

# Acronis

Report  
2021



# MSPs Speak:

Cybersecurity and the future  
role of the MSP

Survey conducted by  
Vanson Bourne in 2H'21



VansonBourne

With media  
sponsor:

**ChannelProNetwork**

# Table of contents

Executive Summary .....	3
Survey Methodology .....	4
<b>▶ Key Findings</b> .....	<b>6</b>
▶ Security threat level .....	6
▶ Cost concerns and coping with the rise of remote work .....	10
▶ Vulnerabilities created by usage of SaaS tools .....	15
▶ Cybersecurity service delivery complexity and the path forwards: Approaches to consolidation, integration and automation .....	19
▶ The case for consolidating and integrating cybersecurity, backup and disaster recovery .....	27
How Acronis can help .....	35
More information .....	43

# Executive Summary

**MSPs face numerous challenges in providing cybersecurity services which could be leaving them and their clients vulnerable to attack**

Service providers should be made aware of the threat level they and their clients are facing, so that they understand the need to improve their services. Vendors need to make service providers aware of the ways that their products can address the challenges that they are facing with regard to the security threat level, cost concerns, the rise of remote work, and SaaS tool usage.

**Many are taking steps to integrate and consolidate their cybersecurity, backup and disaster recovery services**

By mapping out the steps that MSPs are taking to do this, vendors can help them to discern where they stand on their own path towards integration and consolidation, compared to the rest of the market. By doing so, service providers will understand the need to integrate and consolidate to keep up with their competitors.

**MSPs which have integrated and/or consolidated their cybersecurity, backup and disaster recovery services are experiencing numerous benefits as a result**

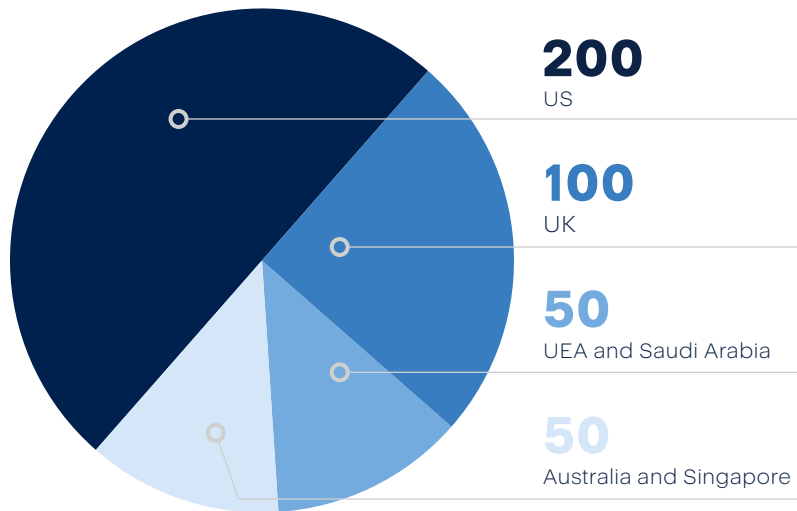
Demonstrating these benefits to MSPs will help to build demand for vendors whose solutions offer these capabilities, and has the potential to drive conversations between these vendors and their clients.



# Survey Methodology

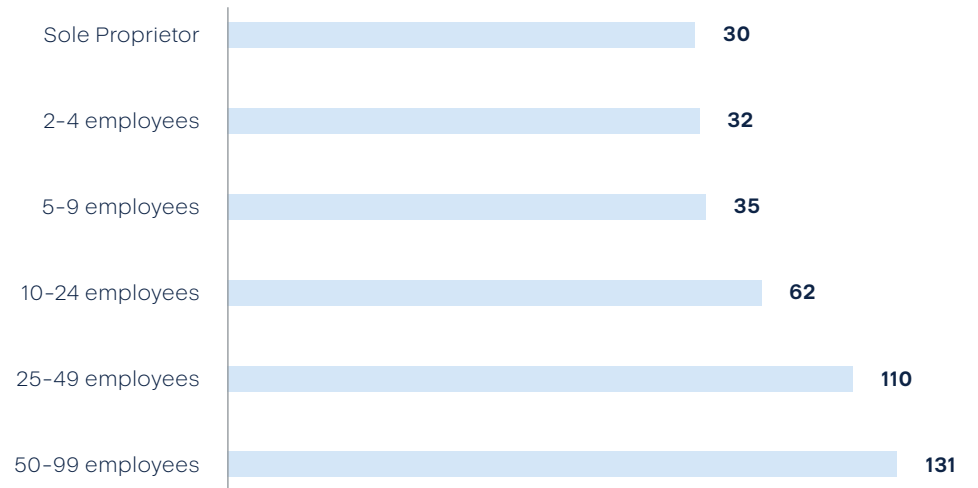
A total of 400 senior decision makers from MSPs which provide cybersecurity, IT security consulting and/or backup or disaster recovery services were interviewed in August and September 2021, split in the following ways:

## ...by respondent country



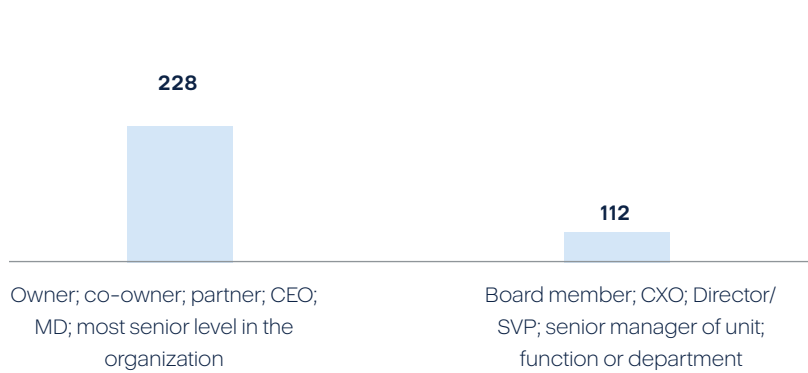
## Respondent country

## ...by organization size



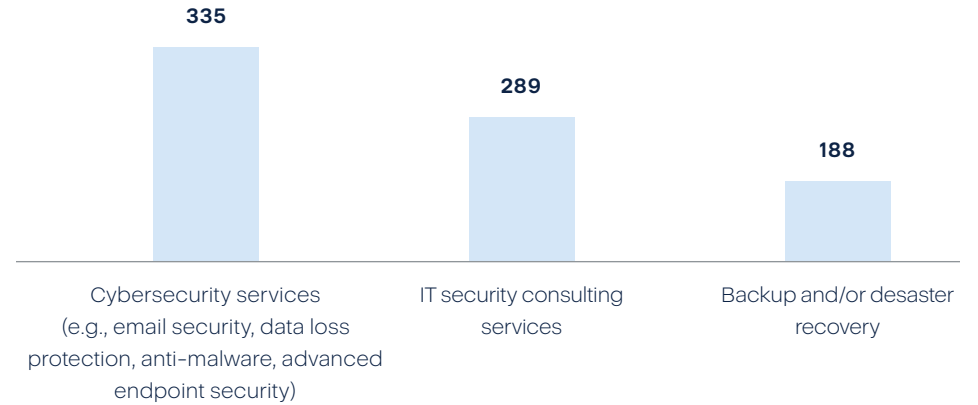
 How many employees does your organization have globally?

### ...by respondent position



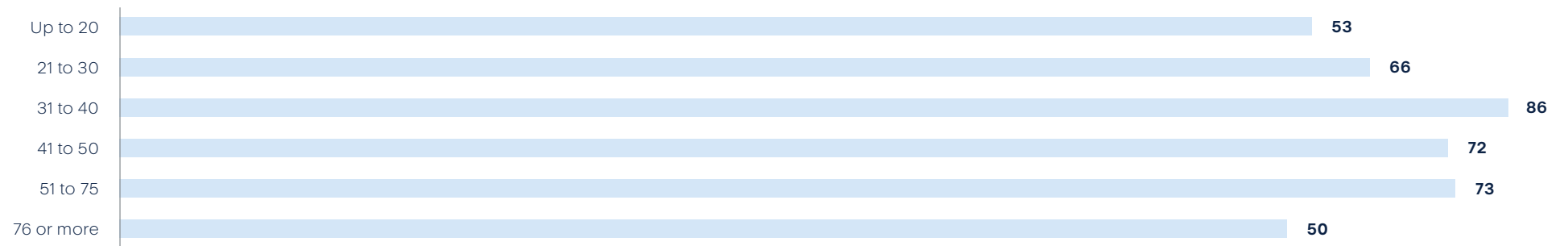
**?** Which of these best describes your position in the organization?

### ...by services provided



**?** Which of the following services does your organization provide to clients?

### ...by number of clients



**?** How many clients does your organization currently serve?

# Key Findings

The cybersecurity, backup and disaster recovery challenges facing MSPs and their clients:

## Security threat level

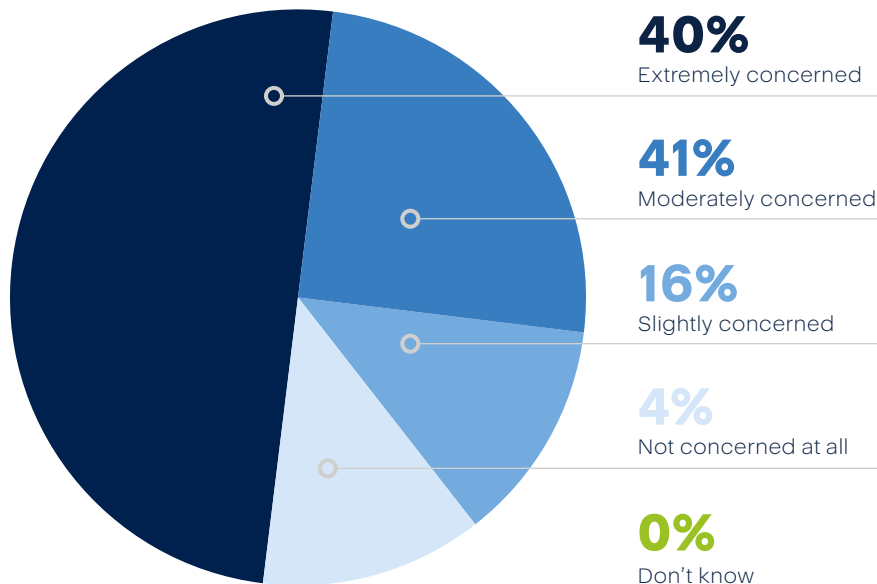


# Concern is very high about the risk of suffering a cybersecurity breach through which clients' IT systems are compromised

Supply chain attacks of this nature appear to be a huge concern for service providers. If an attacker is able to break into just one of the tools or solutions that a service provider uses, all of their clients could be at risk of an attack. The scale of attacks of this nature has the potential to be devastating to the service provider, as it will likely erode the trust that all of their clients hold in them.

This level of concern highlights the importance to service providers of not only protecting their clients, but protecting themselves. Key to this is the

vendors that service providers choose to work with to provide IT services to their clients. If these vendors don't themselves have strong protections in place on their tools, they could be open to an attack through which they, the service providers, and the service providers' clients could all be vulnerable. It is therefore crucial that service providers assess the protections that their vendors have in place.



**97% are concerned**



How concerned are you that your organization could suffer a cybersecurity breach through which your clients' IT systems are compromised in the next 12 months?

## A lack of trustabounds

If clients aren't able to trust the security of the services provided to them, the business relationship between them and their service providers could be put at risk, as clients may decide to seek out alternative providers who offer more extensive protection. The concern that MSP clients' have when it comes to security appear to be justified, given that the majority of providers

themselves don't trust the vendors they are using to provide cybersecurity services. Service providers who don't currently trust their vendors should look to alternatives who offer more robust levels of protection, in order to ensure their clients don't fall victim to an attack which could further degrade the level of trust their customers have in them.

# 49%

Admit their clients **do not completely trust the security** of the services their organization provides

# 53%

**Don't completely trust the vendors** their organization currently uses to provide cybersecurity services



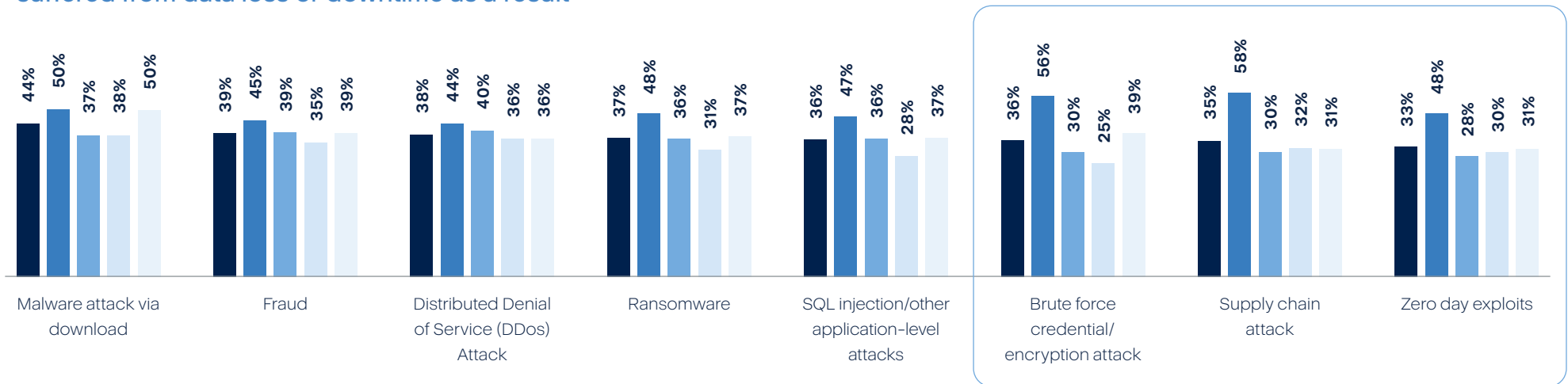


# The clients of smaller MSPs have suffered from data loss or downtime as a result of cybersecurity breaches

The smallest MSPs, those with only 1-4 employees, appear to struggle more than their larger competitors to provide security services which protect their clients against these types of attacks, and prevent them experiencing data loss or downtime as a result. This may be in part due to their low number of employees meaning that they lack the talent and skillsets in their workforce to provide robust security services. In order to ensure they are offering comprehensive security protection to their clients, smaller service providers are therefore likely

to be reliant on the tools they use to make up for any skillsets they are lacking. However, it appears that for many these tools aren't currently up to task. These service providers should therefore prioritize identifying new tools and solutions which can protect their clients against the threats they are currently vulnerable to, particularly brute force credential/encryption attacks and supply chain attacks. Tools which allow them to integrate and automate their services are likely be of huge value to these service providers.

“At least one of our clients experienced this, and they suffered from data loss or downtime as a result”



Showing the proportion of organizations' clients who have suffered each of the following, and suffered data loss or downtime as a result

■ Total (400) ■ 1-4 employees (62) ■ 5-24 employees (97)  
 ■ 25-49 employees (110) ■ 50-99 employees (131)

# Key Findings

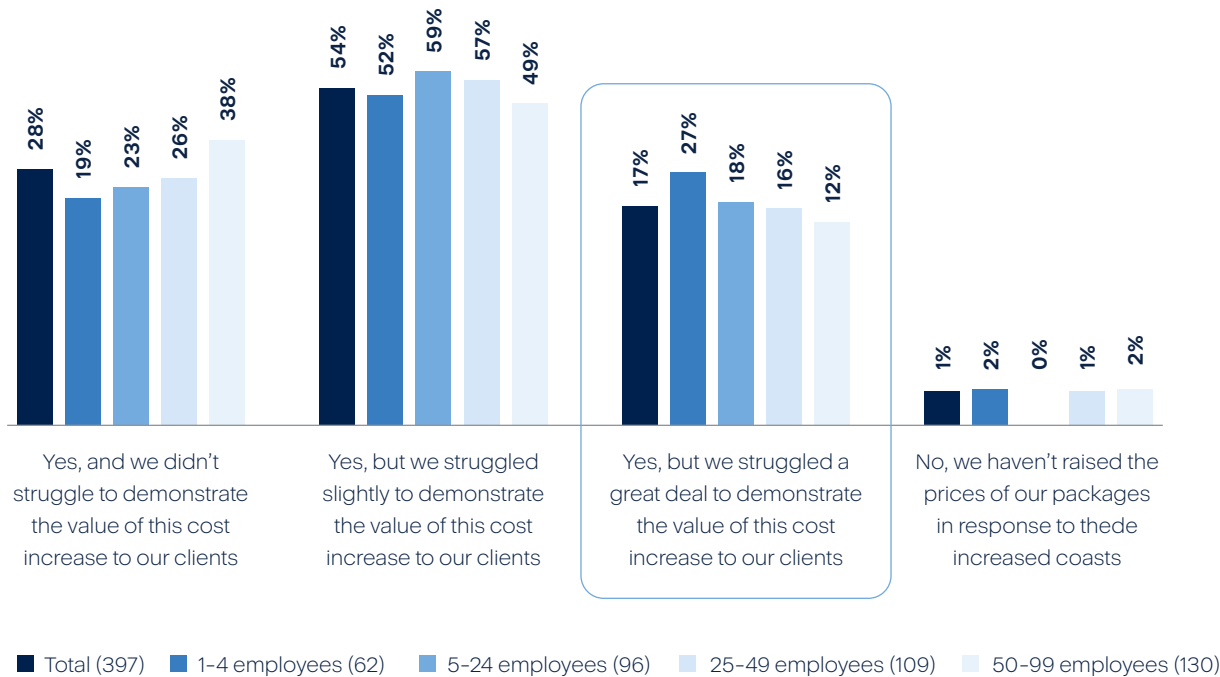
The cybersecurity, backup and disaster recovery challenges facing IT service providers and their clients:

**Cost concerns and coping with the rise of remote work**



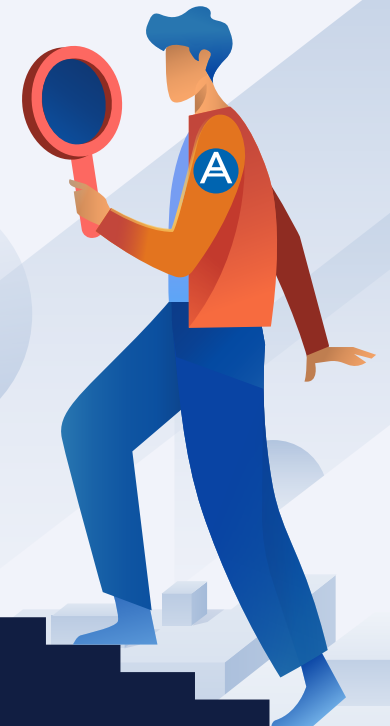
# MSPs struggle to justify their rising costs to clients

The escalating cost of providing these services, likely impacted by the cost implications of the rise in remote work has potential to cause huge problems for service providers. They cannot avoid investing in the necessary solutions to keep their clients protected, otherwise they risk losing their trust even further. However with many, particularly the smallest service providers, struggling to demonstrate the value of these cost increases to their clients, convincing their clients of the need for any future increases may prove challenging. If service providers aren't able to demonstrate the value of cost increases, they risk either losing the clients completely, or having to shoulder the burden of the increase themselves, without adjusting the cost paid by the clients, thus reducing their own profit margin.



# 19%

**Average increase in the cost** of providing cybersecurity, backup and/or disaster recovery services in the past two years



**?** Has your organization passed on the rise in these costs to your clients by adjusting your pricing packages?

# Increasing costs are eroding margins

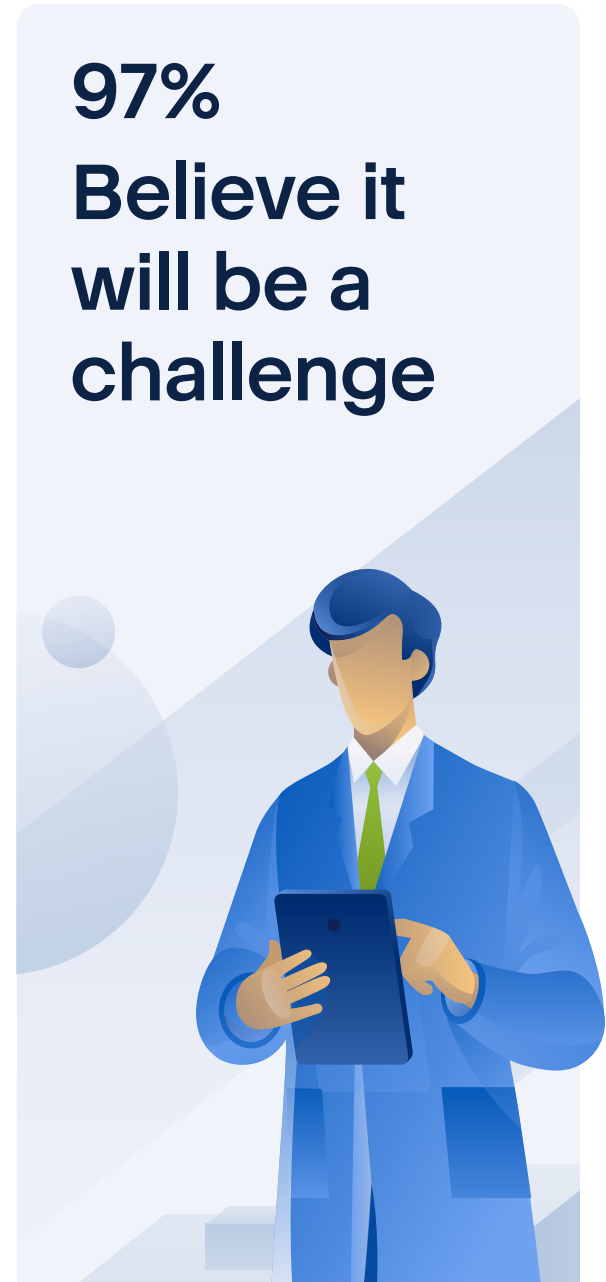
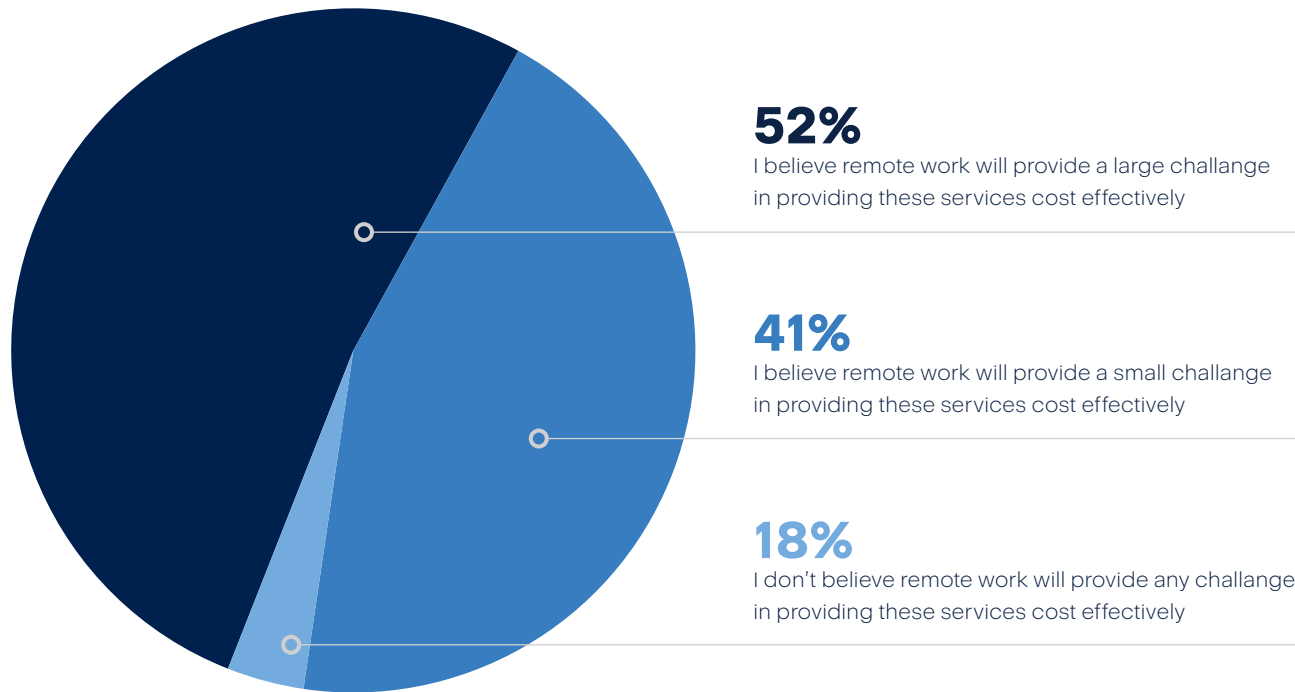
Many MSPs are not yet achieving the profit margins they would like to from the services they sell, and that this is a situation which is likely to be exacerbated further by the rise in remote work. It is imperative that service providers identify solutions which help them provide the services their clients need, without costs escalating further. Doing so will have positive consequences for not only the profit the service provider is able to make, but also for the relationship between them and their clients, if they don't have to continue to pass cost increases onto them.


Are not “very satisfied” with the profit contribution their organization gets from selling each of the following



Showing the proportion who state they are “Slightly satisfied”, “Neither satisfied nor dissatisfied”, “Slightly dissatisfied”, or “Very dissatisfied” with the profit contribution their organization gets from selling each of the following

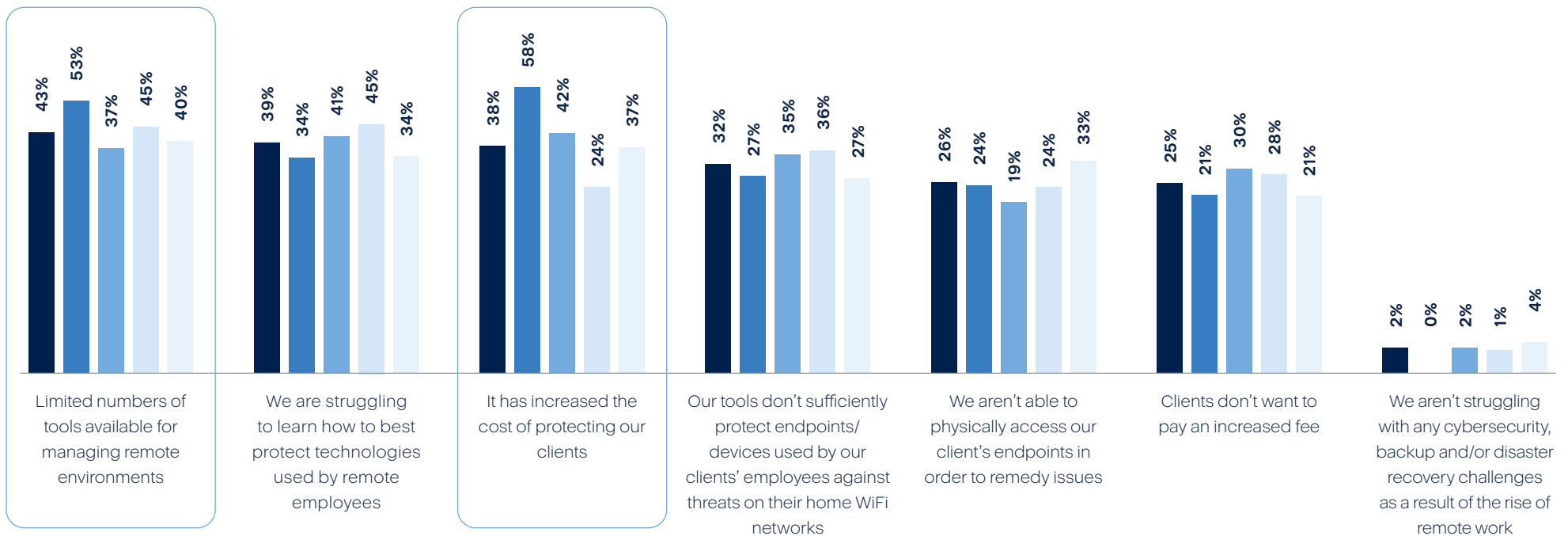
# Supporting remote work makes it even harder



 To what extent do you believe remote work will pose a challenge for your organization in cost effectively providing cybersecurity, backup and disaster recovery services to your clients going forwards?

# Supporting the “new normal” of remote work creates new challenges MSP must face

It is imperative that service providers identify and adopt tools which can help them overcome these hurdles, as remote work is not just a short term fad, with recent research indicating that 47% of employees expect to be working both at home and in the office through to 2025. Smaller service providers in particular are struggling with increased costs coupled with a lack of tools available to manage their remote environments, highlighting the critical need for them to seek out vendors who offer these capabilities, but do so without escalating the cost of protecting their clients.



**Which of the following cybersecurity, backup and disaster recovery challenges related to the rise of remote work is your organization currently struggling with?**

■ Total (400)
 ■ 1-4 employees (62)
 ■ 5-24 employees (97)
 ■ 25-49 employees (110)
 ■ 50-99 employees (131)

# Key Findings

The cybersecurity, backup and disaster recovery challenges facing IT service providers and their clients:

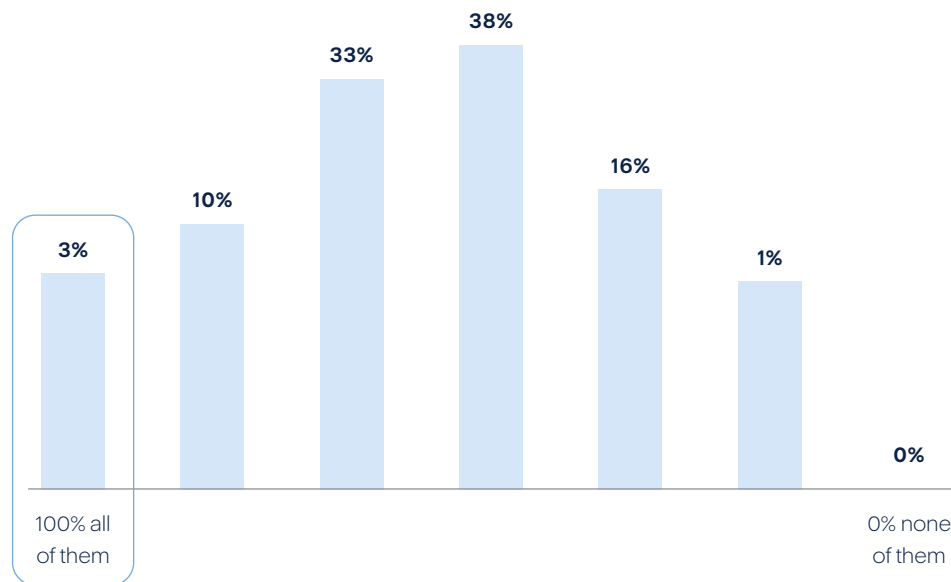
**Vulnerabilities created by  
usage of SaaS tools**



# Clients are using a number of SaaS tools, however MSPs are managing just over half of them

The number of SaaS tools that their clients are using may in actuality be even higher, if there are tools which MSPs aren't even aware of. This could lead to the existence of blind spots on their clients' networks which they are unable to protect. Even where MSPs are aware of the SaaS tools their clients are using, if they aren't managing them, they are likely to struggle to protect them or troubleshoot any issues their clients have with them.

Indeed, only a tiny minority state that they manage all of the SaaS tools their clients use, indicating these problems are likely widespread. There is however a huge potential for growth for service providers if they are able to prove to their clients that there are benefits to them managing the licenses, onboarding, security and performance of these SaaS applications.



# 14

**Average number** of SaaS tools currently in use by respondents' organizations' clients

# 58%

**Average proportion** of clients' SaaS tools that MSPs are managing on their behalf



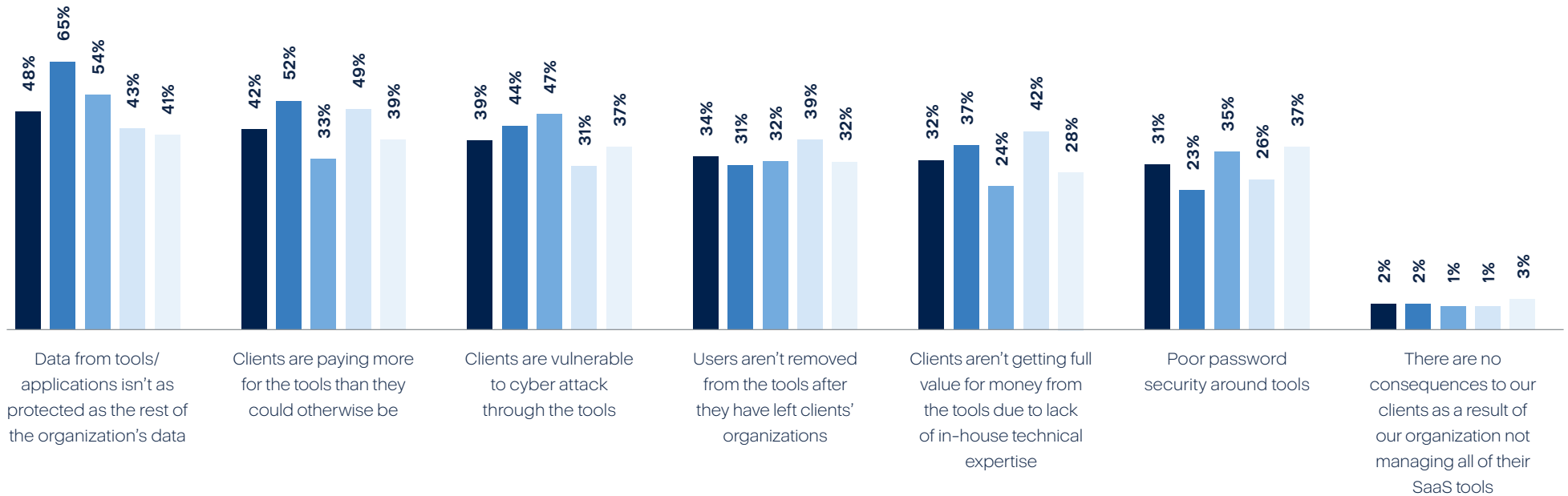
**Approximately what proportion of your clients' SaaS tools is your organization managing on their behalf?**



# This results in greater vulnerabilities for clients, particularly those of smaller MSPs

These security implications need to be made clear to clients, and could help service providers build a case for expanding their service offering to include management of SaaS tools. However, it is not just security which is compromised when service providers don't manage these tools, clients can also end up paying more, and not getting full value for their money when

they are managing them themselves. MSPs have huge value to offer not only by securing SaaS tools, but by using their technical skills to optimize them to meet their clients needs, and by negotiating better rates for them. MSPs should ensure they are talking to their clients about the benefits they stand to gain by passing on the responsibility for management of these tools.



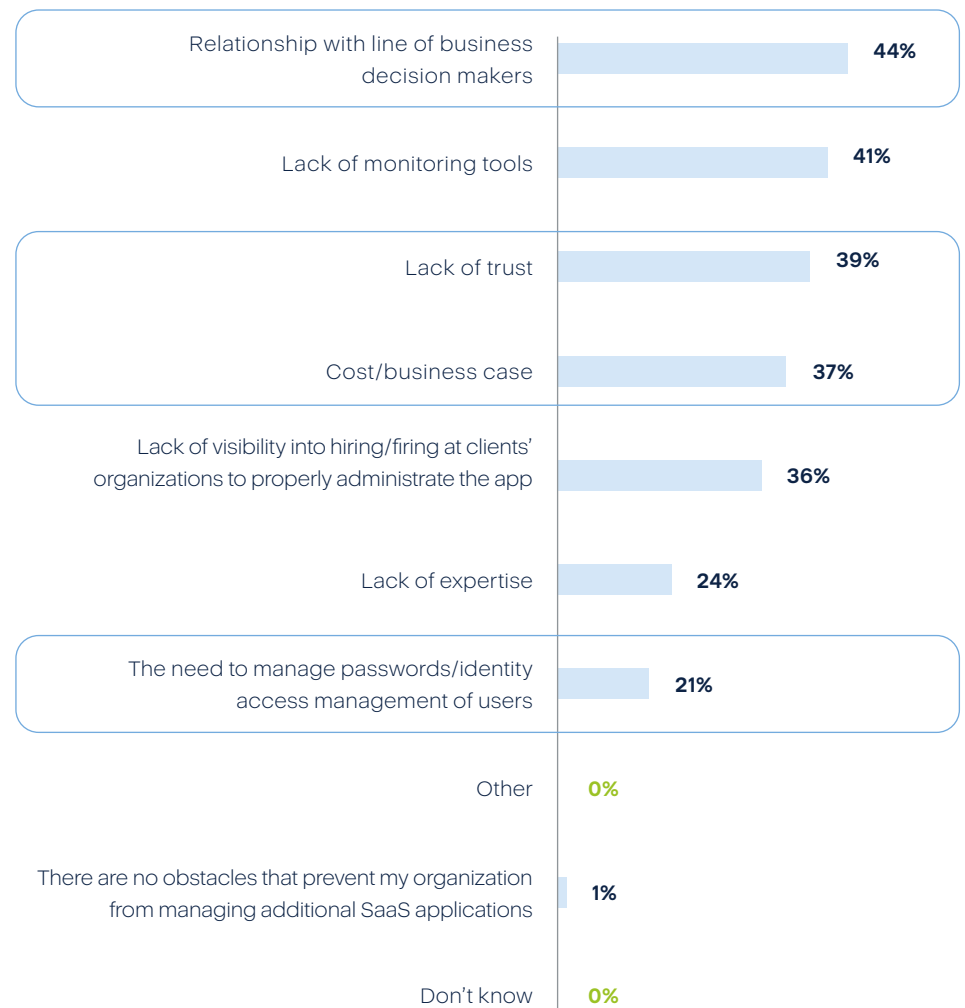
**What are the consequences to your clients of your organization not managing all of their SaaS tools?**

■ Total (390)
 ■ 1-4 employees (62)
 ■ 5-24 employees (97)
 ■ 25-49 employees (108)
 ■ 50-99 employees (121)

# To increase SaaS management, MSPs need new relationships and improved trust levels

MSPs need to consider the obstacles which are currently preventing them from managing their clients' SaaS applications, if they are to expand their services to include management of all of these tools. It is rarely the case that a lack of expertise is preventing them from doing so, with the relationship with line of business decision makers and a lack of trust far more likely to be obstacles. Along with adopting the tools which allow them to monitor SaaS applications, MSPs need to focus on ensuring they can be trusted by their clients.

Using tools and solutions with demonstrable security credentials will be key to helping to build this trust and improving or building relationships with line of business decision makers. Similarly, by making a clear case for the benefits that clients themselves can receive by passing responsibility of managing tools on to their service providers,, service providers will be able to build trust by demonstrating that they have their clients security and business interests at heart



**What are the biggest obstacles that prevent your organization from managing additional SaaS applications?**

# Key Findings

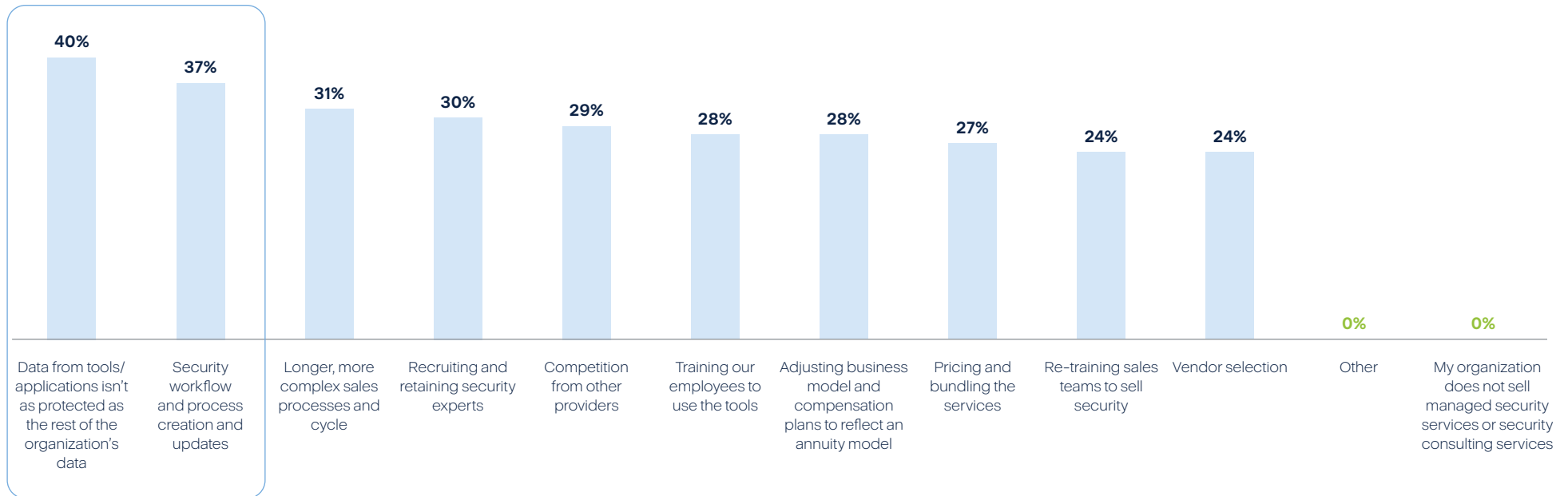
Cybersecurity service delivery complexity  
and the path forwards:

## Approaches to consolidation, integration and automation



# There are a number of challenges MSPs face when it comes to selling security services

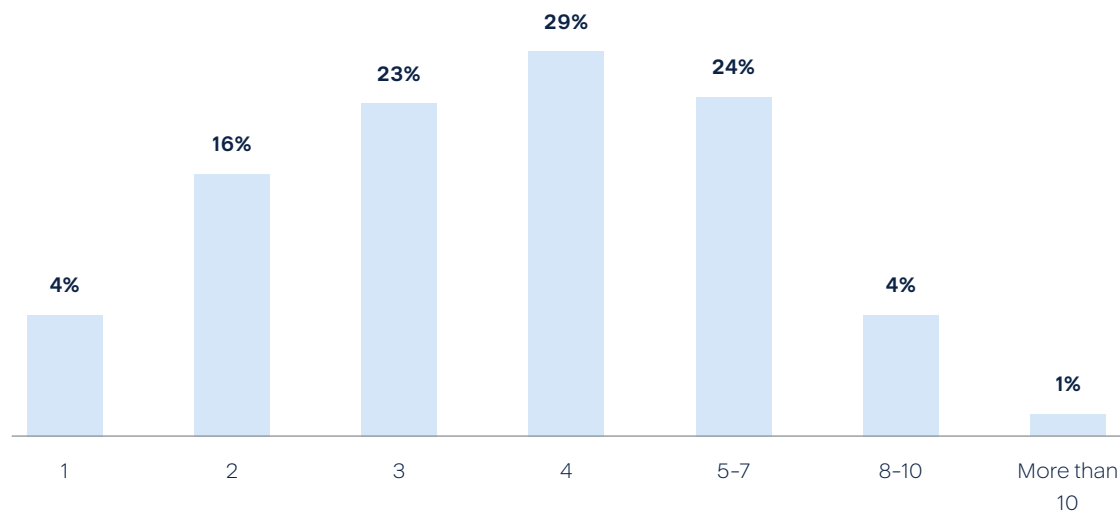
The two most commonly faced challenges are the integration of security offerings with existing business and IT systems, and security workflow and process creation and updates. These reflect the particular challenge that service providers face when setting up their security tools so that they seamlessly intertwine into their clients' systems, while still providing a robust level of security. However, the range of issues service providers face are vast. Vendors of security services to them must ensure that they provide their customers with a competitive advantage, and can be sold and used by service providers which are experiencing a skills shortage.




**?** What are the biggest challenges your organization faces in selling managed security services and/or security consulting services?

# Most MSPs use multiple vendors to provide cybersecurity, backup and/or disaster recovery services to their clients

By using multiple vendors to provide these, many may find that there is overlap between the vendors in the services they provide, resulting in money being spent on solutions which aren't entirely necessary. On the flip side, there may also be gaps between them which leave areas on their clients network undefended and irretrievable in the event of data loss occurring, as it has in many organizations in the last 12 months. Additionally, by having to manage each vendor's tools separately, service providers could be increasing the time they are spending setting up and managing their services.



 How many vendors does your organization use to provide cybersecurity, backup and/or disaster recovery services to its clients?

# 4

Average **number of vendors** currently used

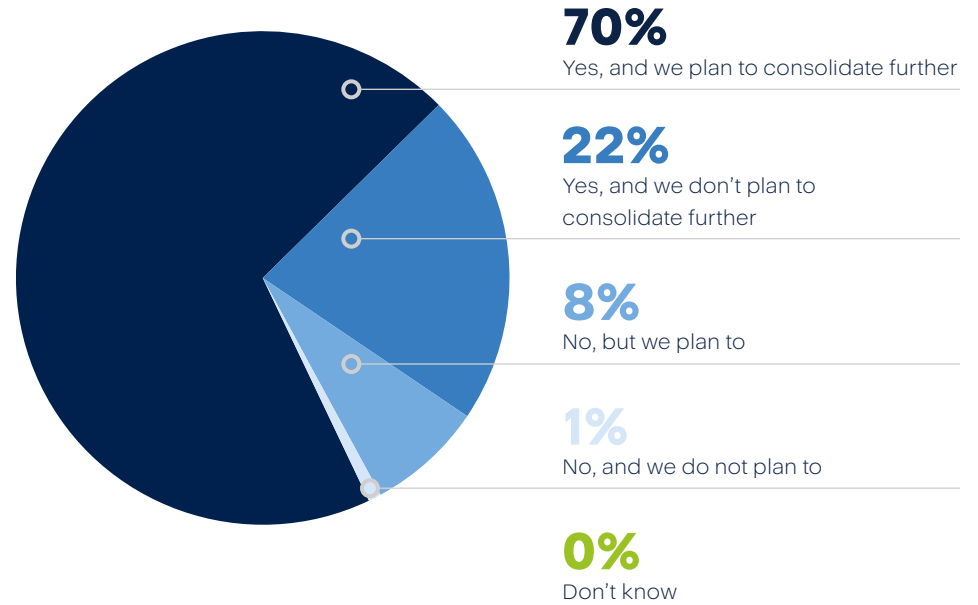
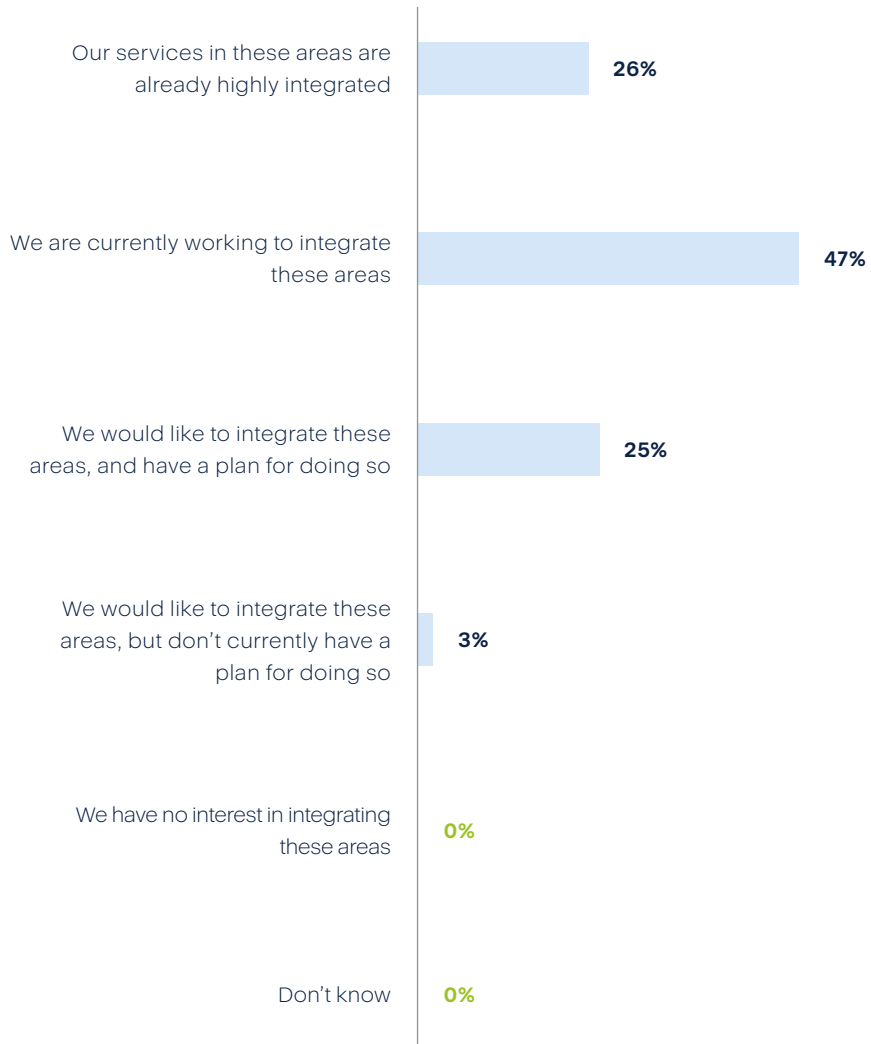


# There is a strong trend towards integration and consolidation of cybersecurity, backup and/or disaster recovery services (what Acronis calls cyber protection)

Many service providers appear to recognize the challenges that using multiple vendors for these purposes can create, and are acting to reduce the number of vendors and integrate their services. Integration in this context refers to integration at the operational and technical level, with the help of AI, Machine Learning or Machine intelligence, so that the services can be managed through a single user interface. With the market

clearly moving towards consolidation and integration of these services, vendors who offer consolidated or integrated services are likely to be in high demand. Service providers who haven't yet started to integrate or consolidate their services should take note of these trends in the marketplace when considering how to improve their own cybersecurity, backup and/or disaster recovery services.





**92% are consolidating**

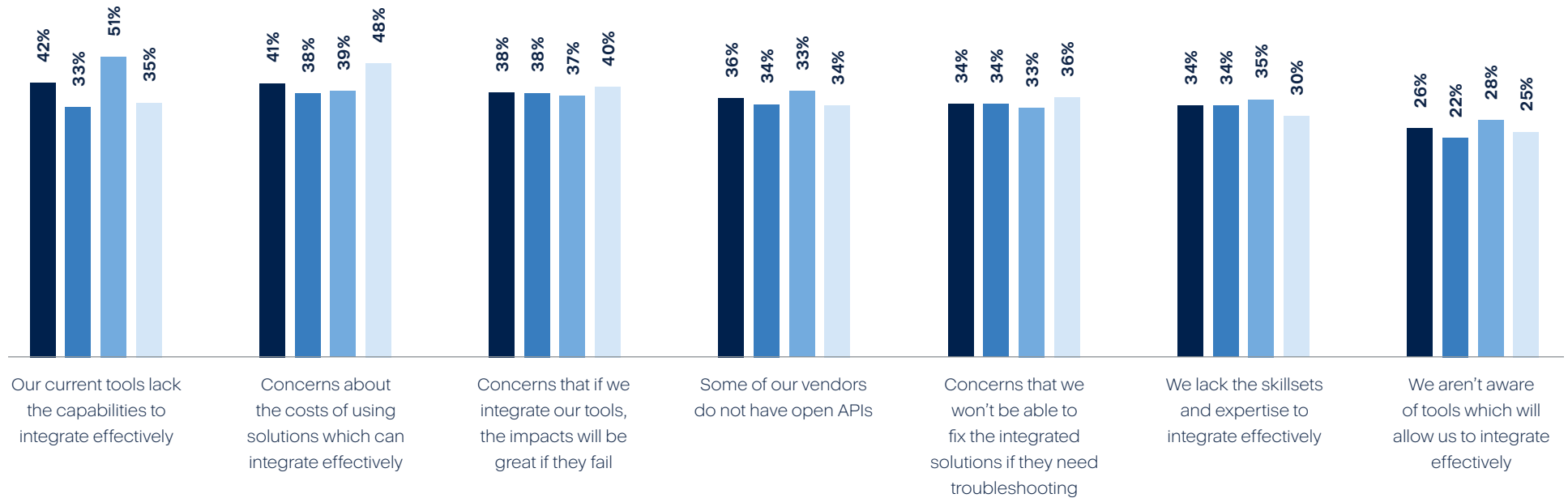
**?** Which of the following best describes your organization's approach to integrating its cybersecurity, backup and disaster recovery services?

**?** Has your organization consolidated the number of vendors it works with for cybersecurity, backup and/or disaster recovery services in the last two years?

# However integrating these services will not be without its challenges

With the most common challenge facing service providers who have or would like to integrate being a lack of tools with the capabilities to integrate, there is a clear need for service providers to investigate whether there are alternative tools out there which could help them to do so, and aren't restricted by not having open APIs, or being difficult to integrate. It is notable that concerns over cost

are reported to be a challenge to a greater extent in service providers which haven't yet integrated than it is in those which have already started to integrate - indicating cost is not actually proving to be a challenge to the extent it is expected to be. This should be reassuring to service providers which haven't started to integrate yet, and hold concerns about the costs of doing so.



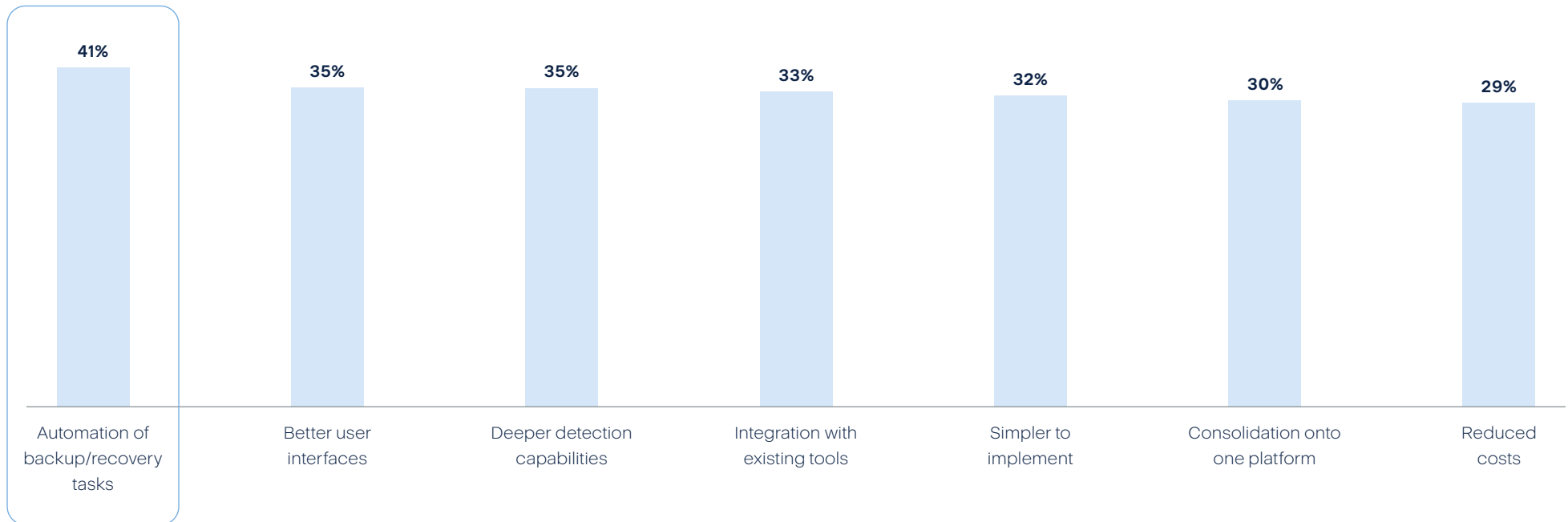
**What challenges is your organization facing/do you expect your organization will face in integrating its cybersecurity, backup and disaster recovery services?**

- Total (399)
- Our services in these areas are already highly integrated (103)
- We are currently working to integrate these areas (186)
- We would like to integrate these areas (110)



# MSPs want a holistic solution - for cybersecurity services to automate backup/recovery tasks

This indicates the importance that MSPs are placing upon the integration of cybersecurity with backup and disaster recovery tasks. Improving automation of these services is more likely to be a priority to them than other improvements they could be focusing on, such as those to user interfaces, detection capabilities and simplicity of implementation. With service providers likely to be on the look out for tools which offer the capability to integrate, those which also offer automation can be expected to have an additional edge in attracting these customers.

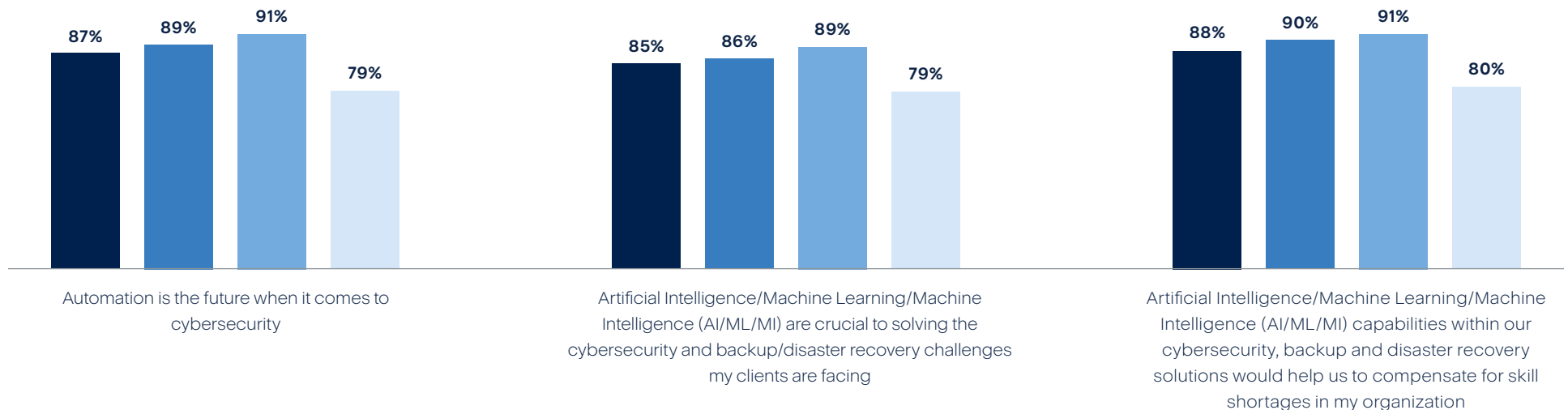


Which of the following improvements would you like to see to the functionality of the tools you are currently using to provide cybersecurity services?

# The importance of automation and machine intelligence is undeniable

With such a strong consensus about the importance of automation and machine intelligence, it is apparent that by using cybersecurity, backup and disaster recovery solutions which include these functionalities, service providers could gain a competitive edge over competitors using solutions which don't offer these capabilities. For example, by helping organizations to compensate for skill shortages, these solutions could help smaller service providers, who may be struggling with a lack of skillsets, to better

protect their customers. However, not all service providers are yet aware of the benefits that automation and machine intelligence can provide, with those who haven't yet integrated not as aware of them as those who have. This highlights the need for vendors to make clear not only how using automation and machine intelligence can help them, but to reduce any fears and concerns these organizations might have about the difficulty of adopting and implementing tools which utilize them.



Showing the proportion of respondents who state they “Strongly agree” or “Slightly agree” with the following statements

- Total (400)
- Our services in these areas are already highly integrated (103)
- We are currently working to integrate these areas (186)
- We would like to integrate these areas (110)

# Key Findings

**The case for consolidating and integrating cybersecurity, backup and disaster recovery**

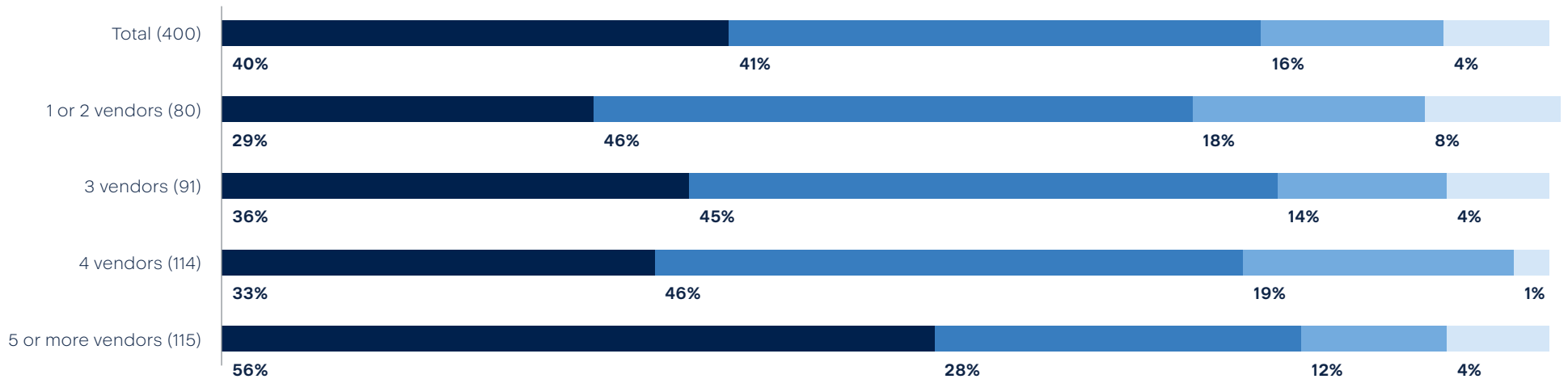


# Using fewer vendors have a positive impact on how well MSPs can protect their clients against cybersecurity breaches, and data loss or downtime

The case for consolidating the vendors in use to provide cybersecurity, backup and disaster recovery services is made clear by the lower concern that organizations using only one or two vendors have about experiencing an attack in the next 12 months, compared to those using five more vendors. A similar trend occurs when looking at whether service providers' clients

have suffered various cybersecurity attacks, and experienced data loss or downtime as a result. Service providers looking to improve their security offering therefore should look to consolidate the number of vendors they are using, in order to better protect their clients against cybersecurity threats, and reduce the risk of data loss or downtime occurring.

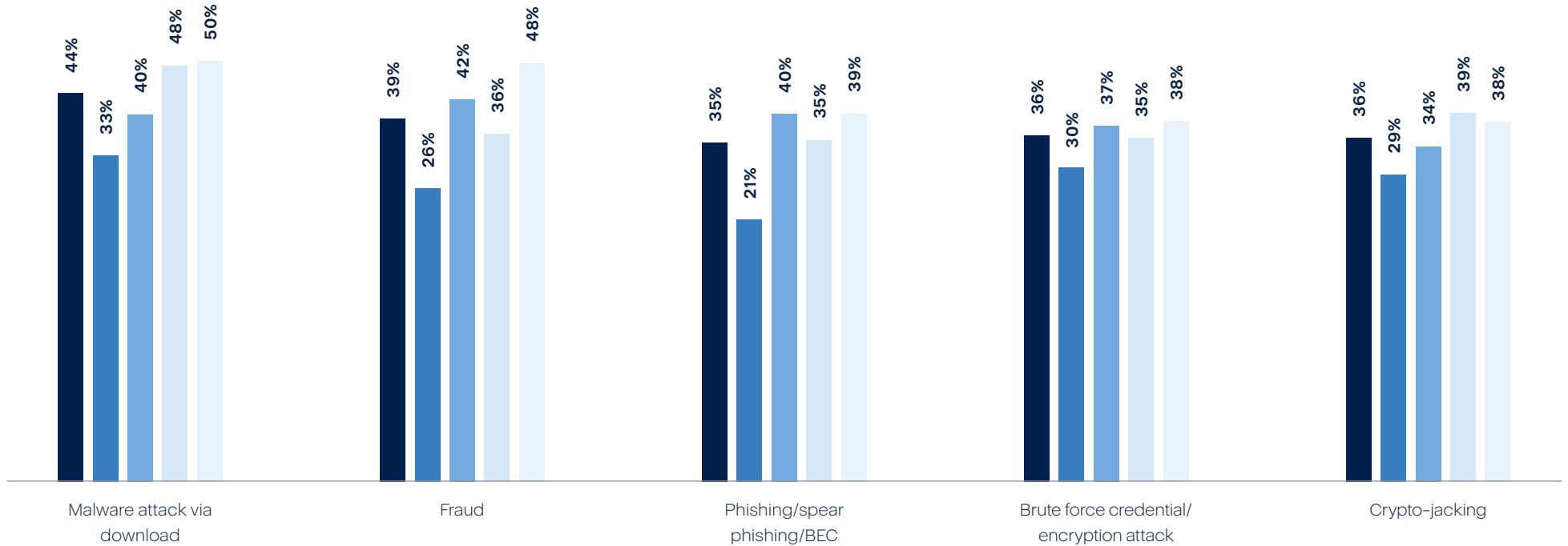
## Concern that organization could suffer a cybersecurity breach through which clients' IT systems are compromised in the next 12 months



**How concerned are you that your organization could suffer a cybersecurity breach through which your clients' IT systems are compromised in the next 12 months?**

Extremely concerned
  Slightly concerned  
 Moderately concerned
  Not concerned at all

At least one of our clients experienced this, and they suffered from data loss or downtime as a result



Showing the proportion whose clients have suffered each attack and suffered data loss or downtime as a result

■ Total (400) ■ 1 or 2 vendors (80) ■ 3 vendors (91) ■ 4 vendors (114) ■ 5 or more vendors (115)

# There are also huge cost savings that could be made by consolidating these services

There are numerous areas which could be contributing to these cost savings. These could include lower licensing costs as a result of using fewer vendors, lower training costs as a result of not needing to train employees on multiple solutions, the costs of managing documentation and any cost savings related to improvements made to employee productivity as a result of consolidating.

The size of this cost saving should encourage service providers to further consolidate their services, as it is likely to improve the profit which they are getting from selling them. Consolidating vendors therefore provides the dual benefit of improving clients' protection levels while reducing the cost of providing cybersecurity, backup and/or disaster recovery to their clients. This will mean that service providers can get a better profit contribution from their services without having to raise their prices, or reduce the level of service they provide - likely contributing to a better long term client-service provider relationship, and all the benefits this can bring.

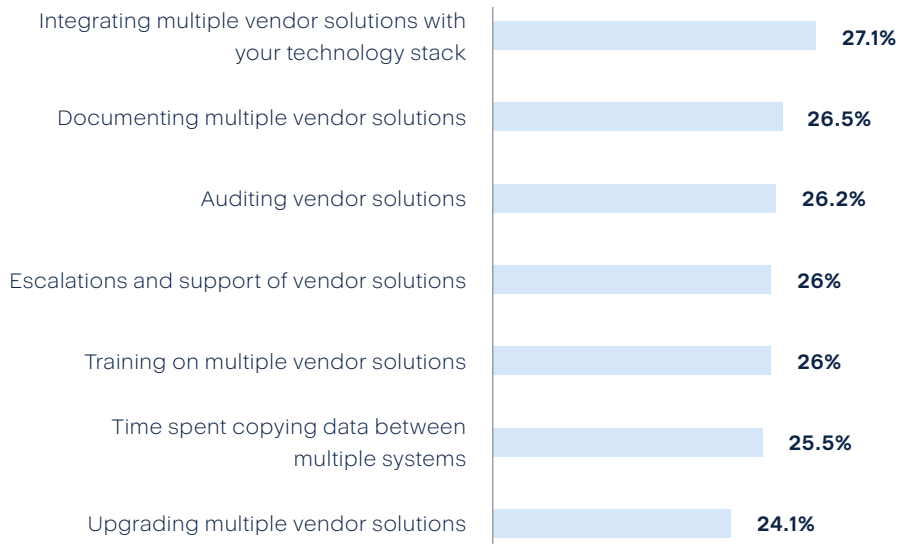
# \$229,159

**Estimated total cost savings** made by MSPs as a result of consolidating their cybersecurity, backup and disaster recovery services



# Integration results in greater operational efficiencies

Reducing the time that their employees spend on various operational activities, as well as in recovering from a cybersecurity breach or data loss incident, will mean that they are instead able to focus time on other activities, including revenue-generating activities, allowing the service provider to include its profitability. It also gives employees more time to provide direct hands on support for customers, which, along with the ability to more efficiently manage tools, is likely to improve the relationship between service providers and their clients.



# 5 hours

Average reduction in the **amount of time spent recovering from a cybersecurity breach** or data loss incident in a client's IT network, as a result of integrating its cybersecurity, backup and/or disaster recovery services

Showing the average percentage reduction in time that employees spend on the above activities, as a result of integrating cybersecurity, backup and disaster recovery services

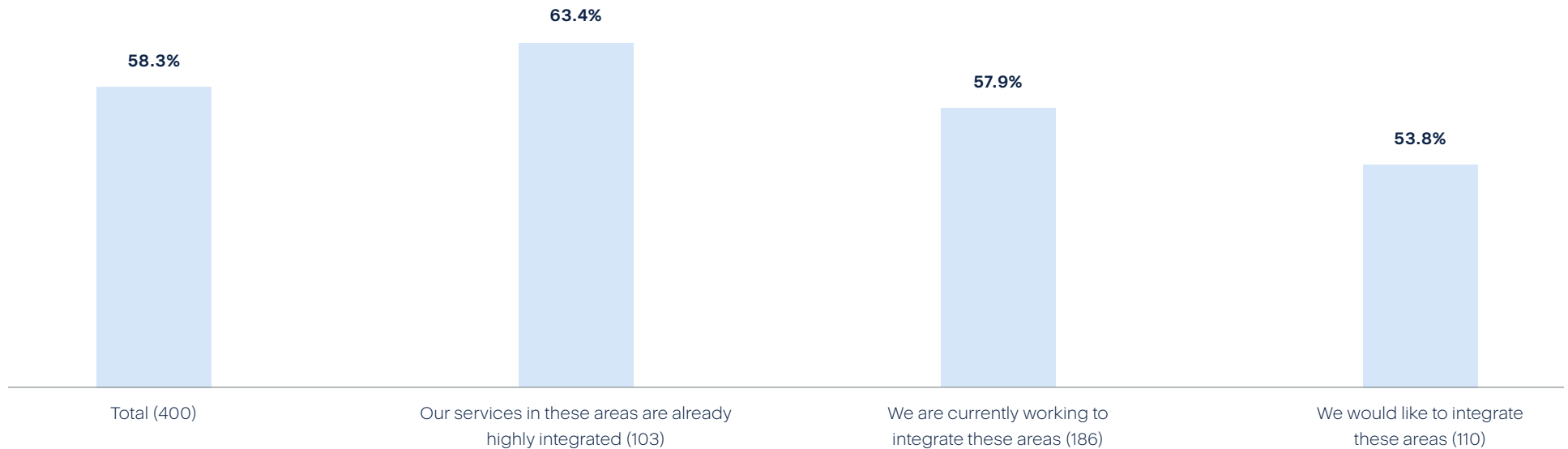
Respondents from organizations which have highly integrated cybersecurity, backup and/or disaster recovery services

# Integration results in better profits and more SaaS tools under management

By increasing the level of trust in them by clients, many service providers may be presented with the opportunity to expand their offering to include management of more of their clients' SaaS tools – something a lack of trust is currently a common hurdle to achieving. Service providers which have integrated their services can spend less time and money managing them,

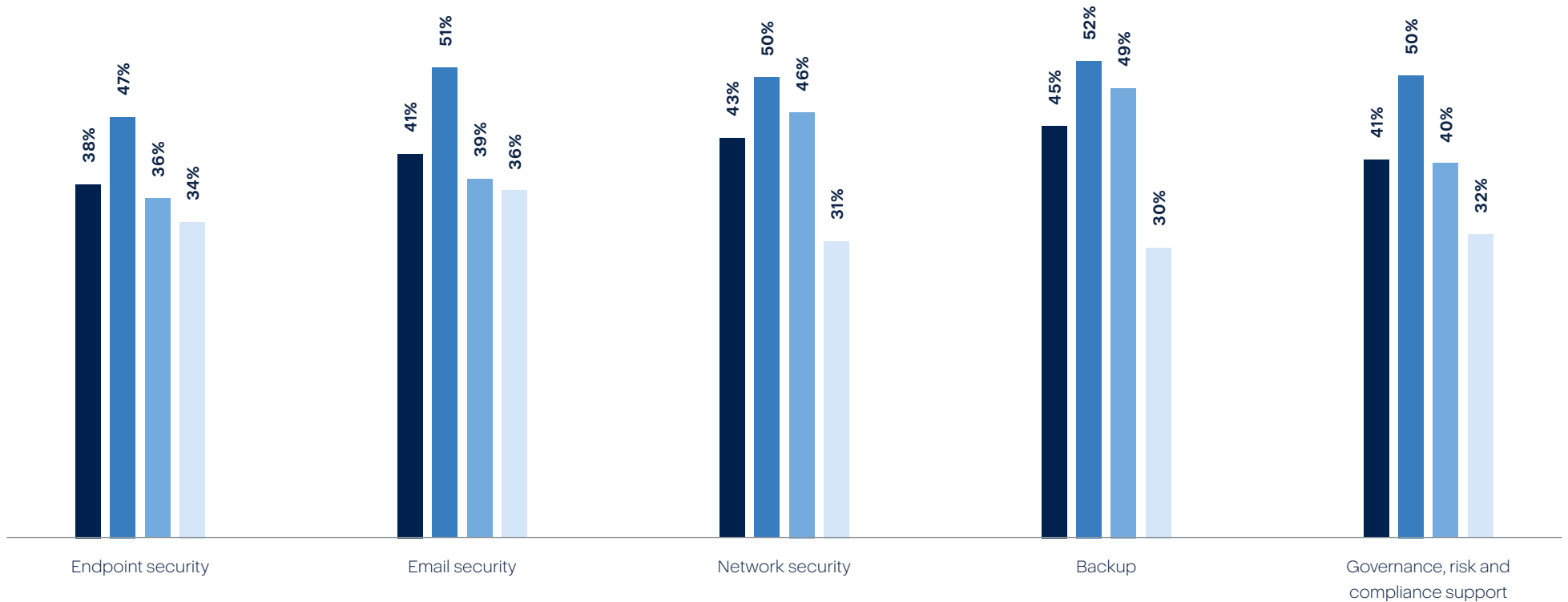
resulting in greater satisfaction with the profit contribution they get from selling their services. Together, these trends demonstrate that integration does not only provide the benefit of improving cybersecurity protection levels, but also helps service providers to grow and expand their own business, and contribute to their revenue growth.

## Average proportion of clients' SaaS tools the organization is managing on their behalf





At least one of our clients experienced this, and they suffered from data loss or downtime as a result

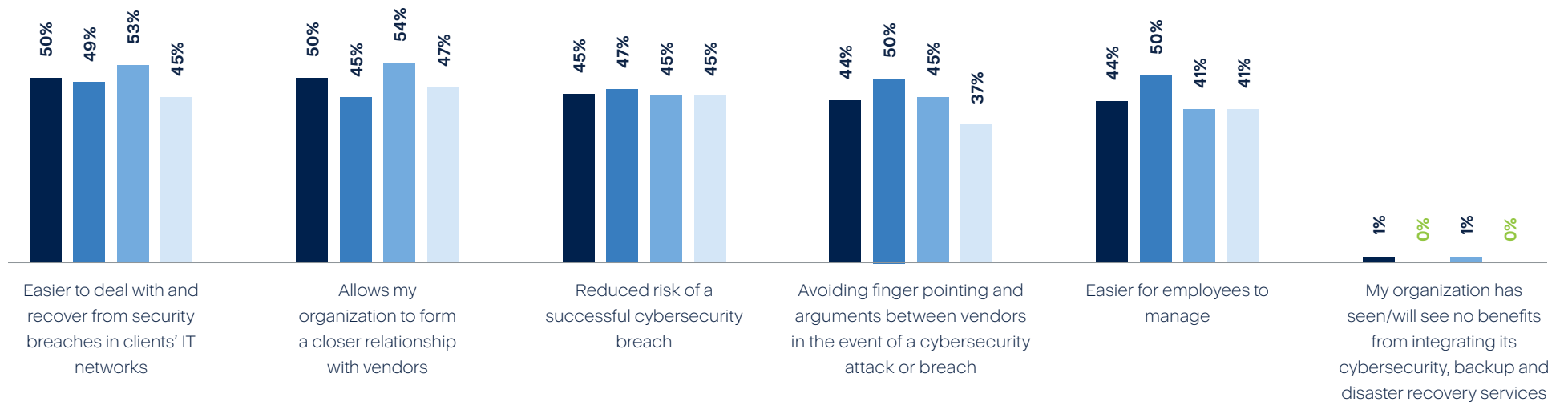


In general, how satisfied or dissatisfied are you with the profit contributions your organization gets from selling the following services?

- Total (400)
- Our services in these areas are already highly integrated (103)
- We are currently working to integrate these areas (186)
- We would like to integrate these areas (110)

# There are numerous other additional benefits to integration

Only a tiny minority of organizations which have integrated have seen no benefits as a result of doing so. The numerous benefits that integration can offer, including to the level of protection they can offer and the ease of management, provide further evidence that service providers should start integrating if they haven't already. There are even some benefits they may find which they do not expect, such as avoiding finger pointing, and the increased ease of management, as those who are highly integrated already are more likely to say they have experienced these, than those who haven't integrated are to say they expect to.



**?** Apart from any financial benefits, or reduction in time spent on the areas already asked about, which of the following benefits has your organization seen/do you believe your organization will see as a result of integrating its cybersecurity, backup and disaster recovery services?

- Total (399)
- Our services in these areas are already highly integrated (103)
- We are currently working to integrate these areas (186)
- We would like to integrate these areas (110)

# How Acronis can help MSPs



# The Acronis Cyber Protect Cloud

Keep Your Client's Business Protected Against Modern Threats

## Acronis Cyber Protect Cloud



Cybersecurity

+



Backup and recovery

+



Endpoint Protection  
management

## Acronis Cyber Protection Framework



Prevention



Detection



Response



Recovery



Forensics

# Modernizing your security is actionable today

Technology partners need to start fast: simplify, consolidate, secure

## Legacy Backup & AV solutions



### Complex

Complicated licensing, deployment, and training, as well as agent conflicts



### Expensive

Multiple tools, vendors, administration costs



### Unsecure

Lack of integration creates gaps in defenses, management burden compromises security

## Acronis Cyber Protect Cloud

### All services managed from one place

Remove the complexity and risks associated with non-integrated solutions

### Smarter use of resources

Faster operations with integration and automation lets your team focus on your clients

### Total peace of mind for clients

Customize your services and deliver complete protection for every workload

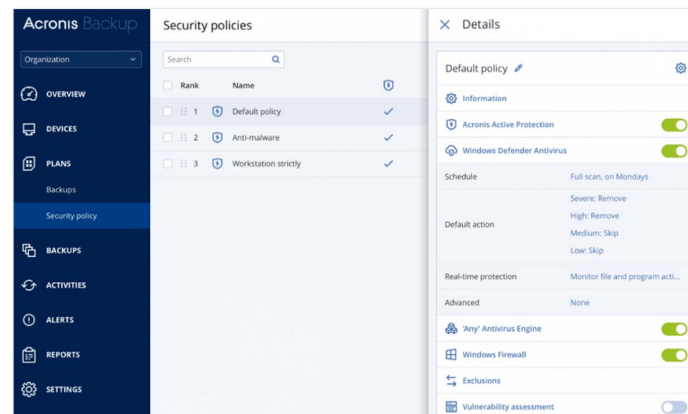
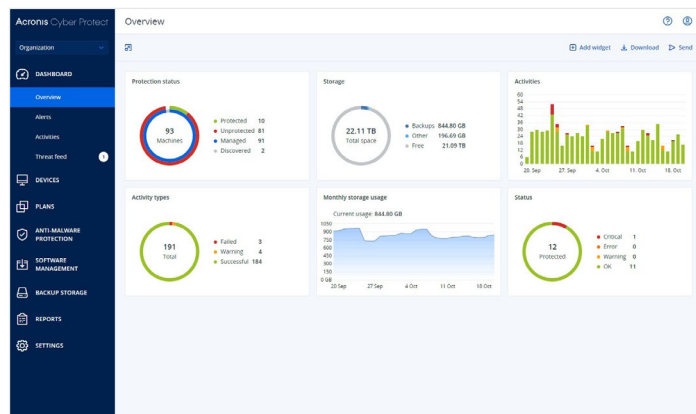


# Acronis Cyber Protect:

One cyber protection solution for all workloads

Flexible deployment models and broad environment support that meet the demands of service providers and IT professionals. Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions.

- Vulnerability assessments
- Patch management
- Anti-ransomware/malware
- Backup & Disaster Recovery
- Remote management and assistance
- Health and Performance Monitoring
- Reporting



# Acronis Cyber Protect Cloud and Advanced Packs

One cyber protection solution and flexible options for all workloads

## Advanced Security

Enhance your security services with integrated cyber protection that includes full-stack anti-malware

## Advanced Management

Streamline workload management with a comprehensive toolset, incl. fail-safe patch management

## Advanced Backup

Never lose data, even between scheduled backups, cover more workload types

## Advanced Email Security

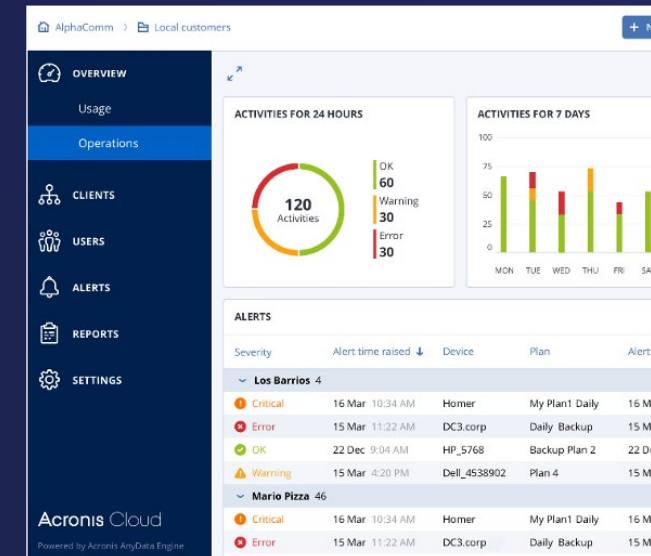
Block email threats, incl. BEC and zero-days in seconds before they reach end-users

## Advanced Disaster Recovery

Get clients back to business in mere minutes

## Advanced File Sync and Share

Offer secure collaboration services with embedded data authenticity



**Coming Soon:** Advanced Security + EDR; Advanced DLP

Get a demo

# Benefits of Acronis Cyber Protect Cloud

**Fastest return to productivity: autonomous, integrated and modular cyber protection**



## Ease of Use

Fewer human errors, faster deployment, more workloads supported by an IT professional, more customers protected



## Low TCO

Protection accessible for customer of any size, and low cost means higher margins for partners



## Reliability

Scalable and highly available cyber protection allows partners to offer higher SLAs to their customers



## Security

Protection solutions natively designed for security decrease partner risk of liability



## Control

Control over data location, protection configuration and rights delegation reduced partner risks



# Industry Recognition

Recognized by top security alliances, tests and certifications



MVI member



AV-TEST participant and test winner



Anti-Malware Testing Standard Organization



AV-Comparatives approved business security product



VirusTotal member



ICSA Labs certified



Anti-Phishing Working Group member



VB100 certified



Cloud Security Alliance member



MRG-Effitas participant and test winner

and more...

and more...



## Acronis Cyber Protect

Windows 7 / Windows 10

WildList detection ..... 100%

Diversity Test rate ..... 99,9%

False positive rate ..... 0%



**100% detection** rate in dynamic real-world test with 6,932 samples

**0 false positives** out of 180,000 files



**4.5 Excellent**

# What actual Acronis partners and industry analysts are saying



Before Acronis we had multiple platforms and customers had services in all of these different platforms. Acronis offered us one solution for all our backup needs and cyber protection. We know our customers are safe and protected within a few clicks so now we can see everything for one customer or all our customers in a single product.



**Jarne Else**  
Second Line Support  
Engineer, Cavere



Before Acronis, I was using at least three different solutions for backup (Datto and Crashplan), remote access (TeamViewer), and endpoint antivirus (ESET) – forcing me to use three different agents. Now with Acronis, I have one agent which saves time, money, and also improves performance for my end user.



**Kevin Schwarz**  
Owner, Techne



We believe that Acronis Cyber Protect is among the most comprehensive attempts to provide data protection and cyber security to date. Acronis shows potential to disrupt traditional IT security vendors by delivering integrated components for backup/recovery and malware detection and protection.



**Phil Goodwin**  
Research Director, IDC





## About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated [cyber protection](#) that solves the safety, accessibility, privacy, authenticity, and security ([SAPAS](#)) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, [backup](#), [disaster recovery](#), and endpoint protection management solutions powered by AI. With advanced [anti-malware](#) powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 25 languages. For more information, visit [www.acronis.com](http://www.acronis.com)