



The State of IT at Modern Workplaces



Table of contents

Report: The State of IT at Modern Workplaces

03	Modern workplaces have changed dramatically
04	A snapshot of today's IT management landscape Outsourced vs. In-house IT management
06	Workplace security is priority number one Case study: When workplace security goes awry
11	The top IT challenges of 2021 From the experts: IT is an investment, not a line item
15	Employee compliance is a major concern Opportunity for customer/respondent quotes
17	What happens when data is lost? Case Study: How Cozad Community Health System Dealt with Data Loss
20	Advice from the front lines Modern workplaces have changed for good, but with the right tools, today's teams can adapt

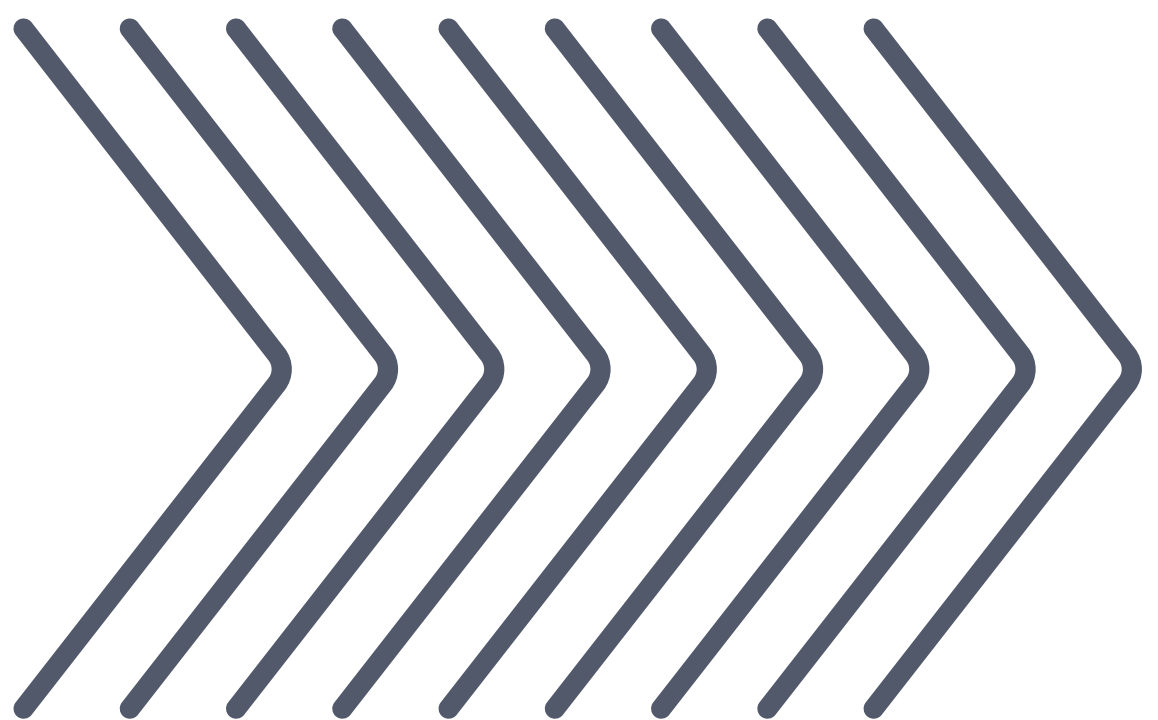
Modern workplaces have changed dramatically

The workplace as we know it has changed immensely in the wake of the COVID-19 pandemic. While remote work has been gaining popularity for quite some time, the pandemic pushed most workplaces into a non-negotiable remote-first setup.

There was a seismic shift in 2020 when every business needed secure, easy-to-use IT solutions that would go off without a hitch. We wanted to learn more about how today's workplaces have been affected by these changes.

Along with Pulse, we surveyed 100 small-to-medium business (SMB) IT leaders to understand their pain points, gather their advice for peers, and learn more about how outsourcing and/or automating their IT has helped them tackle their biggest challenges.

This report will examine which IT trends and solutions are most important to today's business owners, what areas are still vulnerable, and what we have collectively learned during this unprecedented time in IT solutions.

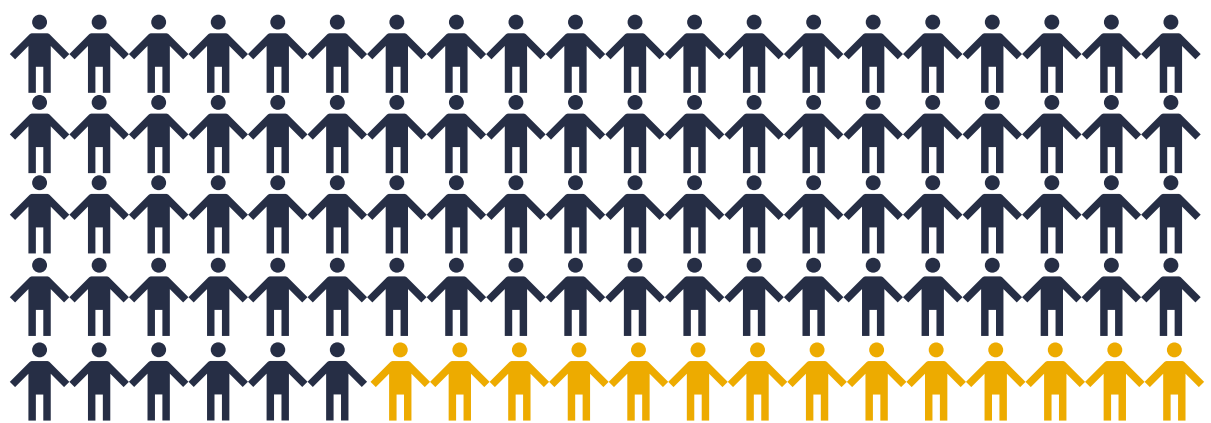


A snapshot of today's IT management landscape

We aimed to capture a sampling that reflected the reality in which today's businesses exist. The answers you'll see in this report come from a number of IT professionals—from managers to executives—in businesses that represent each point on the "small to medium sized business" spectrum.

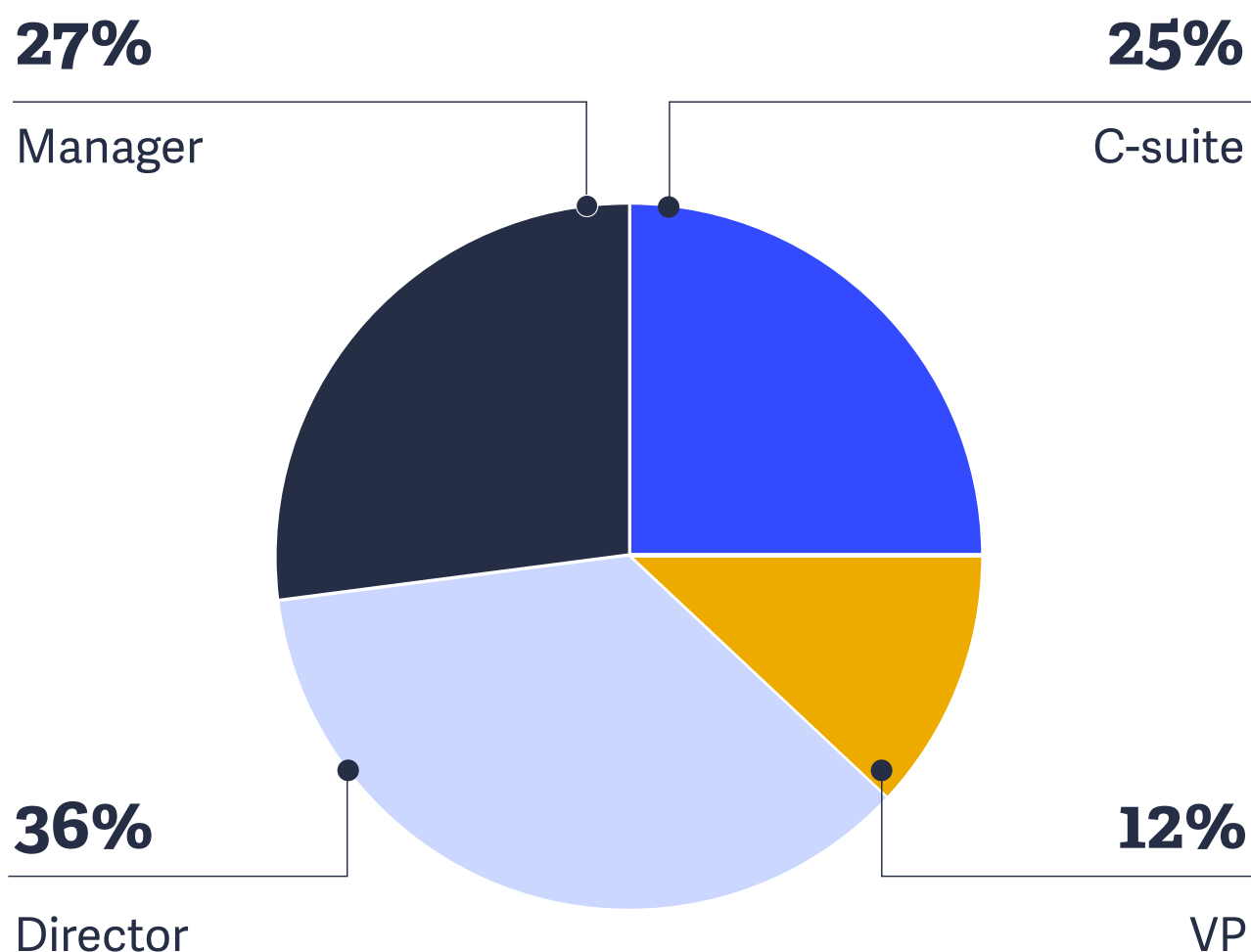
Survey Respondent Breakdown

Location

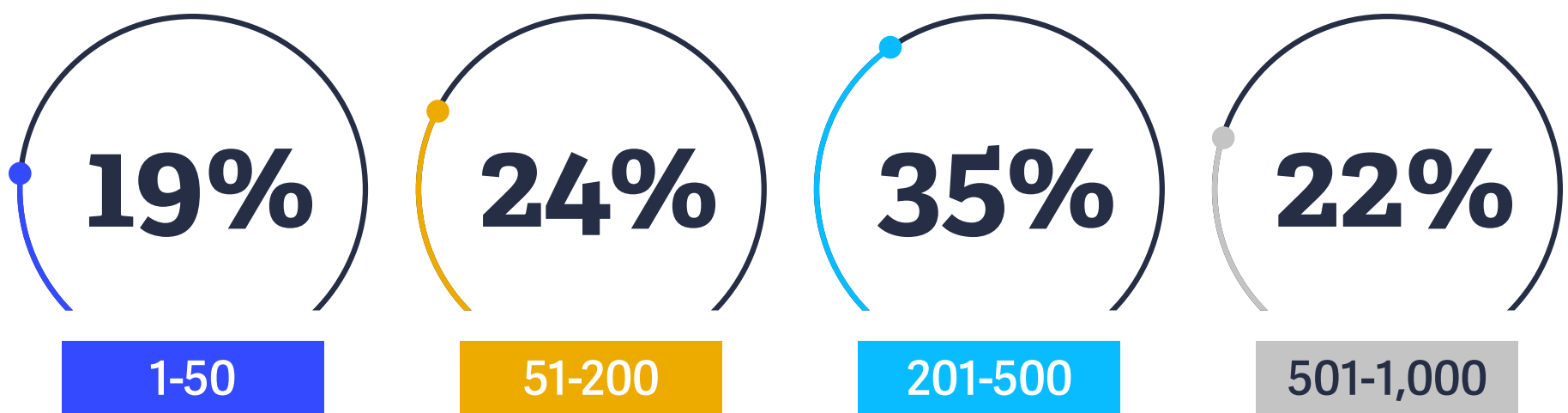


Eighty-six percent (**86%**) of people are from North America, while fourteen percent (**14%**) of people are from EMEA.

Titles



Company Size

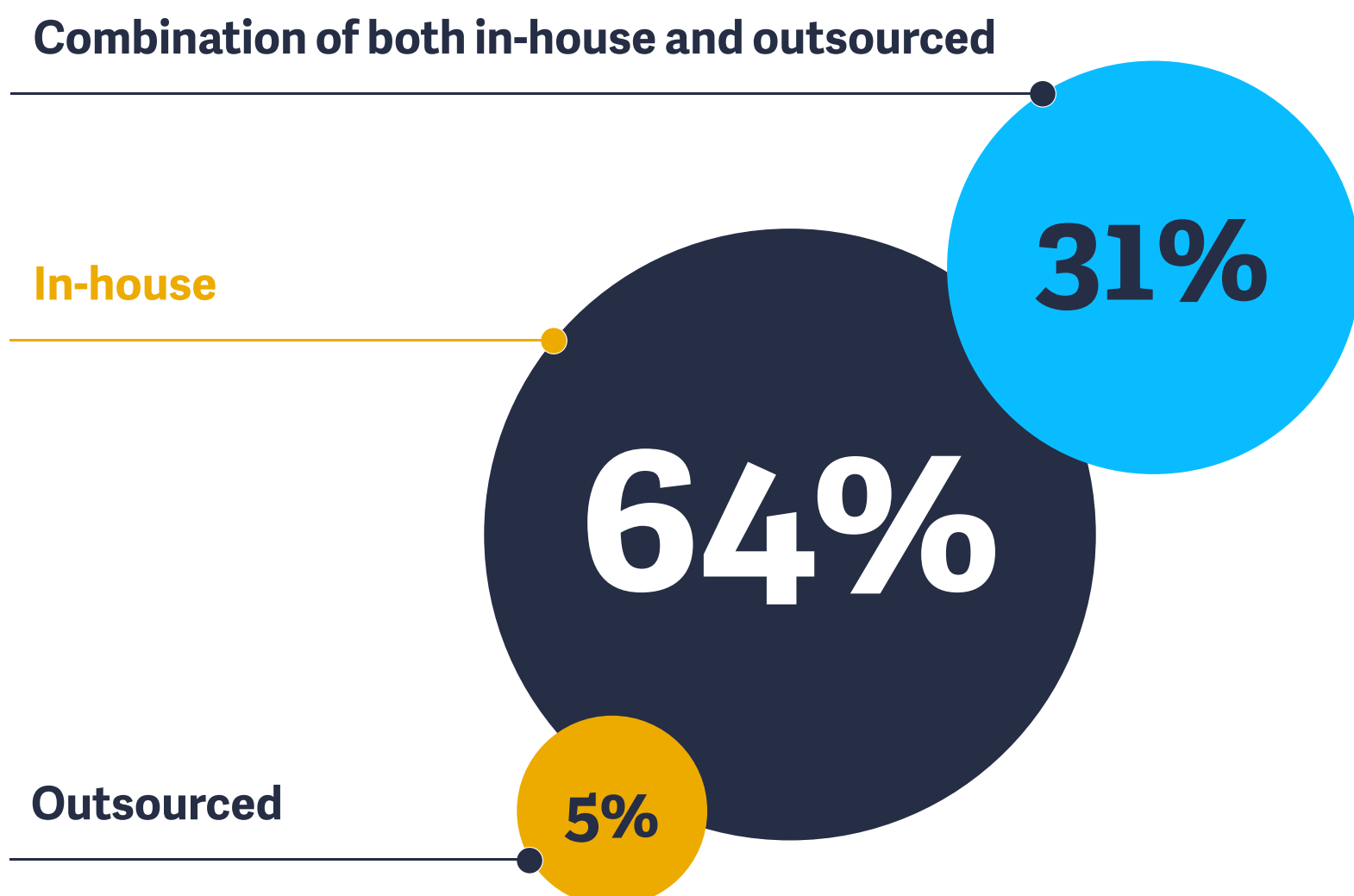


Outsourced vs. In-house IT management

IT management is a big job. Not only do IT managers have to scope out the best hardware, software, and security solutions for their business, but they also have to troubleshoot issues, manage licences, and (often) act as the sole expert on anything technology-related.

Given how demanding the role is—and how essential a well-run IT system is to growing a healthy company—it may surprise you that so many companies still have a house-run IT department.

Q: Is your IT staff in-house or outsourced?



Workplace security is priority number one

No matter where people are working, be it from home or on-site, workplace security remains a major concern. According to Patrick Kinsella, SVP Engineering and Chief Technology Officer at 1Path, this concern was only accelerated as most workplaces went remote in 2020—and for good reason.



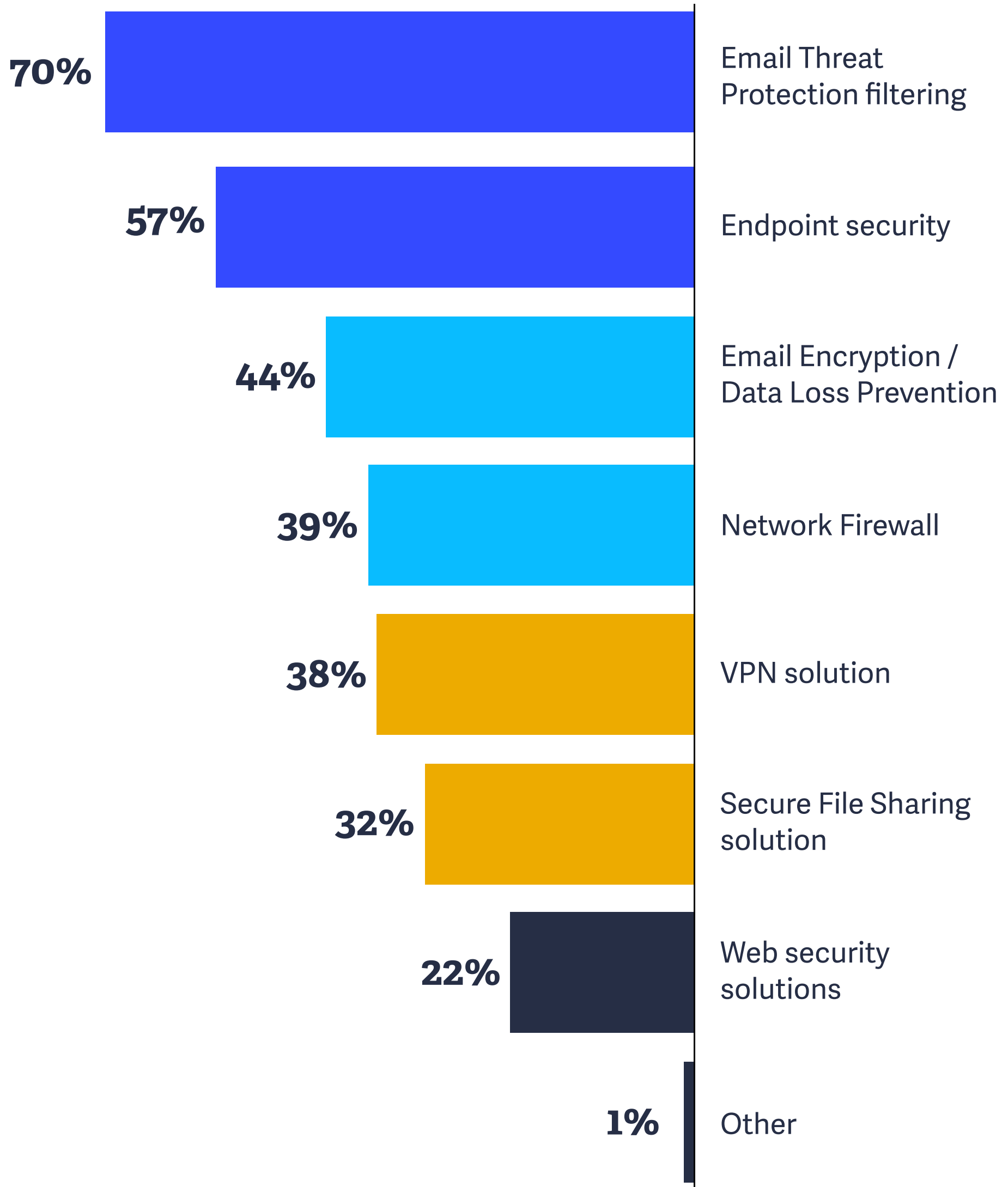
“The cybersecurity landscape changed very quickly,” he says. “With workers moving to uncontrolled networks, the number of fake phishing emails were on the rise as early as April of 2020.”

Without the proper security measures in place—and the right processes to ensure employees actually follow them—it can be difficult to trust that a company’s data will be kept safe.

When we asked our survey respondents which solutions they viewed as most important to their overall workplace security, the feedback we received was very much in line with these concerns.

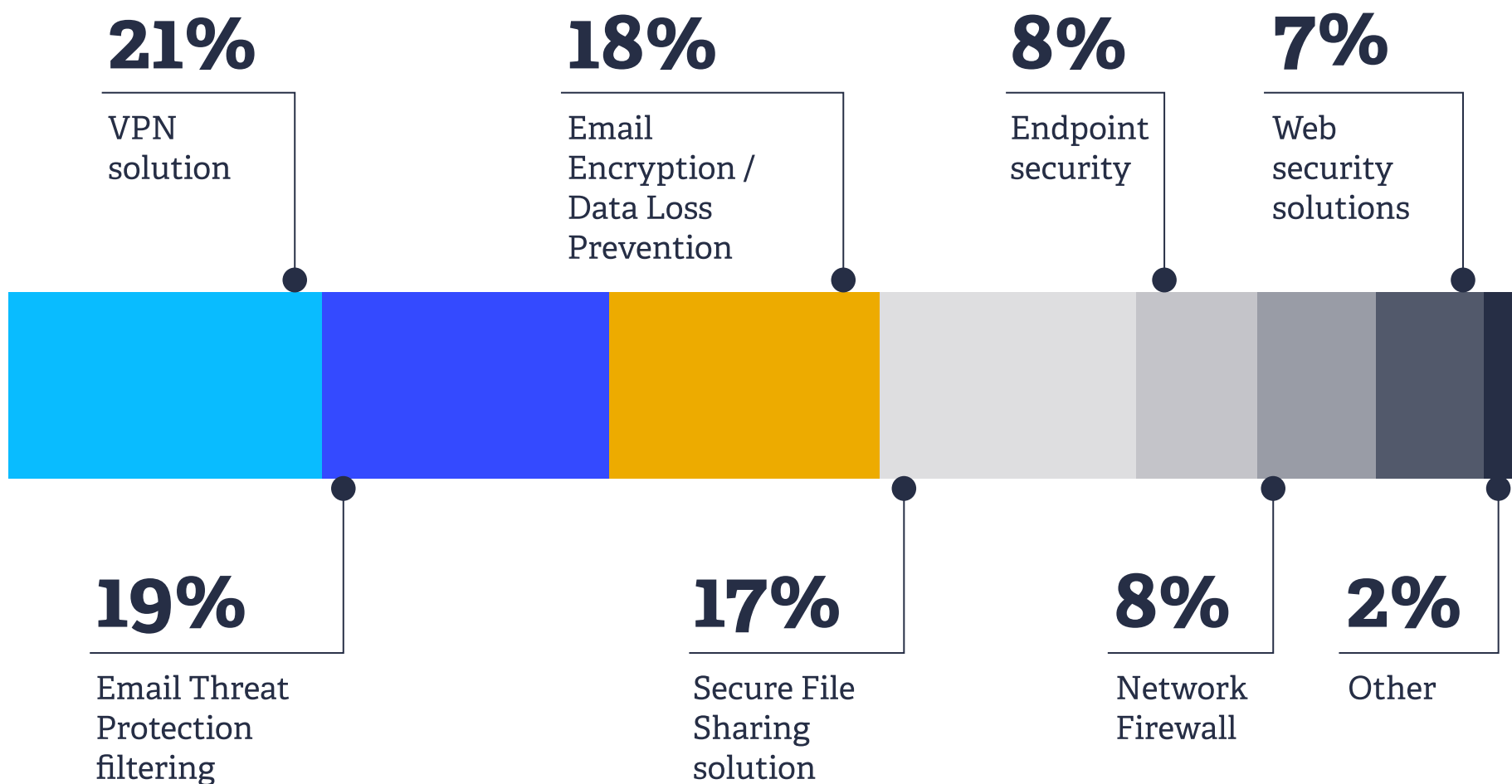


Q: Which solutions do you view as most important to your overall workplace security?



We also asked our survey respondents where they felt today's IT solutions are lacking. Perhaps it's no surprise that the very issues they felt were important were also the ones they wanted a better solution to address.

Q: Which of the following IT solutions do you have deployed that you are LEAST satisfied with?



These answers make a lot of sense: having a secure infrastructure in place to support remote work should be priority number one for today's workplaces. For those that have implemented these solutions but find them lacking—well, what then? How can you be sure anything is secure if the measures you have in place aren't cutting it?

Perhaps most interesting of all, **25% of survey respondents** that selected email encryption and data loss prevention solutions as most important to overall workplace security also reported that they're not satisfied with the solution they have deployed.



Case Study: When workplace security goes awry

As all IT leaders know, it's never a question of if you'll get hacked, but when. For Jamion Aden, IT Director and Director of Rural Health Clinics at Cozad Community Health System, it happened in the middle of the night.

Prior to the Cozad Community Health System being targeted by a ransomware attack, Jamion already knew the company's existing anti-virus spam filtering could be better.



We investigated what we had in place, and the virus definitions we were getting from those solutions weren't actually blocking Ryuk attacks. We had already started recommending to our leadership team that we get something more robust in place.

— **Jamion Aden, IT Director and Director of Rural Health Clinics at Cozad Community Health System**

Unfortunately, hackers beat them to the punch before Jamion could upgrade their anti-virus software, resulting in the aforementioned attack on Cozad Community Health System's servers.

While Jamion and his team had a well-planned course of action for such attacks, it still took some time to get things under control, and they didn't come out of the attack unscathed. After shutting down all 50 servers, blocking the sub-net, and using a VMWare environment to boot up each server one by one to investigate, **Jamion and his team found that 20 servers had been affected and would have to be rebuilt.**

As soon as everything was under control, Jamion made a case for switching to two new anti-virus protection providers, one of which uses AI to constantly update its virus definitions. He also implemented Zix for email spam filtering, as the Ryuk attack had been initiated through a phishing email. "Overall, we wanted to make it foolproof for our end users," says Jamion. "We didn't want anyone worrying about what they were clicking on, and we wanted people to feel assured and safe."

Since the upgrade, it's been smooth sailing for Jamion and his team. "We've had zero issues so far," he says. And though they have the advantage of AI, keeping safe is also a matter of staying informed. "We're constantly looking for what the next ransomware is going to be," says Jamion. "We also rely on third-party companies to investigate that for us. **Zix does a great job of making sure the rules and definitions are up to date, and it catches a ton of stuff that we wouldn't have caught on our own.**"

Overall, this experience was a hard-won lesson for Jamion. Though his team works hard to keep the Cozad Community Health System network safe, there's only so much a person can do to protect a company against security threats.

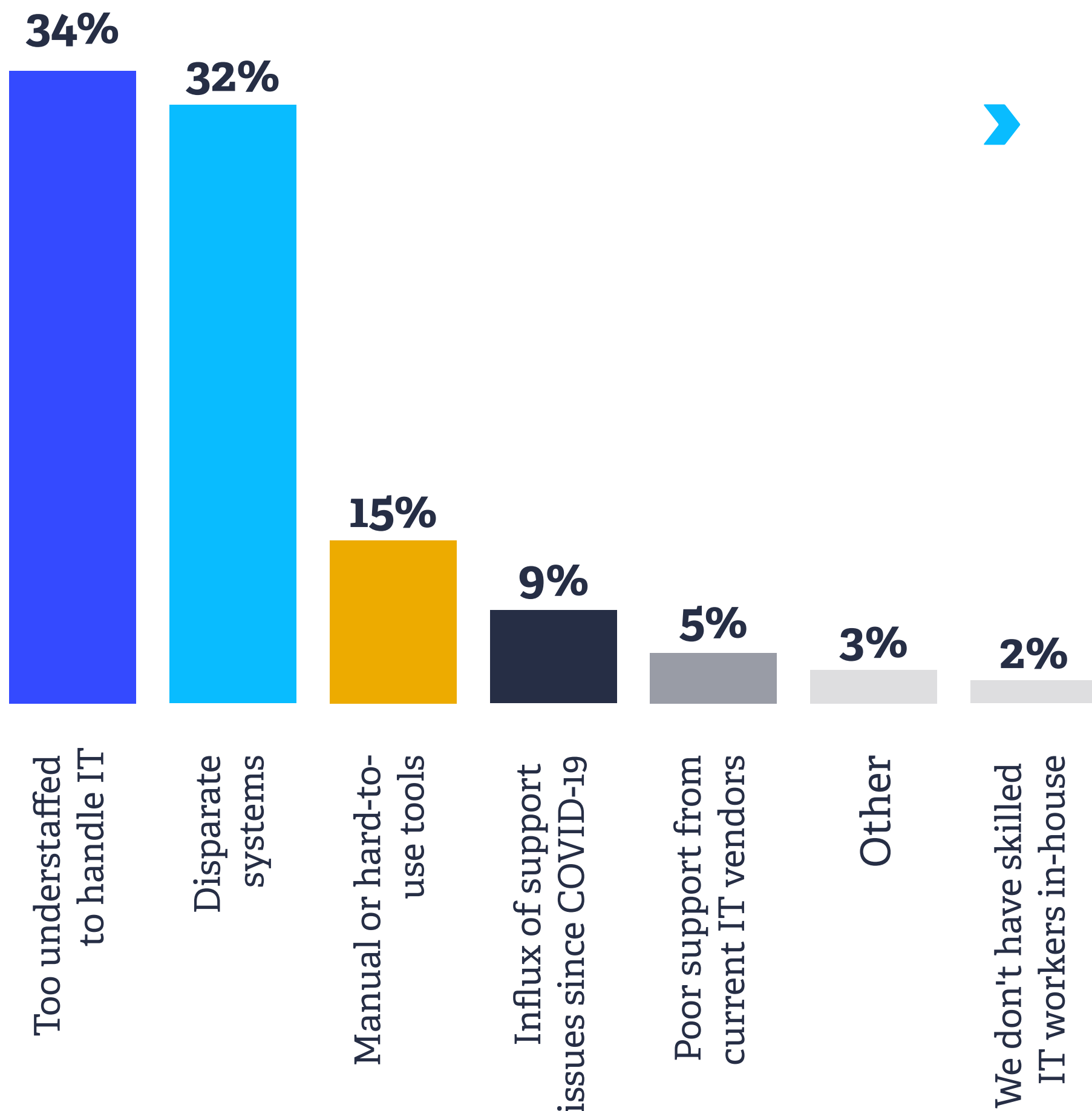
The real protection comes from having the right solutions in place that sensitivity of the company and the information it houses.



The top IT challenges of 2021

While it's true that many are opting to manage their IT in-house, that doesn't necessarily mean it's going well. In fact, **34%** of respondents reported that their biggest challenge to productivity was that they were too understaffed to manage IT well. Another **32%** reported that disparate systems were contributing to their productivity challenges.

Q: What is the biggest productivity challenge you face today?



Interestingly, for respondents whose IT is completely outsourced, **only 1 in 5 of them said they experienced the challenge of understaffed IT**, and they also completely avoided the challenge of not having skilled IT workers in-house.

We also asked our respondents to rank the complexity of a number of IT activities, in order from most to least complex. Here's what they said:

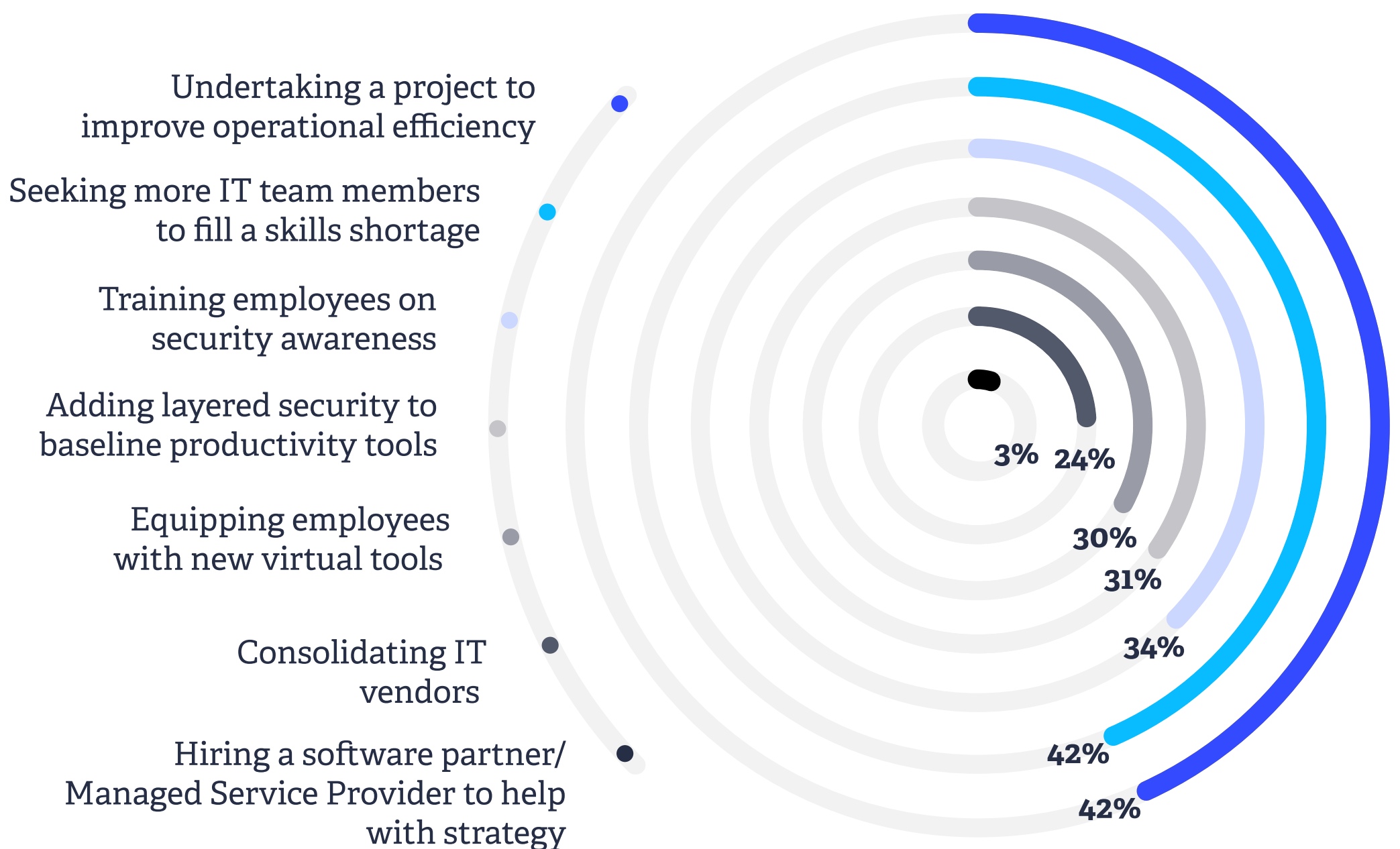
Q: Rank the level of complexity from most to least complex involved in managing and governing each of the following:



Understanding the IT challenges today's businesses are facing is one thing. **How they plan to address these challenges is another.**

Most survey respondents' action plans are focused on improving operational efficiency (42%) or looking to hire more IT team members to make up for the current skills shortage they're experiencing (42%).

Q: What is the company focusing on to improve IT team productivity?




From the experts: IT is an investment, not a line item

Talk to any expert in the MSP world and they'll tell you something similar: seeing IT as a cost center—rather than an investment—will only make it harder to overcome the challenges your business is facing.

And the challenges are plentiful enough as it is. For Eric Marcus, founder of Marcus Networking, he realized just how challenging IT management could be while working as an IT Director. "I was working with a cabling company, a phone system company, router providers... I basically had to have someone for each of the 10 things I needed," he says.

He found it difficult to rely on so many disparate providers and services just to do his job, and he also found that there was an uncomfortable tendency for each of his vendors to blame "the other guys" when something wasn't working. **"It became a blame game,"** he says. "The cabling company would say, 'Hey, it's not our cabling that's the problem, it's the phone,' and the phone guy would come out and say, 'The cabling's the problem.'"

Eric's wish as a client was one that he came to fulfill on his own when he founded Marcus Networking: **to have a place where all IT services would be provided in a streamlined way, under one roof.**

While Marcus Networking, and other MSPs like it, have found a huge amount of success in providing clients with a holistic, full-service IT management solution, there tends to still be reticence among some businesses that are struggling with their IT management and are looking for a way to simplify things. 

The problem arises when businesses fail to see IT services as an opportunity for future growth. As Patrick Kinsella of 1Path tells it, "IT is not simply a line item or something that can be cut. Our best customers are organizations that view **IT as a utility and as a resource.**"

Warren Finkel, founder of ACE-IT Solutions, echoes a similar sentiment. "A big part of what we do is helping people understand risk, and that productivity in their business means operational efficiency with IT and cyber. We can't work with clients who refuse to acknowledge that they could be hacked, or don't see the importance in upgrading their software."

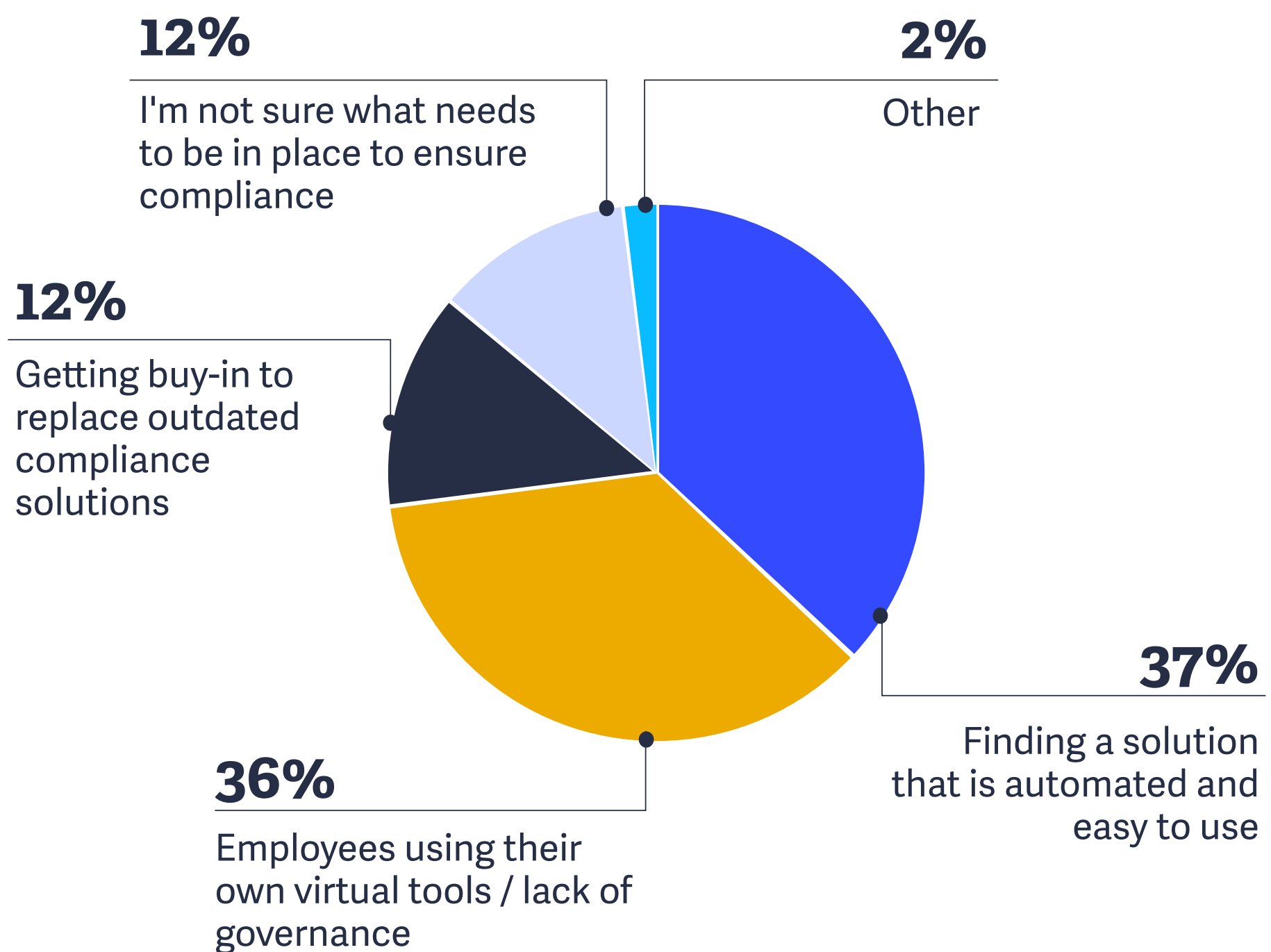
The key takeaway here is that for businesses struggling with IT management, **it may be time for a shift in perspective.** Having IT infrastructure that's secure, well-run, and streamlined is a serious undertaking, and much of the time, requires a strategic partnership in order to roll out at scale. Seeing it as something to invest in, rather than a problem you may never outrun, is a way to reframe challenges as opportunities.

Employee compliance is a major concern

While most security concerns have increased as workplaces go remote, one stands out as especially pressing: maintaining compliance. How can you ensure that everyone's using the systems they should be using to keep your data safe?

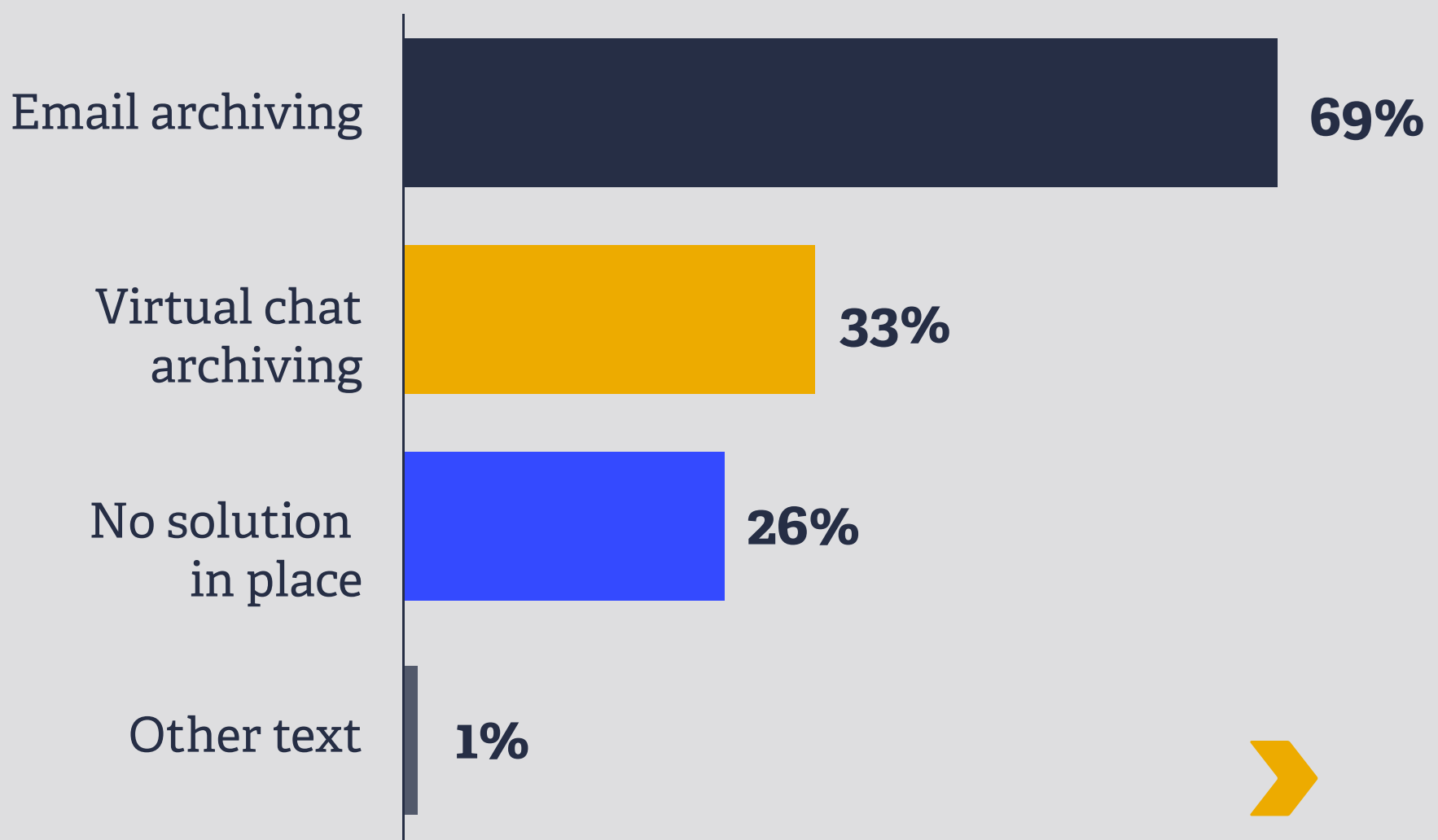
Two issues stood out with our respondents when reporting their biggest challenges in maintaining compliance virtually: finding a solution that is automated and easy to use (37%), and employees using their own virtual tools with a lack of governance (36%).

Q: What is the biggest challenge you face in maintaining compliance with a virtual workforce?



And while the majority (**69%**) of organizations have an email archiving solution in place for compliant communication retention, **26%** have no solution in place at all.

Q: What is the biggest challenge you face in maintaining compliance with a virtual workforce?



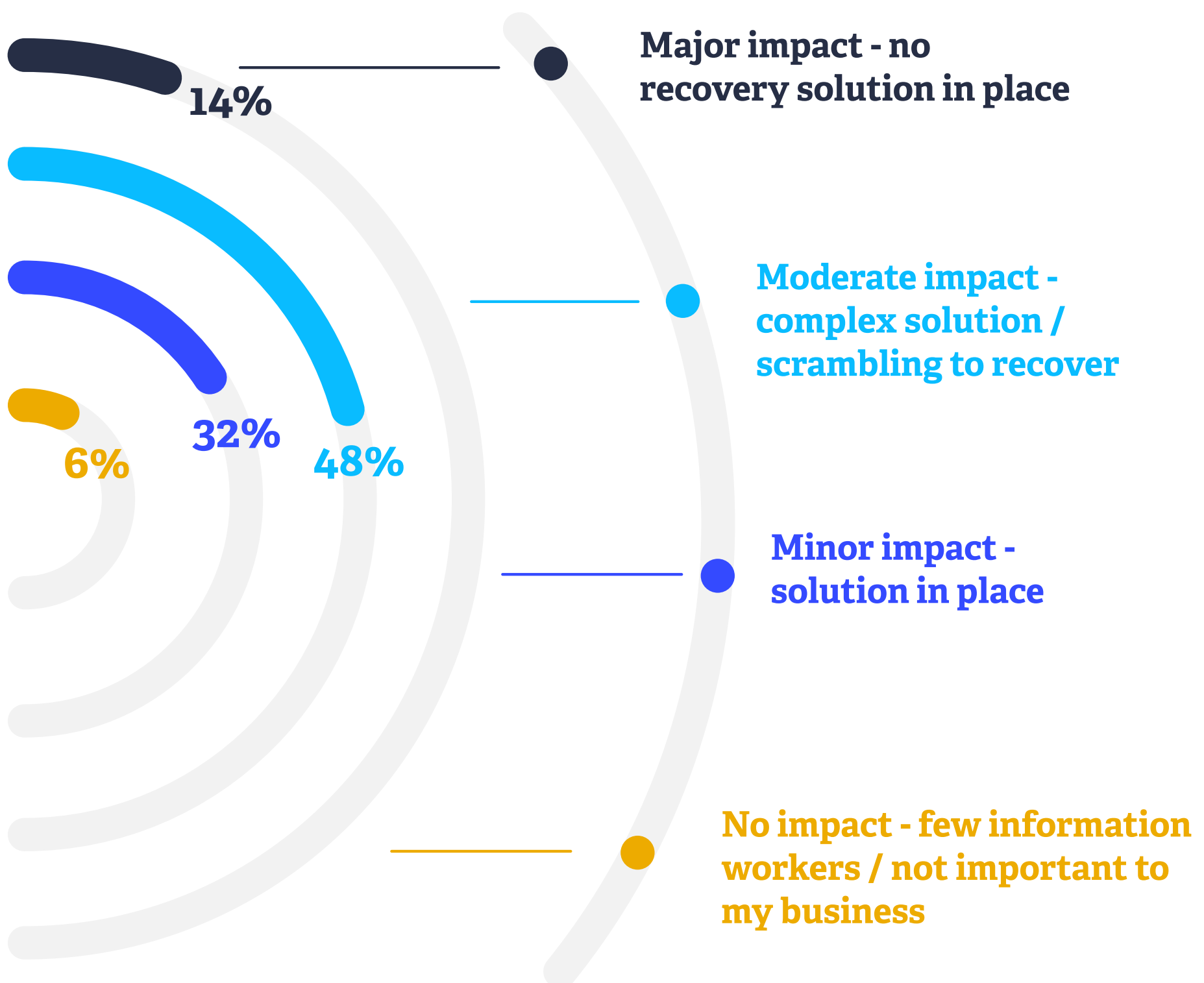
42%

We also found that **42% of respondents** are only archiving email communications, without a solution for archiving other virtual communications through apps like Zoom and Microsoft teams.

What happens when data is lost?

It's every IT manager's worst nightmare: losing data you can't recover. No one wants to be at fault when a system failure or security breach compromises company information. Almost two-thirds of our respondents (**62%**) said that a data loss event would have a moderate to major impact on their business because of lack of recovery solutions or complexity of recovery.

Q: If your cloud solutions (ex. Salesforce, Dropbox, Microsoft) experienced data loss today, how much of an impact would that have on your workforce?



Regardless of the potential for catastrophe, data loss is something that happens. Only **34% of respondents** reported that they'd be able to very quickly recover records in the event of a data loss, while a further **9%** said they wouldn't be able to recover them at all.

Q: If you experienced data loss with one of your cloud solutions (ex. Salesforce, Dropbox, Microsoft), how quickly would you be able to recover your records?



Case Study: How Cozad Community Health System Dealt with Data Loss

Let's revisit Jamion's story from earlier in this report. As you may recall, his workplace was targeted by a ransomware attack in the middle of the night, which infected the system through a phishing scam.

Jamion and his team were notified very quickly after the attack took place. **Within 15 minutes**, a nurse alerted one of Jamion's team members that a printer was down, which was the tipoff that something was wrong.

Jamion and his team moved quickly, shutting down all the servers and then booting them up one by one using VMWare to assess any damage done. The biggest concern was protecting patient data, but thankfully, the company's electronic medical record system is housed offline, outside of the network.

While patient data was safe, Cozad Community Health System wasn't completely out of woods. Of the 20 servers that were affected and had to be rebuilt, one of them lost three months' worth of data that was ultimately unrecoverable.

While things certainly could have been worse, there was a hard-won lesson for Jamion to learn: **"You should always have a backup plan in place,"** he says. "And a backup plan to backup plan." This means regularly checking that your backup solutions are working and that you also have offsite backups in place. "You can never have too many," says Jamion.



Advice from the front lines

Even with the best laid plans and the strongest and most secure systems in place, **things go sideways in the IT world all the time**. We've gathered feedback from our survey respondents on the top three pieces of advice they can offer to other IT professionals.

01

Find a trusted partner

Many respondents said that finding a single- vendor MSP provider helped them immensely.

02

Finding the right solution takes work

You won't arrive at the perfect solution with one try, but with patience, documented processes and some testing exercises, you'll find one that works for you over time.

03

Security is the goal

"Secure the endpoint". No one wants to deal with lost data. Whatever solution you choose, the goal should always be to prioritize security.

Modern workplaces have changed for good, but with the right tools, today's teams can adapt

Changes to security threats, compliance concerns, and a distributed workforce have all contributed to a higher-risk environment for IT professionals to adapt to.

While there are more challenges than ever, **there are also more solutions available** to help streamline, secure, and strengthen workplaces against the biggest and most prevalent problems facing today's team.

One thing is clear: staying informed and finding the right help when you need it can help you go far in bringing your business into the future.

zix[®]

appriver[®]

 **PULSE**