staff with AI, something many worry may eventually be a reality. For now, MSPs en masse are leveraging AI to build workflow automations, automate parts of the sales process, and ticketing. Vendors are investing in this too. In the RMM and PSA spaces the most common vendor product improvements in 2024 have been around AI in ticket response automation, backup automation, patch monitoring and deployment, and managed detection and response.

The key impact of AI on business and revenue models, and profitability in particular, should not be to replace staff but to redeploy their valuable skills to areas of value generation and customer experience management. The ultimate goal for an MSP is to specialize in high-value and complex technology areas which customers are unlikely to manage themselves, and to be able to keep ahead of the tech curve. Any MSP that can achieve this makes itself harder to replace, something which has been a major issue in 2024 as customers spent more time scrutinizing their costs.

49%
of channel partners in this survey expect growth greater than 20% in managed services revenue in 2025.

FIGURE 2

By how much will your overall revenue grow in 2025?

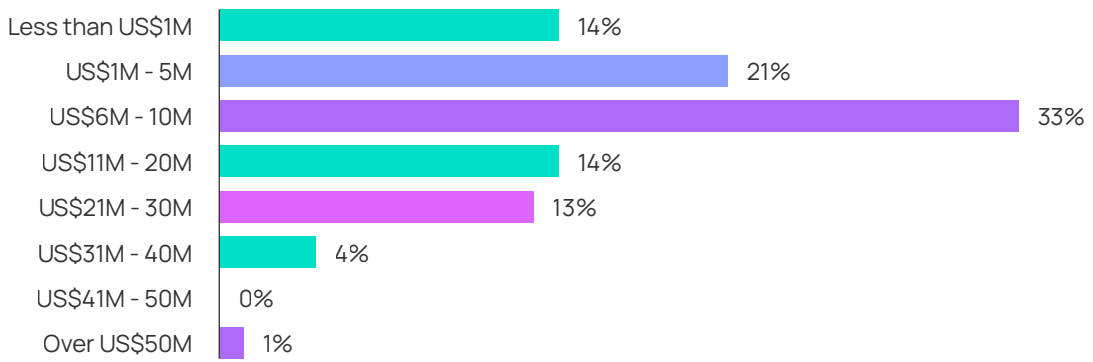


Source: Canalys, Candefero survey, 440 respondents, October 2024 to November 2024

Customer churn has been a feature of 2024, according to Canalys' conversations with partners, and while Canalys believes this is unlikely to be as high in 2025 it is important MSPs improve customer retention rates. Profits are tied directly to retention, and revenue growth is much easier and cheaper to achieve if net retention is above 90% rather than below. To achieve this, MSPs must go beyond managing IT in the long run.

FIGURE 3

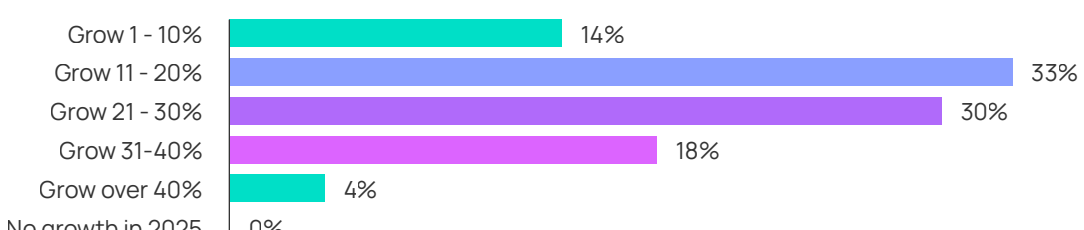
How much managed services revenue will you make in 2025?



Source: Canalys, Candefero survey, 449 respondents, October 2024 to November 2024

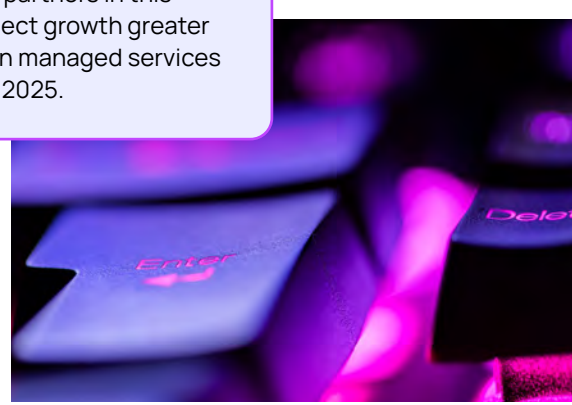
FIGURE 4

How much managed services revenue will you make in 2025?



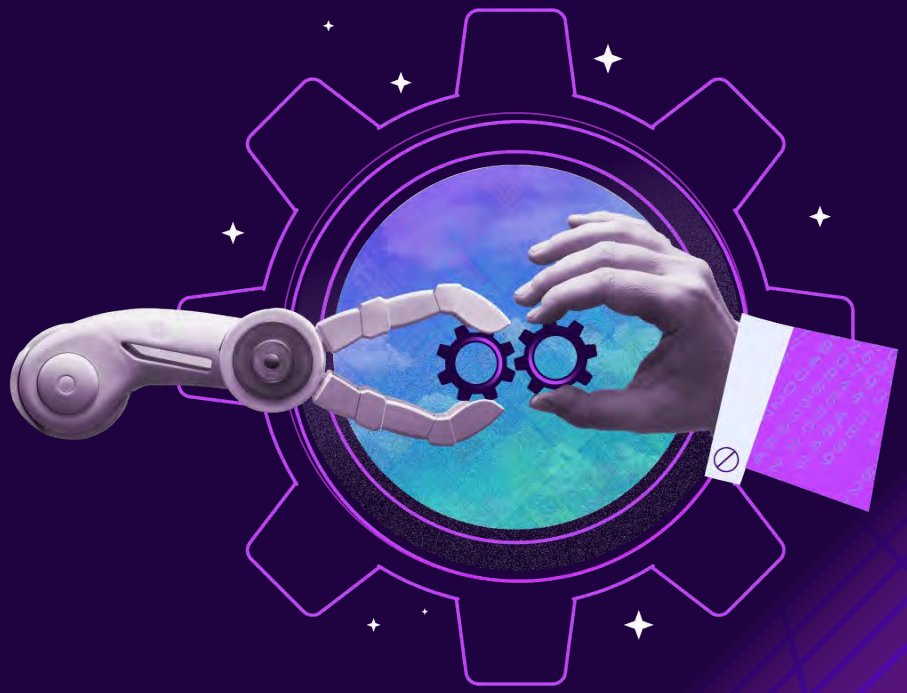
Source: Canalys, Candefero survey, 440 respondents, October 2024 to November 2024

49%
of channel partners in this survey expect growth greater than 20% in managed services revenue in 2025.

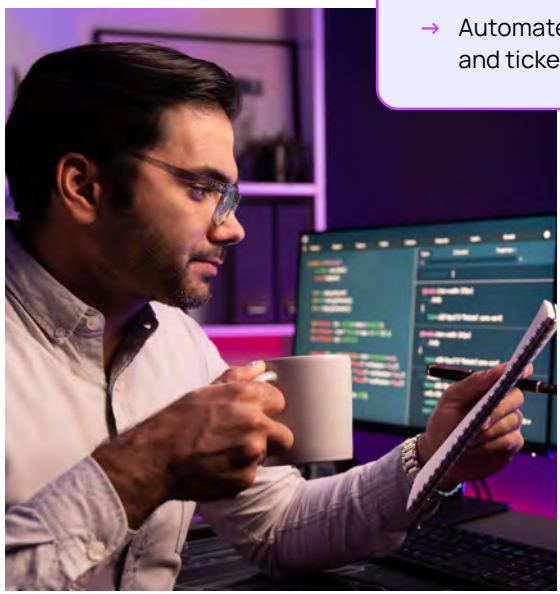


OBSERVATION

AI and automation continue to impact the MSP business model



The managed services model is in constant evolution, and there is an acceleration towards tech and services stack rationalization. Some of the fastest growing areas of investment for MSPs are in automation, as they explore every avenue to minimize administrative and low-level management overheads. Partners are not yet at the point of replacing staff with AI, something many worry may eventually be a reality. For now, MSPs en masse are leveraging AI to build workflow automations, automate parts of the sales process, and ticketing. Vendors are investing in this too. In the RMM and PSA spaces the most common vendor product improvements in 2024 have been around AI in ticket response automation, backup automation, patch monitoring and deployment, and managed detection and response.



Many MSPs are leveraging AI to...

- → Build workflow automations
- → Automate parts of the sales and ticketing process

The key impact of AI on business and revenue models, and profitability in particular, should not be to replace staff but to redeploy their valuable skills to areas of value generation and customer experience management. The ultimate goal for an MSP is to specialize in high-value and complex technology areas which customers are unlikely to manage themselves, and to be able to keep ahead of the tech curve. Any MSP that can achieve this makes itself harder to replace, something which has been a major issue in 2024 as customers spent more time scrutinizing their costs.

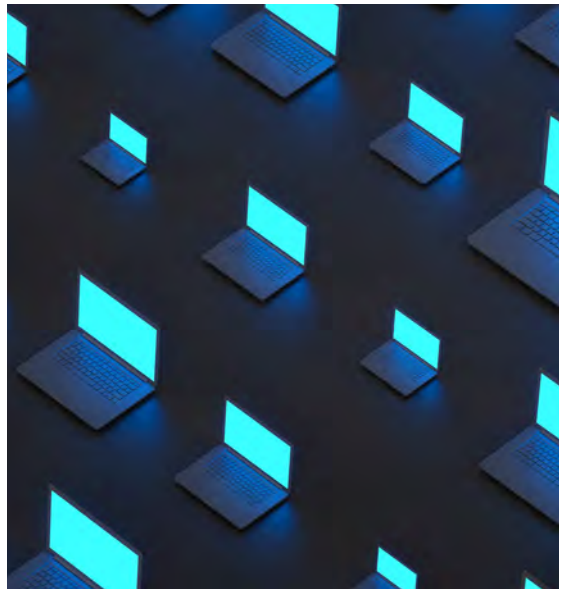
Customer churn has been a feature of 2024, according to Canalys' conversations with partners, and while Canalys believes it is unlikely to be as high in 2025 it is important MSPs improve customer retention rates. Profits are tied directly to retention, and revenue growth is much easier and cheaper to achieve if net retention is above 90% rather than below. To achieve this, MSPs must go beyond managing IT in the long run.

Most common AI product enhancements in 2024...

- → Ticket Response Automation
- → Backup Automation
- → Patch Monitoring & Deployment
- → Managed Detection and Response

OBSERVATION

MSPs are under pressure from commoditization and standardization of IT support services



Product commoditization and standardization of IT support services have put pressure on MSPs. To maintain revenue growth they must master a much broader ecosystem today and this is only becoming more complex. Compliance and regulation are two areas where partners need to stay ahead of their customers, but these are only subtopics of a larger whole. Breaking down IT into business outcomes has long been the mantra for partners of all kinds, but to generate recurring revenue on a multi-year basis with the same customer, partners must also become experts on the customer.

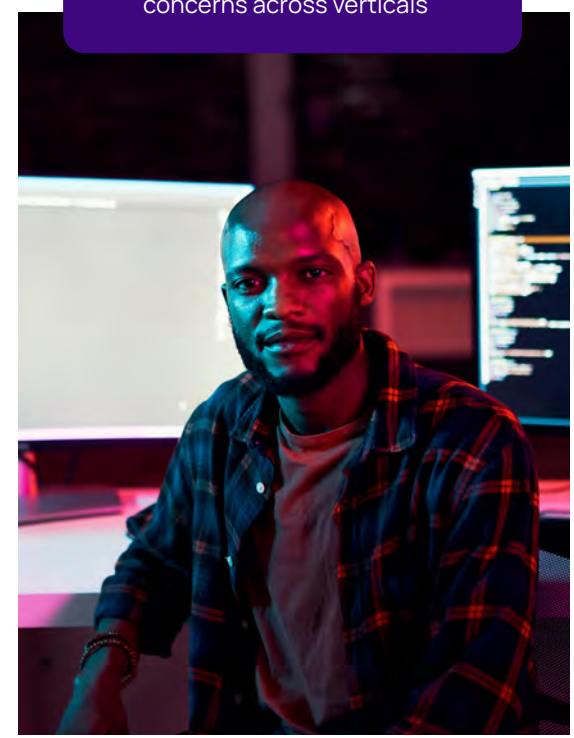
For some, this can mean vertical specialization, something which many MSPs fall into rather than target specifically. But it does not necessarily mean that only those that have become masters of a vertical will thrive, far from it. An ability to spot the concerns across verticals, solving similar business problems without creating a bespoke service for each customer is also important.

An example might be working in healthcare or in higher education. There will necessarily be some tailoring required to really land a customer in each vertical, but only some elements of these two deals will be specific. The regulatory environment for each is different, and knowledge of these is key, but both have customers (users) with datasets that will need protecting and analyzing. Data research may also be a requirement for both higher education and healthcare data management. Both will be looking for cost management capabilities on infrastructure, and both will require a mix of on-premises and cloud data and application management. Securing these two can be done in similar ways, regardless of the vertical.

AI is on everyone's mind – an insight that has again come from Canalys' conversations with partners – but in many cases the use of artificial intelligence will be horizontal as well as vertical, and this is one area where MSPs must stay ahead of the tech curve, providing clearer use cases and ROI calculations for customers who are often still looking for clarity.

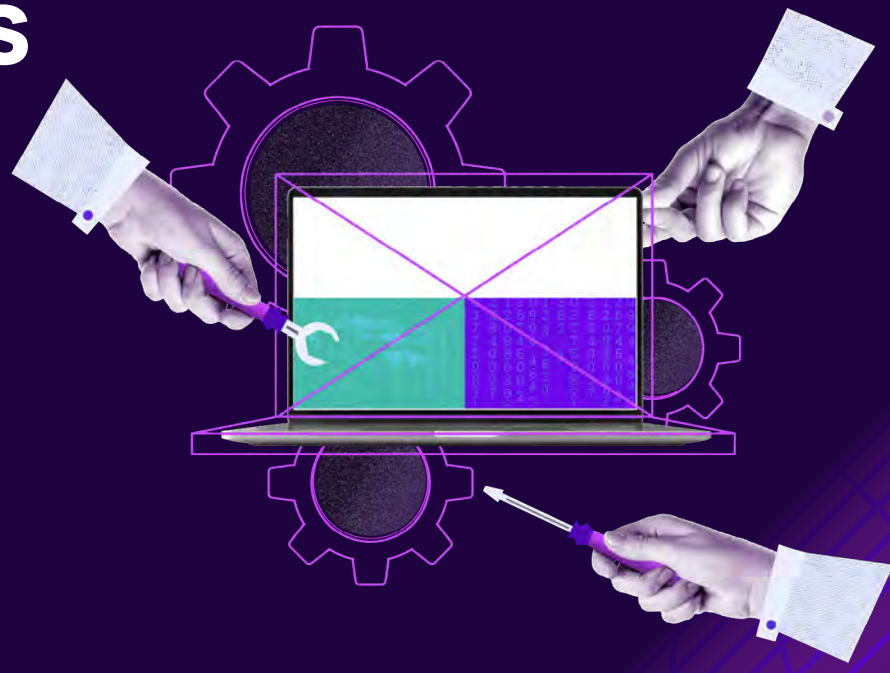
MSPs wanting to sell to specialized verticals need two things:

- → Knowledge of the regulatory environment
- → Ability to spot the common concerns across verticals



OBSERVATION

Owned management is preferred, but co-management is trending fast



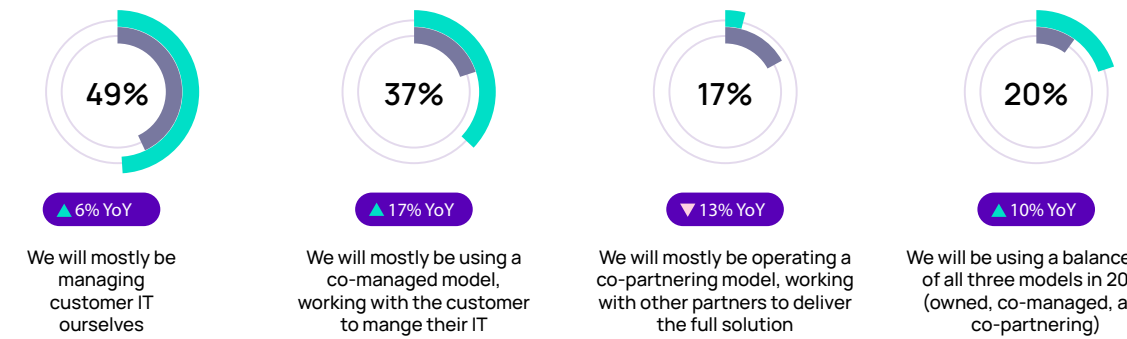
Most MSPs are planning to manage their customer's IT environments themselves (49%) in 2025, which grants them greater control over service quality and eliminates the potential cost of outsourcing. This aligns with MSPs lowering their co-partnering expectations (-13 percentage points Y/Y).

In 2025, more MSPs (+17 points Y/Y) will co-manage with customers (37%) compared to 2024. Done right, co-managing can establish a stronger relationship with clients, leading to higher customer satisfaction and retention rates. To be sustainable, MSPs must develop co-management guidelines with their client's IT team to avoid potential friction or redundancies.

As MSPs acquire larger enterprise clients, co-management may become a more preferred model, and they must be ready to work alongside bigger in-house IT teams. In the grand scheme, the co-management model can act as a launch pad, opening the door for MSPs to enter new markets and verticals.

FIGURE 5

Co-managed IT is on the rise



Source: Canalys, Candefero survey, 432 respondents, October 2024 to November 2024

+6% from 2024

Most MSPs (49%) are planning to manage their customer's IT environments themselves in 2025.

+17% from 2025

In 2025, more MSPs (37%) will co-manage with customers compared to 2024.

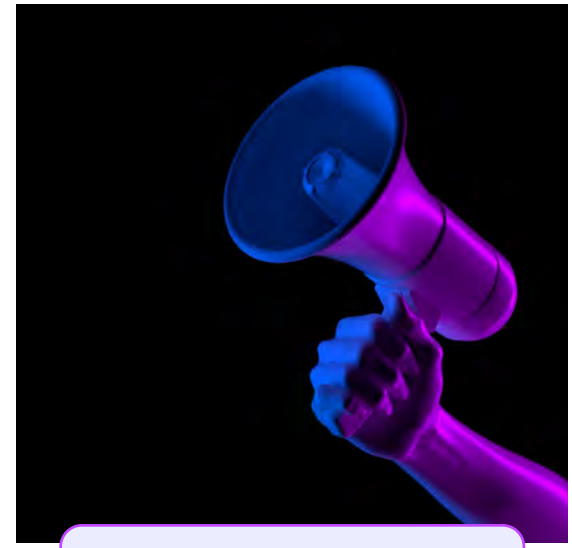
OBSERVATION

Acquiring new clients remains the biggest growth challenge

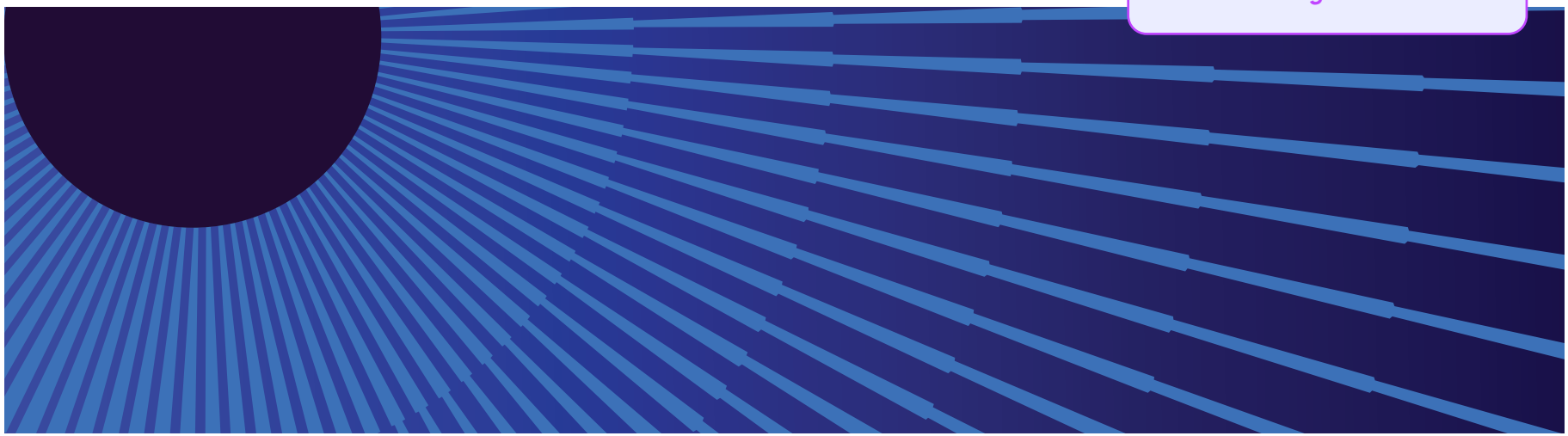
MSPs face an extensive number of challenges, both internally and externally. The issues are compounded by the fact that they are typically small firms, with less than 100 staff, limited budgets, reach and brand awareness. As a result, MSP staff often must wear multiple hats and fill different roles from sales and marketing to engineering.

As compliance requirements become more stringent and technology advances, MSPs face an uphill battle retaining and acquiring new customers, hiring the right talent to address new tech developments, and adhering to new regulatory requirements, while operating on usually marginal profits.

The MSP Horizons survey once again found that MSPs' top challenge to growing their business remains new client acquisition, as a competitive market makes it difficult to differentiate and attract new customers. MSPs must invest in themselves by identifying the key markets where their services are needed and use the proper tools — customer relationship management (CRM), social media marketing, etc. — to increase their efficiency and brand awareness in those key markets.



> *We're going all in on marketing and sales."*



OBSERVATION

Upskilling and retaining staff are becoming major hurdles

In addition, MSPs are challenged by significant IT professional skill shortages (tied for new client acquisition for most challenging), making it more difficult for them to acquire new talent especially in high demand areas like cybersecurity and AI.

Obtaining new talent is difficult on its own, MSPs must also invest in their current staff by providing them with the proper upskilling, training, and certifications and development programs, so they are experts in today's new technologies and avoid becoming obsolete.One of the biggest tech challenge areas is cybersecurity, so it comes as no surprise that securing customer infrastructure was a top hindrance.

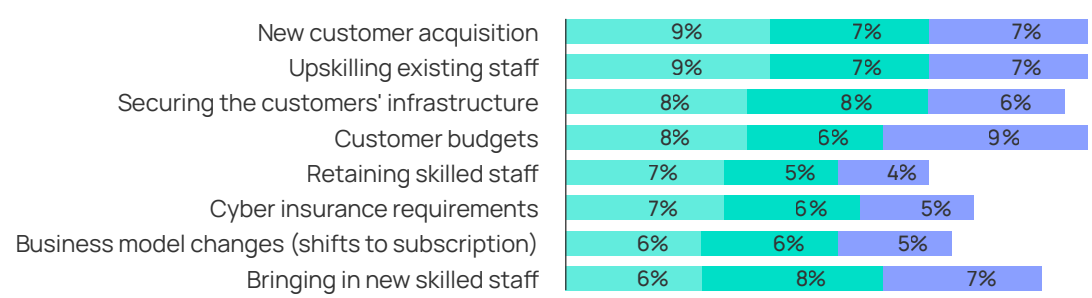
> *We will be enforcing metrics and SLAs in the future and need to be better at investing in training and skills."*

MSPs must make the decision to outsource their security operations or adopt more robust security practices in-house by using advanced cybersecurity (AI-powered) tools at a time when cyber-attacks are on the rise and data breaches remain in the headlines. Regularly updating their cybersecurity posture and complying with the latest compliance standards will be key to their security resilience. MSPs that differentiate their cybersecurity services by investing in elite cybersecurity teams or partnering with one, can turn this challenge into an opportunity.

> *Security, compliance and regulation are making it difficult to be a good MSP. It's starting to weed out people who aren't 100% committed. You need to be more professional and look across the whole client's business environment for security issues."*

FIGURE 6

Which of these are your most significant challenges to growing your managed services business today?



Each column represents the percentage split of those that provided an answer for that question.
Source: Canalys, Candefero survey, 414 respondents, October 2024 to November 2024

OBSERVATION

Cybersecurity services still top the growth agenda

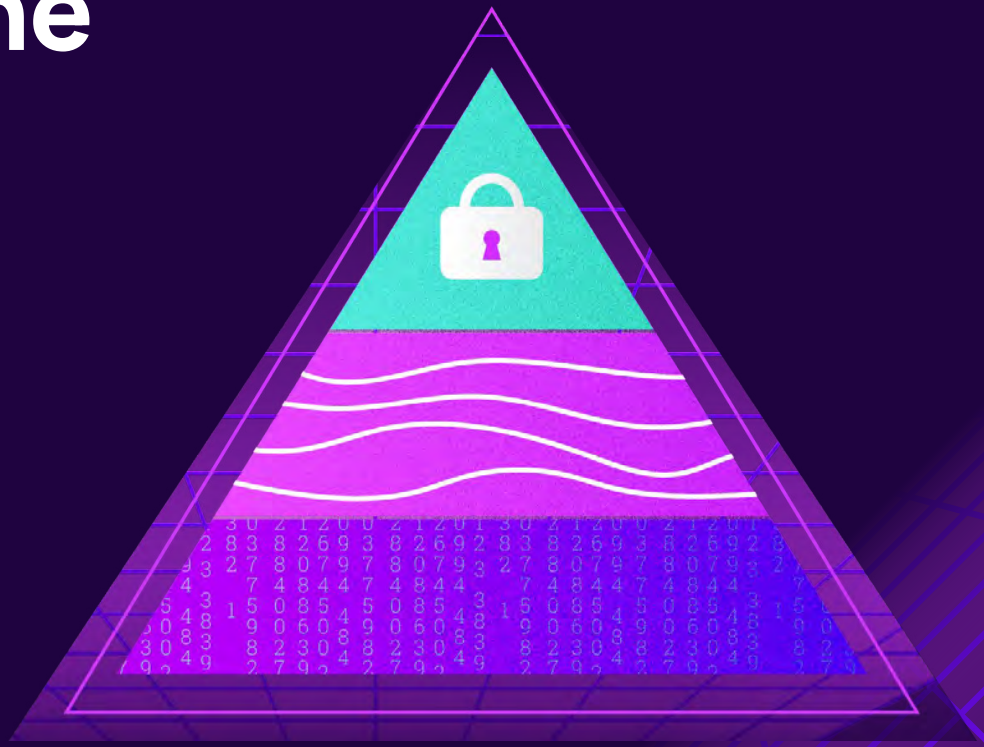
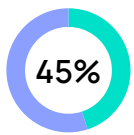
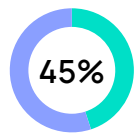


FIGURE 7

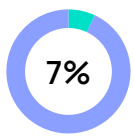
How is your cybersecurity managed services business changing?



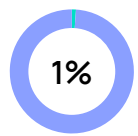
We are selling a small percentage of cybersecurity managed services today, but we are planning to grow this a lot over the next three years



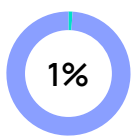
We are selling a large percentage of cybersecurity services today and this will grow in the future



We are selling some cybersecurity managed services today, but this will go down in the future



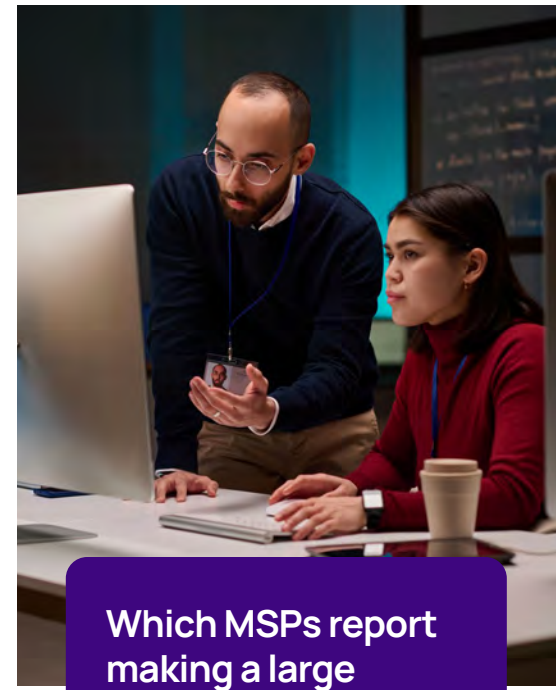
We are not selling cybersecurity managed services today, but we plan to in the future



We are not selling cybersecurity managed services today, and do not plan to in the future

Source: Canalys, Candefero survey, 372 respondents, October 2024 to November 2024

According to our survey, 90% of partners in the study are expecting growth in their managed security services revenue over the next three years — this is up from 80% in last year's study. Only 2% of respondents this year said they were not selling any managed security service today, with a further 7% saying they sold it but were expecting a decline in that business in the future. This suggests the partners that took part in this study are already established within managed cyber. This points to the conclusion that maturity is no barrier to growth, particularly as the 90% was split evenly between those that are doing a small amount of cybersecurity managed services and those with much larger practices. Breaking down the cybersecurity managed services survey question from the 2025 MSP Horizons survey into small (less than US $10M annual revenue) versus large (US $10M+) MSP respondents, results showed that larger MSPs are selling a higher percentage of cyber services; 57% of large firms reported selling a large percentage, compared to 40% of those with smaller firms.



Which MSPs report making a large proportion of their revenue from selling security services?

57% of large MSPs

40% of small MSPs

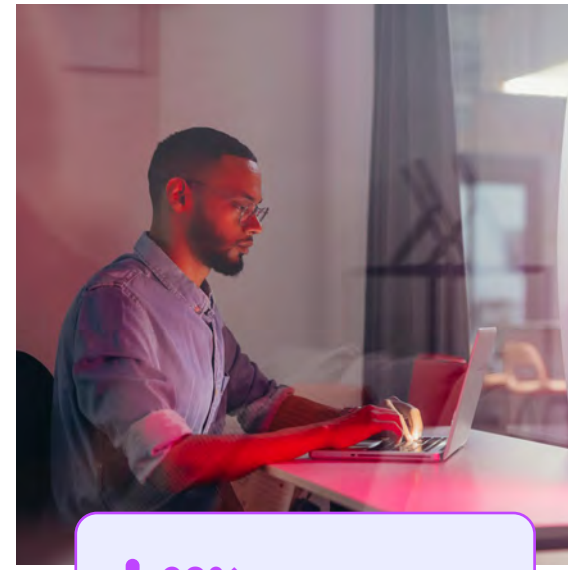
In planning for the future, MSPs must also look at those areas with the most margin opportunity.

Tools and services such as endpoint detection and response (EDR) and multi-factor authentication (MFA) are becoming saturated, though certainly this is no reason to abandon them. Newer areas such as DMARC, password management, and SaaS monitoring can carry with them much higher margins and lower competition, but they also bring with them a potentially longer sales cycle as customers may be unfamiliar with them and need education.

> ***We're constantly investing in cybersecurity."***

MSPs view cybersecurity as one of the most (if not the most) profitable areas of their businesses. Because it is so valuable to customers there tends to be a higher mark-up on sales of security software and hardware, and a higher margin on security services. What the data confirms for us in this study is this is likely to continue for at least the next three years.

There is a long-standing problem in cybersecurity that is still not being solved, and while technology can bridge some of the gaps it will likely only lead to another version of the same issue. The IT channel, and the IT industry as a whole, has been discussing skills gaps since cybersecurity was created. Today, we are at a point where cybersecurity is no longer a product but an organizational strategy. However, there is no one strategy that will work for everything,

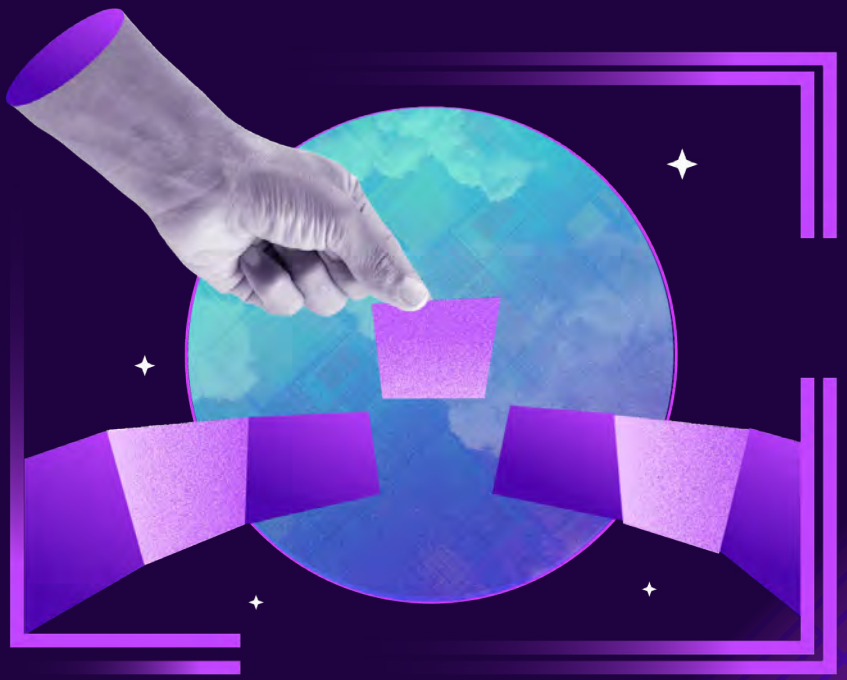


90%
of partners expecting growth in managed security services revenue over the next three years — up from 80% in last year's study

no silver bullet, and no magic formula — some work better than others, and some are quite plainly wrong.

OBSERVATION

Profitability widens the cyber skills gap



The MSP industry has fallen behind in cybersecurity skills training and hiring every year. Partners and vendors in cybersecurity need to hire at 3X the current rate to meet the demand for cybersecurity managed services over the next three years. The cost of cybersecurity staff has long been an issue for channel partners.

The industry needs vendors and channel partners that can sell the value of a true cybersecurity managed service and charge an amount that covers the cost of well-paid technical staff and expensive technology. This is also where regulations help, as compliance pushes customers to invest in the right strategy, and the channel can start to offer services at a reasonable profit. Many partners today are starting to lean on vendor MDR services to help them with this equation, maintaining profitability without losing out on service (though it is vital partners get access to remediation services in these agreements, or they will risk providing a subpar service to their customers).

There are other problems with cybersecurity services sales that are harder to overcome. Cybersecurity sales tend to involve multiple stakeholders within the customer, from the C-suite to technical staff to compliance officers and legal (depending on the size of the company). The sales cycle can be 12-18 months, which places a cost burden on consulting staff. It also requires a very specific combination of credible technical and persona-based skills to sell a true cybersecurity 'solution' i.e., a technology and services deployment that is solving a problem.

Sales cycles can be 12-18 months long
which places a cost burden on consulting staff.

These sales skills are not easy to find, and often it is best to train these people internally. This is often the final barrier for partners in building cybersecurity managed services practices, one which can be described not as a skills gap but a courage gap. Investing in sales engineer-style roles which can offer a vendor-backed MDR service, for example, can be a good way to share the burden of cost of the offering while maintaining differentiation.

OBSERVATION

M&A interest is on the rise as interest rates fall

"MSPs of up to six employees can't keep up with the pace of change. So, I'm going to eat them. Surely someone out there plans to eat us too."

There have been over 140 mergers and acquisitions in 2024 in the IT industry at time of writing (December 2024), down nearly 70% from last year (source: Channel E2E). Big tech firm acquisitions may make the most headlines, but M&As are agnostic and occur regularly across the entire IT landscape. M&As can happen for several reasons, like a large MSP deciding to acquire a competitor; or several small firms choosing to merge to improve their purchasing power or expand their market reach; they remain an industry staple. Unfortunately, it is often the smaller businesses that are forced to sale before they would like for reasons outside of their control, like macroeconomics.

"One of the things I'm worried about is the introduction and the continuation of private equity, money and investment into MSPs that will come into fruition soon. Smaller players like us will struggle to compete."

In this year's survey, when asked if they were looking to acquire any other MSPs within the next three years, a resounding 90% (up from 44% last year) stated they were. The motives behind their sentiment drilled down from considering all options, to adding specific skills, entering new markets, or expanding into specific verticals. M&As offer various advantages to MSPs — like improved competitiveness in current or new markets, influx of experienced talent, and diversification of revenue streams — which reduce the risks associated with being too dependent on certain customers or market segments.

"The biggest change is going to be M&A. We're looking to acquire other MSPs. It's much easier for us to grow through acquisition and leverage some of the talent and systems that we've built over the years."

As M&As persist, MSPs must be diligent and adapt their business practices accordingly to remain competitive as the landscape around them constantly changes. Staying informed about any M&A activities will help them foresee any potential new opportunities or gaps they can capitalize on that are created as the result of an acquisition.

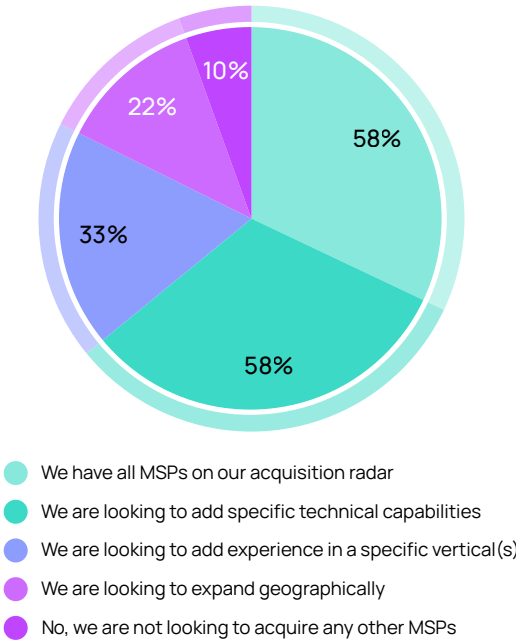
% of MSPs interested in M&A

- → 44% (2023)
- → 90% (2024)

FIGURE 8

Are you looking to acquire any other MSPs within the next three years?

(Choose all that apply)



Source: Canalys, Candefero survey, 407 respondents, October 2024 to November 2024

SECTION 2

Technology

Where risk is managed, business risk grows

Introduction

'A man is only as good as his tools.' This is a phrase that could not be truer in the MSP market. MSPs have a plethora of tools at their disposal to help them deliver their services. MSPs' most useful tools are those that help protect customers from data loss (backup and disaster recovery), secure their environments (cybersecurity), streamline their in-house operations and automate routine tasks (AI), maintain both on-premises and cloud environments (hybrid management), provide robust monitoring and management (RMM), or ease the management of multiple clients (PSA).

Key Takeaways

- This year's MSP Horizons Report highlights growth of network and endpoint security, and the focus on managing and securing the infrastructure of the end-customer.
- Risk management is key for MSPs moving forward. Managing customers' data and compliance requirements can be a strong differentiator for any MSP, but they must also be careful to maintain control of the customer awareness and liability.
- Cybersecurity continues to be leading technology trend. Cloud infrastructure, SaaS management, and ongoing monitoring, alerting, and remediation are all considered table stakes.
- BDR is in the top five of all IT managed services offered by respondents, and its importance to partners' managed services revenue is expected to remain just as strong three years from now.
- SaaS backup —for applications like Microsoft 365, Google Workspace, or Salesforce — is leading BDR addition for MSP, with 53% of partners saying they will be adding it in the future.
- Managed Detection and Response (MDR), security operations center as a service (SOC-aaS), and Extended Detection and Response (XDR) are key future additions to service stacks.
- MSPs make it clear they can't live without multi-tenant management tools, which allow them to manage multiple clients from a single interface.
- The influence of AI will only continue to get stronger for MSPs, as they increase their reliance on fully autonomous AI tools to handle tasks like customer support tickets, generating marketing, and basic coding. In future, this greater AI adoption could lead to staffing reductions or at least reduced hiring.
- Costs, security, technical skills, and multi-cloud complexity are challenging MSPs when offering cloud services.

OBSERVATION

MSPs are focusing on securing client infrastructure

The MSP Horizons study asked partners what kinds of technology they currently manage for their customers.

The top five categories were:

- Network security
- Managed network services
- Endpoint security
- On-premises datacenter management
- Managed backup and disaster recovery.

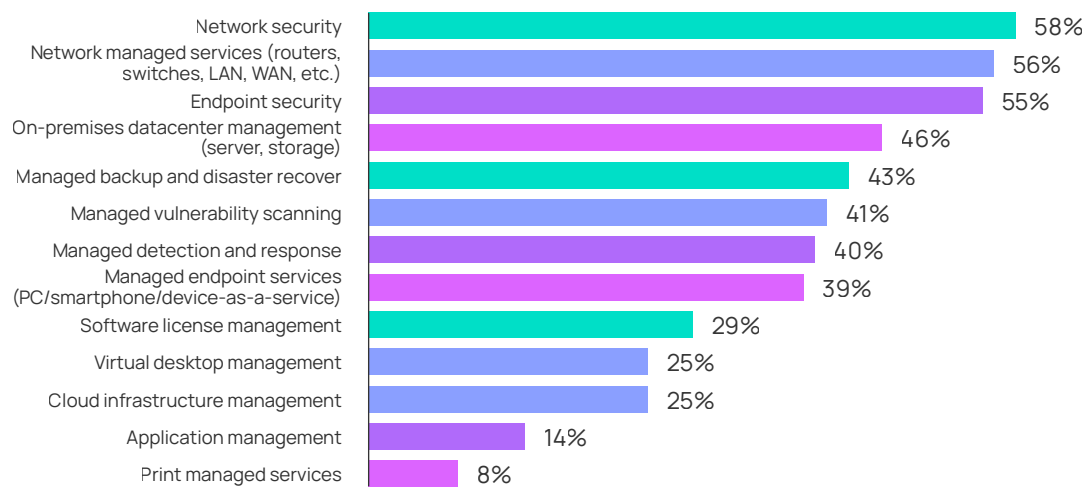
The key changes year on year are the growth of network and endpoint security, and the focus on managing and securing the infrastructure of the end-customer.

Risk management is the key phrase for the future. Managing the data and compliance requirements of the end customer can be a strong differentiator for any MSP in the coming years, but they must also be careful to maintain control of the customer awareness and liability. Too often we see MSPs and customers caught in legal battles following a breach, primarily due to a lack of oversight. This can either be because the customer has not taken on board all the recommended best practices mandated by the MSP in its SLA, or because the consulting process did not vet the customer's security awareness and maturity properly. In any circumstance, the initial discovery phase between MSP and customer is important to the overall success of the relationship, setting expectations and standards, and making the job easier for those mature MSPs with customer experience roles.

The most interesting picture emerges when we ask partners what services they will be offering in three years' time.

FIGURE 9

Which IT managed services do you currently offer? (Choose all that apply)



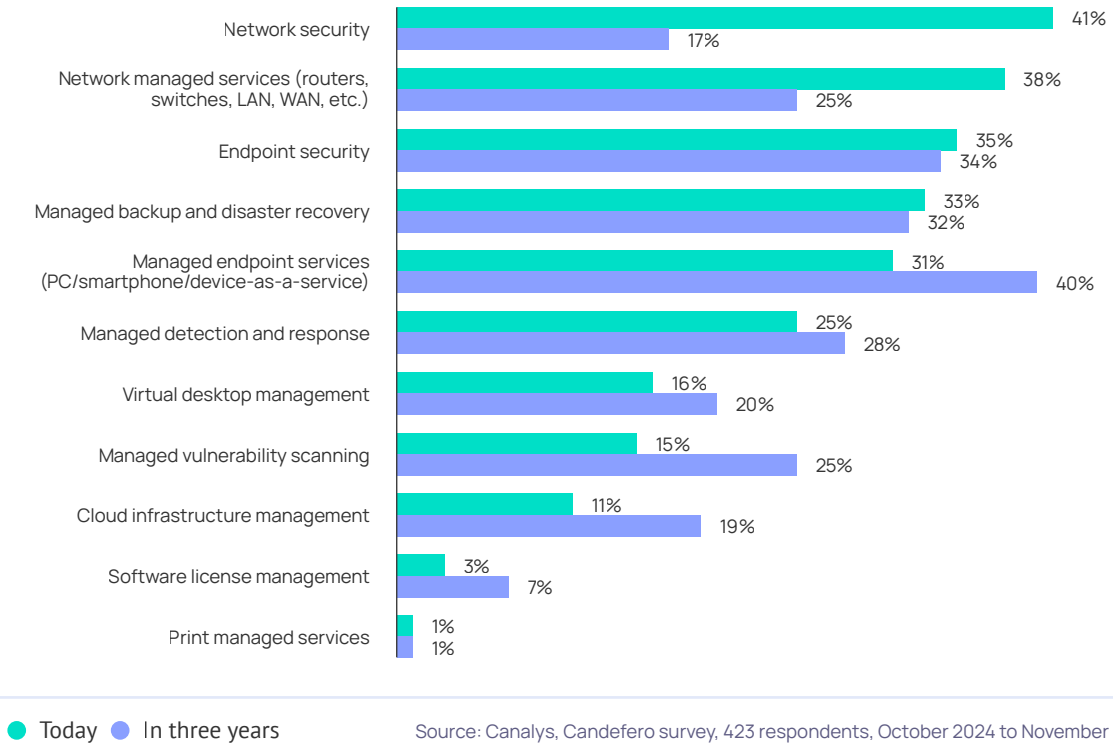
Some options were slightly reworded (i.e. managed backup and disaster recover (2024) vs. Managed Backup (2023)
Source: Canalys, Candefero survey, 449 respondents, October 2024 to November 2024

"We just woke up one day and we were cyber cops. Over the next five years, security will evolve into compliance and managing risk. We are not just IT people anymore; we are consultants guiding businesses through compliance as government and insurance regulations become more focused."

It is no surprise that cybersecurity has been the biggest ongoing technology trend of the past few years, and one that is clearly continuing based on the data in this study, is cybersecurity. Cloud infrastructure, SaaS management, and ongoing monitoring, alerting, and remediation are all considered table stakes for MSPs now and looking to the future.

FIGURE 10

Which of these (IT managed services) is most important to your managed services revenue? (Choose all that apply)



Source: Canalys, Candefero survey, 423 respondents, October 2024 to November 2024

Regional variations are also very important for MSPs and vendors, to consider. In Asia, the business environment is dominated much more by smartphones and tablets, with fleet and mobile device management (MDM) developing strongly there.

The massive growth in local mobile device technology from companies like Oppo, Vivo, HONOR, Xioami, and Nothing has meant vendors and partners must be able to integrate with and manage devices on operating systems outside Windows and MacOS/iOS. RMM vendors have noticed the growing customer demand for MDM capability and have been building integrations with Android and Apple operating systems, but the specialist MDM vendors have a part to play here due to their specialist focus. This means MSPs can benefit if RMM, PSA, and MDM vendors develop deeper integrations.

> *"The business environment for MSPs as a whole is changing due to the commoditization of product, forcing us to focus more on services."*

Predicted changes in MSP service offerings

Growth areas

- Managed vulnerability scanning
- Software license management
- Managed endpoint services
- Cloud infrastructure management
- Application management
- Managed detection & response (MDR)
- Virtual desktop management

Biggest declines

- Network manages services
- On-premise datacenter management
- Network security

OBSERVATION

BDR is now an integral part of risk management

Backup and disaster recovery (BDR) has long been key pillars in the MSP tech stack.

The latest channel polling data from Canalys shows 88% of partners attach backup to their managed services deals, with 36% of partners saying it is attached in over 60% of those deals. In the MSP space it is even higher.

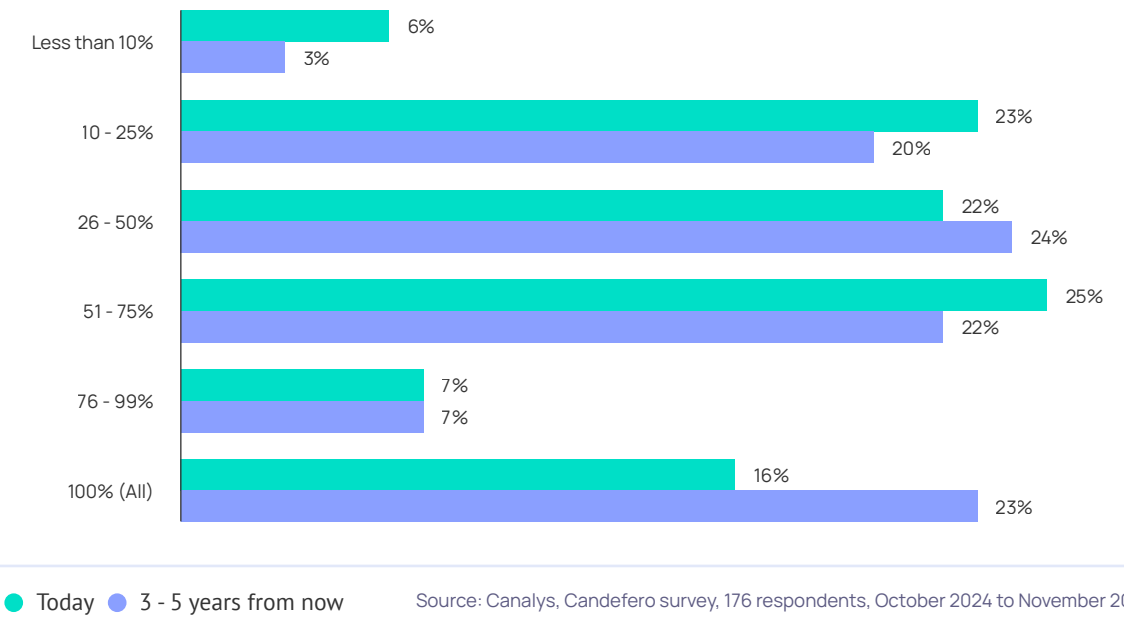
> ***Backup is one of the fundamental pillars of what we do. If we cannot properly back up and restore data, we might as well close our doors. It's crucial now and will always be."***

This year's MSP Horizons study confirms this importance, as BDR is in the top five of all IT managed services offered by respondents, and its importance to partners' managed services revenue is expected to remain just as strong three years from now. There are two key drivers for this: firstly, BDR is, generally, a higher margin offering and, secondly, it is central to compliance. Many security and compliance frameworks globally — including NIS2, Cyber Essentials, CMMC, and Essential Eight (to name just a few) — mandate BDR deployments as best practice, and it is equally important for vertical regulations (financial services, for example) and cyber security.

FIGURE 11

What percentage of your managed backups are stored in the cloud?

(Choose all that apply)



Source: Canalys, Candefero survey, 176 respondents, October 2024 to November 2024

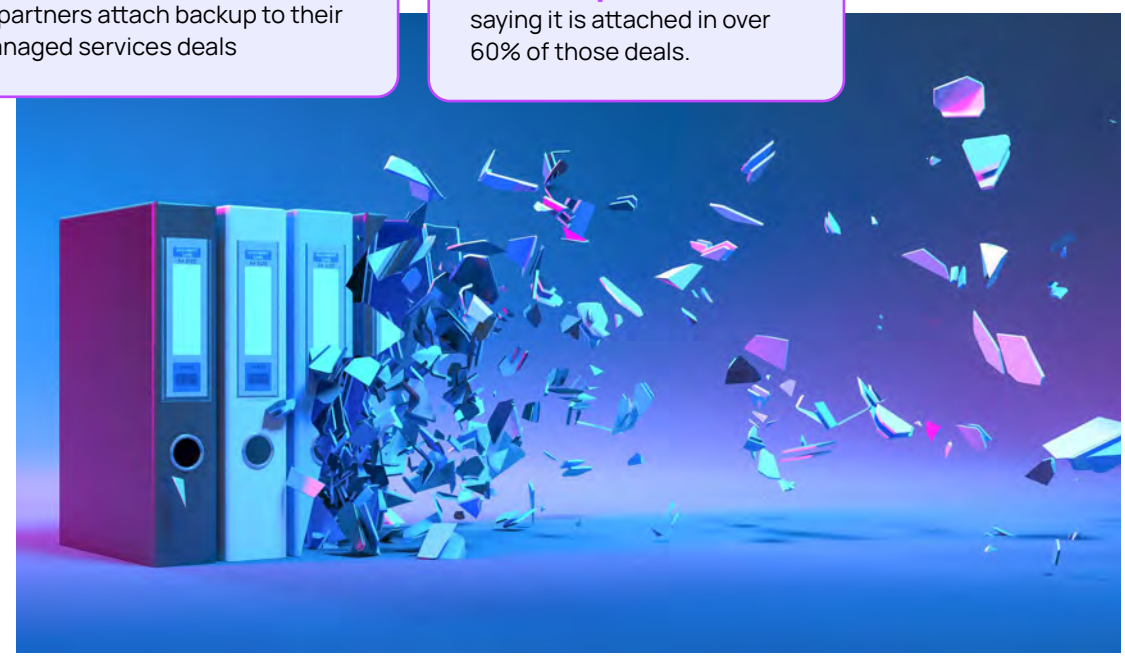
On-premises backup deployments will almost certainly continue to be important moving forward, especially as best practice for many industries requires a separate, on-premises backup for compliance purposes, but cloud-based backups are becoming increasingly important.

However, as with last year's study, location has a big impact on this balance. Urban environments are more easily served by cloud technology due to bandwidth stability, but rural locations are still not fully connected in many parts of the developed world. Customers in these locations lag behind others in their move to cloud, but this is likely to be a less prevalent problem in years to come as cloud service providers build edge datacenters and local governments improve connectivity.

> *Backups are stored in the cloud. Ransomware has played a huge factor in that decision. The backups need to be immutable so that attackers can't delete them."*

88%
of partners attach backup to their managed services deals

36% of partners
saying it is attached in over 60% of those deals.



OBSERVATION

Backup technology and how you deploy it is changing rapidly

One of the growth areas highlighted by respondents was SaaS backup — for example for applications like Microsoft 365, Google Workspace, or Salesforce — which 53% of partners said they would be adding in the future. As customers are pushed towards SaaS, backing up the data in these applications becomes standardized. AI-powered backup — i.e., backup that uses AI to reduce the need for manual interventions to troubleshoot failures and/or recover data — was second on the list at 51%.

53%
adding Backup for SaaS apps (ie Microsoft 365, Google Workspace, or Salesforce) in the future

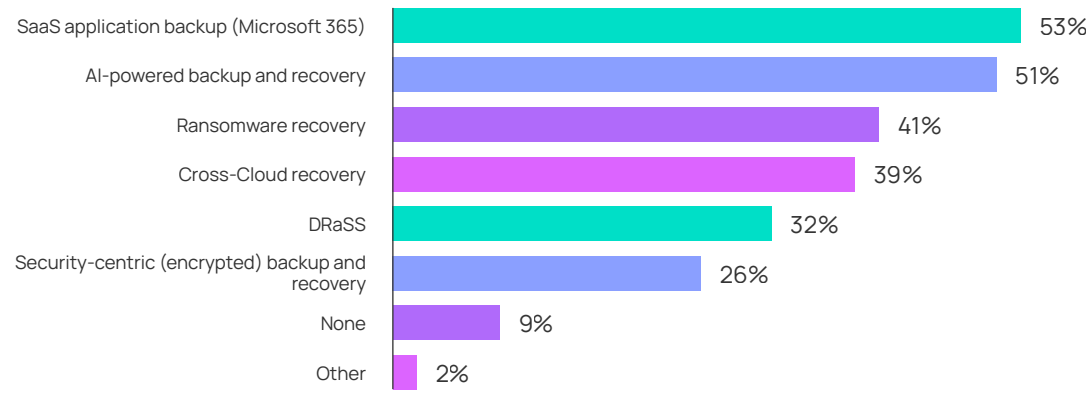
The automation drive MSPs are undergoing today covers all the key areas of the service stack, backup being one of them. If MSPs can offer fully automated backup technology to customers it will certainly save resource costs, however this also poses an inevitable threat to their business models. Margins on standard backup services will go down and partners are aware of this already, as demonstrated by investment in other areas, such as ransomware recovery services (41%), cross-cloud recovery (39%), and encrypted backup and recovery services (26%). The need for on-premises managed backup can also potentially act as a backstop for them here, too.

The future for backup and disaster recovery is also one that is being shaped by acquisitions today. RMM vendors are acquiring or building backup technologies, enterprise vendors are acquiring small and medium-enterprise (SME)-focused players and vice versa, and the platform drive continues its seemingly endless march forward. Backup also affords vendors and partners the opportunity to increase their total addressable markets due to its strong potential resell motion. As more resellers and systems integrators develop managed services practices, and private equity-backed MSPs acquire for scale, backup offers a way for the former to adopt managed services and risk management practices for line of business customers, while the latter can more easily satisfy the demand for improved valuations.

FIGURE 12

What new kinds of managed BDR services will you be adding in the future?

(Choose all that apply)



Source: Canalys, Candefero survey, 176 respondents, October 2024 to November 2024

OBSERVATION

As cybersecurity offerings grow, ecosystems still need to work together

Managed Detection and Response (MDR), Security Operations Center as a Service (SOC-aaS), and Extended Detection and Response (XDR) are among the key future additions to service stacks according to respondents to this year's survey.

Only 20%
of partners will be looking to deliver their own MDR, so partner-vendor collaboration will be key in the future.

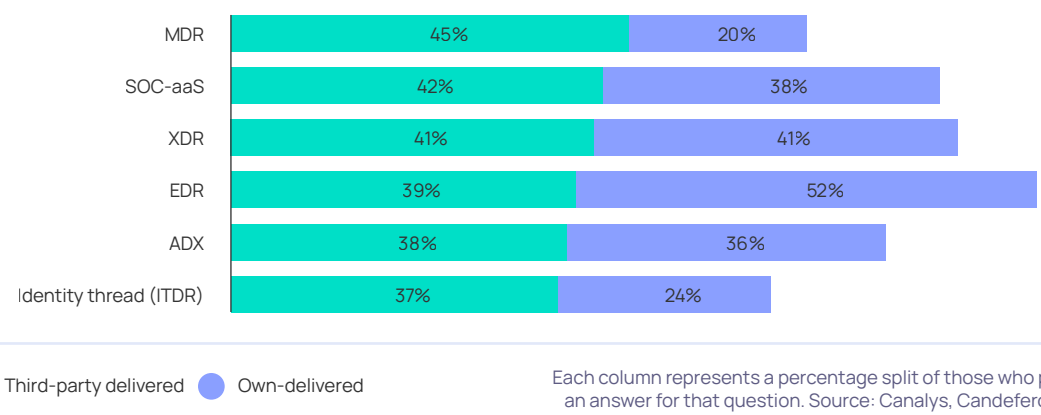
XDR and Endpoint Detection and Response (EDR) will see the highest overall adoption by those not currently providing these services. EDR is perhaps the simplest to define; data gathering, analytics, and alerting for threats across endpoints, such as laptops or servers. MDR goes further with a proactive, human element attached. XDR provides threat detection and response for cloud security tools, services, endpoints, and networks. It is an extension of traditional EDR solutions. XDR works best in complex and hybrid cloud environments.

For MDR, the future appears to be third-party delivered according to most partners. The main reasons for this are cost, skill, and scale-related. Partners are happy offering MDR from a third-party to a customer, either entirely resold or co-managed. Unless they are looking to become specialist MSSPs, most partners will not build their own SOCs, and the reliance on a vendor or MSSP to deliver detection and response services to customers is the only way to build scale in managed security solutions in a cost-effective

FIGURE 13A

What new kinds of cybersecurity services will you be adding in the future?

(Choose all that apply)



Each column represents a percentage split of those who provided an answer for that question. Source: Canalys, Candefero survey,

manner that delivers both value for the customer while maintaining the partner's profit margins.

In the first scenario, the partner can sometimes offer the service for resell, but the contract is held between the end-customer and the vendor (or MSSP). In the latter, the partner offers some front-line services and manages the relationship with the vendor or MSSP, but the alerting and remediation is done by the third party. MDR, like XDR, is often a multi-party engagement, but the issue will always remain managing the critical moments of attack and remediation when responsibility is shared.

It was clear from the direct interviews Canalys did as part of this year's survey that Extended Detection and Response (XDR) is reshaping the IT managed services market. As in every other area of the MSP market, this is being partly driven by increasing demands for compliance and regulatory adherence. Customers are also investing in XDR to improve visibility into an ever-broadening tech stack, helping them stay ahead of the threat actors trying to leverage a wider attack surface. The convergence of these trends will significantly influence how XDR is adopted and leveraged by MSPs.

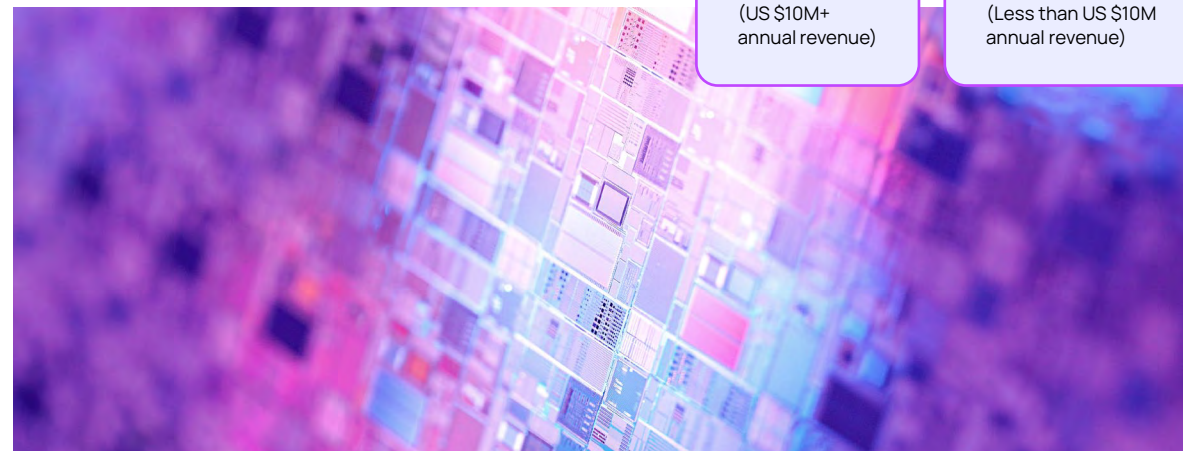
Regulatory requirements such as GDPR, HIPAA, CCPA, and emerging cybersecurity mandates require organizations to demonstrate rigorous monitoring, incident response, and data protection. XDR's ability to integrate data across endpoints, networks, servers, and cloud environments makes it a natural fit for ensuring compliance, at least in an ideal world.

XDR helps with regulatory compliance by providing visibility into security events and incidents, so organizations can identify and investigate potential data breaches. It also automates incident response, helping customers meet regulatory requirements for timely threat detection and response. XDR generates reports on security controls and their usage, which can help with reporting for regulators. Equally, XDR's integration with Identity and Access Management (IAM) systems helps with access controls and traceable user activities, which are also key compliance requirements. These are helping MSPs to offer value-added services so that their clients remain compliant while enhancing their security postures.

Who is delivering EDR in-house?

71%
large MSPs
(US $10M+ annual revenue)

43%
smaller MSPs
(Less than US $10M annual revenue)

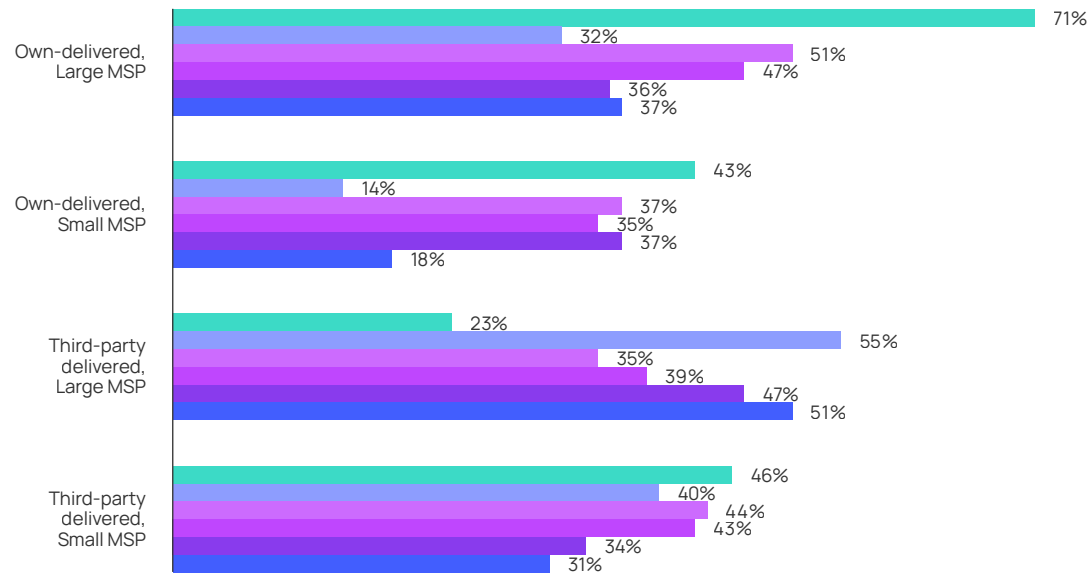


Breaking down the new kinds of cybersecurity services question from the 2025 MSP Horizons survey into smaller (less than US $10M annual revenue) versus larger (US $10M+) MSP respondents, results showed large MSPs favoured adding and delivering cybersecurity services in-house more than their smaller counterparts e.g., large MSPs will deliver EDR in-house (71%) vs small MSPs (43%). This comes as no surprise given the resources, skills and budgets large MSPs have, affording them an advantage to deliver more services in-house vs. outsourcing. Whichever solution partners are delivering, be it EDR, MDR, or XDR (or a mix of all three), it is vital the ecosystem of vendors, partners, and customers work together to provide a true security-first posture.

`

FIGURE 13B

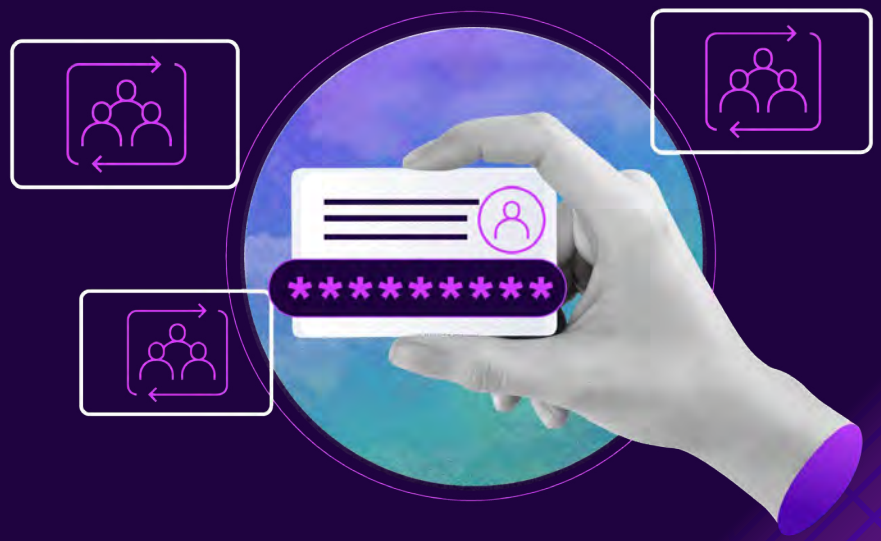
What new kinds of cybersecurity services will you be adding in the future? (large vs. small MSP breakdown) (Choose all that apply)



Note: N/A responses excluded from each category. Each column represents a percentage split of those who provided an answer for that question. Source: Canalys, Candefero survey, 372 respondents, October 2024 to November 2024

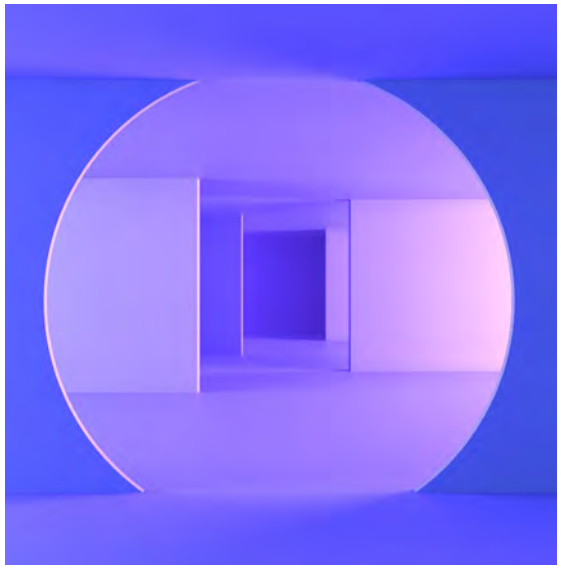
OBSERVATION

Multi-tenancy is non-negotiable



There is one feature that MSPs made clear that they could not live without: multi-tenant management tools, which offer several benefits, including managing multiple clients from a single interface.

> ***All services provide multi-tenancy as it is a standard for all solutions; it creates more overhead without it."***



Multi-management tools allow MSPs to scale operations and increase their client base without adding headcount. As MSPs grow they need more tools that apply consistent security policies and configurations, as well as performing compliance checks across all tenants. Reduced risks from human error when dealing with complex configurations and multiple clients is crucial and a key trait of multi-tenancy.

The choice of multi-tenant management tools is a critical one which MSPs don't take lightly and requires them to employ a rigorous five-step process to ensure they get the right solution.

> ***Everything I buy is multi-tenant. I want to see all the backups, cameras, Azure virtual machines and I want to control them from one point and be in control financially and operationally."***

Multi-tenancy is now the standard for MSP tools, and it won't be long before AI-powered multi-tenant management becomes the new standard.

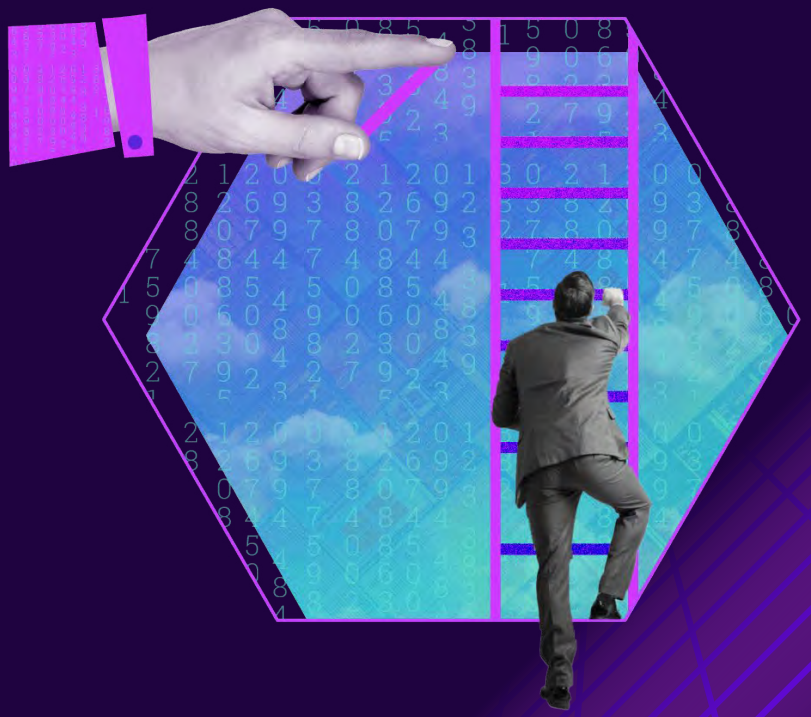
> ***There's a few services not providing multi-tenancy and we're switching those out for scale and efficiency. It's difficult to manage the clients without it. If you keep logging in and logging out, it just doesn't help."***

Five Steps to Selecting the Right Multi-Tenant Management Tool

1. Selecting tools that best fit their business needs and have the necessary features e.g., automation, security policy enforcement, and scalability.
2. Ensuring they receive proper training and education on the tools and any new or updated features.
3. Partnering with vendors to access specific certifications and support necessary to optimize the use of their tools.
4. Establishing standard operating procedures (SOPs) for managing tenants, onboarding, and configuration.
5. Setting up continuous monitoring and alerting to detect and respond to security threats in real-time.

OBSERVATION

Gen AI presents huge opportunities, but comes with its own challenges



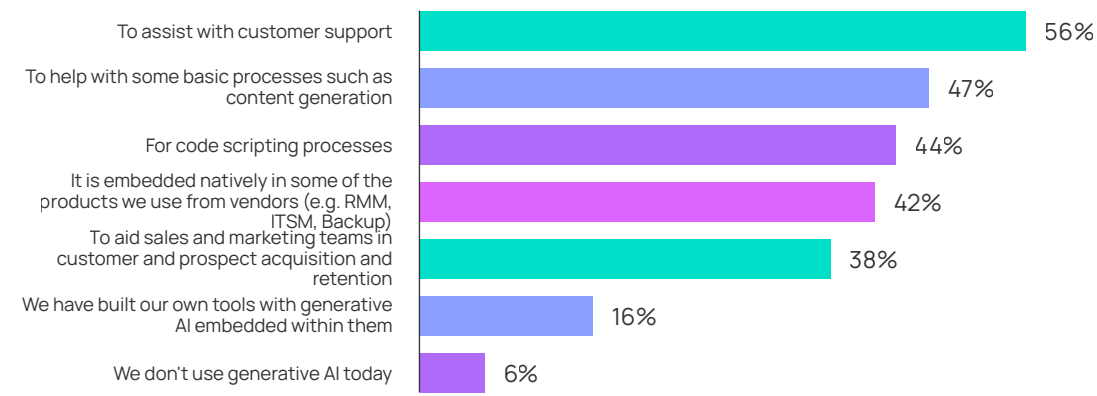
Artificial intelligence can serve almost any purpose the user wants — be it good or evil. MSPs use AI for a variety of reasons including the daunting task of combating threat actors that use AI to power their cyber-attacks.

According to data for this year's MSP Horizons survey, adoption among MSPs is growing as those that describe themselves as "non-users" declined 19 points year over year.

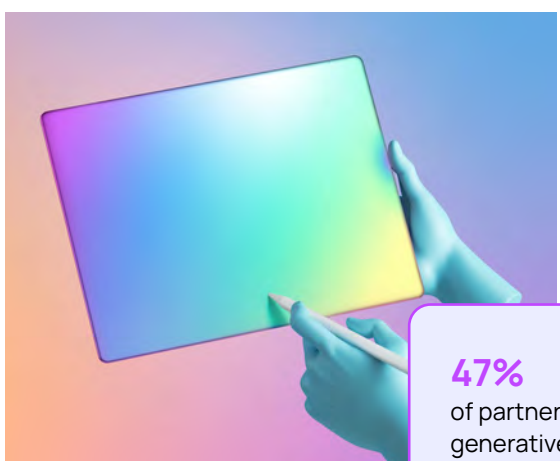
MSPs stated that they mostly use Gen AI to assist with customer support (56%). Tools like ChatGPT, Co-pilot, chatbots, and virtual assistants are helping MSPs create content and improve customer support, reducing the workload of their limited support staff. The capabilities of AI are limitless therefore it is important that MSPs continuously invest in the latest AI tools to achieve service efficiency.

FIGURE 14

How are you currently using generative AI tools in your business today? (Choose all that apply)



Source: Canalys, Candefero survey, 418 respondents, October 2024 to November 2024



47%
of partners are using generative AI to create content.

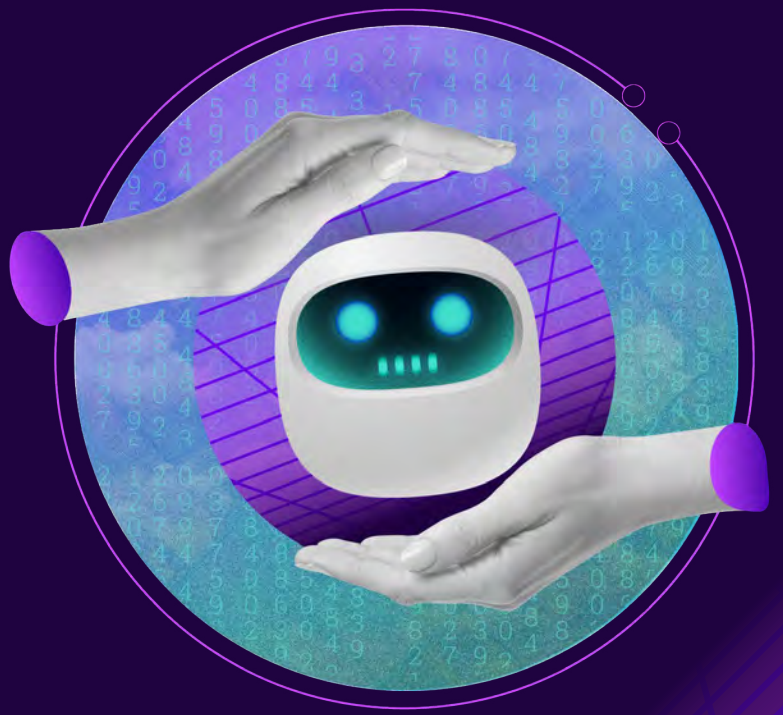
Creating content (47%) is another application of AI that partners are making use of. Given their limited resources and the multiple roles many staff play, routine tasks like marketing materials and technical document creation are no-brainer usage models.

For MSPs that optimize AI tools, it will play a pivotal role in personalizing customer content and providing enhanced customer experiences which can be rewarded with bottom-line improvements. This will take time to realize, but all good inventions do.

The influence of AI will only continue to get stronger for MSPs, as they increase their reliance on fully autonomous AI tools to handle tasks like customer support tickets, generating marketing, and basic coding. In future, this greater AI adoption by MSPs could lead to staffing reductions or at least reduced hiring.

OBSERVATION

AI is still in its infancy, so it needs supervision



Having said all the above, AI doesn't come without its flaws. MSPs must put up guardrails and set rules for how to use AI responsibly. According to this most recent survey, many MSPs (40%) have already established AI data governance rules, designed guidelines to balance automation vs human oversight (40%), or taken ethical training (39%). These steps are important to ensure their practices comply with industry regulations and standards. They also confirm ethical AI usage is being properly considered which is important to avoid biases. Having clear governance guidelines is a benefit to businesses' employees and customers alike.

> ***Really, humans are the Co-pilot for AI. Information, text, whatever content AI generates, we have to clean it up, be responsible and make it more human sounding or realistic in terms of, no, I actually can't deliver that."***

As AI use grows, MSPs must remain diligent by ensuring that governance policies are adhered to, reviewed and updated often because all it takes is one slip up and the company's reputation could be on the line and in the news for all the wrong reasons. The threat of more stringent AI data governance could curtail its use, giving those with established AI usage frameworks a significant advantage.

How are MSPs preparing for AI?

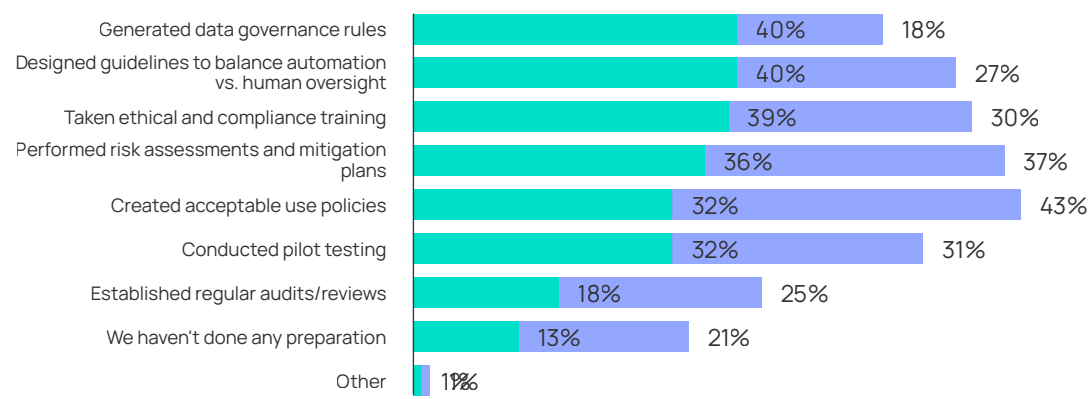
39% taken ethical training

40% already established AI data governance rules

40% designed guidelines to balance automation vs human oversight

FIGURE 15

What has been done to prepare your business and customers from AI usage? (Choose all that apply)



Source: Canalys, Candefero survey, 416 respondents, October 2024 to November 2024

OBSERVATION

AI isn't optional anymore

MSPs have limited staff; therefore, they must augment their skills with the tools they use, so it comes as no surprise that they are frequent users of AI-embedded tools for managed services delivery. Products with integrated AI offer advanced features that can help improve service delivery, via predictive analytics and automated workflows.

But the most important part of the process is still the staff operating the tools, which makes it vital for MSPs to work with vendors to ensure they are properly certified and trained on the latest AI features. Without this, features and functionality may go unused, resulting in basic results from advanced tools. MSPs that become highly specialized in optimizing the capabilities of their AI-powered tools will be likely be highly coveted by vendors and customers in the future.

> ***AI is layered into endpoint protection and other areas. I'm not actively seeking AI solutions, but I'm open to integrating them as they become available."***

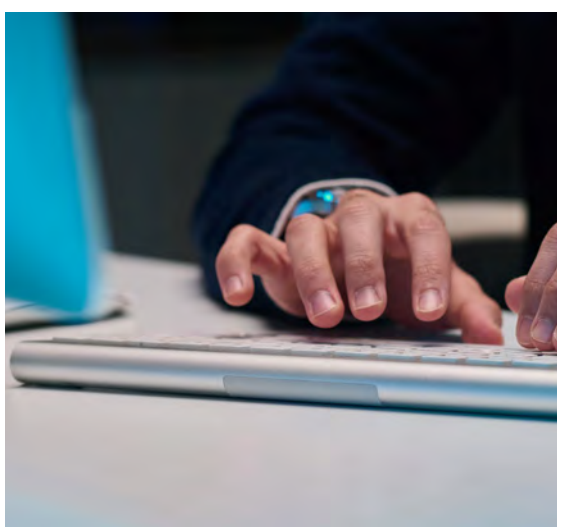
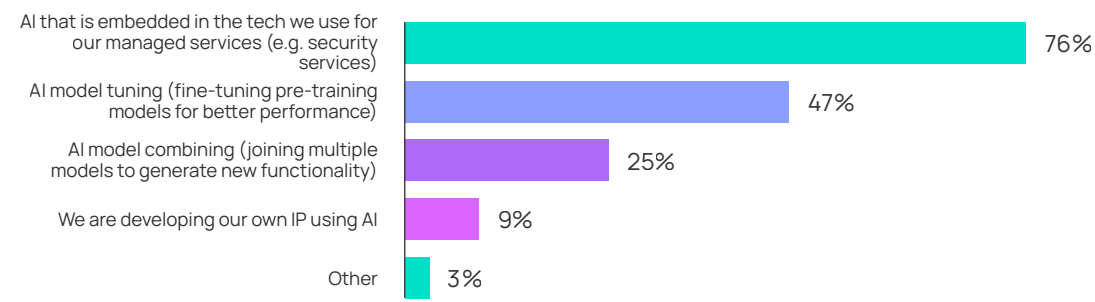


FIGURE 16

Are you using any other form(s) of AI technology today (Choose all that apply)



There were only two options in 2023, compared to five in 2024.
Source: Canalys, Candefero survey, 416 respondents, October 2024 to November 2024

OBSERVATION

Hybrid management models are customer-driven

Cost, data security, industry regulations/ compliance, and connection limitations remain key reasons why businesses will not be only managing cloud but will continue to manage some on-premises infrastructure. In fact, over 90% of MSPs say they are moving away from managing on-premises to cloud environments to some degree, and those with strong feelings rose 19 points from last year.

> *I'm coaching clients to move to the cloud, especially for disaster recovery. However, some clients with poor internet connections prefer to keep their servers on-prem."*

Hybrid management environments offer MSPs several benefits, including the scalability to dynamically increase resources and eliminate the costs of maintaining physical infrastructure, as well as providing built-in redundancy and recovery giving customers assurance in the event of a cyber-attack or natural disaster.

As the market evolves it is imperative for MSPs to update their cloud management posture to ensure they adapt to their customers' latest needs. MSPs should consider utilizing AI and automation tools to optimize hybrid cloud resource allocation, performance monitoring, and predict maintenance. Security is always top of mind; therefore, MSPs must integrate robust security that prevents data breaches, misconfigurations, and compliance issues. As a failsafe, MSPs should also make automated failover and data replication services that minimize downtime and data loss a standard cloud management package.

> *Moving people to the cloud will continue, but there are exceptions where on-prem makes sense. For small businesses, the cloud is a strong solution because it avoids large CapEx investments."*

Over 90% of MSPs
say they are moving away from managing on-premises to cloud environments to some degree

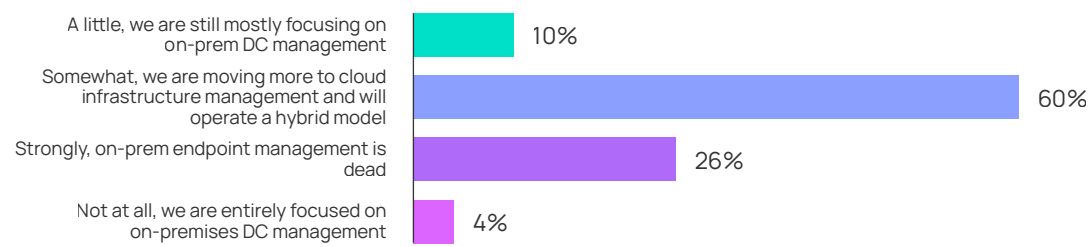
70%
of MSPs will be managing hybrid environments

25%
of MSPs seeing on-prem endpoint management as dead

+19% from 2023

FIGURE 17

To what extent are you moving away from managing on-premises datacenter (server, storage, applications) to cloud environments? (Choose all that apply)



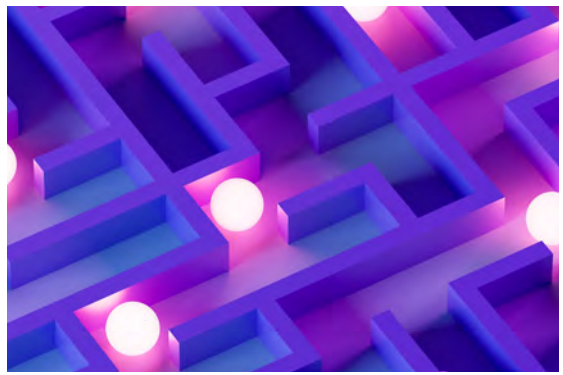
2023 referred to 'moving away from managing on-premises devices (server, storage) to virtual / cloud devices.
Source: Canalys, Candefero survey, 193 respondents, October 2024 to November 2024

OBSERVATION

Cloud costs and security are pausing migration

The times have changed from the initial thinking that moving workloads to the cloud would be less expensive and solve all your business problems. Sadly, reality is starting to set in, and some cloud benefits don't have the desired effect or have become more of a burden than initially promised when the 'all-in' cloud push was a hot trend. MSPs live in a new reality and have expressed some of the major challenges with offering cloud services today include costs, security, technical skills, and multi-cloud complexity.

> *We're seeing more SMB customers coming off the cloud because of the increased prices in the cloud tiers in Azure and AWS. They're more interested in going back to a Colo or something like that."*



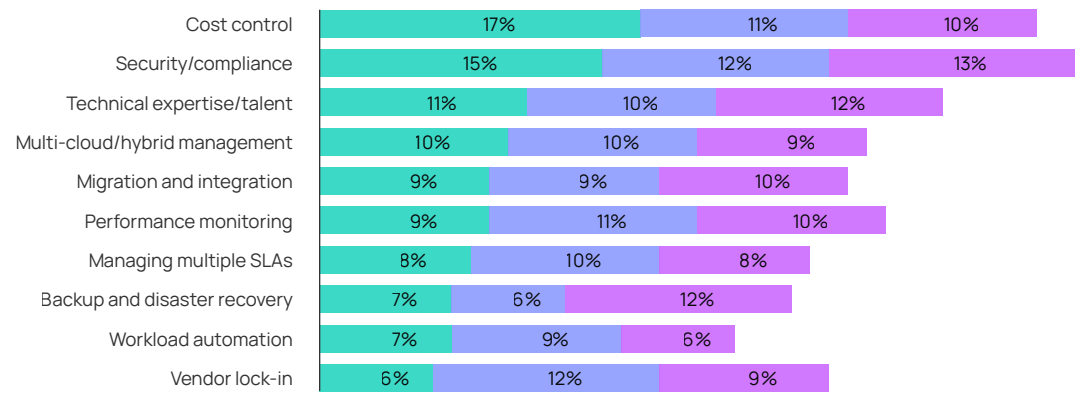
Cloud adoption is becoming more complicated due to unpredictable cloud costs and lack of cost optimization tools e.g., "cloud sprawl" or inefficient resource-use resulting in rising unexpected costs. Hybrid and multi-cloud environments are adding vulnerabilities by expanding the cyber-attack surface. Talent shortages, especially in high demand areas like cloud services, are making it more difficult for MSPs to recruit and retain talent. Multi-cloud environments provide redundancy yet add complexity to managing disparate workloads. Consequently, rising cloud costs could prompt MSPs to renegotiate service-level agreements (SLAs) to pass costs onto clients instead of absorbing them themselves.

MSPs should offer specialized "compliance-ready" or "security-first" cloud services to differentiate themselves and garner premium cloud services pricing.

FIGURE 18

What are your most significant cloud service challenges today?

(Choose the top three that apply, starting with your most significant challenge)



2023 referred to 'moving away from managing on-premises devices (server, storage) to virtual / cloud devices.
Source: Canalys, Candefero survey, 193 respondents, October 2024 to November 2024

SECTION 3

External Factors

How to deal with the three C's:
Compliance, certifications and cyber-insurance

Introduction

MSPs are navigating a transformative landscape shaped by risk management and operational efficiency. Cyber insurance adoption is driven by the pressing need for data breach coverage, business continuity, and regulatory compliance, reflecting a heightened focus on resilience. Some of these concerns can be addressed through training and certifications, from third parties or vendors. However, managing numerous vendor relationships has become cumbersome, with MSPs seeking to consolidate their vendor base to improve efficiency and streamline operations. This presents a pivotal opportunity for vendors to strengthen partnerships by aligning solutions with MSPs' compliance needs, offering integrated platforms, and delivering proactive support that fosters long-term loyalty.

Key Takeaways

- Managing numerous vendor relationships has become cumbersome. MSPs are seeking to consolidate their vendor base to drive efficiency and streamline operations.
- It is in MSPs' best interest to invest in building Compliance-as-a-Service practices that offer automated audits, policy management, and incident reporting.
- To ensure their business doesn't fall short, MSPs leaders must advocate for continuous learning within their organization.
- Core drivers for cyber insurance differ between MSP and customer. MSPs need to be aware of this…68% of MSPs cited business interruption coverage as their biggest driver, whereas data breach coverage was cited as the main motivator for their clients.
- MSPs must take time to carefully evaluate their existing vendors based on integration ease, pricing, support, and alignment with business goals. Comparing vendor programs and features like marketing development funds (MDFs), lead generation, and technical training is crucial.

OBSERVATION

Tech and finance compliance are the most prevalent amongst MSP customers

To avoid penalties, ensure contracts, and qualify for cyber insurance MSPs and their clients must adhere to certain compliance requirements. In addition, governments and industry regulatory bodies are enforcing stricter rules on cybersecurity, driving adoption of compliance standards and failure to comply can result in fines, lawsuits, and loss of business opportunities through being blacklisted.

> ***Compliance and regulation pressures, plus specialization in specific industries will become more important as compliance requirements expand."***

As the IT environment grows more complex, businesses are adhering to compliance standards and adopting frameworks like ISO 27001 and NIST to ensure secure and standardized practices, which MSPs must align with as well. According to the 2025 MSP Horizons survey, respondents claimed the most common regulatory statutes affecting their customers were financial (93%) and simple tech (89%), with 86% also citing cyber insurance compliance.

Understanding and meeting compliance requirements presents a major challenge to most businesses, so it is in MSPs' best interest — if they haven't already — to invest in building Compliance-as-a-Service practices that offer automated audits, policy management, and incident reporting. This will be especially useful in highly regulated industries like finance, healthcare, and government. On top of this, compliance education offers another avenue for MSPs to pursue. Hosting workshops, webinars, and training sessions on the latest compliance standards that they and their customers will have to comply with, not only offers another potential revenue stream, but also helps build their trusted advisor status.

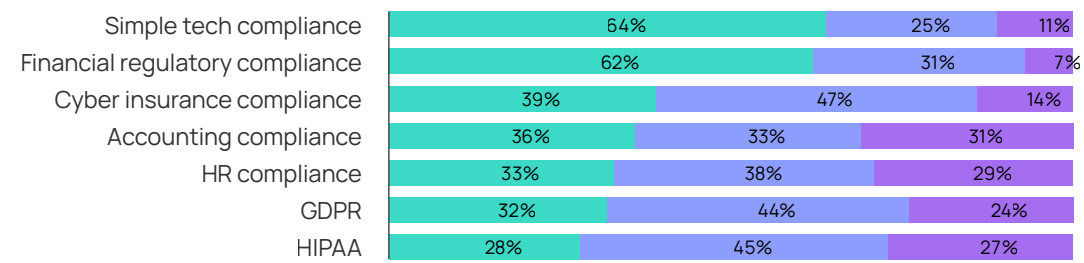
Most offered compliance:

64% Financial Regulatory Compliance

62% Regulatory Compliance

FIGURE 19

Do your customers have to adhere to compliance standards today, and what kinds do you offer?



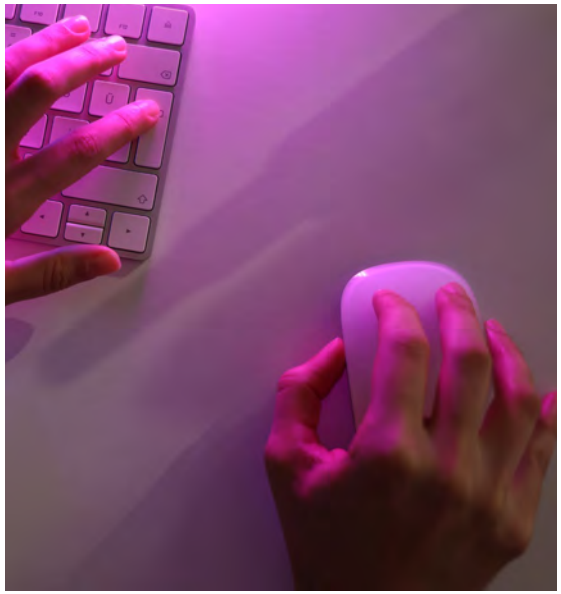
- Yes, they do, and we offer services to help them with this
- Yes, they do, but we don't offer services around any of these today
- No, they don't

Each column represents the percentage split of those that provided an answer for that question. Source: Canalys, Candefero survey, 407 respondents, October 2024 to November 2024

OBSERVATION

Successful MSPs are trained and certified

A major part of the upskilling that MSPs are finding challenging involves ensuring staff have proper training and certifications, this is critical for MSPs that operate in highly regulated industries. Certifications help MSPs differentiate themselves while validating that they have the necessary expertise to perform the services they offer.



Cybersecurity and data protection are key areas where certifications and training are crucial for meeting the latest industry standards and protecting client data. To ensure their business doesn't fall short, MSP leaders must advocate for continuous learning within their organization. Incentivizing employees to pursue certifications and rewarding them for achieving these is a strategy most employees will welcome. Identifying key certifications that are relevant to the markets they serve and aligned with their service offerings is a crucial step in that process. Proper budgeting and setting reasonable timelines for staff certifications is also key. Once training and certifications have been obtained, they can be used as marketing tools to showcase and promote the organization's competencies.

Recognizing the growing demand for certifications among their clients, MSPs should also consider adding certification training to their portfolio and use it for both internal and external purposes.

> ***We're big on certifications – even our HR team does an Azure training because we want everyone on the same level."***

> ***We will be enforcing metrics and SLAs in the future and need to be better at investing in training and skills."***

OBSERVATION

Top cyber-insurance drivers: Business interruption and data breach coverage

Breaches are increasingly costly, with expenses including everything from recovery costs to legal fees, and reputational damage. Cyber insurance can help mitigate these risks by ensuring MSPs and their customers are financially protected.

> ***Cyber insurance is the best salesperson I've ever had. Insurance requirements push clients to adopt good solutions. We support these requirements as long as they align with protecting our clients' businesses."***

While clients are the most obvious victims of cyber-attacks, MSPs can also suffer irreparable reputation loss as a result. The surge in ransomware attacks and data breaches has made cyber insurance non-negotiable. Cyber insurance providers require adherence to stringent security protocols before issuing or renewing policies, these impact both MSPs and their clients.

The MSP Horizons survey found that MSPs understand these circumstances and are adapting accordingly: 68% of respondents stated that business interruption coverage was their biggest driver for obtaining cyber insurance, whereas data breach coverage (66%) was the main motivator for their clients. Cyber insurance and compliance go hand in hand as the former is often required to comply with industry standards.

MSPs realizing these trends would be advised to exploit them by offering consulting services to help clients navigate cyber insurance requirements, from assessing readiness to implementing mandatory controls, thereby creating new revenue streams. Also, they should consider partnering with cyber insurers to offer bundled services that include managed security and pre-approved insurance plans for clients thereby simplifying the buying process for their customers.

> ***(We are) definitely seeing some pressure on the cyber insurance side, which is good because it drives value for the MSP."***

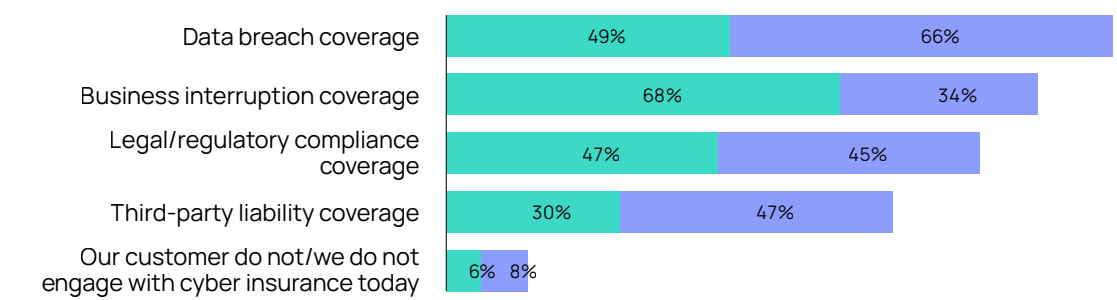
Key Drivers for Cyber Insurance

MSPs
Business Interruption Coverage (68%)

Customers
Data Breach Coverage (66%)

FIGURE 20

What are the biggest drivers for you and your customers in buying cyber insurance today? (Choose the top two that apply in each column)



Each column represents the percentage split of those that provided an answer for that question. Source: Canalys, Candefero survey, 410 respondents, October 2024 to November 2024

OBSERVATION

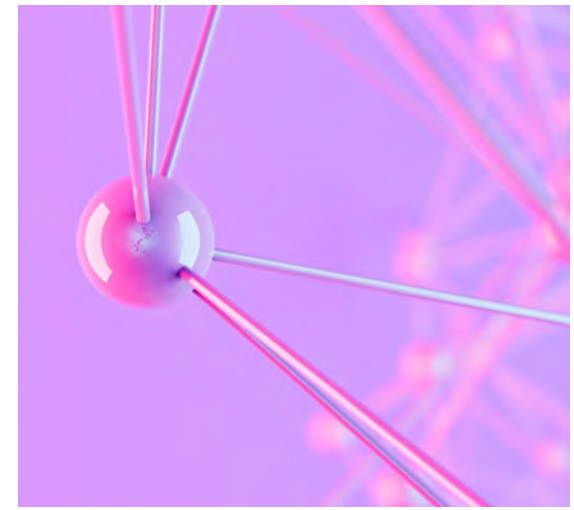
MSPs want to manage fewer vendors, not more

Small MSPs have a lot of roles to fill without a lot of people to fill them, add to this the fact that they may use a lot of different tools to complete those roles, and it's easy to understand why they must choose the tools and vendors they buy them from carefully. Managing multiple vendor relationships, contracts, and integrations adds administrative overhead and resource strain to MSPs.

Increasing vendor counts adds complexity to interoperability, creating inefficiencies in service delivery. As a result, vendor consolidation helps MSPs negotiate better terms, reduce licensing overlaps, and minimize redundant tools. By standardizing on a set of tools or platforms offered by certain vendors, MSPs can streamline their operations and deliver consistent customer experience.

> ***"Probably between 10 and 15 vendors. We'd like to consolidate if possible. We create custom integrations between different vendors because we prefer one vendor over another for specific products or services."***

Before consolidating vendors, MSPs should take time to carefully evaluate their existing vendors based on integration ease, pricing, support, and alignment with business goals. Comparing vendor programs and features like marketing development funds (MDFs), lead generation, and technical training will be important. Once the proper vendors have been identified MSPs need to prioritize them based on those that offer multi-functional solutions or platforms that simplify the process of buying multiple solutions. After onboarding, developing performance scorecards will help MSPs regularly assess vendors based on KPIs like responsiveness, support quality, and value delivered.



> ***"We have been trying to consolidate that number. Our goal is to have an all-inclusive integrated solution under one pane of glass, making it easier for an MSP to manage."***

The downside of this consolidation is that it can increase the gap between the haves and have-nots, potentially putting smaller or niche vendors at a disadvantage if they are unable to supply the platform-based solutions MSPs prefer. Ultimately this may increase the number of vendor M&As over the next few years, creating fewer vendor options in the market leaving only the dominant players.

OBSERVATION

Vendor partnerships have room for improvement

During the 2025 MSP Horizons interviews most MSPs were satisfied with their vendor relationships, yet there were some that expressed concerns. Some of their sentiments can be attributed to a desire to reduce the number of vendors they manage, as mentioned in the section above. Other feelings were based on factors like inadequate training or technical support, inconsistent or unplanned pricing changes, or general lack of communication.

> ***"In previous years, vendors regularly walked us through their current vision, connecting us to their strategy – this year, instead of vision, all we received was a push to sell more and trust the process. It's disappointing, but there's no choice but to participate as those are key market players."***

This type of feedback is vital for sustaining vendors' success in the channel and should not be taken lightly. In response vendors need to stay on top of their game and not rest on their laurels or else MSPs will take the action of choosing their company as one of those it will remove in their consolidation efforts.

To avoid becoming a consolidation casualty, vendors should focus on fostering long-term partnerships with MSPs by investing in partner success programs, including technical enablement, co-selling, and marketing resources. They should also develop integrated offerings or bundles that address multiple MSP needs, such as combining security, backup, and monitoring into a single platform. By providing regular updates and roadmap discussions, it creates feedback loops to keep MSPs informed. Vendors will be wise to design pricing models and programs that scale with MSPs' growth and align with their business goals.

> ***"When vendors change prices mid-cycle or something like that, that definitely does something with our margin, but usually that price change would get passed to the customers and yeah, that's how it goes."***

The fact that MSPs are looking for deeper, more strategic relationships with fewer vendors, should inspire them to invest in more modern partner programs using value-based or point-based systems, joint go-to-market strategies, simplified pricing, and co-innovation initiatives; and those unwilling to do so will see the most churn.

Conclusion

Turning obstacles into opportunities

In 2025, Canalys estimates more than 330K channel partners will generate close to US $600B in managed services revenue, representing +13% growth vs. 2024. The MSP industry is entering a pivotal era defined by strong revenue growth potential, shifting operational dynamics, and evolving customer expectations. These trends are driven by the convergence of escalating cybersecurity threats, the complexity of hybrid cloud environments, growing compliance demands, and the need for deeper customer collaboration.

Going beyond the basics in cybersecurity

Managed security services revenue will continue to soar, given 90% of partners are expecting growth in this area, as businesses face escalating cyber threats and stricter compliance requirements. Over the next few years, MSPs will go beyond basic firewall and endpoint protection to deliver comprehensive security ecosystems, including AI-driven threat detection, incident response as a service, and proactive compliance management. This trend will push MSPs to integrate advanced threat, zero-trust, and real-time security platform-based solutions. Leveraging vendor relationships for co-marketing/selling, cyber insurance partnerships, and education will allow MSPs to remain at the forefront of security innovation.

Embrace M&A to gain competitive advantage

Also, MSPs must refine vendor relationships, consolidating partnerships to foster deeper collaboration and access to platform-centric solutions. The world around them is in flux, so they can look to M&A as an effective way to expand their technical capabilities, enhance their reach, and obtain competitive advantages in a crowded market. By turning obstacles into opportunities and addressing challenges such as acquiring new clients and adapting to compliance complexities, MSPs can ensure sustained growth

while solidifying their position as indispensable technology partners.

To capitalize on these shifts, MSPs should prioritize building scalable and secure service portfolios focused on cybersecurity, backup and disaster recovery, and compliance—critical areas that resonate with client needs and align with regulatory pressures. Co-management, supported by multi-tenancy tools and embedded AI solutions for customer support, will enable MSPs to strengthen client partnerships while differentiating their offerings.

Specialization is crucial to survival

While 59% of partners said their revenue would grow more than 20% year on year in 2025, this expansion will come with heightened competition and client demands. To sustain growth, MSPs must specialize in more niche industries (e.g., healthcare, financial services) or technology areas (e.g., cybersecurity, backup (BDR). Adopting scalable service delivery models that leverage automation, multi-tenancy tools, and hybrid cloud platforms will help them manage larger customer bases without proportionally increasing overhead. Developing vertical-specific expertise and tailored service bundles will allow MSPs to command premium pricing and differentiate.

The future is hybrid

A notable 7% of MSPs are projecting to go all-in on cloud backups in 3-5 years from now, reserving on-premises backups for specific industries and use cases with low-latency needs or stringent data regulations (e.g., government or healthcare). More affordable cloud storage, advancements in multi-cloud, and enhanced backup performance will make cloud-first strategies more enticing. MSPs are expected to offer hybrid backup solutions that blend the scalability of cloud storage with on-premises solutions for critical workloads. Guiding clients through seamless cloud migration to secure and cost-effective cloud backup environments will be pivotal to growing cloud services.

Compliance changes everything

Compliance, led by financial regulations (93% of customer adherence), simple tech (89%), and cyber insurance (86%), will become non-negotiable, especially in highly regulated industries, with insurers mandating more rigorous cyber hygiene and compliant business operations for coverage. Governments will impose stricter regulations, especially regarding privacy (e.g., GDPR) and emerging AI governance, forcing businesses to align with updated standards. MSPs will need to bundle compliance and risk assessment services into their offerings to meet new client demand. Staying ahead of regulatory changes by partnering with compliance experts and integrating tools that simplify adherence to multiple frameworks must also be explored.

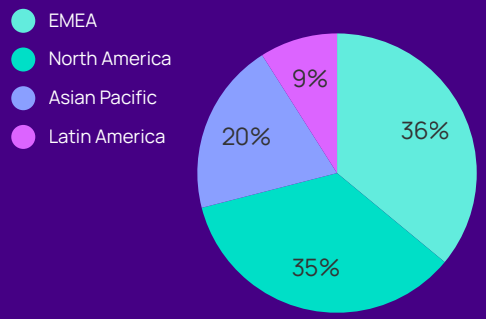
Over the next decade, MSPs that embrace agility, strategic consolidation, and a customer-first approach can flourish. Those who fail will risk being left behind as the industry shifts toward leaner operations, innovative service models, and transformative technologies. To survive and thrive MSPs must evolve, invest, and lead in the rapidly changing IT ecosystem.

Methodology

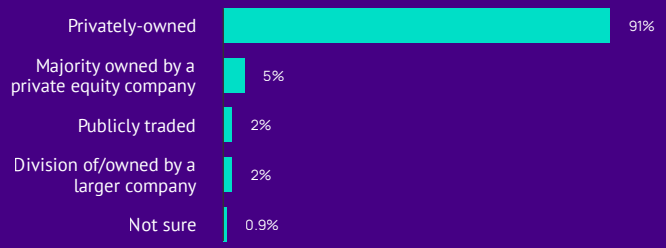
The MSP futurology study survey was conducted from October 2024 to November 2024. Partners were asked to provide feedback via an online questionnaire distributed by N-Able and Canalys via its Candefero website.

- The survey captured feedback from 451 business-to-business channel partners, with at least 411 partners answering at least 16 questions.
- Canalys interviewed 16 partners during the process, which afforded qualitative feedback regarding key topics and trends in the IT market.

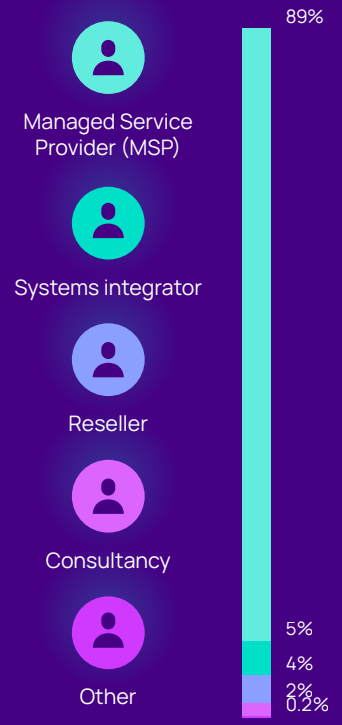
Breakdown by Region[1]



Breakdown by Ownership Type[2]



Breakdown by Partner Type[1]



Sources: 1 Canalys, Candefero survey, 451 respondents, October 2024 to November 2024
2 Canalys, Candefero survey, 434 respondents, October 2024 to November 2024