

The Surprising New State  
of IT in a Remote World:

# Tackling Challenges and Redefining IT for Future Success

# Table of Contents

Introduction	03
7 Key IT Trends During the Shift to Remote Work	04
Top IT Challenges and Surprises	12
Mission-Critical Solutions Uncovered	20
Defining Changes in IT Roles, Budget and Priority	21
Speed of Transition and Importance of Business Continuity Planning	27
What to Stop / Continue / Start Doing	30
How to Prepare for the Future of Remote Work	32



# Introduction

If changes to the IT landscape could be summed up in one word for this year, it would be: **Remote**. The spread of the COVID-19 pandemic forced businesses worldwide to adapt to sudden and unexpected challenges. Practically overnight, companies of all sizes across many industries were forced to shift employees from offices to remote work. IT teams grappled with the realities of facilitating remote work while making sure company data stayed safe, operations ran smoothly, and IT maintained oversight of key systems.

Just how drastic was the impact of COVID-19 on IT teams? What challenges did they face in the transition to remote work, and what do IT leaders expect the long-term impacts to be? LogMeIn Central commissioned the market research firm Lab 42 Research LLC to reveal the current state of IT in the new era of remote work, while quantifying the impact of COVID-19 on IT roles and priorities for small to medium-sized businesses.

We surveyed 400 IT and IT Security professionals at organizations ranging from 1 - 3,000 employees, across a variety of industries in the United States and Canada. Most survey respondents are IT decision makers, with 95% making some or all decisions regarding new technology for their company. Among the participants are C-level executives (10%), directors and managers (75%), and individual contributors (15%). Nearly all respondents (99%) are partly or solely responsible for implementing new technology for their company. 84% currently have an internal IT role, while 16% have an external IT or Managed Service Provider (MSP) role.

In this report, we reveal the massive shift in the day-to-day work of IT professionals, and the broader impact of the transition to remote work for the majority of businesses. We uncover how the budgets, priorities, and functions of IT teams at small and medium-sized businesses continue to be shaped by ongoing global upheaval and uncertainty. We also share insights into how IT professionals are adapting their roles and teams to these challenges.

# 7 Key IT Trends During the Shift to Remote Work

## 1 Remote work is the new norm.

Prior to the COVID-19 epidemic, most employees (72%) worked in a traditional office setting. While remote work was increasingly popular prior to the pandemic - with 15% of employees working remote only, and 13% working a mix of in-office and remote - it wasn't yet the standard. The prior norm of office-centric was also the standard across the board regardless of company size, geographic location, and number of offices.

As a result of COVID-19, the makeup of the work landscape changed dramatically. Over the space of a few months, 65% of employees shifted to remote only, while only 20% of employees continued to work in-office, and 15% worked a mix of in-office and remote.

Overall, during the COVID-19 pandemic, 87% of companies had employees that transitioned to working from home, and 13% had employees that transitioned to part-time remote.

In other words, there was an almost **complete reversal** in the work environment of the majority of employees. That is a **seismic shift in the makeup of the work landscape** over the course of just a few months, with an equally large impact on the priorities and challenges facing IT teams.

## 2 Better control and more time spent on IT Security.

The average number of endpoints IT professionals are managing have declined over the years, but IT pros are more in control overall. In 2020, only 1 in 10 don't know how many endpoints they are managing, compared to nearly 3 in 10 in 2018.

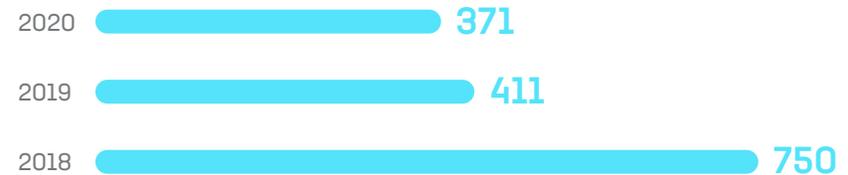
Even though the number of managed endpoints has decreased, the amount of time dedicated to security has increased over the years. On average, nearly half (47%) of IT professionals are spending 5 to 8 hours per day on IT security, compared to 35% in 2019 and 36% in 2018. In 2020, 19% dedicate up to 8 hours a day on IT security. **The increased complexities of BYOD and BYOA (Bring-Your-Own-Devices and Access) work environments combined with advancements in cyberattacks have increasingly monopolized the focus of IT professionals.**

Over half of respondents (53%) from large companies spent 5+ hours on IT security a day, while only 45% of respondents from smaller companies spent 5+ hours on IT security.

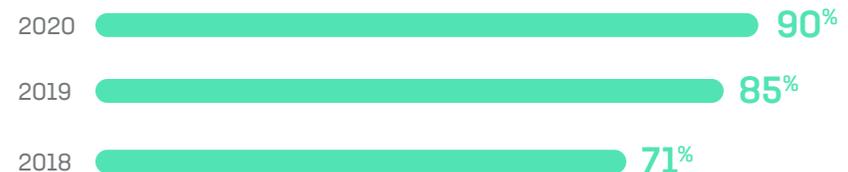
With a disperse workforce and ever-evolving cyber-threats, time spent addressing IT security is on the rise, making it even more critical to ensure the solutions you implement protect your organization from sophisticated online threats.

### IT PROS ARE MORE IN CONTROL OF THEIR ENDPOINT INFRASTRUCTURE THAN EVER BEFORE

#### AVERAGE NUMBER OF ENDPOINTS



#### PERCENTAGE OF IT PROS WHO KNOW HOW MANY ENDPOINTS THEY MANAGE



### 3 | Virtual tasks and security concerns demand more IT time.

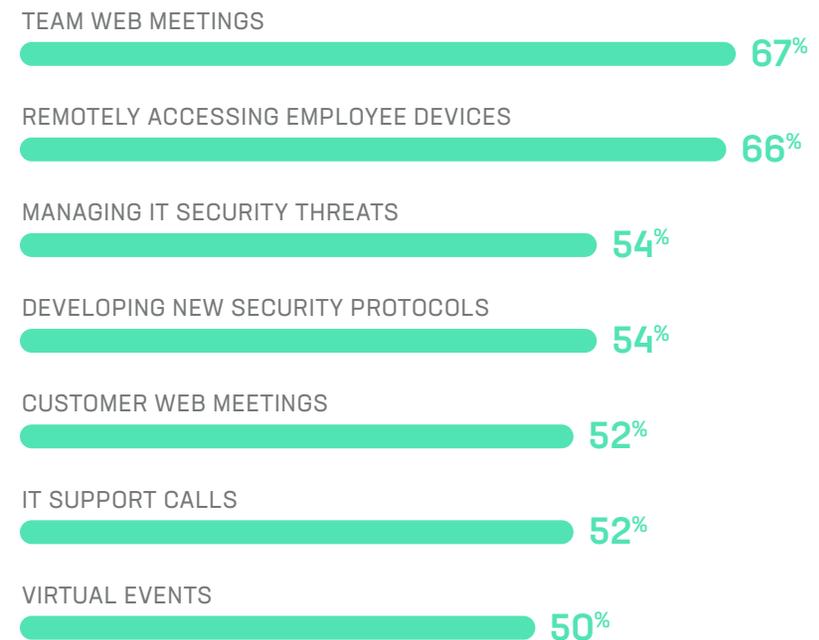
With the onset of COVID-19, the types of tasks that filled a typical IT team member's day changed significantly. Virtual tasks like team web meetings, remotely accessing employee devices, and customer web meetings demanded more time. Security also gained increased focus, with more time spent managing IT security threats and developing new security protocols.

On the other hand, managing hardware and equipment demanded about the same amount of time as before the shift to remote work. Any in-person activities – like in-person team meetings, customer meetings, events, and on-site visits – occupied less IT time than before COVID-19.

Interestingly, Canada spent significantly less time doing on-site visits during the COVID-19 crisis than their IT counterparts in the US, with 74% of IT professionals in Canada spending less time doing on-site visits compared to 55% of US companies. The difference is indicative of their respective national and local COVID-19 policies, and the impact those policies had on IT teams in both countries.

Larger companies experienced a more dramatic shift in day-to-day IT tasks, with 67% of respondents spending less time doing in-person meetings, compared to 57% at smaller companies.

#### TOP 7 TASKS IT PROFESSIONALS ARE SPENDING MORE TIME ON

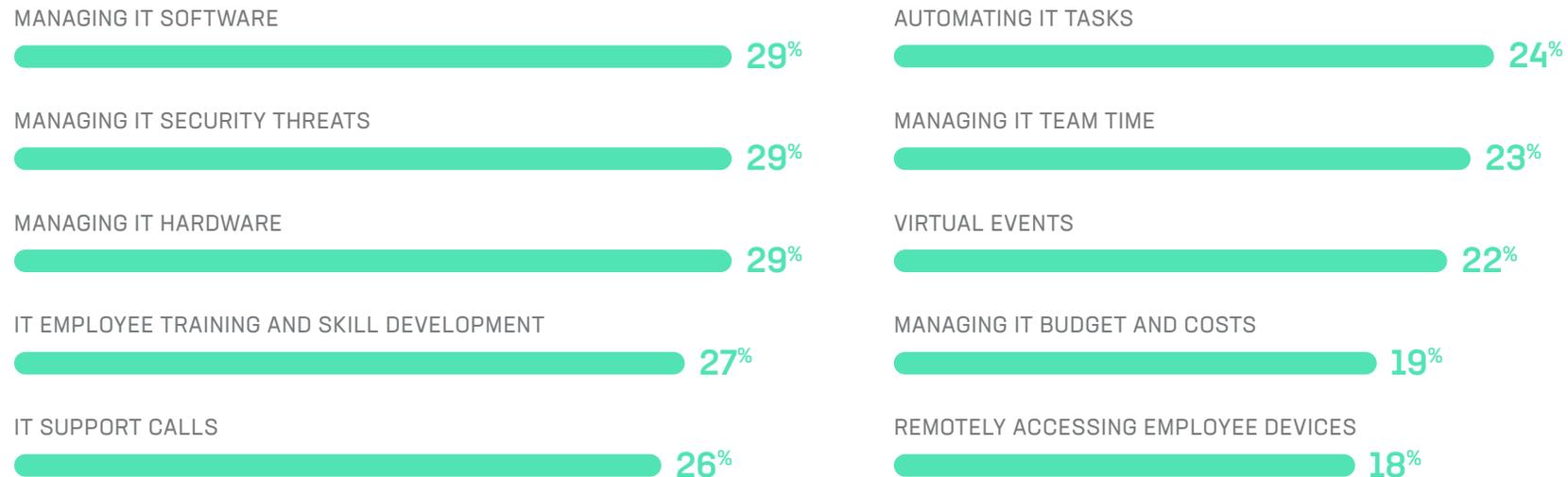


## 4 | IT redefined what was possible in a remote work environment.

Before COVID-19, IT teams assumed many tasks could never be automated or executed remotely. When they were forced to work remote, most IT professionals found they were able to adapt and execute most if not all of their tasks remotely.

With this development, many companies across industries are stating they will never return to a 5-day in office work week, so ensuring IT teams are able to perform the above tasks remotely becomes a necessity for success in the future state of the world.

### TOP 10 TASKS TRANSITIONED TO REMOTE WORK



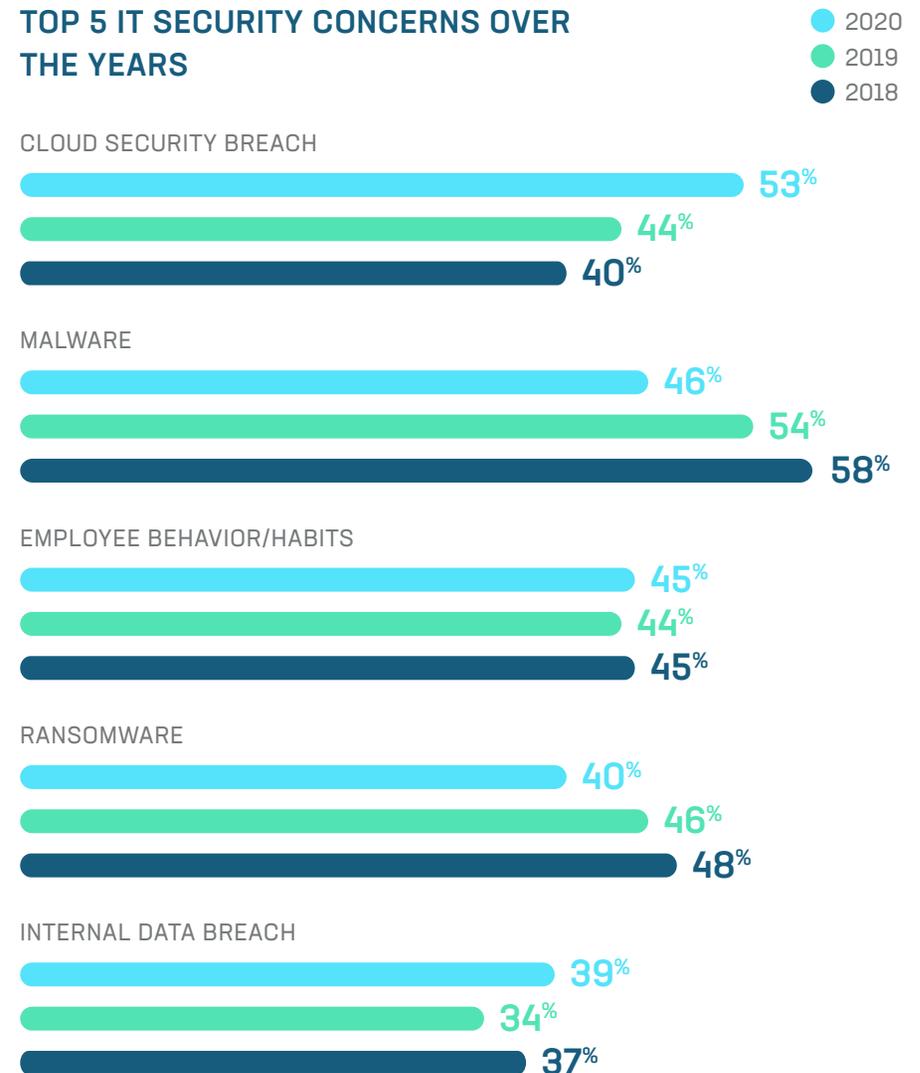
## 5 | IT is most worried about a breach.

The COVID-19 crisis has significantly shaped IT concerns and priorities in 2020. The top IT security concerns continue to be data breaches (cloud, internal, and external), malware, employee behavior, and ransomware. With cloud technology and adoption skyrocketing over the years, fear of a cloud security breach has increased significantly just in the past two years, with 40% of IT professionals expressing concern in 2018 and 53% citing it as a top security concern in 2020.

Ransomware and malware are slightly less of a concern now than they were in the past few years, while cloud security breaches and rapidly evolving business technology practices are now of greater concern. One thing that hasn't changed: concern over employee behavior. In 2018, 45% of respondents worried about employee habits. In 2020, 45% of respondents still mark it as one of their top 5 concerns.

Another higher priority concern in 2020 compared to previous years is 'Rapidly evolving business technology practices' with nearly a third (29%) of IT professionals stating it's a top security concern in 2020, compared to a only a fifth (20%) in 2019.

### TOP 5 IT SECURITY CONCERNS OVER THE YEARS



## 6 | An increase in remote workforce is currently one of the biggest drivers of change.

Last year, only 19% of IT professionals agreed that an increase in a remote workforce was one of the biggest IT trends driving change in the industry. In 2020, 33% of IT professionals now cite it as the top trend. Considering the volume of employees forced to work remotely with only a few weeks to prepare, the transition to a virtual workforce has had a large impact on IT this year.

Though moving to the cloud remains a top trend, about a third of respondents see it as one of the biggest trends, down from 44% in 2019. On the other hand, a greater focus on IT infrastructure monitoring, a shift from a reactive to proactive IT support, and a shift from the break/fix model to proactive IT support are seen as increasingly important trends.

With a shift from reactive to proactive IT support, more and more companies are implementing Remote Monitoring and Management (RMM) solutions to resolve concerns before they become problems and proactively mitigate the risk of cyber threats.

### TOP 5 IT TRENDS DRIVING CHANGE OVER THE YEARS

● 2020  
● 2019

#### INCREASE IN REMOTE WORKFORCE



#### MOVING TO THE CLOUD



#### GREATER FOCUS ON IT INFRASTRUCTURE MONITORING



#### EVOLVEMENT OF CYBERSECURITY



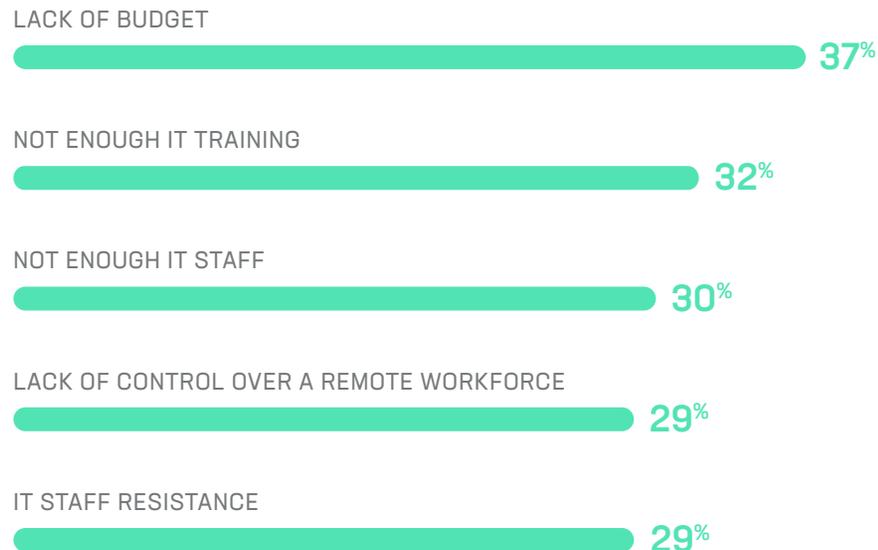
#### A SHIFT FROM REACTIVE TO PROACTIVE IT SUPPORT



## 7 | Lack of budget is the greatest barrier to keeping up with trends in IT.

More than a third of IT professionals (37%) agree that a lack of budget is the biggest challenge their company is facing in trying to keep up with IT trends. IT training, lack of IT staff, lack of control over a remote workforce, and IT staff resistance to change are all seen as the most common reasons IT teams are struggling to adapt to changes in their field.

### TOP 5 CHALLENGES TO KEEPING UP WITH IT TRENDS



With limited budget, IT teams must implement solutions that enable them to do more with less and prioritize implementing tools with security, automation, and monitoring functionality.



Vendor consolidation also becomes critical when dealing with limited budget as bringing more solutions under a single provider brings cost savings and facilitates with logistics of contract management.

Lack of IT training is slightly more of an issue at larger companies (35%) than at smaller companies (31%). Staffing challenges are slightly more of an issue at larger companies (34%) than at smaller companies (28%). Lack of control over a remote workforce is more of an issue at larger companies (34%) than at smaller companies (27%). Both large and small companies struggle with budget.

Companies in Canada struggle significantly more with budget compared to their counterparts in the United States (52% vs 35%) as well as with staffing (46% vs 27% in USA).

### THE STRUGGLES OF SMALL VS. MEDIUM SIZED BUSINESSES

● 1 - 1,000  
● 1,000 - 3,000

#### LACK OF BUDGET



#### NOT ENOUGH IT TRAINING



#### NOT ENOUGH IT STAFF



#### LACK OF CONTROL OVER A REMOTE WORKFORCE



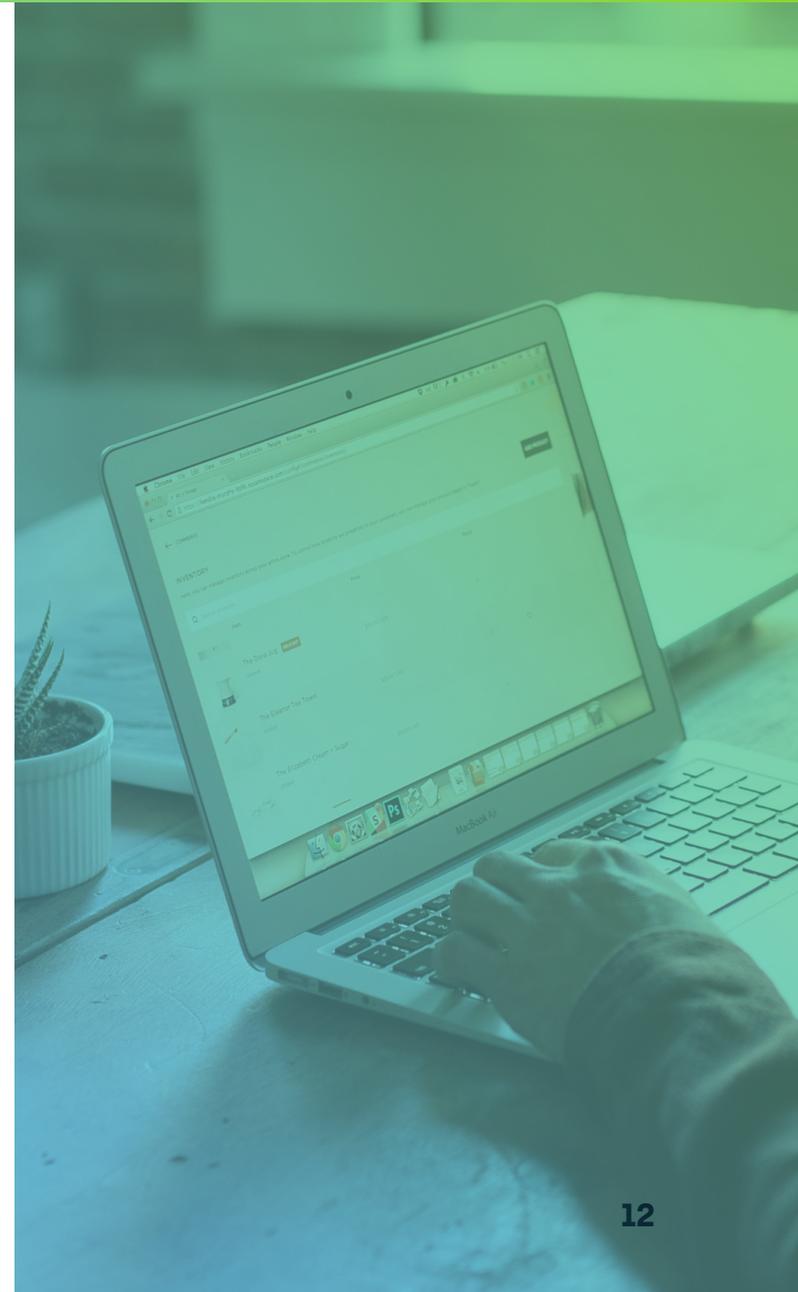
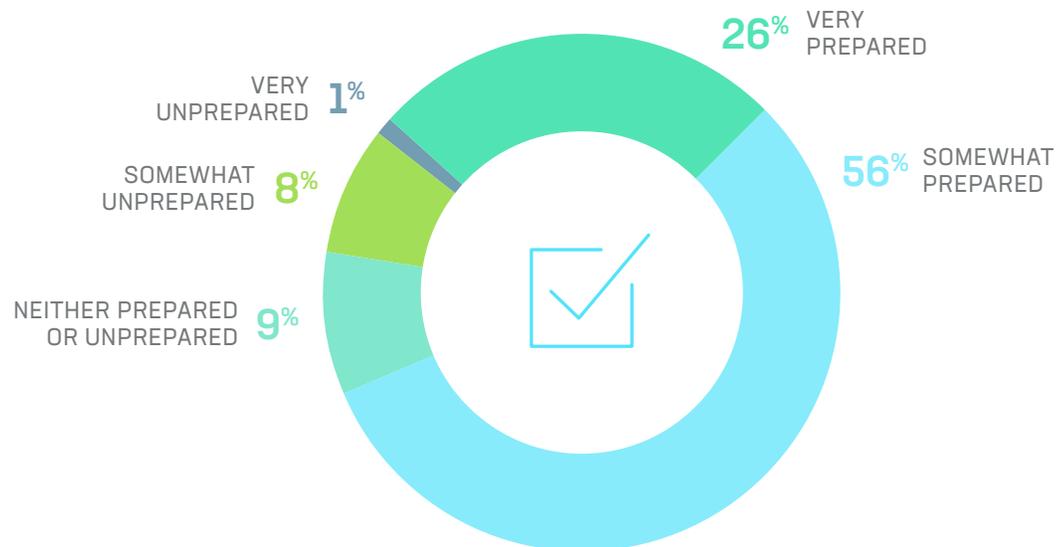
#### IT STAFF RESISTANCE



# Top IT Challenges and Surprises

## Most IT teams felt prepared for remote work.

Though the COVID-19 pandemic escalated quickly, 82% of IT teams said they were somewhat or very prepared to transition all employees to working from home. Most IT teams were prepared for the shift to a virtual workforce, but the transition still required significant IT time and resources.



# But the shift to remote work posed security, technical, and productivity challenges to IT.

Remotely managing IT security threats has been the biggest challenge for IT professionals, which has meant IT pros are spending 5 to 8+ hours per day addressing this one area. That's a significant increase compared to previous years, when IT typically spent 1 to 4 hours per day on security.

Interestingly, employees at companies 1,000-3,000 were more likely to struggle with feelings of loneliness (25% vs 14% of companies 1-1,000) and also less likely to have a home office set up (21% vs 9% of companies 1-1,000).

MSPs and external IT professionals were far more likely to feel like their coworkers were not pulling their fair share (23%, vs 13% for internal IT).

Only 5% of respondents indicated they haven't faced any challenges.

## TOP 5 CHALLENGES DURING THE SHIFT TO WORKING REMOTELY



## IT professionals were most surprised by distractions at home, slow responses from colleagues, and the volume of work required to transition everyone to remote.

When asked to share the **most surprising or unexpected challenges** they faced during the transition to remote work, IT professionals shared frustrations with their **home environment and the realities of collaborating virtually**.

Many respondents mentioned that colleagues would be inaccessible or slow to respond during the workday. **“We were surprised [by] the lack of response from remote employees who report problems,”** noted one IT professional. **“We are accustomed to following up with staff in person and found they are far less responsive remote.”** When the option to stop at someone’s desk was no longer available, it became harder to connect with employees.

Others noted that completing certain tasks remotely was difficult, and it took time to figure out how best to replicate in-person activities online. **“The most unexpected challenge is to provide all the trainings remotely while ensuring efficiency and productivity,”** noted one IT professional.

For some, they were surprised at the daily distractions that affected them and their coworkers. The impact to productivity was compounded by the emotional and psychological effects of coping with a pandemic.

**“The biggest challenge was addressing employees having difficulties dealing with the stay-in-place order,”** admitted one respondent. **“It was nothing work-related, but helping them emotionally, and compassionately, as they had persons effected [by COVID-19], or the isolation from friends and family.”** The COVID-19 pandemic not only impacted IT operations and roles, its effects on everyone’s personal life also impacted the work environment.

## For many IT teams, it's still business as usual after transitioning to remote work.

When asked about their day-to-day responsibilities that were left untouched by the transition to remote work, most IT respondents agreed that their jobs were largely unchanged.

**“All aspects of my job were unaffected. [It's] business as usual,”** answered another IT professional. **“I still do the same work, just remotely now,”** said another. “Honestly, my job as a whole has stayed relatively unchanged since the transition,” added another IT professional.

Another shared that they were at an advantage given their status as a remote IT team for their customers: “Being the remote IT department for customers has given us an edge for ourselves and our customers. What we do see is a greater need for internal training that covers the „what if“ factors. We did not plan for the reason for this disaster but as it turns out, we were pretty well prepared, certainly better than most.”

Servers, networks, databases, and core tasks like user support and customer care were frequently cited as areas that weren't impacted by the transition to remote work.

The way those tasks might be accomplished might have changed – such as over meeting software instead of in-person – but the task or project itself wasn't impacted. Many respondents commented that even the number of hours they work were not impacted much, though how they spend those hours may have shifted slightly.

However, for some IT professionals, the transition to remote impacted nearly all aspects of their job.

“Actually, pretty much everything was turned upside down, and had to be reorganized,” said one IT professional. Another agreed that, “Everything I do has been impacted by the transition.” One IT professional responded that “I think about every aspect of operation has been impacted. Team morale was still amazing, though.”

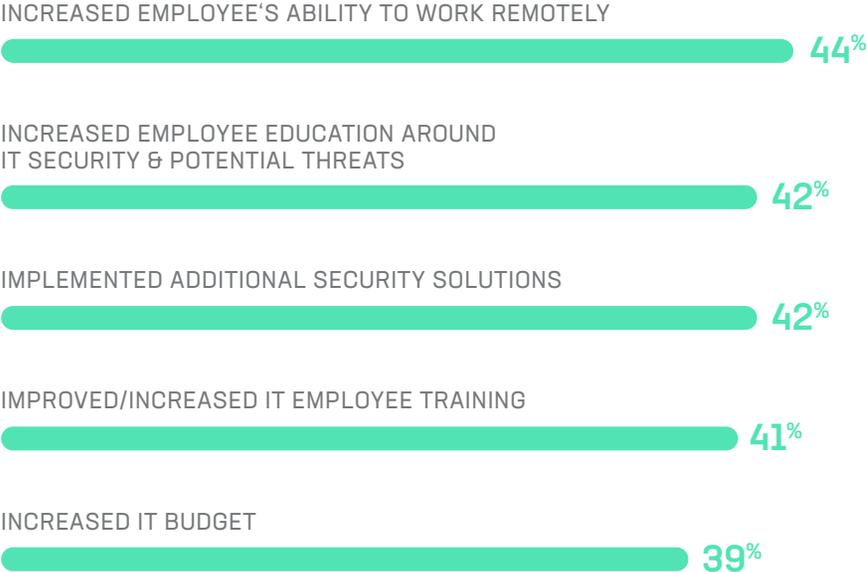
## Most IT teams feel confident in addressing issues caused by remote work.

In response to the COVID-19 pandemic, IT teams have focused on increasing employees' ability to work remotely (44%) and increased employee education around IT security and potential threats (42%). IT decision makers have also prioritized implementing additional security solutions (42%) and increasing IT employee training (41%).

Compared to 2019, IT decreased most other efforts in addressing security concerns as they focused more resources on facilitating remote work. Investment in employee education and training as well as additional security solutions and automating security processes all dropped in 2020. In response to security concerns, more IT professionals did, however, invest in a Remote Monitoring and Endpoint Management (RMM) solution, up from 32% in 2019 to 37% in 2020.

Note that only 8% of businesses have increased the number of IT employees as a result of the pandemic. It seems existing teams are having to shift priorities and adapt, which may require IT employees to continue increasing their already-heavy workload.

### TOP 5 IT ACTIONS TO ADDRESS REMOTE WORK ISSUES



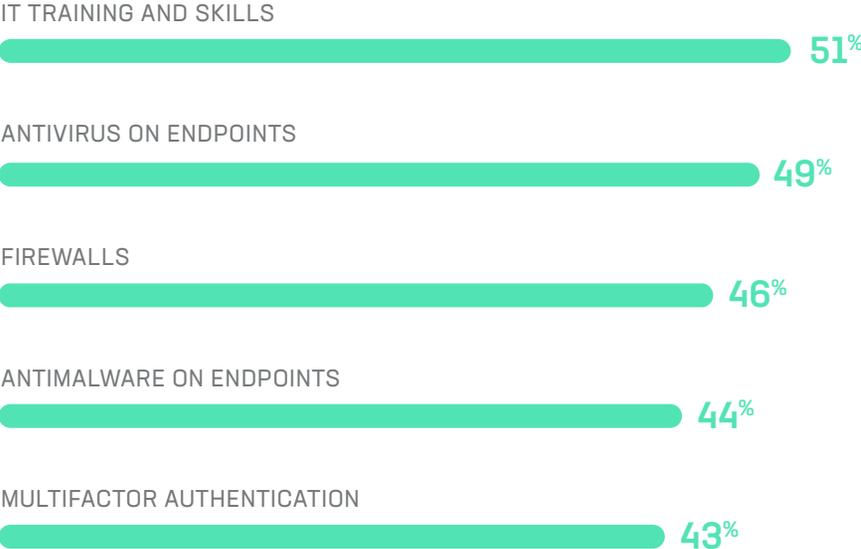
## IT training is core to addressing security concerns.

IT training and skills are still central to IT's confidence in addressing their security concerns, though not quite as common as in years past. Currently, 51% are relying on IT training and skills to address security concerns, and it is the countermeasure most often in place to address security concerns. It is down, however, from 63% in 2018 and 60% in 2019.

Other top tactics for addressing security concerns include antivirus (49%) and antimalware (44%) on endpoints, firewalls (46%), and multifactor authentication (43%). All of these are seen as the most effective countermeasures, and are also areas where IT sees a need for further investment.

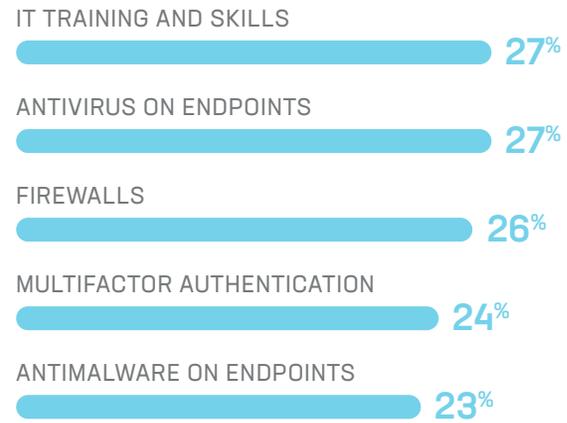
Nearly half of IT professionals (45%) spend most of their time addressing security issues before there is an attack or breach. Being proactive, not just reactive, is important to many IT professionals.

### WHICH MEASURES DO YOU HAVE SETUP TO ADDRESS THESE CONCERNS?

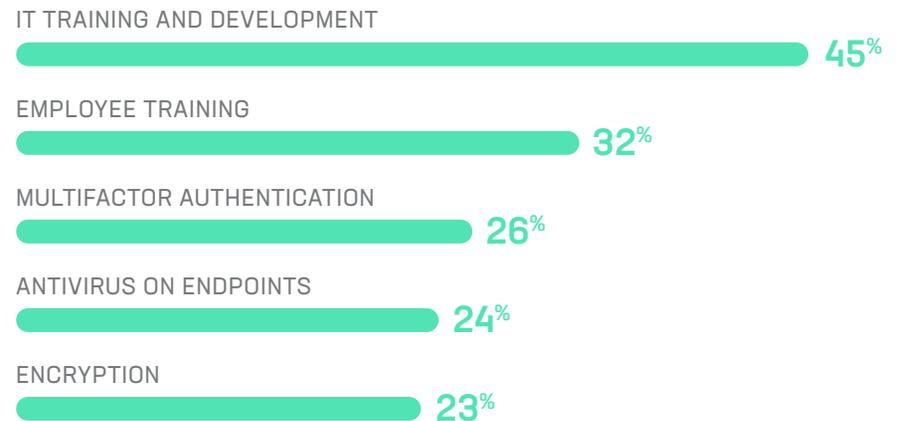




### WHICH IT MEASURES ARE MOST EFFECTIVE?



### WHICH IT MEASURES SHOULD YOU BE DOING MORE OF?



### IT feels confident in addressing security risks.

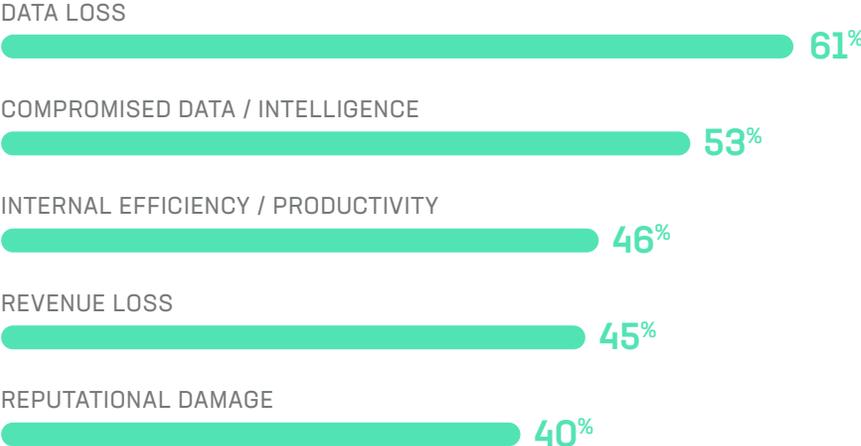
Despite the shifts in the 2020 IT security landscape, the overwhelming majority of respondents - 92% - feel prepared to deal with their IT security concerns.

In fact, confidence this year is higher than in years past - with 82% feeling prepared in 2018, and 86% feeling prepared in 2019. **The fact that more employees are remote doesn't appear to impact IT's confidence in securing the company - only 19% of IT professionals cite a lack of control over a remote workforce as a concern.**

Also, most IT decision makers are confident that their security measures are effective for their end users. 93% of respondents are somewhat or very confident that their security measures are effective for their end users.

When identifying their top security priorities, IT teams are most concerned about risks of data loss (61%), compromised data or intelligence (53%), and the impact on employee productivity (46%) and revenue loss (45%). Though the types of security threats have shifted over the past few years, the risks posed by those threats have not changed much.

### TOP 5 RISKS OF SECURITY THREATS



For those who don't feel confident in addressing security risks, it's most often due to lack of budget (42%), not enough IT staff (39%), and lack of technology (39%). More than a third cite that it's hard to keep up with constantly changing technology (36%), and employee apathy around security also remains a challenge (32%).

# Mission-Critical Solutions Uncovered

## Software facilitating remote collaboration and management proved most valuable to IT.

Given that it was no longer possible to stop by an employee's desk to address any issues, IT teams prioritized remote access software first during the COVID-19 pandemic. With employees working from home, having a way to collaborate with colleagues became mission-critical, so meeting and communications software also topped the list. Security also remained a top priority.

**During the shift to working remotely, The software relied on most heavily by IT teams included:**

1. Remote access software [38%]
2. Meeting software [34%]
3. Remote support software [32%]
4. Security software [30%]
5. Communications software [28%]

Software that did not facilitate remote collaboration or automate remote tasks was seen as far less valuable. **Less than 1 in 10 IT professionals considered the following software solutions to be valuable during the transition to remote work:**

1. Password management software (9%)
2. Onboarding and training software (9%)
3. AI powered chatbot software (7%)
4. Accounting and Finance software (6%)

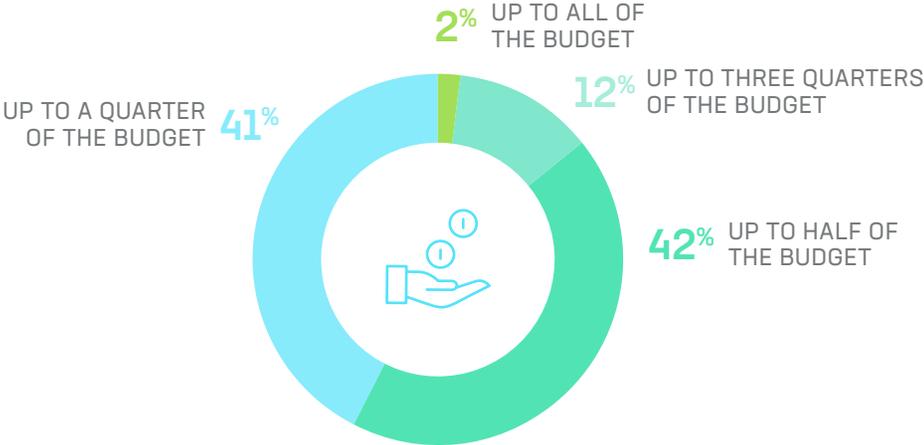
Although password management software has been growing in popularity and adoption over the years, it was not deemed mission-critical by the large majority of IT professionals during the transitory shift to remote work. However, now that companies are more settled in their remote work environments, IT professionals are placing higher priority on password management to facilitate secure credential storage as well as sharing of team logins.

# Defining Changes in IT Roles, Budgets and Priorities

## IT budgets are in flux.

More than half of IT decision makers (63%) reported that the IT budget was reprioritized to support the transition to remote work. For the majority of companies (83%), less than half of the IT budget was reprioritized.

### HOW MUCH OF THE BUDGET WAS REPRIORITIZED?



Only 13% saw a decrease in the IT budget as a result of a shift to remote work. Otherwise, it was a split between those for whom the IT budget remained the same (43%) and those who saw an increase to the IT budget (44%).

IT budgets at smaller companies (1,000 or less) on average had more budget increases than larger companies, with 47% of companies 1-1,000 seeing an IT budget increase while 34% of companies 1,000-3,000 saw a budget increase. Companies 1,000-3,000 were more likely to have no change to their IT budget, with over half (54%) staying the same.

For the companies that experienced an increase in the IT budget, the IT budget increased up to 50%, while few (17%) saw an increase over 50%.

For IT teams that saw a decrease to their budget during the shift to remote work, most saw less than a 25% decrease. 60% saw a 1-25% decrease. Very few (2%) saw more than a 50% decrease.

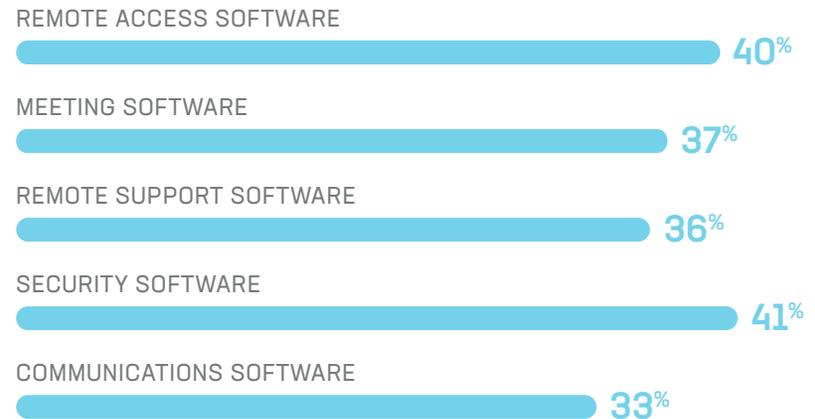
## Software facilitating remote work took priority in the budget.

During the shift to remote work, software that facilitated virtual collaboration, troubleshooting, and security demanded more IT budget. As employees needed to connect to work from home and IT needed to keep the business up and running, software needs shifted accordingly. Remote access and remote support software allowed IT to continue carrying out critical tasks, while meeting software and communications software kept employees informed.

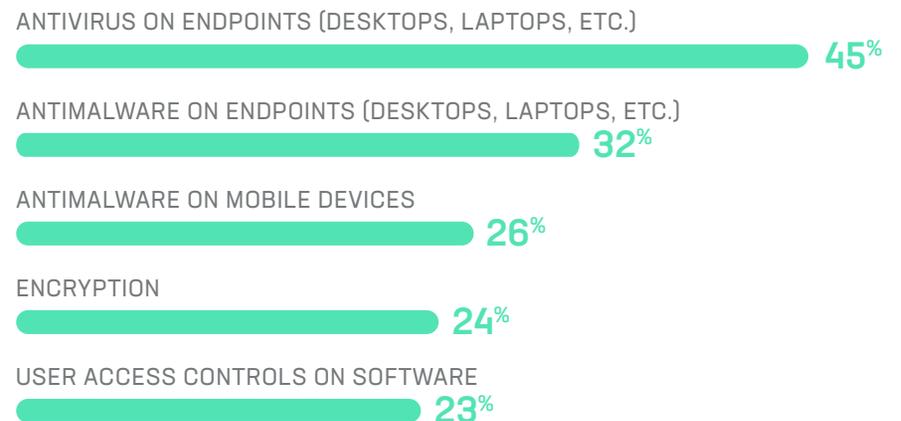
More specifically, antivirus and antimalware on endpoints, as well as encryption and user access controls on software, demanded more IT budget after the shift to remote work. Securing remote devices became a top priority for IT teams.

Budget decreases were less common, but the items most likely to receive less funding included IT training and skill development and employee training. Given the uncertainty generated by the COVID-19 pandemic, any initiatives that were not critical to the business were temporarily put on hold.

### COMPANIES SPENT MORE BUDGET ON



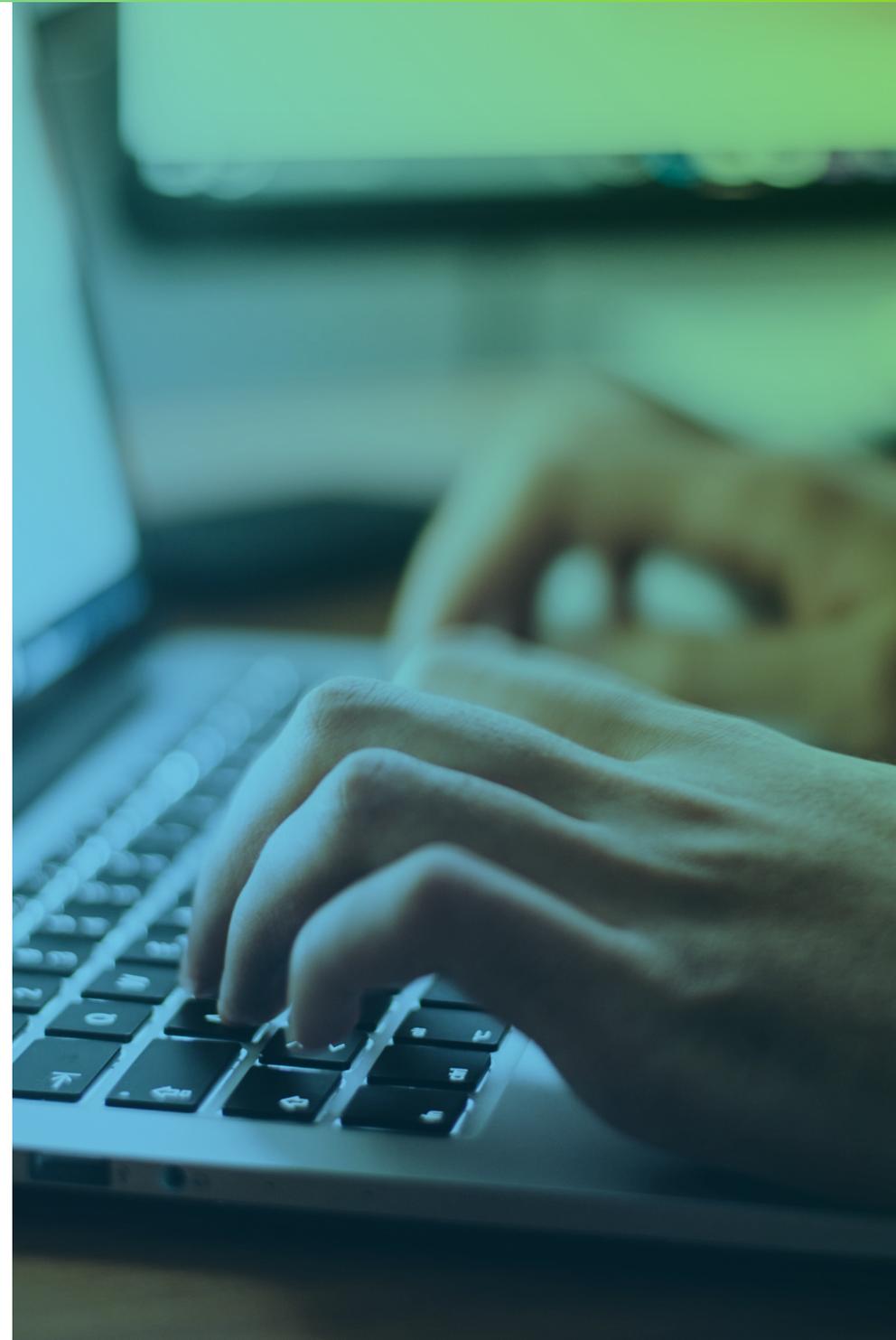
### BUDGET INCREASES DURING THE SHIFT TO REMOTE WORK



## IT was able to expedite wish list items that were also critical to remote work.

Many IT teams were able to capitalize on the shuffling priorities during COVID-19 and expedited items on the IT wish list. 40% of respondents said IT wish list items were expedited - the most common being IT training and skill development (46%), employee training (32%), antivirus on endpoints (30%), and user access controls on software (30%).

For software specifically, about 37% of IT teams were able to expedite items on the IT software wish list. Among the software most often expedited were meeting software (35%), cloud-based storage software (29%), and security software (29%).



## An end to COVID-19 could mean more budget changes.

However, the changes to IT budgets may be temporary. As employees start going back to an office, IT expects budgets to change again, with an increase in employee training and IT training at the top of the list. Once business “normalizes”, those budget items that were dropped are expected to jump back up the list of priorities.

Interestingly, MFA appears to be a high priority for IT teams in the US. 30% of US respondents expect a budget increase for MFA when employees return to the office, nearly double the number of Canadian respondents that expect an increase in that budget item (14%).

A shift back to the office is also predicted to result in redistributing IT budget away from virtual software tools.

Many expect a decrease in budget for remote access software, remote monitoring and management software, remote support software, and meeting software. Software to facilitate remote work will certainly still be part of the IT budget but will not demand such an outsized portion of it as teams expect to return to the office.

### EXPECTED IT BUDGET INCREASES AFTER COVID-19



## When the pandemic is over, IT expects priorities to shift again, too.

As employees plan to return to the office, IT professionals assume that remote tasks will be less important but won't necessarily disappear altogether. According to survey respondents, changes to the role of IT will include:

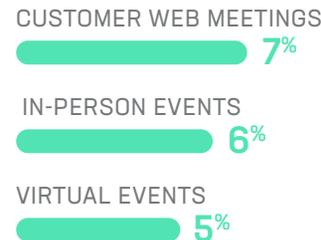
1. Less web/video calls and more in-person meetings with team members (42%)
2. Less reliance on software that enables IT to work remotely (38%)
3. Cybersecurity risks will decline as more employees return to the office (36%)
4. Less web/video calls and more in-person meetings with customers (35%)
5. More work as customers are using more applications (34%)

Only 9% anticipate no changes to the role of IT, indicating that an end to COVID-19 won't bring an end to the need for flexibility and adaptability.

### TOP IT PRIORITIES TO MAXIMIZE PRODUCTIVITY AND DOWNTIME WHEN EMPLOYEES RETURN TO THE OFFICE



### LOWEST PRIORITIES



## 2021 budgets won't decrease for most IT teams.

When asked what they expected of their 2021 budget, most IT teams expect their budget to either stay the same (45%) or to increase (46%). Very few IT teams (9%) expect their budget to decrease.

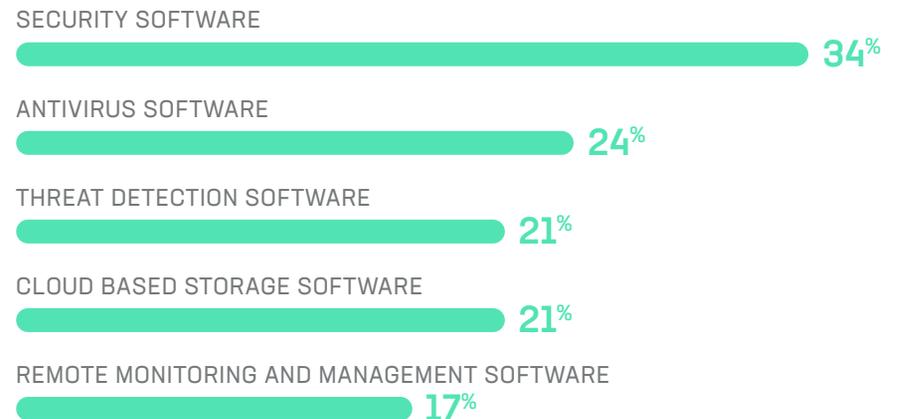
Training and threat prevention top the list of security priorities for next year's budget. IT training and skill development is a top priority for 32% of teams, as is employee training for 24% of teams. Training of both the IT team and end users is seen as essential to a company's cybersecurity strategy. Other priorities include firewalls (30%), antivirus on endpoints (28%), and antimalware on endpoints (27%) to reduce the risk of cyberattacks and data breaches.

Software priorities in the budget reflect the IT team's security priorities, with investment including security software (34%), antivirus software (24%), threat detection software (21%), and remote monitoring and management software (17%). Cloud based storage software (21%) was also among the top 5 software priorities for the 2021 budget. This list of priorities is in line with where IT is spending more of their time these days: in preventing and addressing security risks and issues.

### SECURITY PRIORITIES EXPECTED TO USE A MAJORITY OF BUDGET IN 2021



### SOFTWARE PRIORITIES EXPECTED TO USE THE MAJORITY OF THE BUDGET IN 2021



# Speed of Transition and Importance of Business Continuity Planning

Though the majority of IT teams felt prepared for the transition to remote work, it still required a lot of time and resources to execute. Looking ahead, many IT teams learned valuable lessons from the challenges created by the COVID-19 pandemic and underscore the need for detailed business continuity planning. Those companies that developed business continuity plans prior to the pandemic found that they were able to more quickly complete the transition, and reduced confusion and stress for both their teams and the company overall.

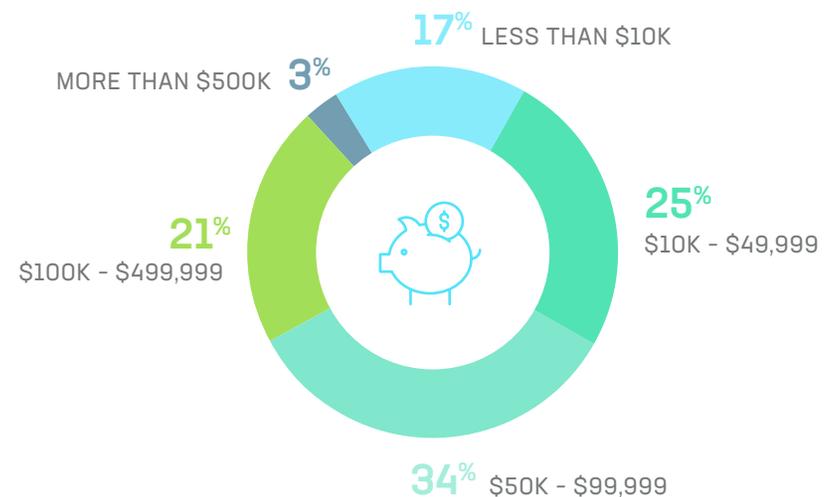
## Business continuity plans made for a smoother transition to remote work.

A majority of IT professionals (71%) indicated that their companies have a business continuity plan. For those that had a business continuity plan, 78% agreed the business continuity plan helped more quickly activate the shift to remote work. Of those who didn't yet have a business continuity plan, many IT professionals (41%) were planning to develop one in the future, given the value it would bring in preparing for unanticipated challenges.

## The transition to remote work meant more IT expenses.

The initial shift to remote work also required significant monetary investment for most IT teams. A quarter of IT teams spent between \$10,000 and \$49,999, while about a third (34%) spent \$50,000 to \$99,000.

## THE COST OF SHIFTING TO REMOTE WORK FOR IT



### And the transition led to downtime and delays for the majority of companies.

For most teams surveyed (76%), 3 - 10 days were spent by the IT team preparing and executing the transition for employees to work remotely. For some companies (11%) the transition took 11 or more days, and few (13%) were able to make the change in 1 or 2 days.

34% of IT teams experienced delays that caused downtime for employees. Almost three-quarters of companies (72%) experienced downtime that caused noteworthy disruptions to the employee workday, with 36% experienced 30 minutes to an hour and another 36% experiencing 2 to 4 hours per day. For many companies (53%), the downtime lasted 3 to 5 days, but for 7% the downtime lasted 11 or more days.

### The silver lining: IT is more prepared for future challenges.

Despite the impact many teams experienced from COVID-19 - from budget, to resource allocation, to project priorities - many cited that their teams are now more prepared.

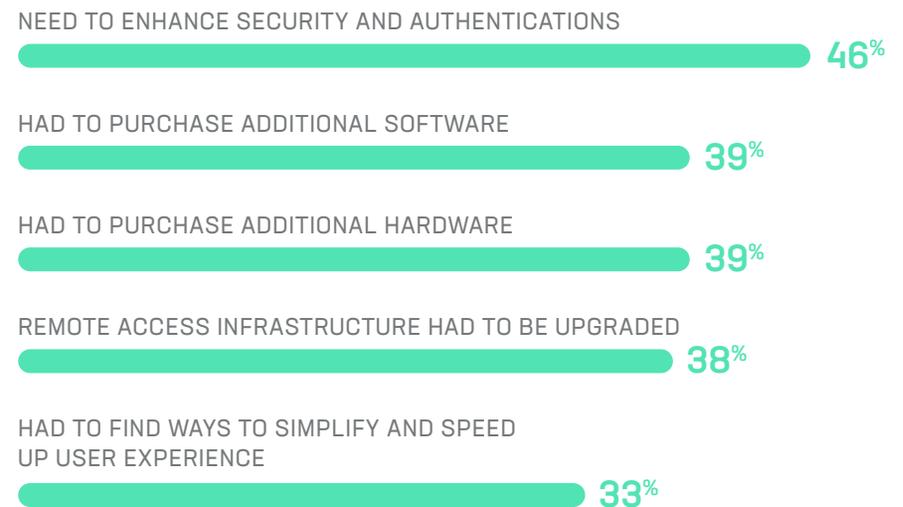
IT professionals agreed that the pandemic has led to improved training for IT (41%) and employees (24%), ensuring all employees have the appropriate hardware (30%) and software (29%), and even installing multifactor authentication (24%) for improved security.

## IT teams see room for improvement in business continuity plans.

For those companies that had a business continuity plan, the experience of navigating the COVID-19 pandemic has helped IT identify ways to improve their plans for future challenges. Changes to business continuity plans included the need to enhance security and authentications (46%), purchasing additional software (39%) and hardware (39%), upgrading remote access infrastructure (38%), and simplifying and speeding up the user experience (33%).

One of the challenges with business continuity planning is the difficulty in anticipating every possibility for any potential crisis. The COVID-19 pandemic provided a unique, real-world opportunity to test out existing business continuity plans and strengthen them for responding to future crises in a way that is hard to replicate in a simulated exercise.

### TOP 5 CHANGES TO BUSINESS CONTINUITY PLANS DUE TO COVID-19



# What to Stop / Continue / Start Doing

During the period of transitioning to and establishing remote work, most IT teams plan to continue their existing tasks and priorities. There are, however, some responsibilities that IT professionals plan to stop doing, and others they plan to start doing, to set their team up for success in the “new normal” of a remote work environment.

Many IT professionals plan to stop offering in-person IT helpdesk (23%) as well as stop attending conferences (22%). Some of the benefits observed in not doing those tasks after transitioning to remote work may incent some teams to do away with them entirely.

Otherwise, most teams will continue to do their existing tasks, especially those that prioritize security and risk mitigation. Tasks that IT will continue doing include installing antivirus (75%) and antimalware (73%) on endpoints, installing user authentication (73%), establishing software and hardware inventory reporting (71%), establishing user access controls on software and hardware (71%), and installing firewalls (71%).

Top of the list to start doing is to continue to improve the IT support experience. That includes offering AI powered chat support for IT troubleshooting (35%) and implementing a remote support solution to offer real-time support with one-click access to employee or client computers (33%). Other things IT professionals anticipate starting are offering a virtual IT helpdesk (31%) and having the right software (31%) and extra hardware on hand - likely a result of struggling to equip all employees with the appropriate resources during the transition to remote work.

TOP TASKS TO STOP, CONTINUE, AND START DOING



OFFER IN-PERSON IT HELPDESK



ATTEND CONFERENCES



RELY ON A REACTIVE IT SUPPORT SOLUTION



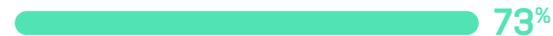
PERFORM ROUTINE IT TASKS MANUALLY



INSTALL ANTIVIRUS ON ENDPOINTS



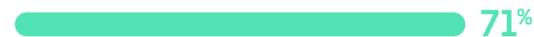
INSTALL ANTIMALWARE ON ENDPOINTS



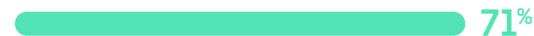
INSTALL USER AUTHENTICATION



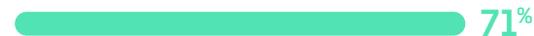
ESTABLISH SOFTWARE/HARDWARE INVENTORY REPORTING



INSTALL FIREWALLS



ESTABLISH USER ACCESS CONTROLS ON SOFTWARE/HARDWARE



OFFER AI POWERED CHAT SUPPORT FOR TROUBLESHOOTING



IMPLEMENT A REMOTE SUPPORT SOLUTION TO OFFER REAL-TIME SUPPORT WITH ONE CLICK ACCESS TO EMPLOYEE/CLIENT COMPUTERS



HAVE ALL THE APPROPRIATE SOFTWARE FOR EMPLOYEES



OFFER VIRTUAL HELPDESK

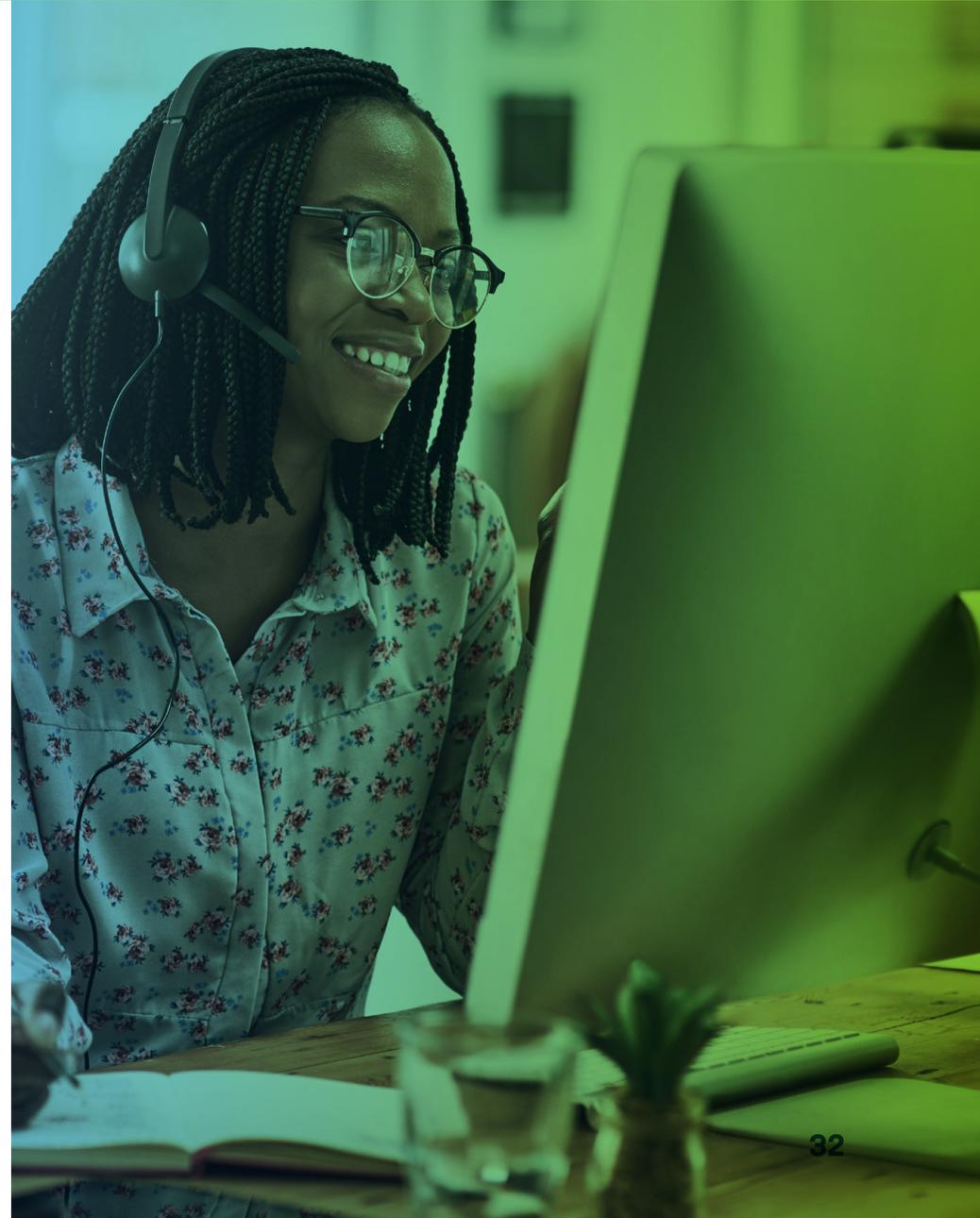


KEEP EXTRA HARDWARE ON HAND



# How to Prepare for the Future of Remote Work

Remote work is not a temporary shift that will reverse once the COVID-19 pandemic passes. Companies of all sizes have seen too many benefits - including improved productivity, employee happiness, better work/life balance, and significant cost savings - to revert to the old norm of office-centric policies. That is not to say that employees will never return to the office, but a hybrid or full remote policy will become the new norm across many organizations.



## To prepare for this future state, consider the following guidelines:

### 1. Create and refine your IT Business Continuity Plan

If 2020 taught us anything, it's to expect the unexpected. Companies that had a business continuity plan in place transitioned to remote work more seamlessly and experienced less downtime.

Keep in mind that having an IT business continuity plan is not a one-and-done project, and it should be revisited every 9-12 months to ensure it's updated accordingly with any company or industry changes.

### 2. Implement Software and Hardware That Facilitate Working from Anywhere

To work away from the office effectively, IT teams and employees need the right tools to get their jobs done. If your company was rushed to pick a few solutions quickly in response to COVID-19, take some time now to re-evaluate the tools you have in place to make sure they meet your specific organizations' needs.

Be sure to have the following 5 software solutions implemented going forward: remote access software, meeting software, remote support software, security software, and communications software.

### 3. Invest in IT Security

Evolving threats and a disperse workforce mean IT professionals need to dedicate more time to address IT Security challenges. To ensure your company is protected, invest in both IT and employee training so everyone is prepared to mitigate risks and ensure company data is protected.

In addition to IT and employee training and development, be sure your company has powerful firewall, antivirus, and anti-malware that protect all endpoints beyond computers and servers.



## SECURE, RELIABLE, INTUITIVE REMOTE MONITORING AND MANAGEMENT

Part of the LogMeIn Inc. Identity & Access Management portfolio, LogMeIn Central is a pure, cloud-based remote monitoring and management solution enabling IT professionals to effectively monitor, manage and secure their endpoint infrastructure. Whether you have remote employees or endpoints scattered across the globe, LogMeIn Central provides IT organizations with the speed, flexibility and insight needed to increase productivity, reduce IT costs and mitigate risk. Rated the #1 remote access tool for small businesses to manage multiple computers, LogMeIn Central equips every endpoint in your network with premium remote access so you can troubleshoot anytime, anywhere.

[LogMeIn.com/central](https://LogMeIn.com/central)