

jumpcloud

# Look for the Helpers:

## The Role of IT Managers in Post-Pandemic Recovery for SMEs

Remote Work Solutions, Security and Cloud Services Drive IT Priorities in 2021



# Executive Summary

As the U.S. starts to emerge from the Covid-19 pandemic, people are now starting to figure out what the “new normal” looks like, both personally and commercially. And despite all the lingering uncertainty, one thing is certain—small and mid-size enterprises (SMEs) are vital to our [shared economic recovery](#), both in the U.S. and internationally. Helping these companies adapt to change and adopt new approaches is more important than ever, which is why IT professionals play such a critical role.

That’s why we commissioned this research—to better understand the role, the challenges and the dynamics of IT professionals who serve SMEs. And behind all the statistics and trend lines, we found a story of dedication and determination to overcome obstacles and keep people productive and secure.

Take this statistic, for example: During 2020, 74.8 percent of SME IT budgets increased, but only 37.8 percent of SME IT salaries increased. Despite the discrepancy, 58.6 percent of IT

professionals are happier now than they were a year ago. That suggests an incredibly service-oriented mindset.

And it’s been vital during a challenging time. The ongoing management of remote workers has been the biggest challenge to IT teams since the start of the pandemic. Nearly two-thirds (66.3 percent) of IT professionals agree that they feel overwhelmed by trying to manage remote work. Consequently, 58.4 percent plan to spend more on remote management technologies and 55.9 percent plan to spend more on security. Clearly, the hybrid workspace is here to stay, and these trends aren’t going away as we emerge from the pandemic.

When it comes to security, the three biggest concerns are software vulnerability exploits, the reuse of the same password across different applications and the use of unsecured networks. More than 80 percent of organizations have implemented some form of multi-factor authentication (MFA) to help secure remote access.

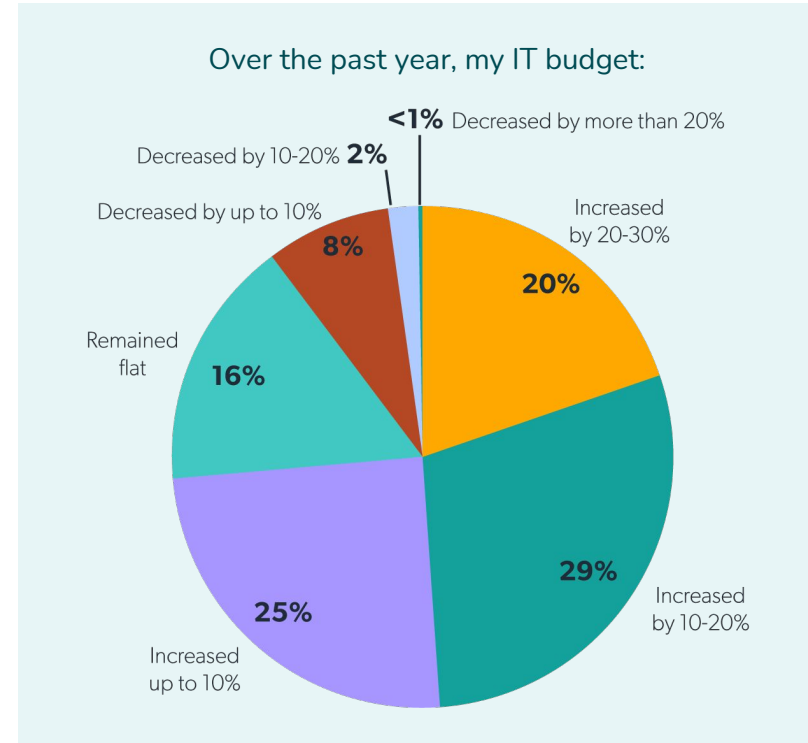
For the remainder of 2021, top priorities for SME IT leaders are adding layered security so work-from-anywhere (WFA) is truly secure, making remote work easier for end users, and making device management easier. In fact, more than half of the SMEs we surveyed have implemented a Zero Trust security architecture to help make this possible.

**In short, SMEs are going to drive the economic recovery. And their IT managers will be the ones who make that possible by empowering work-from-anywhere, cloud and security solutions for this incredibly resourceful and resilient sector.**

# The Financial Impact

## Booming Budgets & Sluggish Salaries

Nearly three-quarters (74.8 percent) of SME IT budgets increased during 2020, and nearly half (49.6 percent) increased by at least 10 percent. Conversely, less than 10 percent (9.4 percent) of SME IT budgets decreased during 2020, and less than two percent (1.9 percent) decreased more than 10 percent.

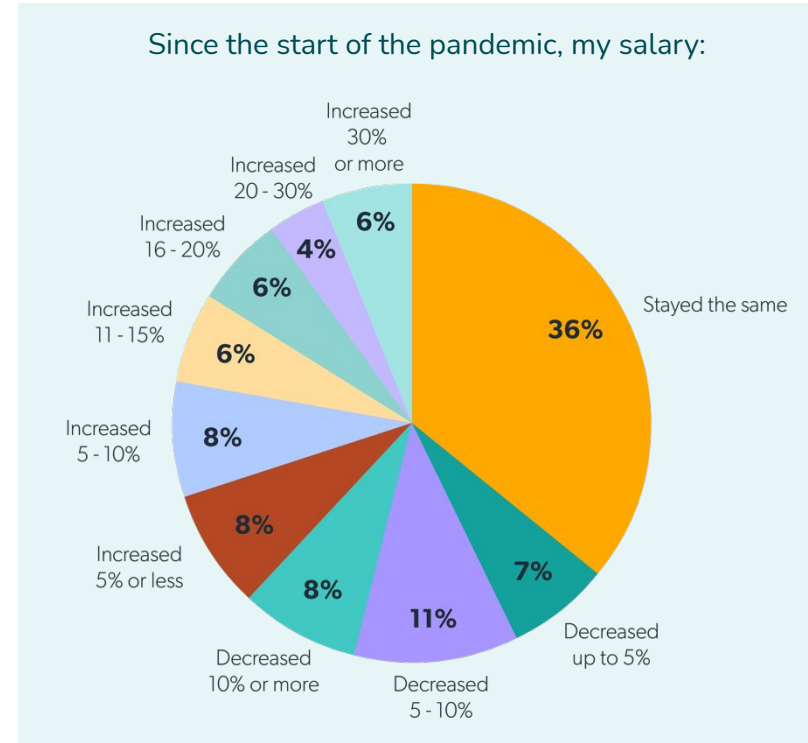


# The Financial Impact

## Booming Budgets & Sluggish Salaries

However, since the start of the pandemic only about one-third (37.8 percent) of SME IT salaries increased. About one-third (35.9 percent) of SME IT salaries stayed the same and the remainder (26.1 percent) actually decreased.

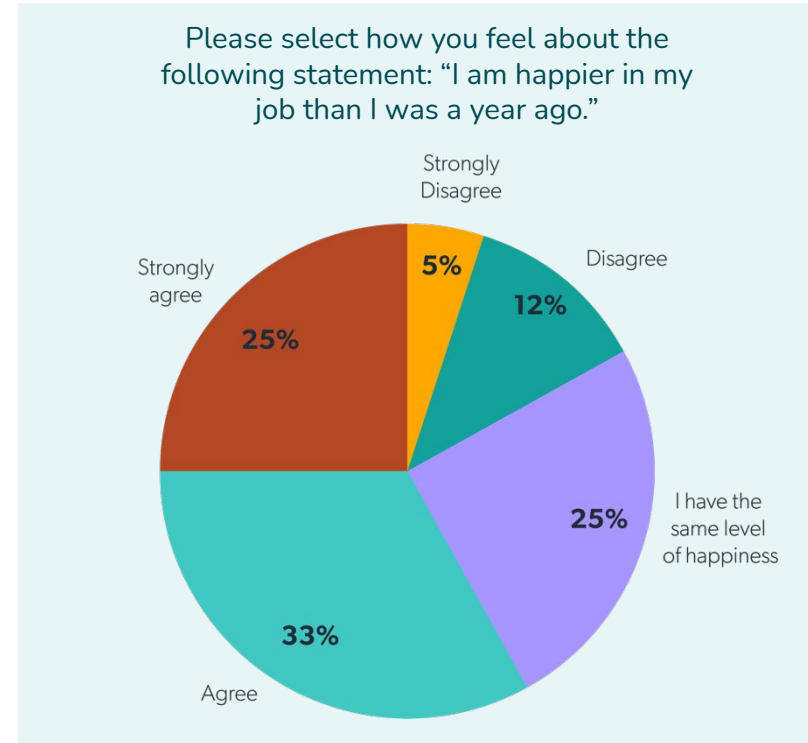
One explanation is that SMEs had to invest in new solutions to enable a remote workforce but were still sensitive to the economic pressures of the pandemic when it came to individual salaries. But that makes the next finding even more astounding — an increasing level of job satisfaction among SME IT workers, even as 41% responded that their work burdens have increased!



# The Pragmatic IT Professional

## Service for the Greater Good

Despite the divergence between IT budgets and salaries, the majority of SME IT professionals (57.6 percent) are happier in their job than they were a year ago. The fact is, most of these people have been more focused on helping their co-workers than helping themselves. And yet they face some of the most important challenges for SMEs to overcome...



# The Pragmatic IT Professional

## Service for the Greater Good

More than half (53.4 percent) of SME IT professionals said the ongoing management of remote workers and people working in hybrid workspaces has been one of their biggest challenges, while nearly half (48.1 percent) cited the cost of remote work and hybrid workspace solutions. IT professionals may have an unquenchable desire to serve their enterprise, but enabling remote work isn't easy.

What have been the biggest challenges to your IT team since the start of the pandemic?

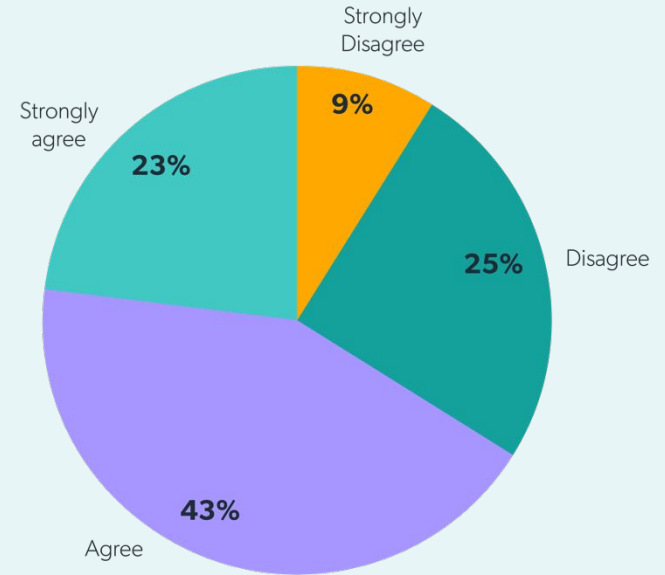


# Remote Work

## An Ongoing Challenge and Priority

Nearly two-third (66.3 percent) of SME IT professionals admit that they feel overwhelmed by trying to manage remote work. Consequently, their budgets and priorities are still squarely focused on remote work. It's a challenge that's likely to get even more complicated as more and more companies switch to a hybrid workspace model that supports WFA, even as they're ramping up new hires and expanding their businesses.

Please select how you feel about the following statement: "I feel overwhelmed trying to manage remote work."

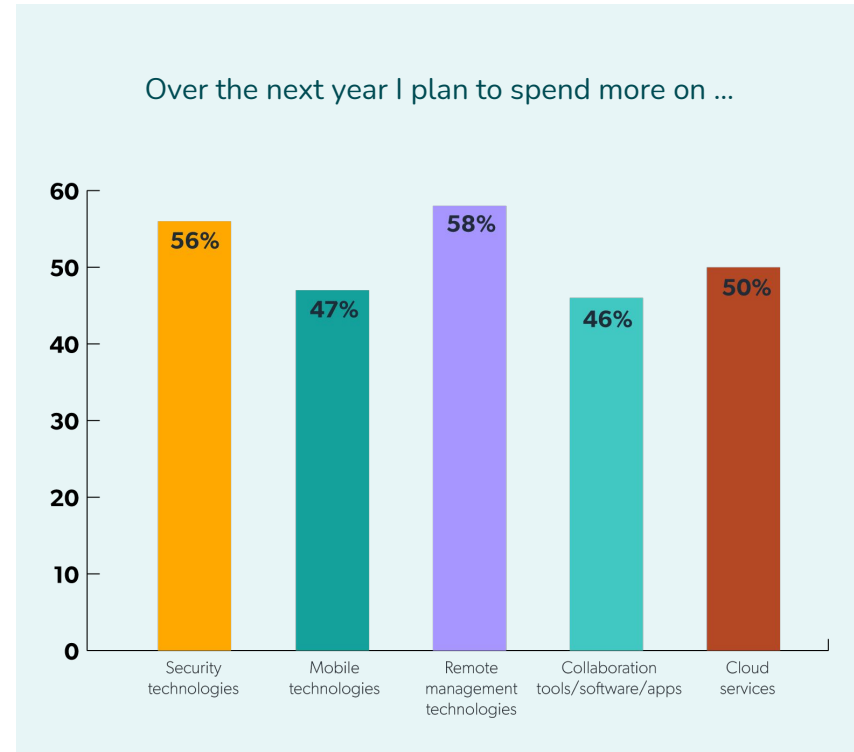




# Remote Work

## An Ongoing Challenge and Priority

More than half of SME IT departments (58.4 percent) plan to spend more on remote management technologies. More than half (55.9 percent) also plan to spend more on security technologies since remote work has introduced new risks. And more than half (50.1 percent) plan to invest in cloud services.

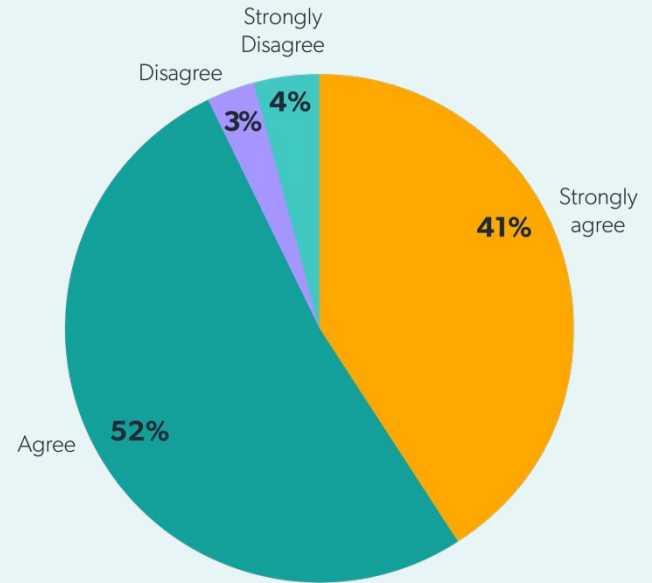


# Remote Work

## An Ongoing Challenge and Priority

At the same time, IT professionals are overwhelmingly focused on providing a positive employee experience. More than nine out of ten IT professionals (93 percent) agree or strongly agree that employee experience is an important factor in making IT purchasing decisions. Together, these two data trends suggest that SME IT professionals are focused on ensuring a positive user experience, and they recognize the utility of the cloud to help them do just that.

Please select how you feel about the following statement:  
“I consider employee experience to be an important factor in making IT purchasing decisions.”



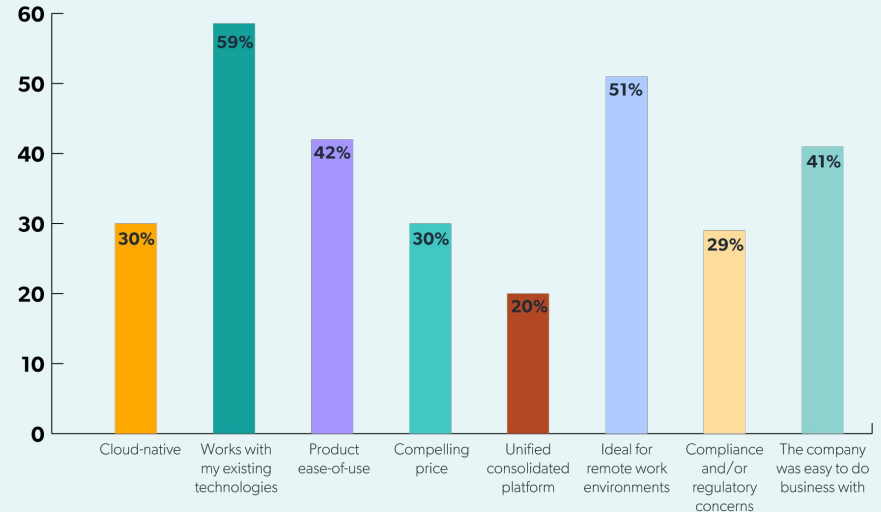
# Remote Work

## An Ongoing Challenge and Priority

Because the “new normal” has been so challenging, SME IT professionals also want a positive experience for themselves. More than half (58.6 percent) say the reason they selected an IT technology is because it works with their existing technologies. More than half (50.6 percent) also cited technologies that are ideal for remote work environments. 42.1 percent select products that are easy to use, and almost just as many (40.9 percent) are looking for companies that are easy to do business with.

In short, SME IT professionals are working hard to empower and secure hybrid workspaces for the long run, and it’s vital to give them the tools, resources and support they need.

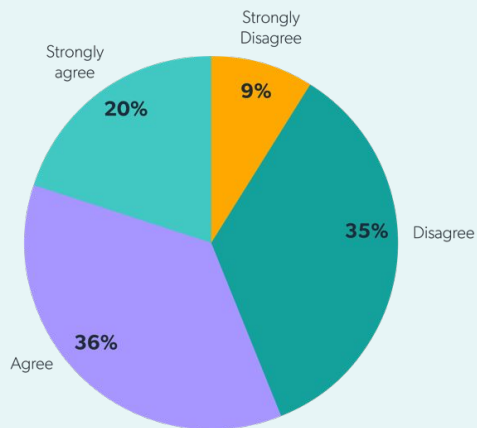
Please select the reason(s) for choosing the IT technology/technologies you selected.



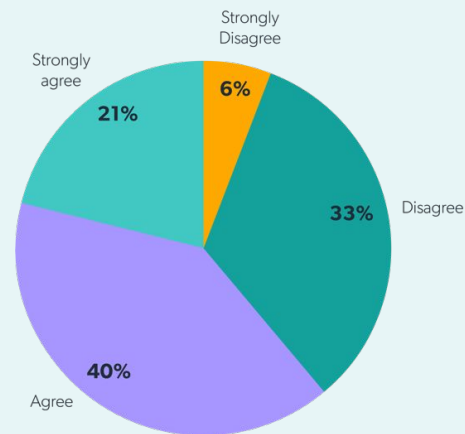
# The Impact of Remote Work on Security

By a slim margin, more than half (55.7 percent) of IT professionals feel like their organization is spending too much to secure and enable remote work. A slightly larger majority (61.6 percent) believe that their company pays far more for tooling to manage users' identities and devices than they need (or use). These costs may be reflected in the increased budgets reported by SMEs. But this trend also reminds us how critical is it for SME IT managers to get every last ounce of value from every dollar of IT spend, especially when it comes to securing and authenticating remote workers and their devices.

Please select how you feel about the following statement:  
"I feel like my organization is spending too much to secure/enable remote work."

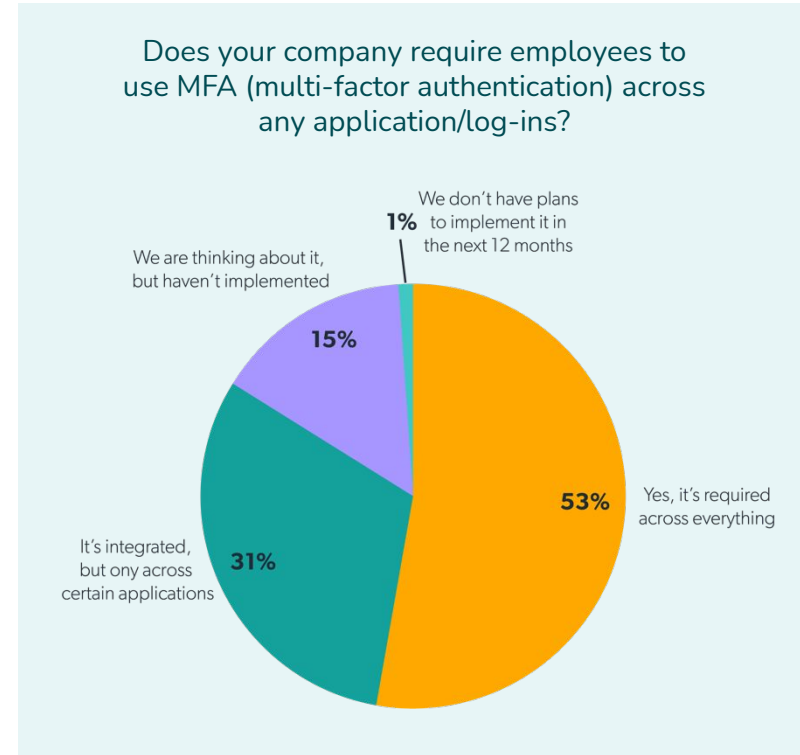


Please select how you feel about the following statement:  
"My company pays for far more tooling to manage users' identities and devices than we need (or use)."



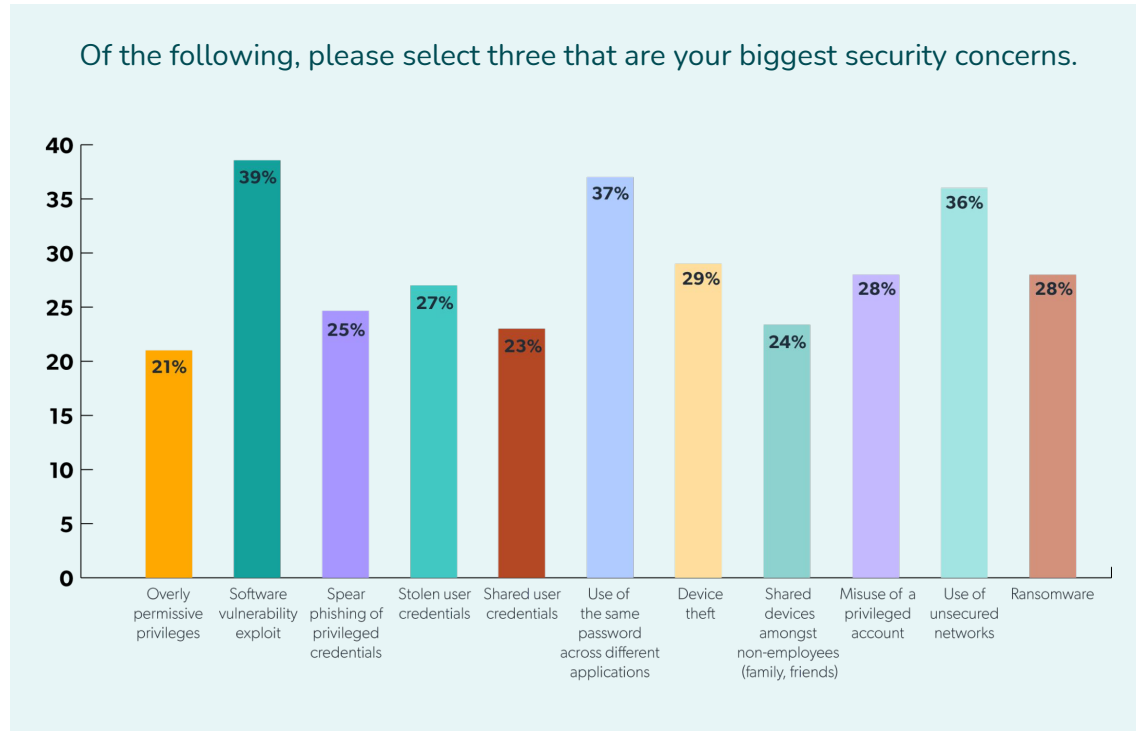
# The Impact of Remote Work on Security

A slim majority of SMEs (52.6 percent) require MFA across all applications and log-ins. Another 30.7 percent have integrated MFA across certain applications. Less than one-in-five organizations have not yet implemented MFA. Clearly, a growing number of SME IT leaders are coming to realize how effective MFA can be in securing remote workers—a priority also reflected in their biggest security concerns.



# The Impact of Remote Work on Security

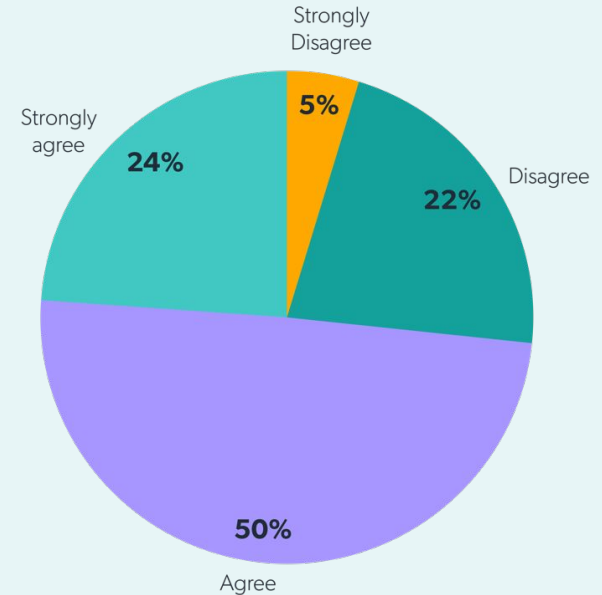
The three biggest security concerns for SME IT professionals are software vulnerability exploits (39.2 percent), the reuse of the same password across different applications (37.2 percent), and the use of unsecured networks (36.4 percent). Password management and unsecured networks, in particular, pose an even greater risk in the work-from-anywhere era—in part because it puts such a burden on remote workers, themselves, to follow good security practices.



# The Impact of Remote Work on Security

Nearly three-quarters of IT professionals agree (49.9 percent) or strongly agree (24.2 percent) that remote work makes it harder for employees to follow good security practices. So, it's not surprising to see, in the next graph, why IT priorities remain focused on remote work for the remainder of 2021.

Please select how you feel about the following statement:  
"I think that remote work makes it harder for employees to follow good security practices."



# The Impact of Remote Work on Security

Adding layered security so WFA is truly secure is the top priority for the remainder of 2021, while making remote work easier for end users took the second spot. The third greatest priority is making device management easier. And while this is a lot harder than it sounds, the right solutions—including Zero Trust security options—can make the difference between expanding revenues and expanding risks.

Please rank what your IT priorities are for managing security for the remainder of 2021. (Top spot is most important, with bottom spot being least important).

Item	Overall Rank
Adding layered security so work-from-anywhere is truly secure	1
Making remote work easier for end users	2
Making device management easier	3
Easier management of user devices	4
Making remote work easier for admins	5
Implementing SSO of unifying identity management	6
Gaining analytical insight into user access	7
MFA	8



# Greater Than Zero

## Organizations Turn to Zero Trust Security

For those unfamiliar with the term, “Zero Trust” security refers to an approach based on the philosophy that an organization should not automatically trust anything either inside or outside its perimeters, and instead must verify anything and everything trying to connect to its systems before granting access. It’s an approach that’s ideal for the work-from-anywhere world, because in this new model, how much I’m trusted shouldn’t depend on where I’m working. It’s also a security model that streamlines tech stacks and workflows, and lets IT teams fundamentally improve their organization’s security without introducing new complications and points of failure by requiring their users to do too much on their end.

This explains why more than half of all the SMEs we surveyed have adopted a Zero Trust security model, or plan to adopt it by the end of 2021. About one-quarter (21.4 percent) have [adopted a Zero Trust solution already](#), 17.5 percent plan on adopting one within the first half of 2021, and 28 percent plan on adopting one by the end of 2021. Surprisingly, about one-in-five IT professionals (19.7 percent) didn’t even know about Zero Trust security—a reminder that many SME IT managers have to wear multiple hats, and don’t always have the luxury of keeping up with the latest cybersecurity trends.

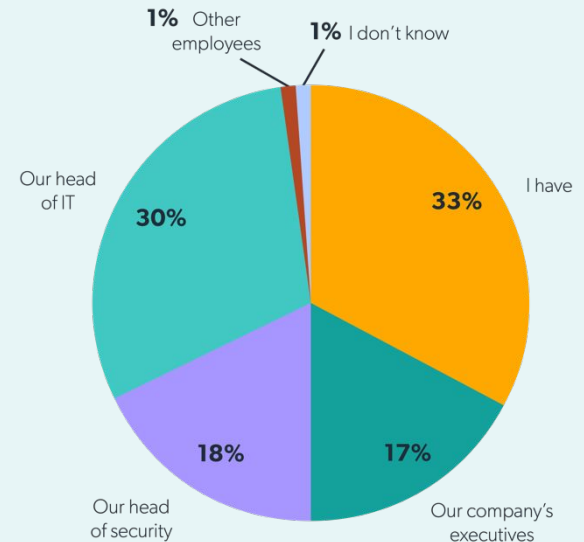


# Greater Than Zero

## Organizations Turn to Zero Trust Security

The champions of Zero Trust security are pretty evenly split across various roles, suggesting it's an idea that's intuitive and appealing to business and IT leaders alike. About one-third (32.8 percent) have championed for Zero Trust themselves, 29.7 percent reported it was championed by their head of IT, 17.9 percent reported it was championed by their head of security, and 17.5 percent reported it was championed by their company's executives.

You stated that your organization is adopting a Zero Trust model. Who has championed the adoption of a Zero Trust model in your company?



# The Zen of Zero Trust and the Promise of SME Growth in the Cloud

As SMEs drive the post-pandemic economic recovery, it is the champions of their IT departments that will enable them to do so. And as IT professionals focus their 2021 priorities on remote work, security and cloud services, it's critical for them to find new ways to accelerate their journey to the cloud, make the most of the cloud once they get there, and adopt a Zero Trust security model.

With the increasing adoption of remote work and the accompanying need for Zero Trust security, IT professionals are turning to JumpCloud. We're uniquely committed to making Zero Trust security affordable and easy to use for SME IT leaders everywhere. Ultimately, our goal is to help these IT champions implement a

highly effective approach to security that will save them precious time and resources, while helping them keep their people productive, happy and secure. And this is how we get to a post-pandemic recovery—one good day at a time.

To learn more about JumpCloud, its commitment to SME IT leaders, and its approach to Zero Trust security, visit [jumpcloud.com/why](https://jumpcloud.com/why).

# Methodology

JumpCloud surveyed 401 U.S. SME IT decision-makers, including managers, directors, vice presidents, and executives. Each survey respondent represented an organization with 500 or fewer employees across a variety of industries. The survey was conducted via Propeller Insights, April 21 - 27, 2021.

---

JumpCloud's mission is to **Make Work Happen®**, by providing people secure access to the resources they need to do their jobs. The JumpCloud Directory Platform gives IT, security operations, and DevOps a single, cloud-based solution to control and manage employee identities, their devices, and apply Zero Trust principles. JumpCloud has a global user base of more than 100,000 organizations, with over 3,700 customers.