MSP market focus in 2021

IT security challenges and opportunities in the new normal

kaspersky BRING ON THE FUTURE

Learn more: kaspersky.com

Contents

Introduction

The role of managed service providers (MSPs) today has changed significantly over the past two years. Far from being just a service and management provider, MSPs are key to their clients' success. According to Gartner, "managed service providers must establish a customer success mindset and lead with continuous innovation to keep clients engaged in the long run."

This has certainly been true during the COVID-19 pandemic with clients looking to their MSP to be that trusted adviser and help them navigate a potentially tumultuous time in business. With digital transformation happening at break-neck speed, MSPs have to keep pace and take care of the evolving needs of their customers, as well as their own business.

With technology underpinning new ways of working and business models, IT security has been thrust into the spotlight. Downtime today is simply not an option. So, what effect has this had on growth in the MSP market and customer needs? Can providers keep up and what challenges are they facing today to continue their growth trajectory and give clients the right support and services?

This report sets out the challenges and opportunities in the market and the role that IT security plays in helping overcome obstacles and achieve success in the long-term.

Methodology

The findings in this report are taken from two data sources:

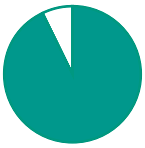
- The Kaspersky MSP 2021 study, conducted in June-August 2021. The research involved insights from 606 quantitative interviews conducted in 21 countries, and eight in-depth telephone interviews conducted with selected respondents from the quantitative study. Businesses interviewed included MSPs and MSSPs who provide IT services to client businesses which supply managed IT and security services. Respondents were managers or those in more senior positions and all have influence on decisions about which IT security vendors are offered to clients.
- Kaspersky Corporate IT Security Risks Survey 2021 – an annual, online survey of business IT decision makers conducted in May-June 2021 across 31 countries.

The report will occasionally refer to different types of MSP, definitions for which are outlined below:

- **Traditional IT service providers** offering old-school solutions, not relying on professional services automation (PSA) software to automate their offering. May use remote monitoring and management (RMM) software
- **Highly automated MSPs** who make use of PSA software to provide a more 'off-the shelf' approach to IT services, to keep up with the demands from clients seeking more for their money
- **Large IT services companies** who traditionally only serve the largest enterprises but are using automation to extend their reach to smaller clients
- **Managed security service providers (MSSPs)** offering specialized IT security services have emerged as a separate category and grown rapidly. Most are between three and five years old but have already grown to considerable sizes

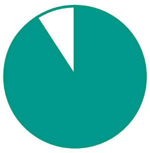
Key findings

93%



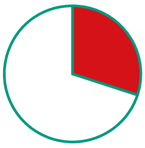
of MSPs stated that they are looking to expand their IT security offering

91%



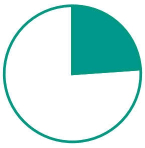
MSSPs reported an increase in their client base since 2019

30%



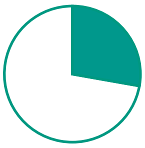
of MSPs report finding new customers remains one of their biggest challenges

24%



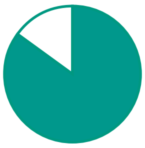
of businesses working with MSPs started the relationship in direct response to a data breach

28%



reported that the SolarWinds event had affected their organization in some way

85%



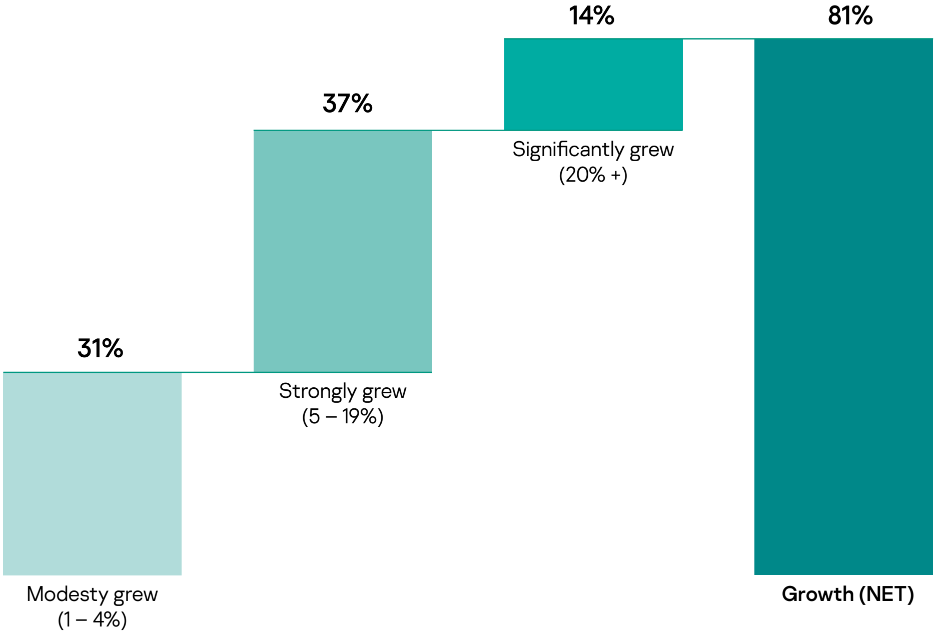
of MSPs who were aware of the event made changes in response

The MSP market today

As with all sectors of business, the MSP market has had to adapt and demonstrate huge resilience and agility during the COVID-19 pandemic, to remain relevant to clients and continue to support their changing business needs. As a result, the sector has seen strong growth since 2019.

This is particularly true for MSSPs, with nine in 10 (**91%**) reporting an increase in their client base since 2019. For MSPs, this figure was slightly lower at **81%** but still extremely positive. Indeed, **94%** of MSPs expect this trajectory to continue, predicting revenues will increase over the next two years.

Chart 1: Change in number of clients since 2019



But sustaining this growth and the effort needed to maintain the current upward trend is not easy. For almost a third of MSPs (**30%**), finding new customers remains one of their biggest challenges. The issue is even more common for traditional IT service providers (**37%**), and highly automated MSPs (**35%**). With **57%** of MSPs/MSSPs currently focusing on providing IT/IT security to one or more specific industries, **70%** believe this breadth of verticals will increase in the next two years.

Meeting client needs

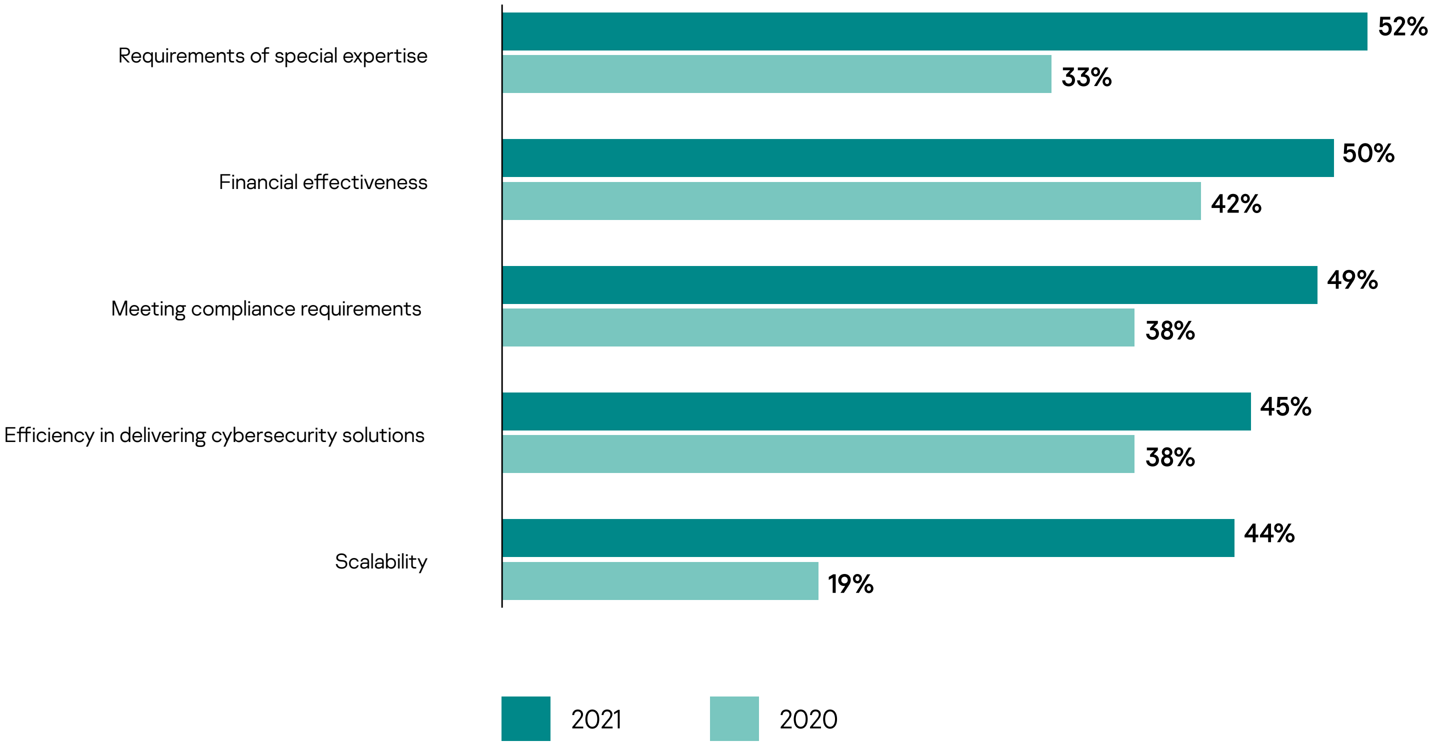
Now more than ever, clients are looking towards external experts to help them navigate the potential pitfalls surrounding technology use, in order to continue to reap the benefits.

As business models evolve, MSPs need to be able to react and remain a trusted partner during times of uncertainty. But this puts extra pressure on them to stay ahead of the game and on top of the very latest customer needs and solutions available.

Our research has shown that client motivation for using MSPs is certainly shifting in this direction, with the need for additional expertise cited as the top reason to use MSPs (**52%**). Advanced cyberthreats and legal requirements, along with the speed at which businesses now need to deploy technology to support today's hybrid working norm, have all increased the need for more specialized IT security support.

Businesses also turn to MSPs in direct response to a data breach. **24%** of businesses using an MSP/MSSP confirmed that. This again demonstrates the need for businesses to have dedicated and specific resources at their disposal to prevent a breach from happening and safeguard against what could potentially lead to huge financial and reputational consequences if not tackled properly.

Chart 2: Top reasons to use MSPs/MSSPs



Remote working: a catalyst for change

For many businesses, the acceleration of technology use to facilitate home working has opened their eyes to the huge potential of digital channels.

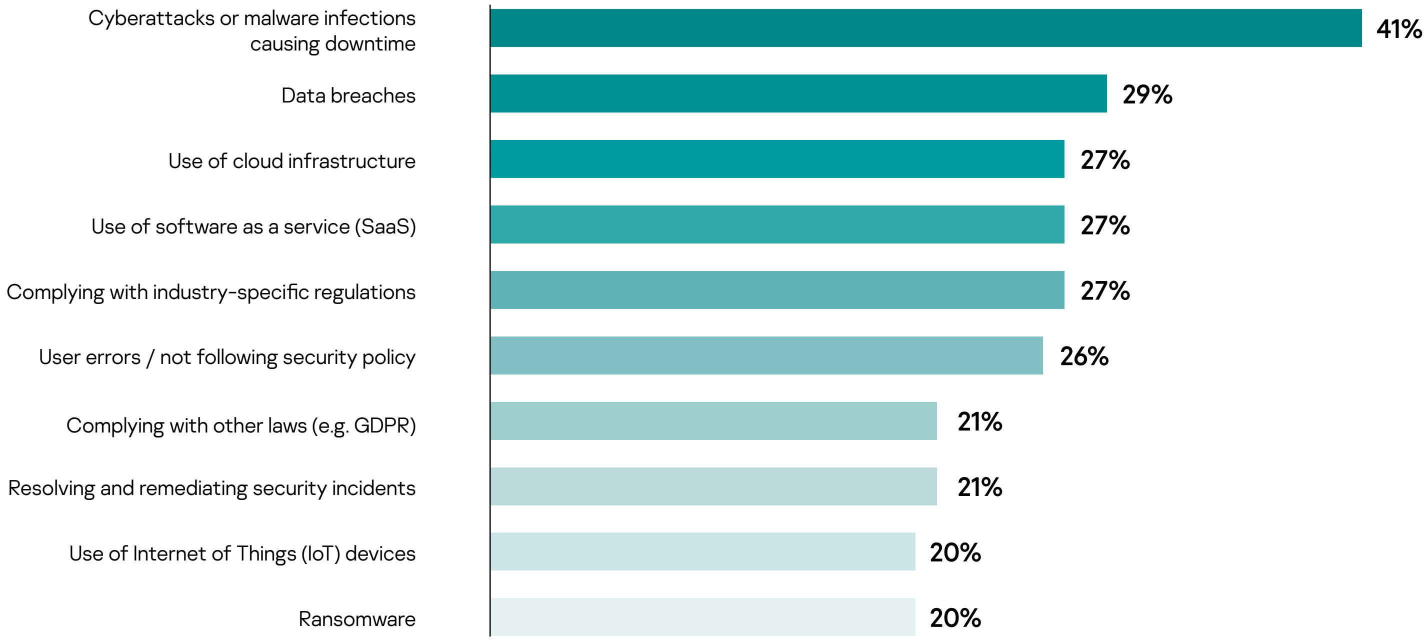
As we come out the other side of the pandemic, despite a shift in priorities, our research found that confidence among businesses in adopting new technologies and solutions is growing. Respondents also confirmed the vital role played by MSPs in supporting this transition and removing tech worries so they can focus on their core offerings.

More reliance on technology has also seen increased understanding by businesses of the need for airtight cybersecurity to safeguard their data. With technology underpinning mission critical processes, it is vital that the connection between IT security and digital dependency is not underestimated.

Indeed, this reliance on digital continuity and complex distributed infrastructures, coupled with a lack of resources and skills, has increased concern among businesses about their ability to ensure cybersecurity. Attacks resulting in downtime, particularly ransomware and cryptolocker type attacks were frequently mentioned by respondents as a key concern affecting their business.

The increase in remote working and greater reliance on digital channels means that any downtime has the potential to hit businesses much harder. In addition, keeping track of increasingly complex and distributed assets has become a major challenge, making their security a huge headache.

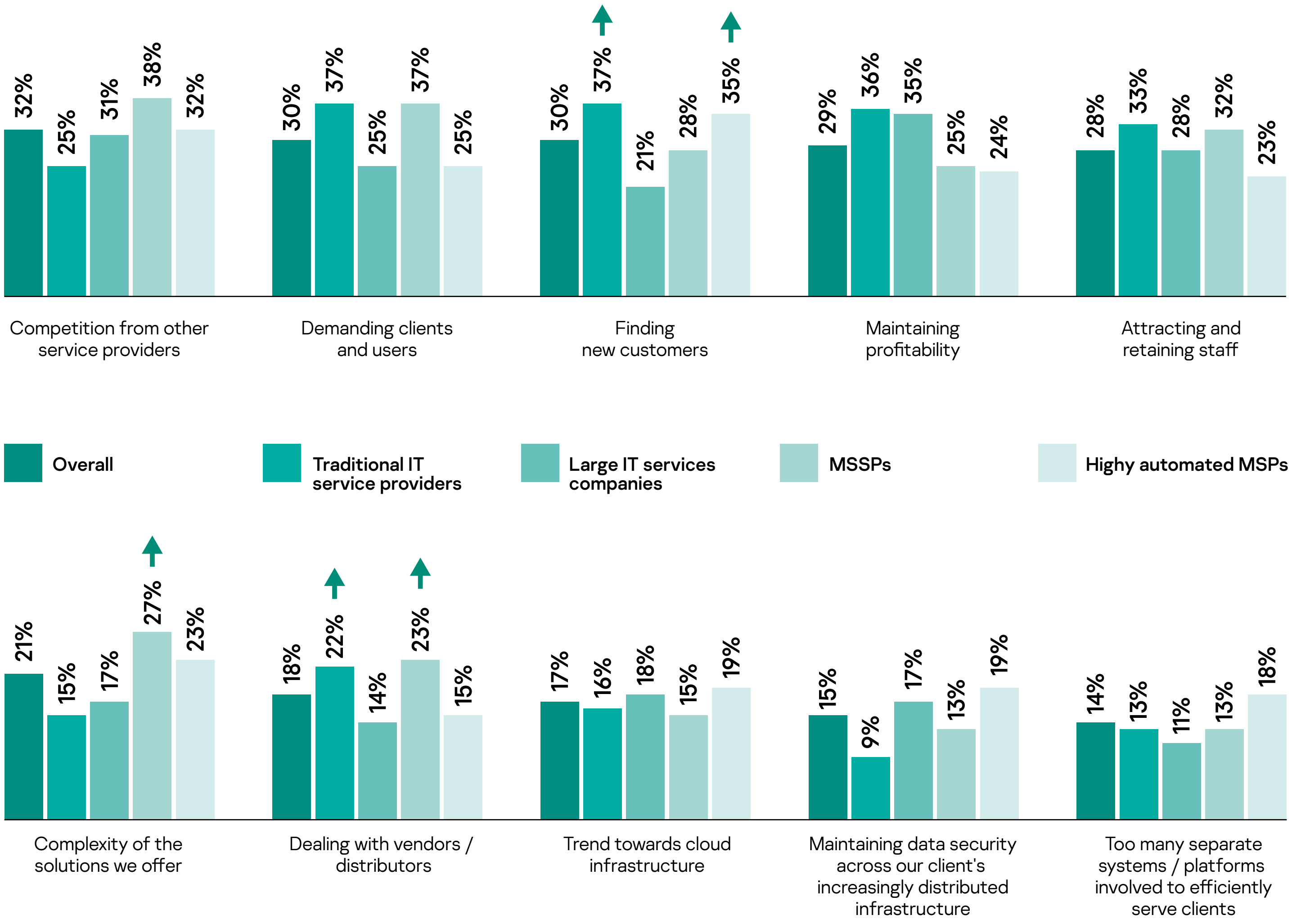
Chart 3: Top 3 unsolved IT security challenges for clients



MSP challenges

Despite expected revenue growth and opportunities for MSPs alluded to earlier in the report, concerns remain about how to maintain profitability. 29% of MSPs cite this as one of their top three concerns in 2021, consistent with findings in 2019 when 30% thought the same.

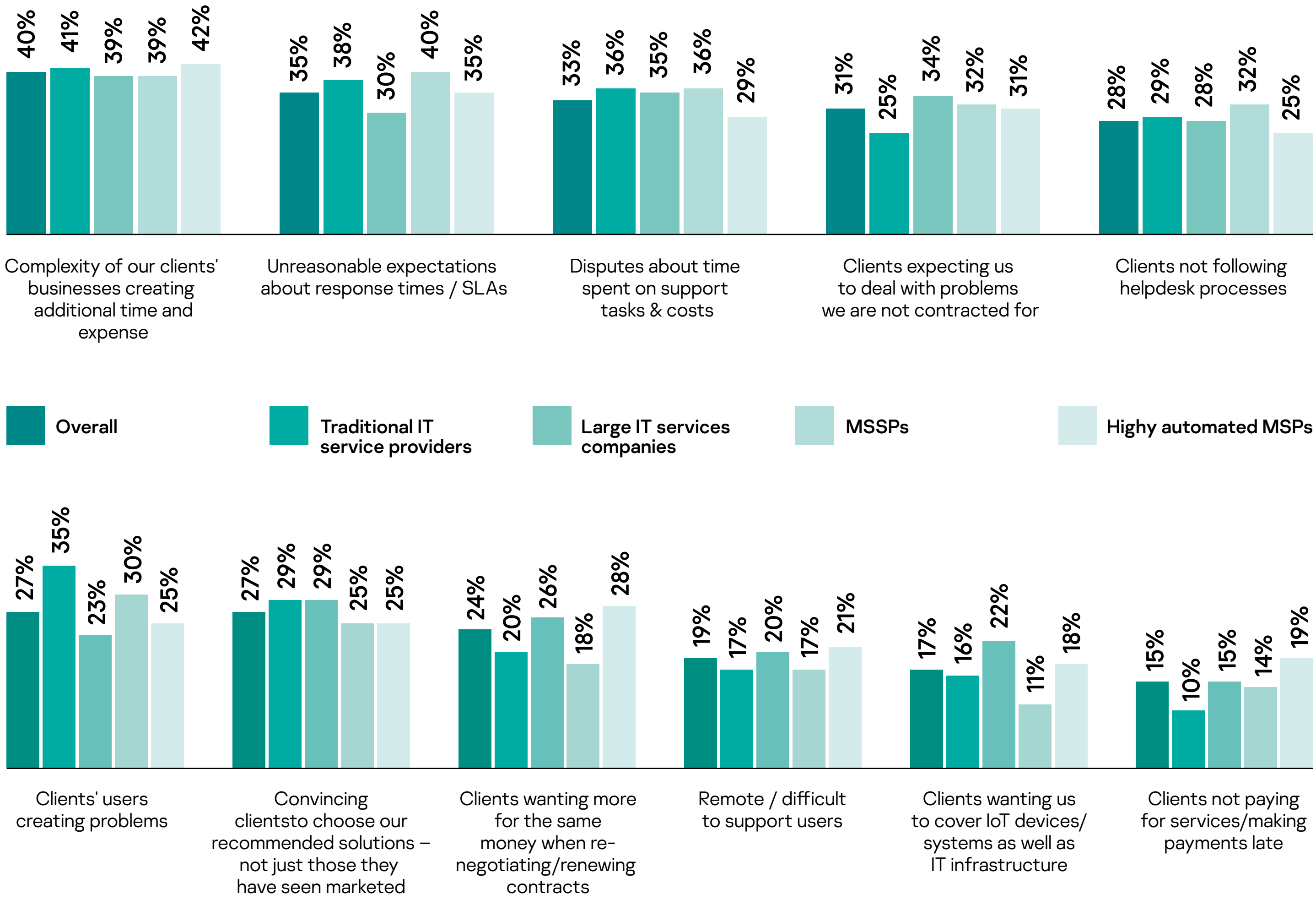
Chart 4: % Selecting each challenge as one of the Top 3 challenges they face (Top 10 challenges only)



What has changed and has a marked impact on MSPs' ability to grow, is the level of competition in the market. Almost a third (**32%**) selected competition from other service providers as one of their top three challenges in 2021, compared to only **19%** in 2019. This concern is well founded, with new entrants in the form of telecoms providers, IT integrators and value-added resellers (VARs), basing their offerings around specialized security skills or automation in a bid to oust the more 'traditional' MSP players.

Alongside challenges, MSPs were asked about specific pain points when dealing with clients. The complexity of client infrastructure remains the top issue but there is also a raft of additional areas which hamper MSPs' ability to service clients. These include keeping up with compliance requirements, unrealistic client expectations and demands, and attracting and retaining skilled staff.

Chart 5: % Selecting each pain point of dealing with clients as one of the TOP 3 most challenging they experience



What MSPs want from vendors

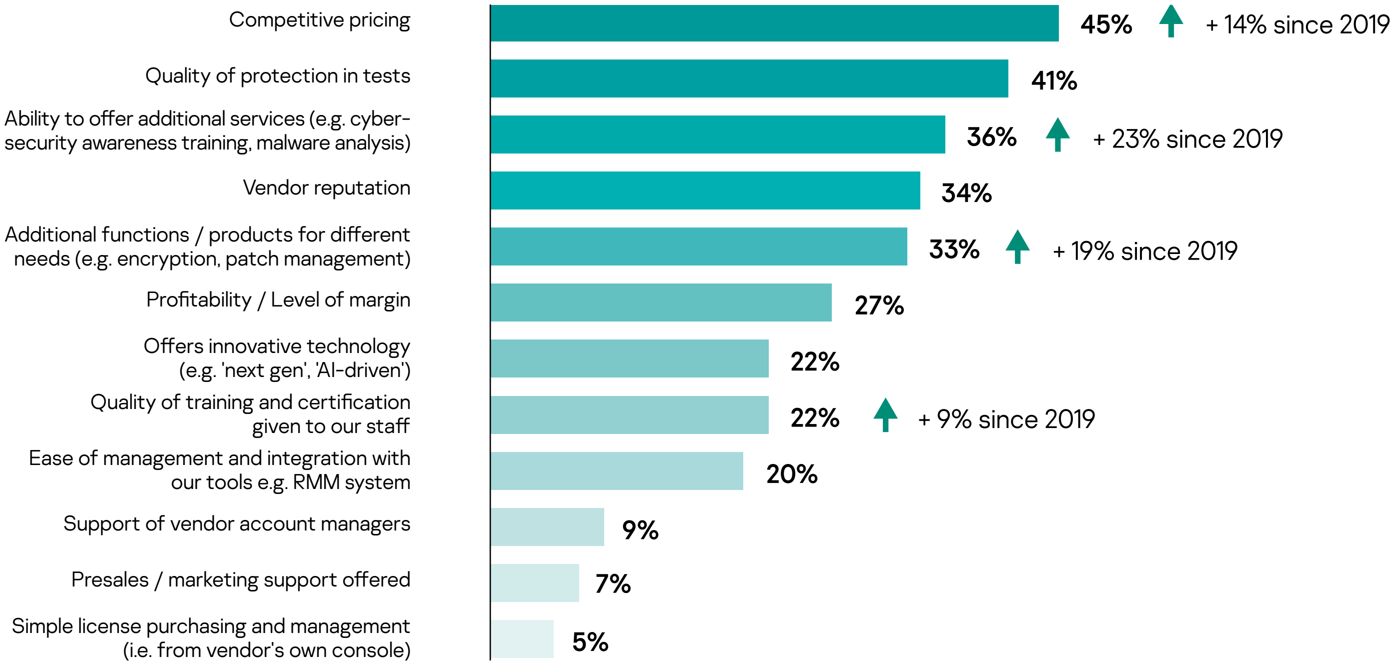
To help overcome the challenges and pain points highlighted, MSPs need the right support from vendors.

Without this, they will be unable to meet the rising demands of clients or remain competitive in a crowded market. In fact, significantly more respondents selected 'dealing with vendors / distributors' as one of the top three challenges they face in 2021 (**18%**) compared to 2019 (**10%**).

For MSPs, competitive pricing has become the number one criterion sought from IT security vendors, mainly among traditional IT service providers (**50%**) who increasingly rely more heavily in the margins they receive on these solutions to remain profitable.

At the same time, MSPs are also placing more emphasis on the ability of vendors to provide additional functionality and services. This is particularly important for MSSPs who are calling for additional functions (**39%**) and services (**41%**) to be made available to them by vendors.

Chart 6: The Top 3 things MSPs look for from IT security software vendors



Over half of MSPs and MSSPs (**57%**) offer specialized solutions, targeting specific industries. But **68%** of these are considering adding at least one specialized industry offering within the next two years.

93% of MSPs stated that they are looking to expand their IT security offering. When asked what type of services this might include, threat intelligence was cited as the top offering (**46%**) being sought from security vendors, closely followed by malware analysis (**41%**) and security assessments (**41%**). This call for more threat intelligence and analysis from vendors is in line with the expertise that customers have requested from their MSPs.

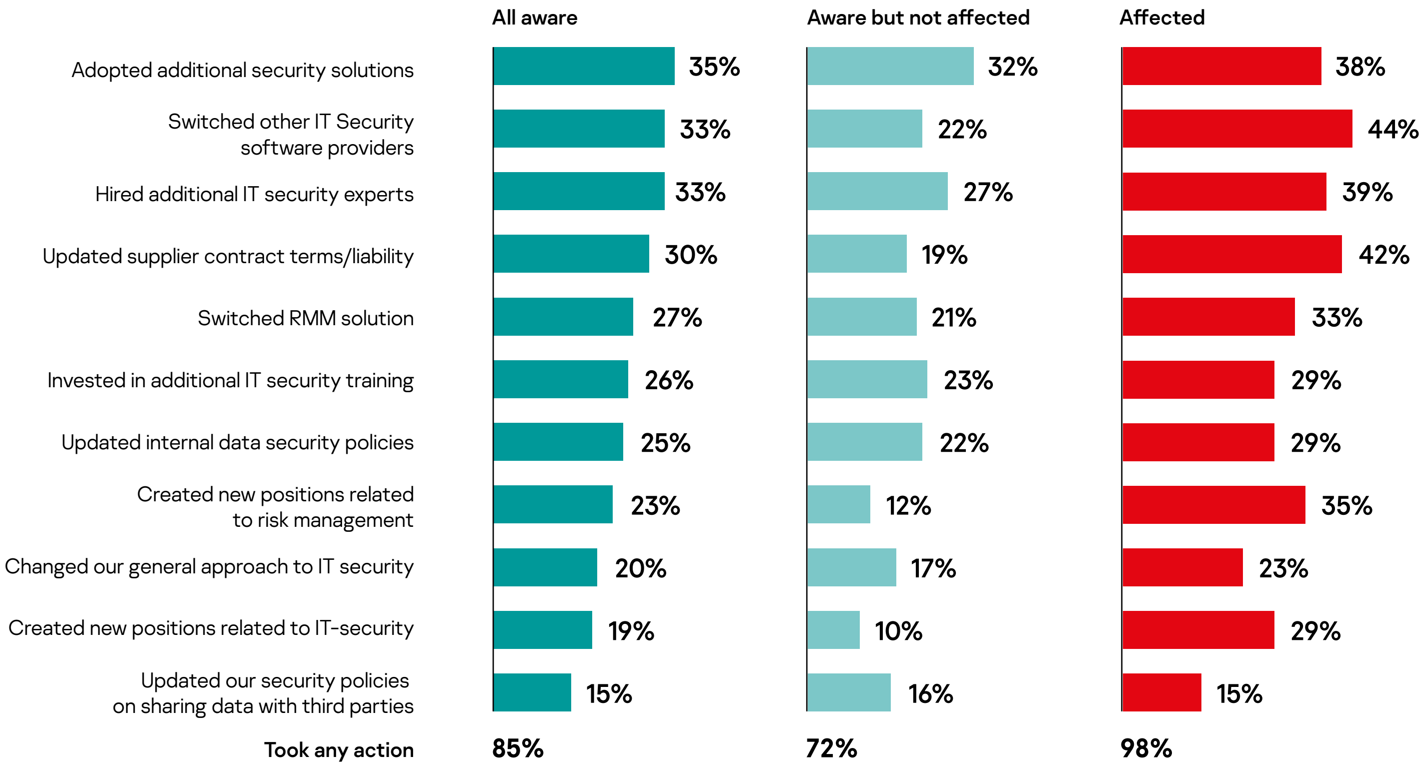
Learnings from the SolarWinds attack

Recent supply chain attacks have underlined the vital role played by IT management software and remote monitoring solutions for the sector.

Indeed, **70%** of MSPs/MSSPs make use of professional service automation (PSA) and remote monitoring and management (RMM) tools to automate the management of their clients' infrastructure.

The SolarWinds attack had a profound effect on the sector. **58%** of MSPs/MSSPs have followed the SolarWinds incident, which was revealed in late 2020, with over a quarter (28%) reporting that the event had affected their organization in some way. In response, 85% of MSPs who were aware of the event made changes. Those who were directly affected took broader measures, including creating new positions related to risk management and changing supplier contract terms and liability clauses.

Chart 7: Actions taken in response to the SolarWinds event



Following the incident, reported use of the SolarWinds solution fell from **21% in 2019 to 8% in 2021** (including mentions of their new brand, 'n-able'). It is clear from the aftereffects of the attack that security issues experienced by SolarWinds in 2020 have had a significant impact on its use amongst MSPs/MSSPs, or at least their willingness to admit to using it.

But it's not just SolarWinds that has been victim to attack. Recently, Kaseya, announced that it had become the victim of a cyberattack on July 2, 2021. Although the company revealed that less than 0.1% of its customers were affected, the knock-on effect for MSPs and their clients should not be underestimated.

Conclusion

When it comes to ensuring continued growth and profitability within the MSP market, there are many different approaches, strategies, and successes.

Large and more experienced providers do not always see the obstacles to entering new markets with tried and tested products. But for smaller companies, the strategy has typically been to hold on to the existing customer base and sell as many new products and services to them as possible. MSSPs often sit so deeply within their customers' business that they can predict the development of services and develop long-term plans to secure future revenues. For traditional IT providers, they see the future in new markets and new products.

No matter what the strategy, it is clear that dependence of businesses on IT is growing and will continue to grow, so it is very important for MSPs to pay serious attention to security. This means strengthening both the security posture and their own protection, which requires the installation of new products, and the provision of layered security on the customer side.

MSPs must take a holistic approach to security, partnering with trusted vendors on issues where expertise and specific resources are necessary but often lacking. As well as ensuring robust defenses, this approach will also help win new business and beat the competition. Ensuring security is seen as a key part of company success also requires the right mindset.

Clients need a trusted advisor, especially in the fallout of the pandemic, with MSPs well placed to be that long-term support which businesses crave. As such, it's important for MSPs to ensure they have the breadth of product line, an integrated approach, training, and support. This should also help them build the right set of security services, monetize them, and win new customers.

Kaspersky can help MSPs achieve this holistic approach to security and protect themselves and their clients. Our MSP cybersecurity framework includes building a multi-layered integrated security system, providing the most advanced services on the market – such as managed detection and response, and threat intelligence services – to support MSPs to gain expertise and knowledge.

To find out more about the research or how Kaspersky can support you on your growth journey, visit our **MSP page**.

Cyberthreat news: securelist.com
IT security news: business.kaspersky.com

kaspersky.com