eBook

jumpcloud™

IT Evolution: How IT Is Securing the Next Stage of SME Workplace Models

Despite a rise in security concerns and uncertainty around world events, 2022 finds SME IT managers committed to making work secure, simple, and easy for end users

Executive Summary

Now two years since the advent of the COVID-19 pandemic, businesses are still wrestling with the demands of dynamic workplace models while also having to address a number of internal challenges and uncertainty wrought by world events. Yet over the last year, in spite of supply chain disruptions, global conflicts, market concerns, rising security risks, and more, small and mid-sized enterprises (SMEs) continue to drive economic growth.

Key to this critical business sector are the professionals who, often without fanfare, provide and manage the IT backbone that powers SME operations. These IT professionals don't have enterprise-level budgets or enterprise-level staff, but they do shoulder the same heavy responsibilities of securing employees and making work work. In addition to dealing with real and potential disruption stemming from external events, these professionals are also juggling complex device environments, managing complicated tech stacks, and facing increasingly sophisticated and varied security threats from multiple directions.

Thirty years ago, IT teams could sit in an office and offer "turn it off and back on" as a solution for a majority of issues. Today's IT teams have a much larger portfolio of responsibility ranging from individual devices to the aftershock of global events: 40.5% of SMEs say their organization has been impacted by the war in Ukraine, 59.4% report their biggest challenge is security, 47.8% report migrating users to hybrid work continues to be a major challenge, and 70.4% are concerned about inflation.

Despite the burden, today's IT professionals are shouldering these responsibilities and preparing for what's next. Our most recent edition of the SME IT Trends report reveals that today's SMEs are being served by committed and disciplined professionals dedicated to keeping employees productive and secure. And they're happier than before.

Because of IT admins' vital function and unquestionable value to the SMEs in which they work, JumpCloud commissions this ongoing research to gain essential insight into their day-to-day challenges, opportunities, and experiences.

This Q2 2022 edition reveals:

- The complex landscape of responsibilities and solutions required to secure and enable hybrid work models
- How teams are adapting in a time of rising security threats
- What the new reality of hybrid work requires to protect user identity everywhere
- The contingencies IT teams are planning for in face of the known unknown
- The technologies and best practices teams are advocating for within their organization

Beyond the uncertainty and fear, the survey finds IT teams have both seen and driven significant growth. IT budgets increased and are expected to continue to grow; teams are making impressive headway with respect to security initiatives; and IT professionals feel happier in their jobs.

2022 finds SMEs responding to modern challenges with agility and grit — and their IT teams boldly accepting the responsibility with incredible dedication and extraordinary resiliency.

The State of the Workplace

Adjusting to the Long Term

Spring 2022 finds SMEs settling into a new workplace mode with more employees in the office and fewer hybrid workers. Now, nearly half of workers (47.1%) are working in-person, a 17% increase from spring 2021. Currently, 24.8% of SME workers are fully remote, and 32.5% are hybrid, a 24% decrease from one year ago.

What is the percentage breakdown of employees working in the office full time/working hybrid/working remotely full time?

APRIL 2022

Item	Average	Standard Deviation	Sum	Total Responses
Office full time	47.1	28.6	45,919	974
Working hybrid	32.5	24.2	31,157	958
Remote full time	24.8	23.4	23,226	938

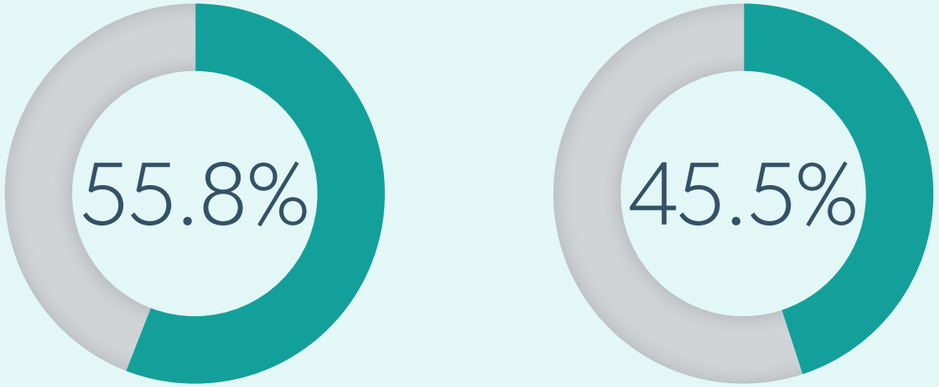
APRIL 2021

Item	Average	Standard Deviation	Sum	Total Responses
Office full time	40.1	25.8	10,540	263
Hybrid: More than 50% of time spent at office	23.7	14.5	6,005	253
Hybrid: Less than 50% of time spent at office	18.8	13.4	4,747	253
Remote full time	22.6	22.7	5,608	248

The State of the Workplace: Managing Remote Work

Managing in-person, fully remote, or hybrid workforces has become less difficult as SME IT admins have been honing their IT skills. Last April, 55.8% of SME IT professionals said the ongoing management of remote work had been one of their biggest challenges, while only 45.5% found it to be a challenge this year.

Remote work was a top challenge last year

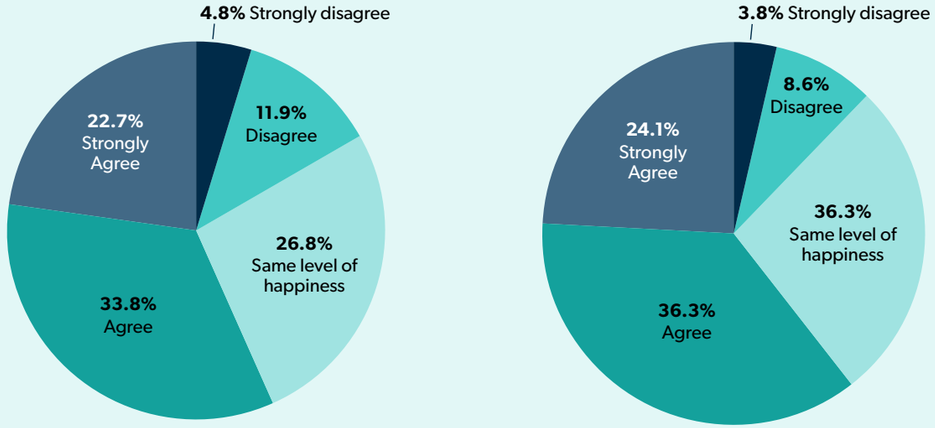


APRIL 2021 APRIL 2022

Business Outlook

IT Professionals Are Happier Despite Increased Stress

"I am happier in my job than I was a year ago."

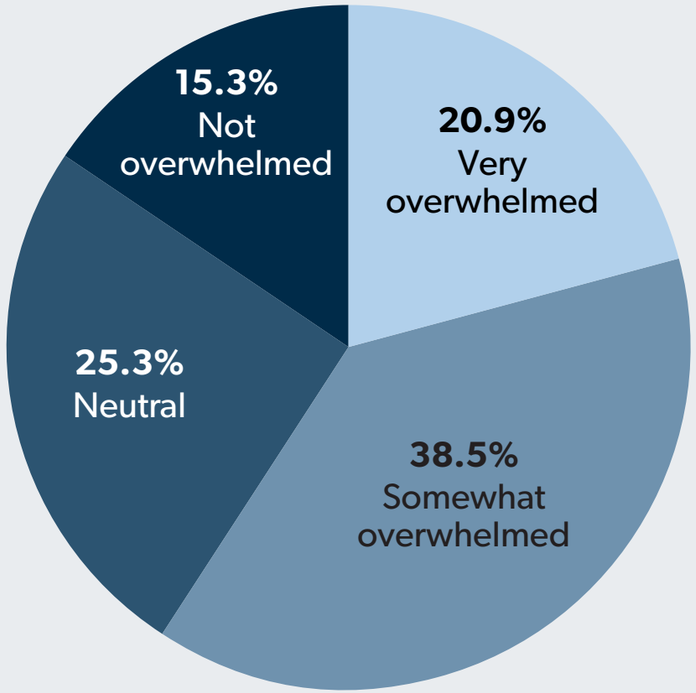


APRIL 2021 APRIL 2022

The State of the Workplace
Managing Remote Work

As SMEs have achieved stability in their workplace models, their IT professionals reported higher happiness levels: 60.4% reported being happier in their job than a year ago versus 56.5% reporting the same in 2021. However, they're still feeling the stress: nearly three-fifths (59.4%) reported feeling overwhelmed in relation to their job and responsibilities.

In terms of my job responsibilities and expectations, I am…



APRIL 2022

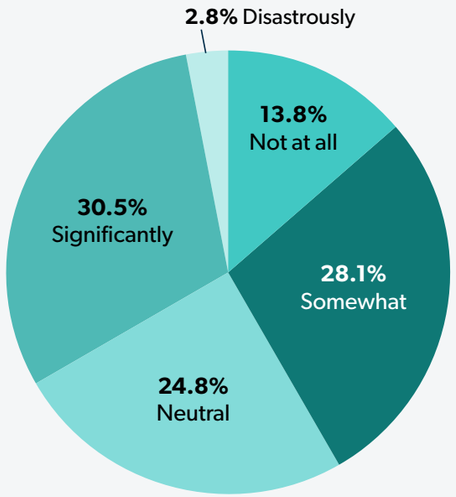
SME Business Outlook

Preparing for Uncertainty

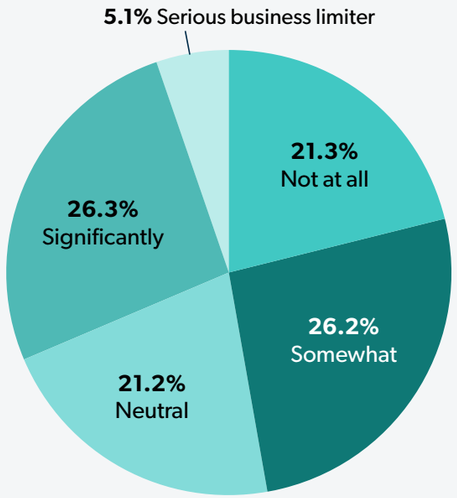
Despite having successfully transitioned to new work models, many SMEs expect turbulent times due both to external and internal system shocks. Sixty-one percent of respondents reported that supply chain disruptions or product shortages have hurt their business, and 57.6% said labor shortages have been an issue for their business.

Broader economic concerns loom. About a quarter (26.2%) of SMEs are actively doing recession planning, and 57.4% are either considering recession planning or think it's a good idea. Similarly, the majority (70.5%) of respondents expressed at least some concern around inflation, with only 5.1% reporting that inflation isn't a worry.

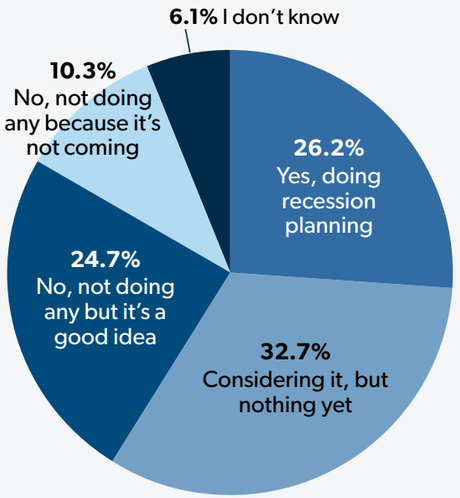
Have supply chain disruptions and/or product shortages hurt your business?



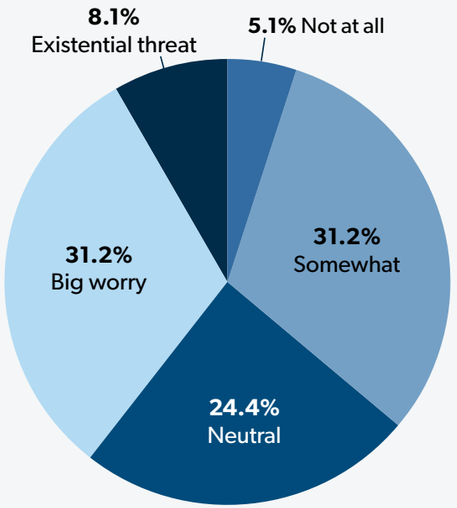
Have labor shortages been an issue for your business?



Are you doing recession planning?



How big a worry for your business is inflation?



Fortunately, SMEs are preparing to meet these challenges directly. Unlike the start of the pandemic, when businesses were ill-prepared and in survival mode, today's SMEs are in a position to plan and allocate resources to best weather whatever comes. For many, this means investing heavily in IT.

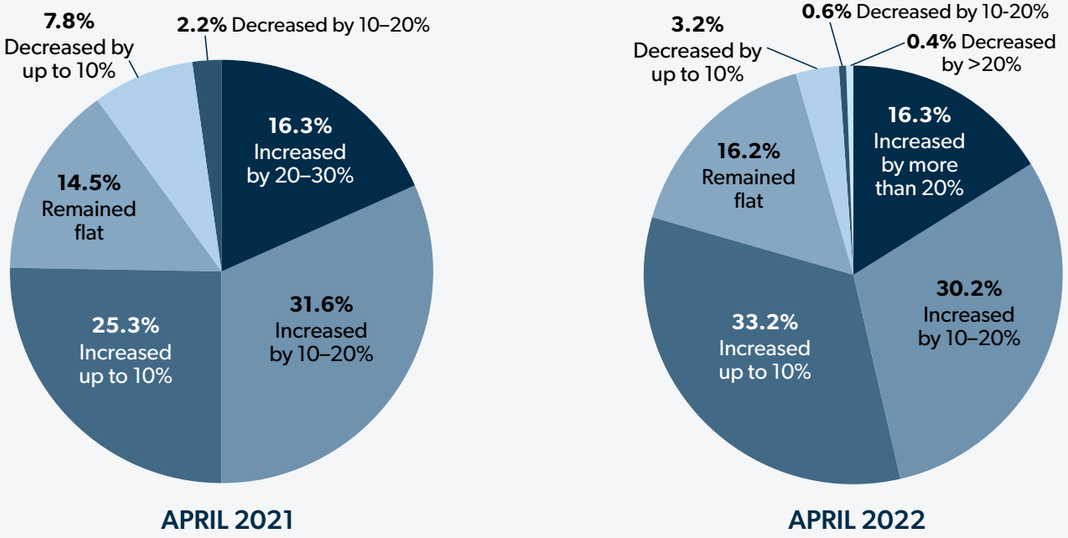
SME Business Outlook

Budgets Reflect IT's Value

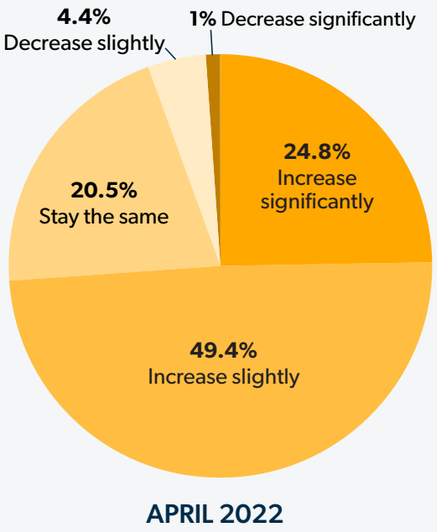
While the future may look uncertain for SMEs, the majority maintain a clear commitment to investing in IT. Nearly three-fourths of all surveyed IT professionals expect their budget to increase (74.2%) over the coming year, and only 5.4% expect to experience a budget decrease.

This uptick in IT investment aligns with what has been a spending trend since the beginning of the pandemic. SMEs have seen significant budget increases since 2020 — over three-fourths (79.2%) of surveyed admins saw IT budget increases in the last year, and 75.5% of surveyed admins reported they had seen an increase between 2020 and 2021, despite pandemic-driven uncertainty and hardship.

Over the past year, my IT budget...



Over the next year I expect our IT budget to...



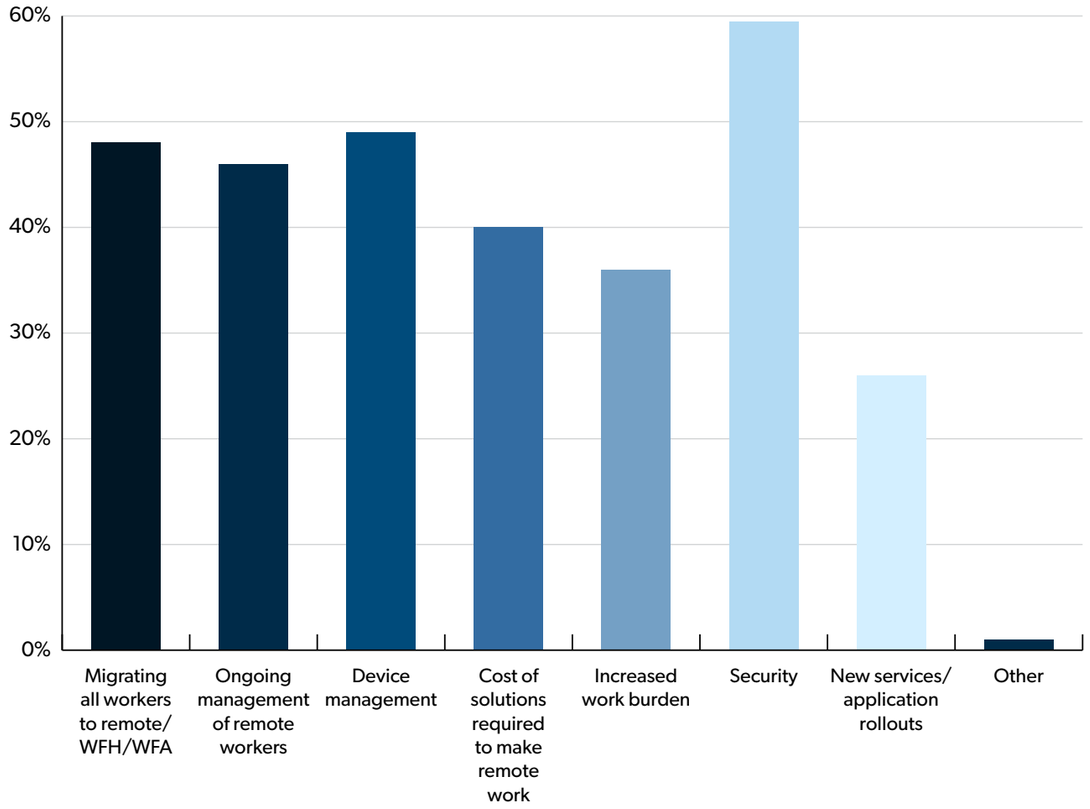
Because of COVID-19, IT teams established themselves as flexible, tenacious, and effective, keeping virtual doors open and lights on. IT professionals were the ones that shouldered the burden of instantaneous transition to remote work, and those same IT professionals have been ensuring employees can access what they need, every day. SMEs are turning to IT again in the face of a new set of impending challenges, and are equipping IT departments with the budget they need due to the trust they've earned.

Securing the SME

Security Is Top Concern

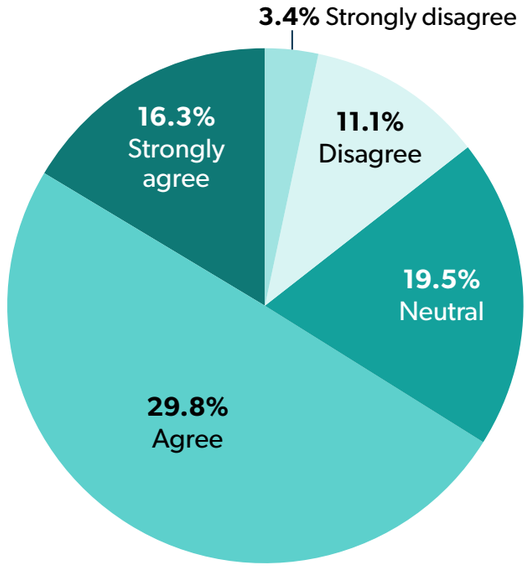
When SME IT admins were asked what their biggest challenge had been in the last year, security was the most popularly chosen answer (59.4%) and beat out all other challenges by at least 10 percentage points.

What have been the biggest challenges for your IT team since April 2021?



Despite innovation and technological advancements, a majority of IT professionals are vexed by introducing more robust security without impacting the user experience. About two-thirds (66.1%) agreed that adding security measures generally means a more cumbersome user experience — an increase from 58.1% who said the same in 2021.

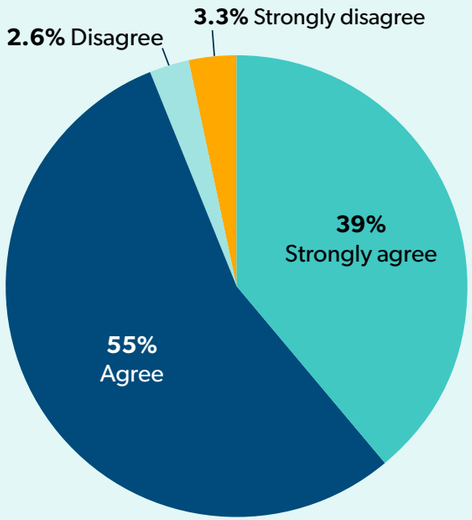
Additional security measures generally mean a more cumbersome user experience.



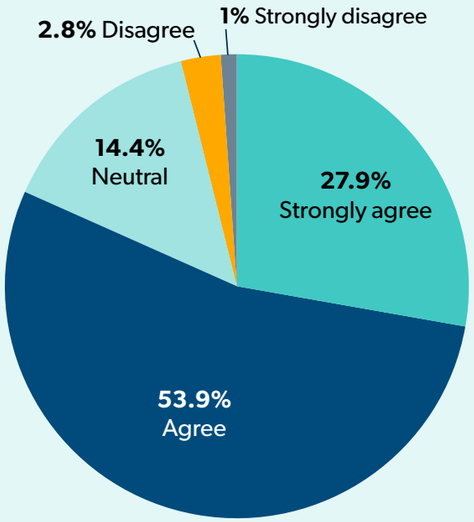
Security is a Top Concern

At the same time an increasing number of admins are reporting this challenge, the same IT professionals are rating user experience as less important in determining their purchasing decisions than last year (82% now versus 93% in April 2021). This slight deprioritization of the user experience makes sense when considering that admins rank security as their top priority by such a large margin.

I consider employee experience to be an important factor in making IT solutions purchasing decisions.



APRIL 2021

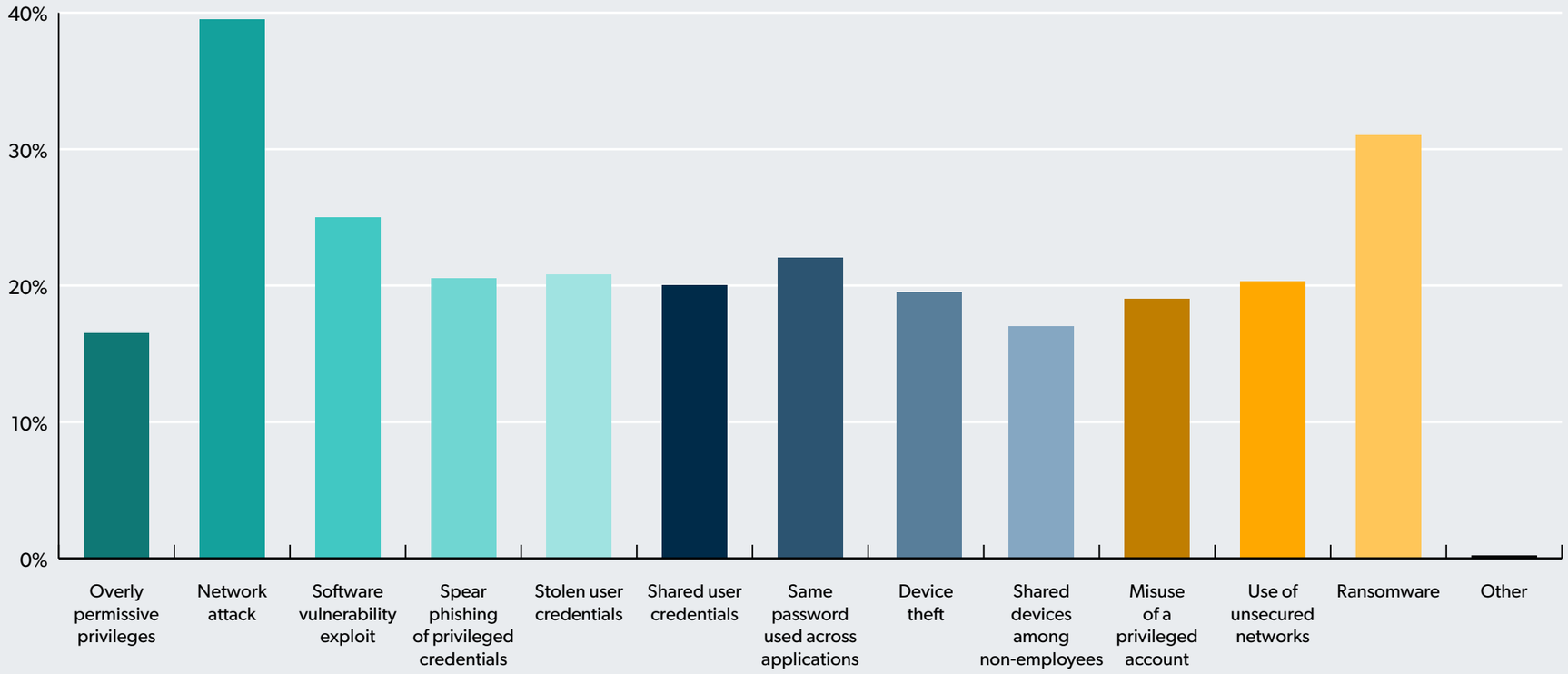


APRIL 2022

Securing the SME

External Threats Loom Large

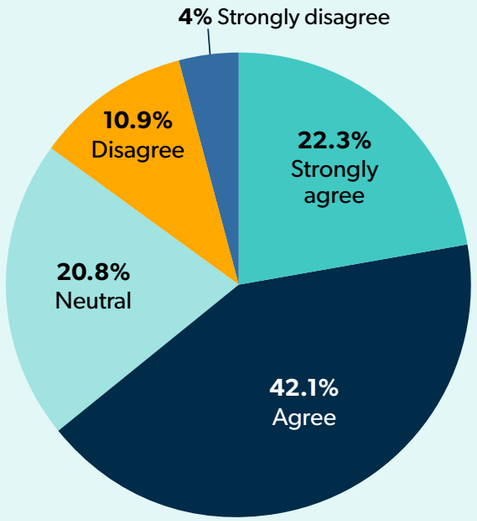
In terms of specific security concerns, outside threats are what keep IT professionals up at night. Their top concern was a network attack (37.9%), which beat out other options by almost 10 percentage points, followed next by ransomware (30.9%) and software vulnerability exploits (30.6%).



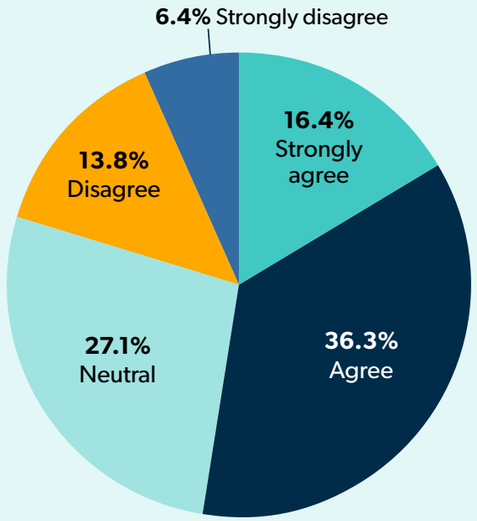
External Threats Loom Large

Adding to economic and security concerns is the issue of global unrest. The Russia-Ukraine war has impacted over a third (39.7%) of SMEs, and it has driven over half (58.6%) to increase their focus on security. This impact was amplified in the U.S.: 64.4% of U.S. respondents agreed the war has increased their organization's focus on security, versus 52.7% in the U.K.

The war in Ukraine has increased my organization's focus on security.



APRIL 2022: U.S. ONLY



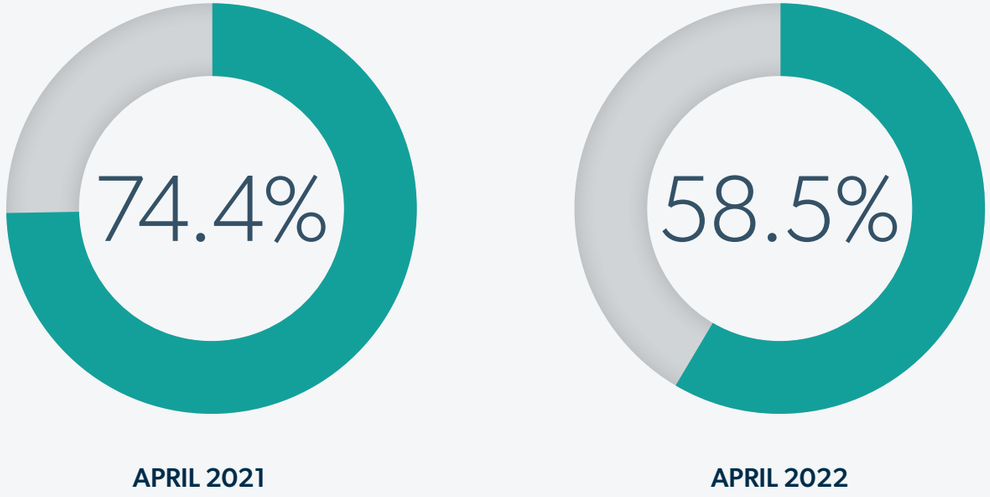
APRIL 2022: U.K. ONLY

Security and the SME

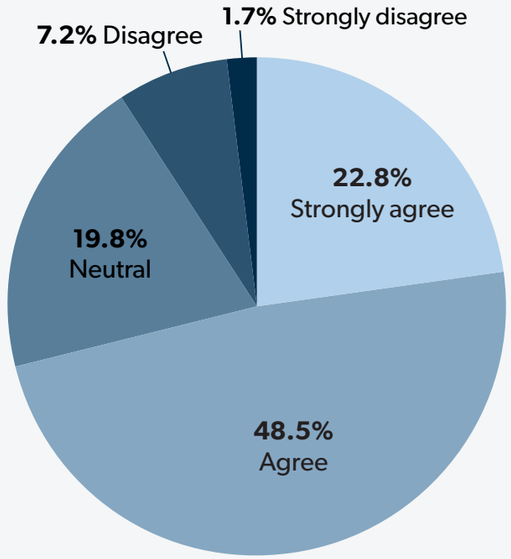
Employees Better at Managing Security

In 2021, many SME IT admins were skeptical about employees' security hygiene. Then, nearly three-quarters (74.4%) of respondents said remote work makes it harder for employees to follow good security practices. One year later, only 58.5% are eyeing their employees as warily (a 23% drop), and 71.3% of respondents also agreed that remote employees are better at following good security practices than they were a year ago. Two years of adjustment to a new hybrid model have given SMEs time to create and communicate company policy and best practices, and given employees time to adjust to new habits.

Remote work makes it harder for employees to follow good security practices



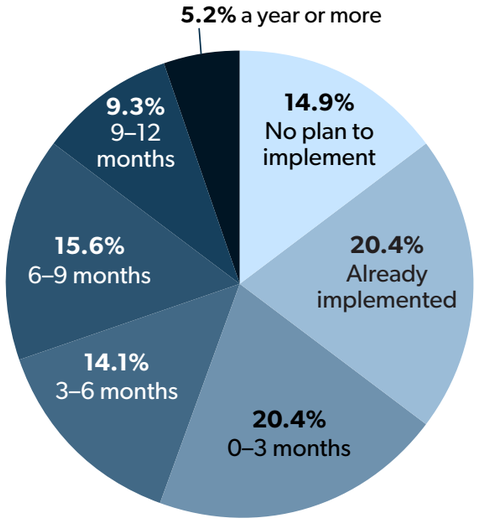
Our remote workers are better at following best security practices now than last year at this time



Single Sign-On Sees Explosive Growth

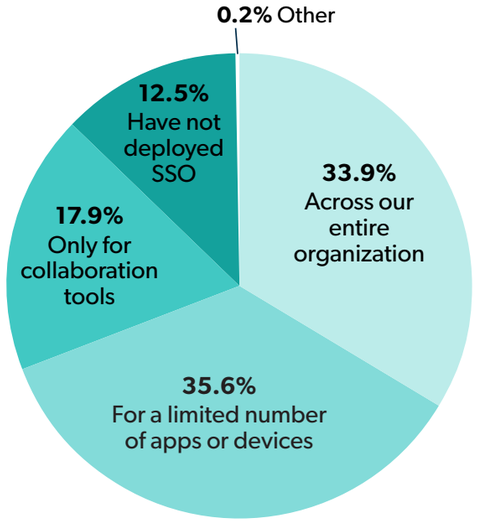
Now that workers can log on from anywhere, easy and centralized authentication has taken center stage. SMEs significantly increased their adoption of single sign-on (SSO): 87.4% of SMEs now use SSO for some applications or devices whereas only 20.4% had already implemented SSO in April of 2021.

How many months out before your company will likely implement single sign-on (SSO)?



APRIL 2021

We have deployed single sign-on (SSO)



APRIL 2022

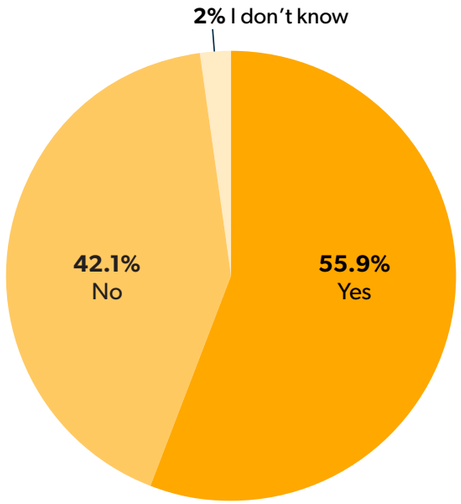
Such growth in SSO can be understood in terms of it simultaneously helping IT professionals manage the user lifecycle while also providing employees with a simpler, consolidated login process. As employees and IT admins confront a complicated ecosystem of necessary IT resources, the demand for SSO aligns with a need for layered security that doesn't add friction to the user experience.

Securing the SME

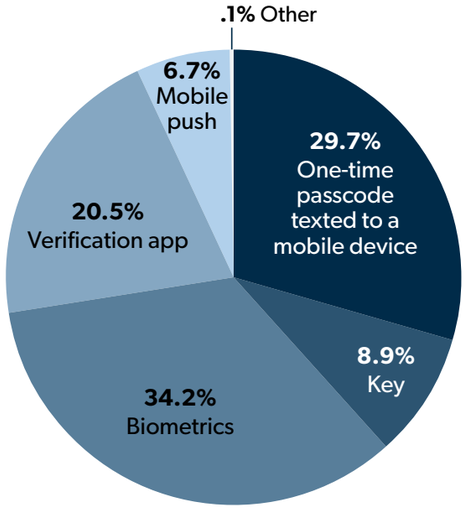
Biometrics Surge

This past year also saw a surge in biometric authentication adoption. Over half (55.9%) of SMEs surveyed currently require biometrics for authentication, a 150% increase from the number who had reported having implemented biometrics in April 2021. When asked what they thought was the most secure authentication factor, biometrics came in a clear first (34.2%) despite admins also reporting they saw it as the hardest to implement.

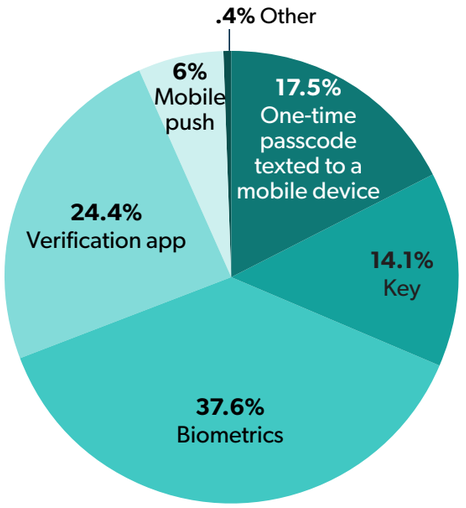
Does your organization require the use of biometrics for employee authentication?



The most secure step for multi-factor authentication (MFA) is:



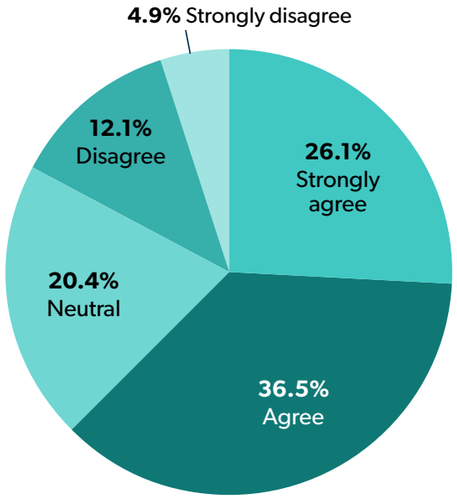
The most complicated MFA to integrate for IT admins is:



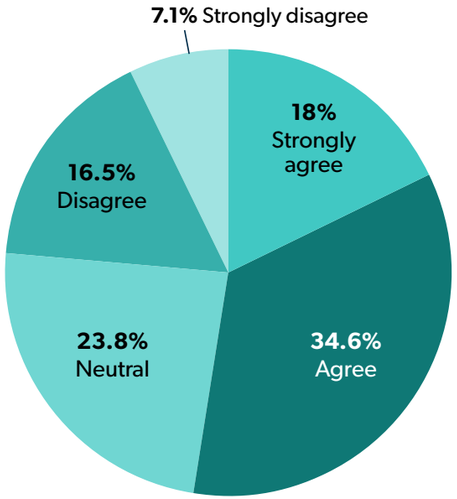
Passwordless Authentication and Central Access Management

While biometrics can greatly reduce friction in the user authentication experience, the issue of passwordless authentication highlighted some perspective differences between SMEs and the practitioners tasked with managing identity. When asked if passwordless authentication is a priority for their company, nearly two-thirds (62.6%) agreed, and in fact, only 17% disagreed. But when the admins were asked whether they agree that passwordless is more of an industry buzzword than an IT priority, 52.6% of respondents agreed.

Passwordless authentication is a priority for our company

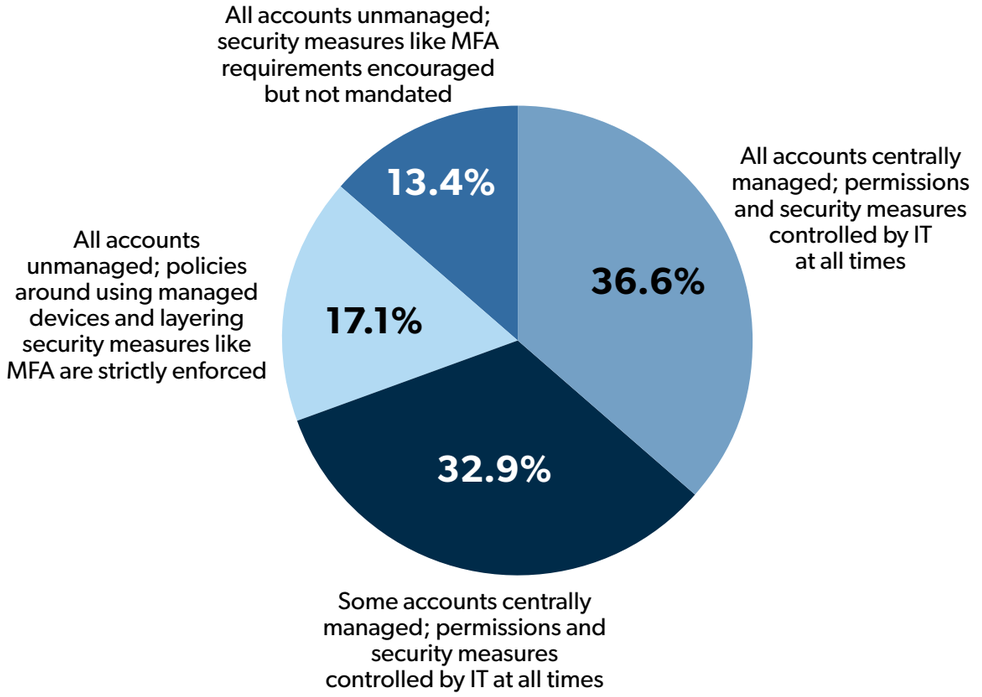


Passwordless authentication is more of an industry buzzword than an IT priority



Despite distributed workforces, IT teams most commonly retain full security control over user access. Over a third (36.6%) of respondents said employees' account access is centrally managed with permissions and security measures controlled by IT at all times, and another third (32.9%) said some accounts are centrally managed, with permissions and security measures controlled by IT wherever possible.

How easy is it for your employees to access what they need?



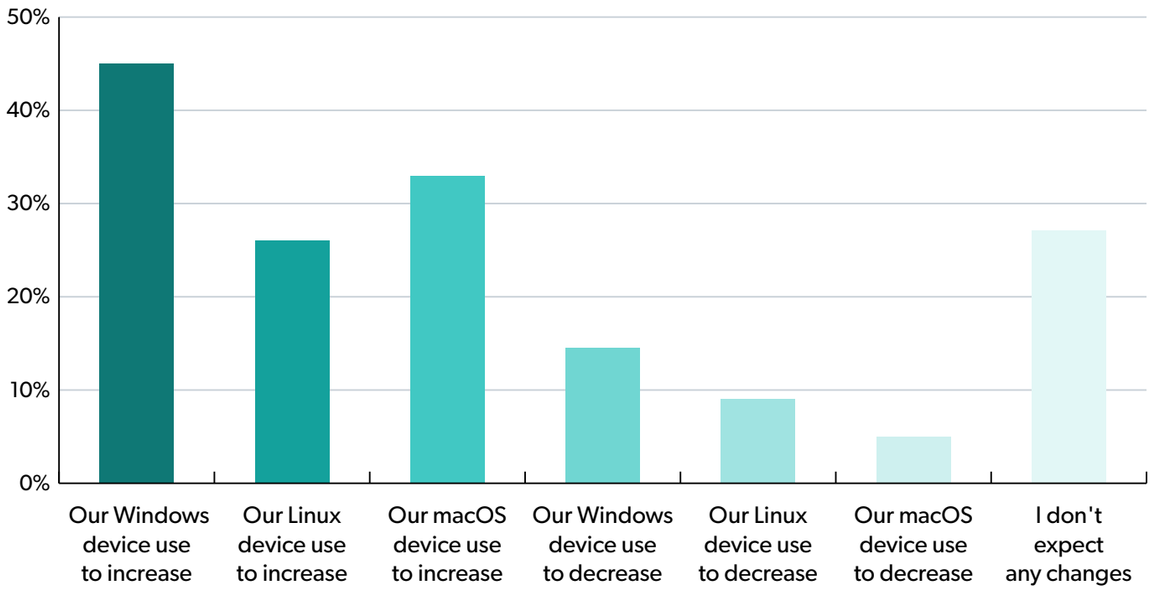
Complex Device Environment

Device Diversity Is Growing

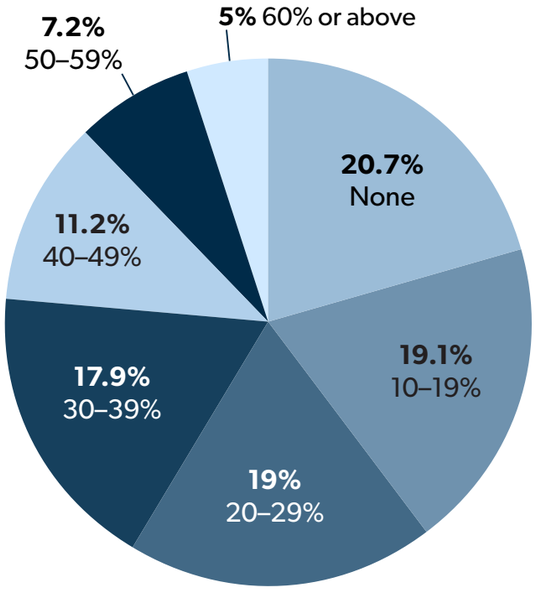
Far from the days of Windows-dominated domains, today's SMEs operate using a variety of devices and operating systems. IT professionals expect to see an increase in Windows, macOS, and Linux use over the next year, as SMEs maintain flexibility to ensure employees have access to whatever device they need to do their work.

In addition, the majority (79.4%) of respondents said that at least some employees at their organization use their personal devices for work purposes. Personal devices can introduce unnecessary risk to an SME if the organization hasn't established device trust or application and access permissions.

Over the next year, I expect...



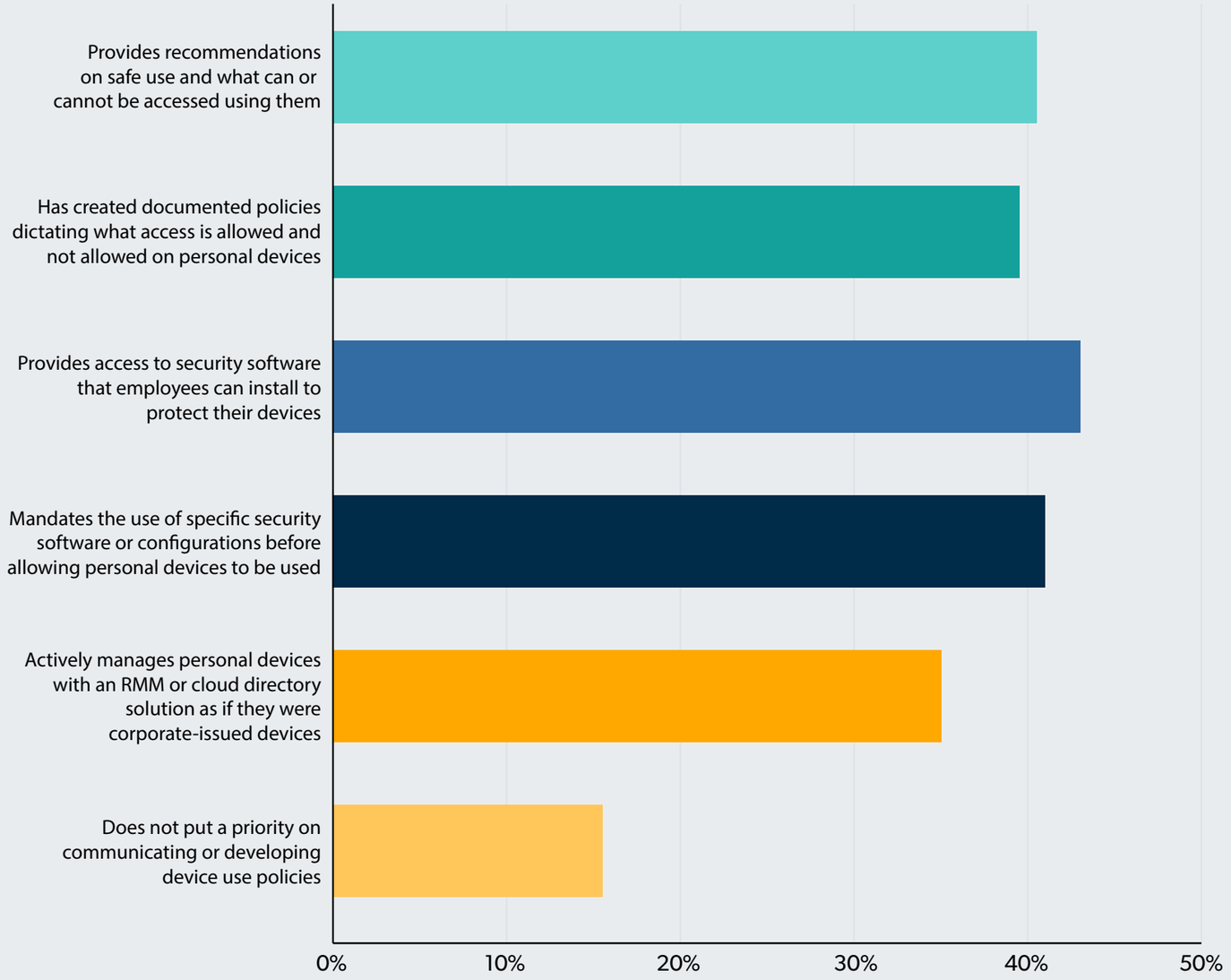
What percentage of employees use their own devices to access IT resources and perform work-related tasks?



Device Diversity Is Growing

An effective approach to device management requires accepting that today's device environments consist of a variety of personal and work-issued device types running different operating systems. In response, many SMEs are committing resources to establishing formalized device management processes or systems, especially for bring-your-own-device (BYOD) environments.

To secure personal device environments, SMEs are most commonly providing access to security software (44%), mandating configuration for software use (42%), making recommendations for safe device use (41%), and using a device management tool (36%). Only 15% of respondents said their company did not prioritize communicating or developing device use policies.



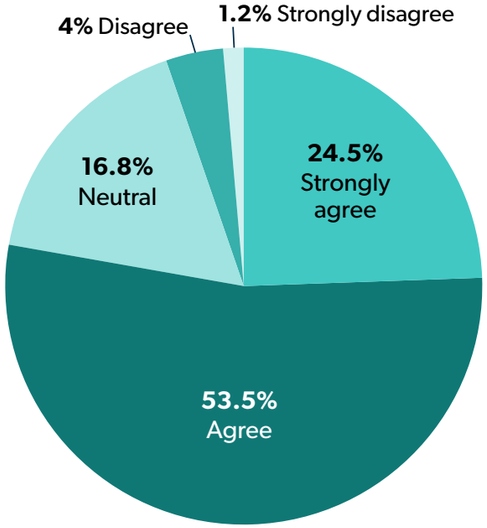
Complex Device Environments

Managing Security Vulnerabilities

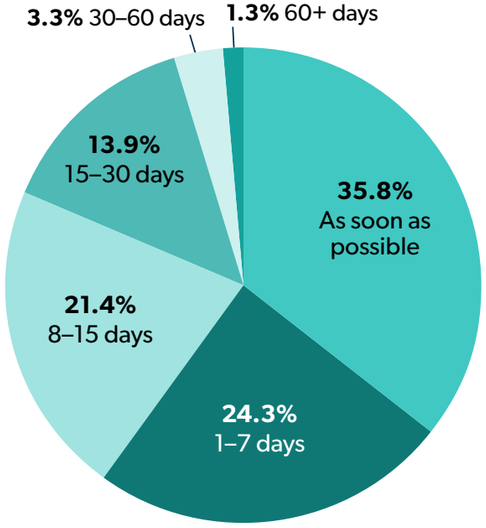
A critical element of effective and responsible device management is the process for patching known security vulnerabilities. In 2022, SMEs are expending significant effort to maintain robust security through a variety of approaches. Over two-thirds (77.8%) of IT professionals are confident their organization's patch management strategy is sufficient to protect against known vulnerabilities. And SMEs are patching quickly; after the patch for a software vulnerability is released, 35.8% report patching as soon as possible, and only 5% wait longer than a month.

To address the increase in external threats, nearly half (47.1%) of respondents said their organization uses a security staff member dedicated to identifying vulnerabilities and performing fixes, as well as managing the execution, mitigation, and remediation of patches. Close to half (46.7%) of respondents also follow patch schedules according to vendors' patch release dates.

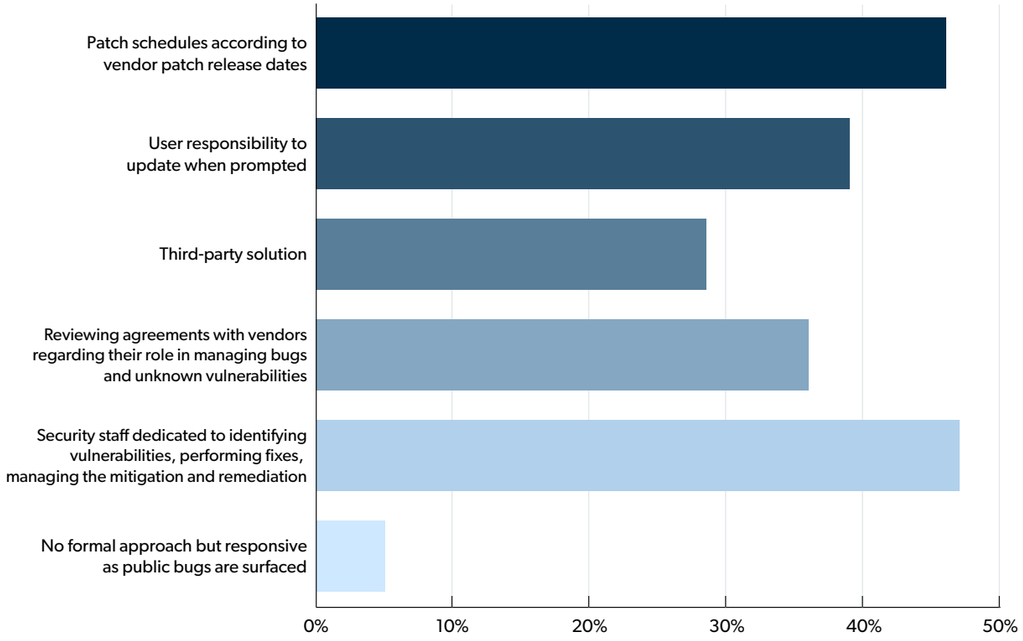
I am confident that my organization's patch management strategy is sufficient to protect against known vulnerabilities.



On average, after a patch for a known software vulnerability is released, how soon after do you update with the patch?



My organization uses the following for patch management:



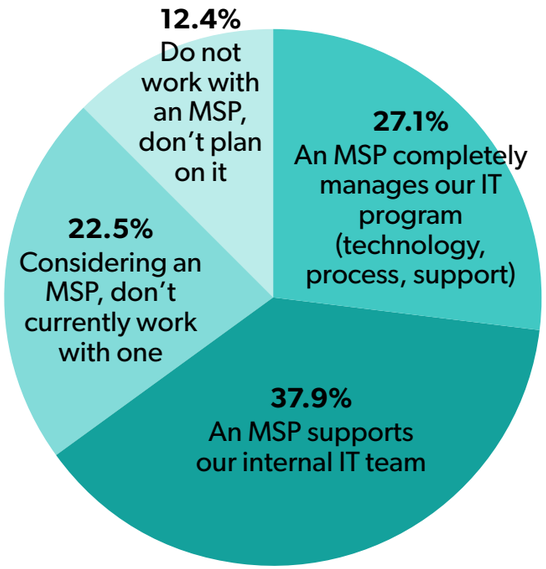
SMEs and the MSP Relationship

SMEs Are Investing Heavily in MSPs

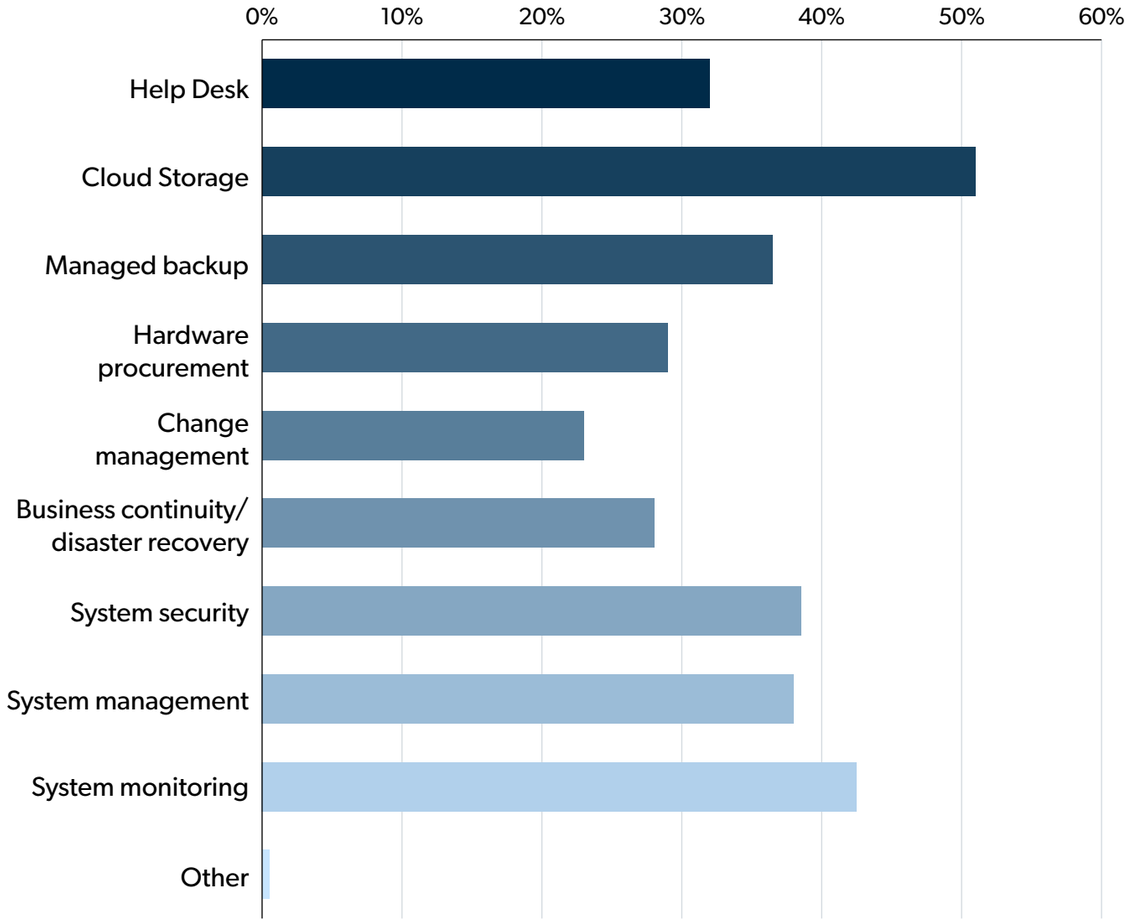
As they navigate an uncertain industry and economic environment, SMEs are investing significantly in managed service provider (MSP) support. The vast majority (87.5%) of SMEs currently use an MSP or are considering using one for a variety of functions. SMEs rely most heavily on MSPs for cloud storage (51.1%), system security (48.4%), system management (47.9%), and system monitoring (42.9%).

Most SMEs use MSPs to support their internal IT team (37.9%), though almost one-third (27.1%) use one to completely manage the IT program.

To what extent does a Managed Service Provider (MSP) play a role in your IT program?



What areas of your IT program are managed by by MSPs?

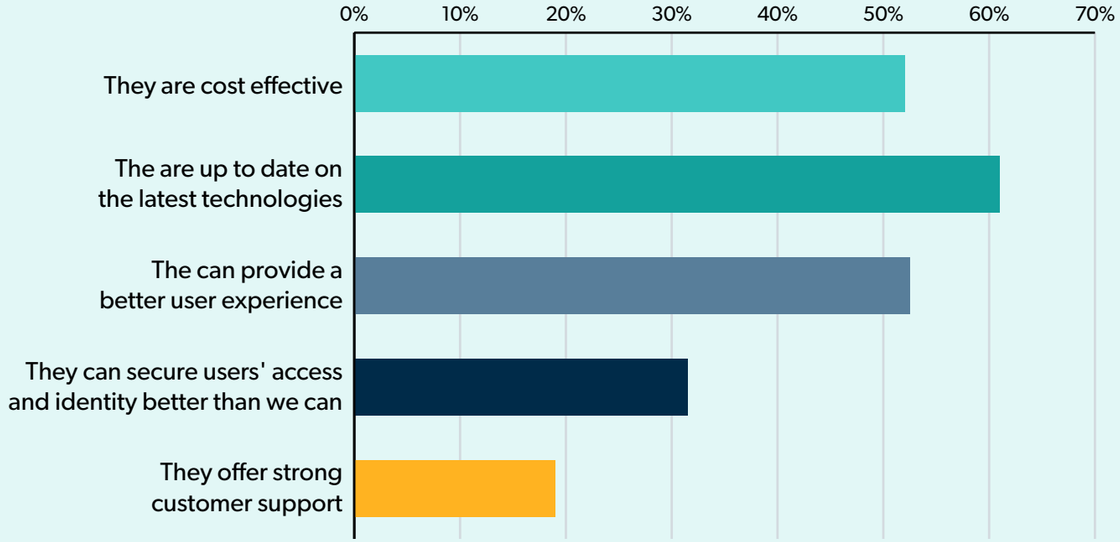


SMEs Are Investing Heavily in MSPs

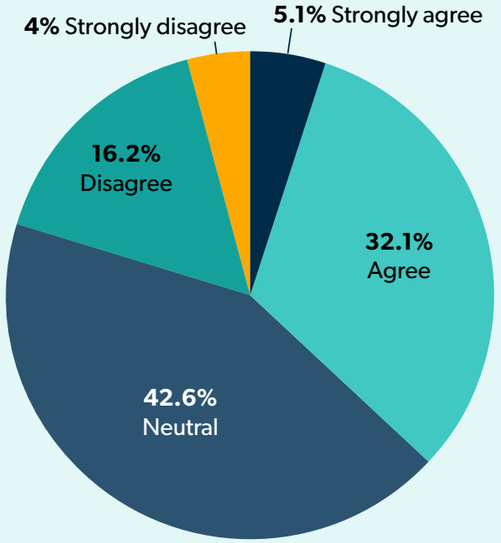
With the number of tools and applications required to manage an IT environment, MSPs provide special value due to their up-to-date knowledge and expertise — the most common reason admins report relying on them.

But despite widespread investment in MSPs, SMEs continue to harbor concerns about their MSPs ability to handle security. Over one-third (37.2%) of respondents agreed that they had concerns about how their MSPs handled security.

We use MSPs because



I have concerns about how our MSPs manage security



Making IT Work

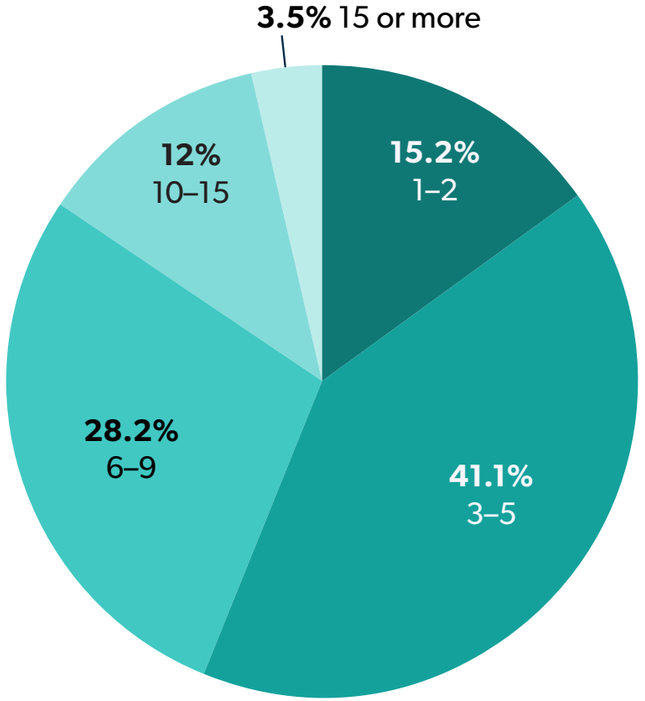
Increasing Tool Sprawl

As IT professionals work to balance their growing security and functionality needs for their remote and hybrid-remote environments, tool sprawl is becoming a challenge. While three-quarters (74.6%) of IT professionals would prefer to use a single tool to manage the employee lifecycle, less than 20% of respondents said they're able to do so with only one or two tools.

Despite the explosion in the number of available tools and applications, IT admins' preference for a single tool is only growing stronger. In 2021, 69.7% of respondents preferred a single tool, and only 20.7% agreed strongly with the preference; in 2022, those who agreed strongly with a desire for a single tool increased by 35%.

And IT professionals aren't the only ones experiencing the effects of tool sprawl: most employees now require several tools just to get their job done. Only 15.2% of employees need one or two accounts to do their jobs, while 43.7% need six or more.

On average, how many different accounts (across devices, applications, networks, etc.) would you estimate employees need to do their jobs?

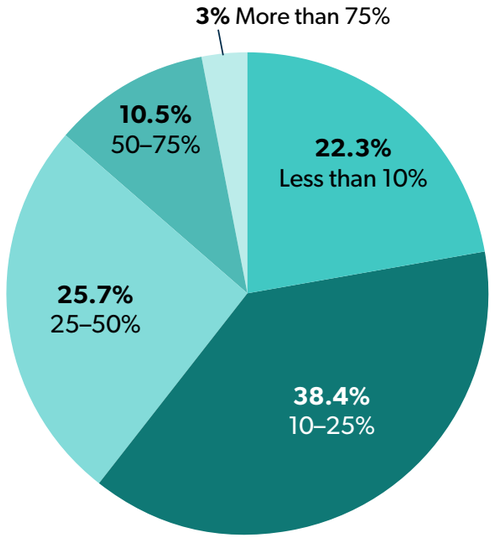


Making IT Work

Vendor Communication Is a Significant Time Investment

Perhaps as an effect of tool sprawl, vendor communication eats into a significant amount of IT professionals' work time. In fact, 39.2% of IT professionals spend at least a quarter of their day working with vendors. In a traditional 8-hour work week, that's at least two hours a day.

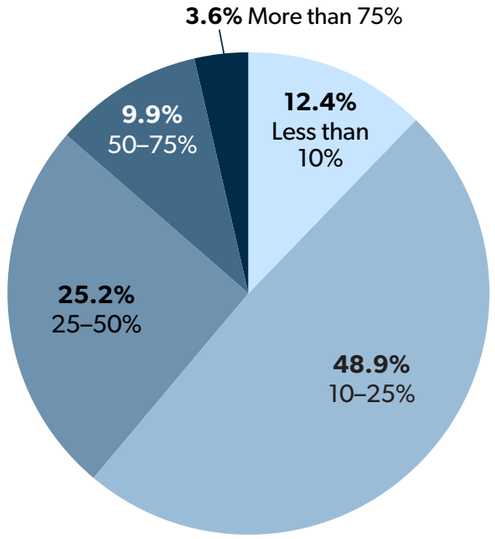
What percentage of your work hours are spent communicating with vendors?



Licensing Costs Are High

While IT professionals are spending a significant amount of time with vendors, SMEs are also spending a significant amount of their budget on licensing costs. While 10-25% of an SME's yearly budget was the most popular allotment for licensing costs, over a third (38.7%) of SMEs are spending over 50% of their budgets on licensing.

What percentage of your yearly IT budget goes toward licensing?

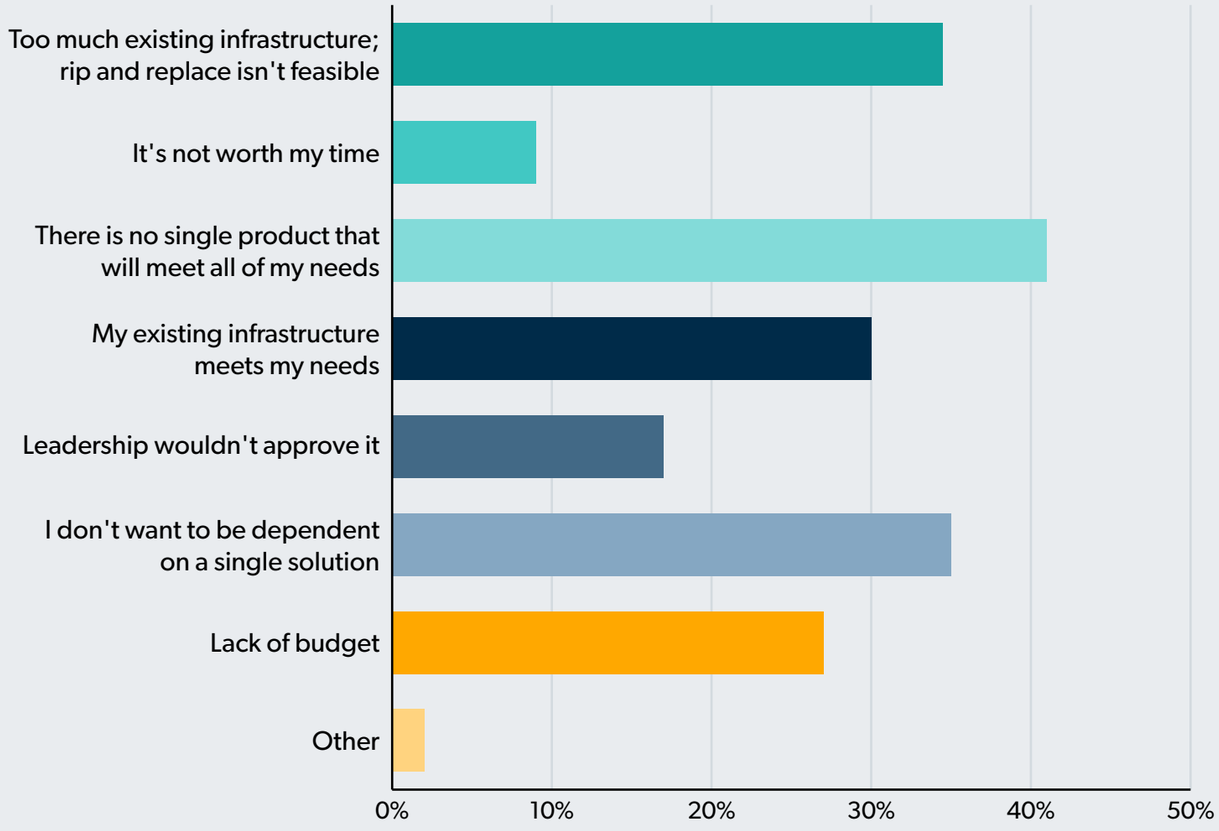


Making IT Work

Roadblocks to IT Unification

While IT admins profess a strong interest in tool unificiation in theory, those same admins remain somewhat skeptical about the ease and utility of unification in practice. When asked about what's preventing tool unification/consolidation in their organization, the top three roadblocks respondents offered were that no single product would meet all their needs (41.4%), they didn't want to be dependent on a single product (34.8%), and they already had too much existing infrastructure (34.4%). Solutions that eliminate the need for multiple point solutions will need to clearly demonstrate value, functionality, and ease of integration to overcome admin reluctance.

What reasons keep you from consolidating IT products?



Final Thoughts

After successfully — and urgently — transitioning organizations to remote work, then establishing support for entirely new workplace models, there's no question that IT teams serve as the central organ ensuring operational stability and growth.

Pandemic-induced uncertainty may be waning, but there is no shortage of internal and external factors that threaten to disrupt operations. In 2022, SMEs may be navigating the unknown, but they're also giving their IT professionals the budget and opportunity to pursue IT initiatives most likely to stabilize operations.

Survey respondents indicated a high prioritization of security and the acknowledgement of permanent work-from-anywhere models. Looking forward, SME IT professionals would be well-served to focus on:

- Bolstering security with automated patch management. While many IT professionals feel confident in their patch management program, a significant portion of SMEs (39.4%) still leave the responsibility of patch implementation up to the users. Automating patch implementation and removing the responsibility (and risk) from the users is an easy mitigation step.
- Establishing stronger BYOD policies. While SMEs have made strides toward creating policies for secure mobile and personal device use, many are still based on recommendation rather than mandated or automated. Like patch management, personal and mobile device policies are much more effective when enforced through automation rather than suggestion. IT professionals still relying on policy recommendations might consider upgrading to automated policy enforcement. Consider a mobile device management (MDM) platform that accomplishes this while also accounting for user privacy by allowing users to voluntarily enroll and restricting the company from accessing personal applications or content.
- Upgrading MFA security. Multi-factor authentication (MFA) makes authentication exponentially more secure; extending it to apply to more (or, ideally, all) authentication points can dramatically increase security.
- IT admins are well aware of the importance of layered security, and are aware of various options to deploy it. Over one-quarter (29.7%) agreed that a "one-time passcode that is texted to a mobile device" is the most secure MFA factor and 35.5% agreed that it was easiest for users to use. However, current evidence suggests that texted codes are susceptible to SMS interception, and typing in a code tends to produce more friction for the user than tapping a push notification button or using biometrics. SMEs using only passcode-based MFA might consider varying their methods to include biometrics and push notifications to both prevent SMS interception and offer a more user-friendly experience, something admins are likely familiar with considering that 74.5% of them report personally using biometrics.
- Tightening central access management. Ideally, SMEs should centrally manage all their employees' accounts. While a majority of SMEs centrally manage accounts where possible, only 36.6% said they did so at all times. Often, tool incompatibility can be a significant roadblock to an organization's ability to keep a handle on all access management. IT unification helps SMEs rein in their central access management and apply it everywhere.
- Consolidating tools. SME IT professionals are experiencing tool sprawl and spending a significant amount of their workdays working with vendors — and most IT professionals would prefer to use one tool to manage the employee lifecycle, even though most currently use several. Consolidating tools doesn't just make life easier for SMEs, it also improves security with sturdy native integrations, reduces spend by eliminating tooling redundancies, makes vendor relationships less time-consuming and more productive, and improves the user experience with streamlined infrastructure that offers seamless, intuitive end-user processes.

Despite global uncertainty, SMEs will continue to drive economic growth, and the IT professionals they rely on will be the force that makes that growth possible. As security threats increase in sophistication and threat, SME IT admins are demonstrating they're anticipating the challenge and prepared to enlist the necessary tools to respond.

For over a decade, JumpCloud has been at the forefront of **Making (Remote) Work Happen®**. Built specifically for the SME market, JumpCloud's open directory platform exists to give enterprise-level IT management without enterprise-level cost or complexity. We'll continue our mission to be the best possible partner to IT admins everywhere, ensuring they can connect their users — securely — to whatever they need, no matter what.

Methodology

JumpCloud surveyed 506 U.S.-based and 501 U.K.-based SME IT decision-makers, including managers, directors, vice presidents, and executives. Each survey respondent represented an organization with 2,500 or fewer employees across a variety of industries.

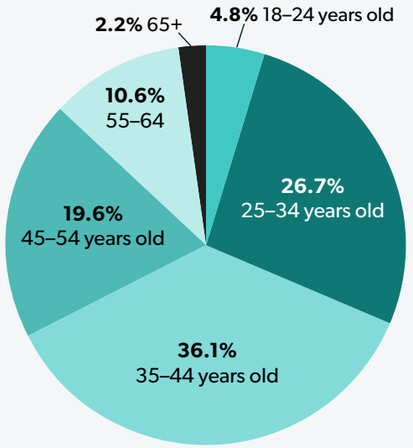
The survey was conducted via Propeller Insights, April 14, 2022 to April 20, 2022.

What is JumpCloud?

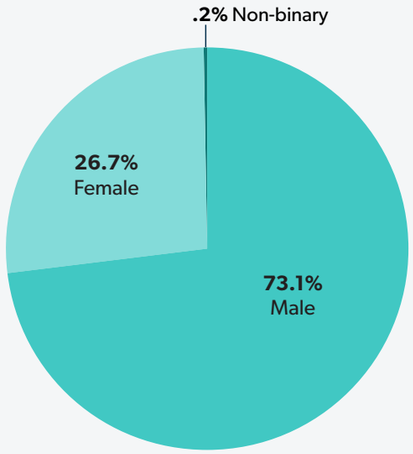
JumpCloud is an open directory platform that offers SMEs everything they need to **Make (Remote) Work Happen®**. That includes everything from core directory services to mobile device management, MFA, SSO, and more. To learn how JumpCloud empowers IT professionals to consolidate their tools and streamline their infrastructure, visit jumpcloud.com/why.

Demographics

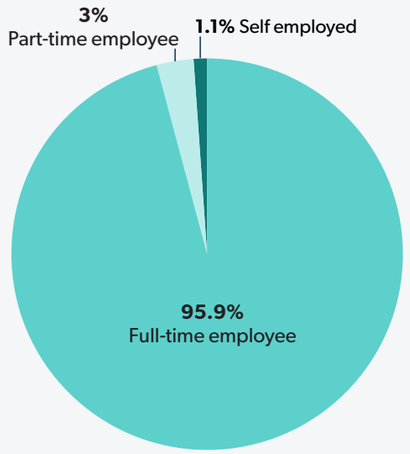
What is your age?



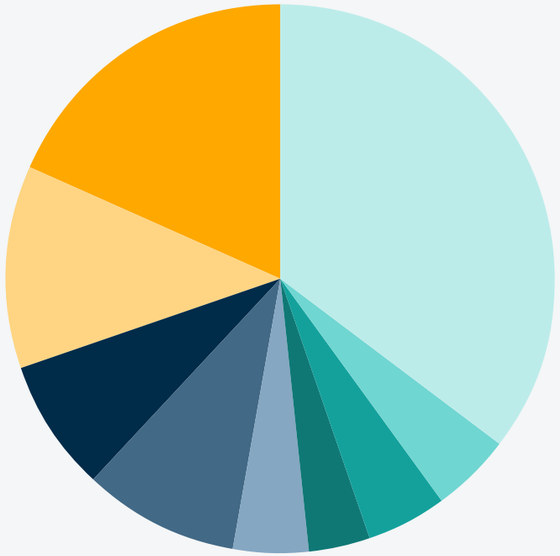
What is your gender?



What is your employment status?

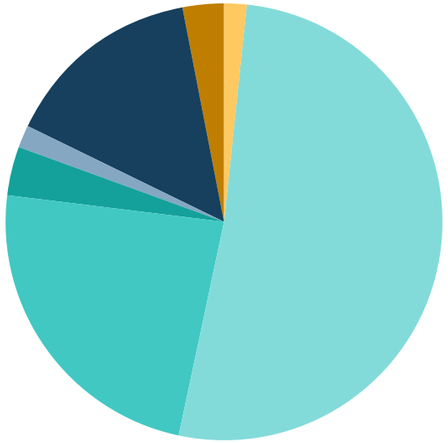


Which industry do you currently work in?



- **35.6%** Computer software
- **4.5%** Education
- **4.9%** Finance, Insurance, Real Estate
- **3.5%** Government
- **4.5%** Healthcare
- **9.2%** Manufacturing
- **7.9%** Telecommunications
- **11.8%** Other
- **18.3%** All others

What best describes your level within the organization?

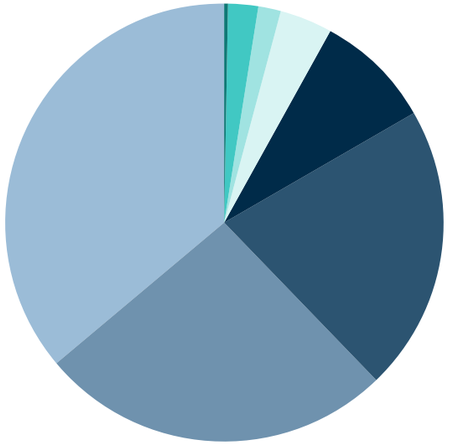


- **1.7%** Non-manager
- **51.8%** Manager
- **23.5%** Director
- **3.6%** Vice President
- **1.7%** Senior Vice President
- **14.9%** C-level executive
- **2.8%** Owner

In what region of the United States do you primarily reside?

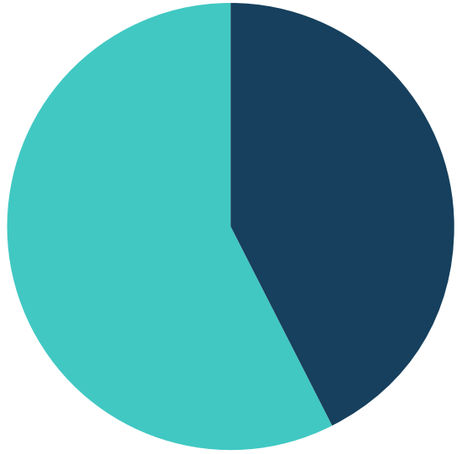
- **19.6%** Pacific: AK, CA, HI, OR, WA
- **4.5%** Mountain: AZ, CO, ID, MT, NM, NV, UT, WY
- **6.1%** Plains: IA, KA, MN, MO, ND, OK, NE, SD
- **14%** So. Central: AL, AR, KY, LA, MS, TN, TX, WV
- **12.8%** Upper Midwest: IL, IN, MI, OH, WI
- **16.6%** Southeast: FL, GA, NC, SC
- **18%** Northeast: CT, MA, ME, NH, NY, PA, RI, VT
- **8.3%** Mid-Atlantic: DE, MD, NJ, VA

Approximately how many employees work in your organization across all locations?



- **.4%** 1
- **2.2%** 2–10
- **1.8%** 11–24
- **3.8%** 25–50
- **8.7%** 51–100
- **21%** 101–500
- **26%** 501–1,000
- **36.1%** 1,001–2,500

In what region of the United Kingdom do you primarily reside?



- **42.7%** Greater London
- **57.3%** Rest of the UK

The JumpCloud Directory Platform helps IT teams **Make (Remote) Work Happen**® by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud® has a global user base of more than 180,000 organizations, with more than 5,000 paying customers including Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

For more information on JumpCloud and how organizations everywhere are providing secure, frictionless access to all their IT resources, visit jumpcloud.com/why.

Try JumpCloud Free →

Learn More About JumpCloud

Blog

Daily insights on directory services, IAM, LDAP, identity security, SSO, system management (Mac, Windows, Linux), networking, and the cloud.

Learn More →

Resources

JumpCloud's hub for videos, documentation, case studies, partner enablement tools, and more.

Learn More →

In the Press

Read what people are saying about JumpCloud.

Learn More →