jumpcloud™

Flexibility and Ingenuity: What's Powering Small and Medium-Sized Enterprise IT Management in 2023

Security is top of mind for admins at small and medium-sized enterprises (SMEs), as external threats grow in sophistication, regulatory and compliance pressures are heating up, and admins are overwhelmed with too many tools to juggle.

Executive Summary

JumpCloud's SME IT Trends Report offers a bi-annual look into the acute challenges, experiences, and opportunities for IT practitioners at small and medium-sized enterprises (SMEs). During the early parts of the pandemic, admins struggled most with how to enable remote employees and support new workplace models—-all while maintaining robust security. The transition wasn't easy, but it accelerated cloud transformation and IT teams were well served by adopting cloud-forward models that accommodated the sudden redistribution of workers and their resources.

Now three years after the onset of COVID-19, the fifth edition of the SME IT Trends Report shows that just after SMEs successfully established the new workplace normal, significant turbulence in the greater macroeconomic environment threatens to upend the system again. Instead of lockdowns and supply chain shortages, businesses now deal with layoffs and recession fears. If IT admins have internalized any lesson over the last few years, it's that modern IT management is a balance of responding to current needs while remaining nimble enough to adapt to the unknown. Flexibility, ingenuity, and innovation have never been more critical for those in the IT trenches.

Part of what's needed is an IT environment built around identity. Identity is now at the core of every IT access transaction; it's the new security perimeter. The ideal environment for SMEs, as it is for larger organizations, is to securely connect the right users with the right resources at the right time in the right way, no matter where users are logging in. Admins are hungry for an open IT approach that delivers on this promise, an approach that unifies and centralizes identity and allows organizations to scale while solving efficiency, complexity, and cost challenges.

IT is the heart of any organization. These professionals are the engine behind operations that keep resources safe. It's not an easy job, especially for those in smaller firms without enterprise-sized teams or budgets.

JumpCloud commissions this ongoing research because SME admins offer critical visibility into the current state of securing SMEs and clarity about how to best position them for success.

This Q2 2023 edition of the SME IT Trends Report suggests:

— Security is top of mind for admins, as external threats grow in sophistication, regulatory and compliance pressures are heating up, and admins are overwhelmed with too many tools to juggle.

— The modern device, identity, and access environments in SMEs are overly complicated and a burden for IT admins to manage.

— IT professionals see massive untapped potential in moving away from closed, legacy systems, toward an open model that enhances productivity, bolsters security, and enables easier IT management.

IT environments built for yesterday's needs are inadequate safeguards against today's threats and are unable to deliver the level of user-friendly productivity that modern alternatives can.

This edition of the SME IT Trends report reveals that as admins face their security and IT fears, they are clear about solutions they believe can better secure their organizations and better enable work to *work well*. They are realistic about the general IT outlook—-economic uncertainty, complicated device environments, an overwhelming breadth of daily responsibilities, and more—and are looking for an open IT approach to identity that balances stringent security and ease of use.

The first half of 2023 underscores that SMEs are leaning into innovation and change and that the IT admins successfully managing the transformation are responding with agility, openness, and incredible resilience.
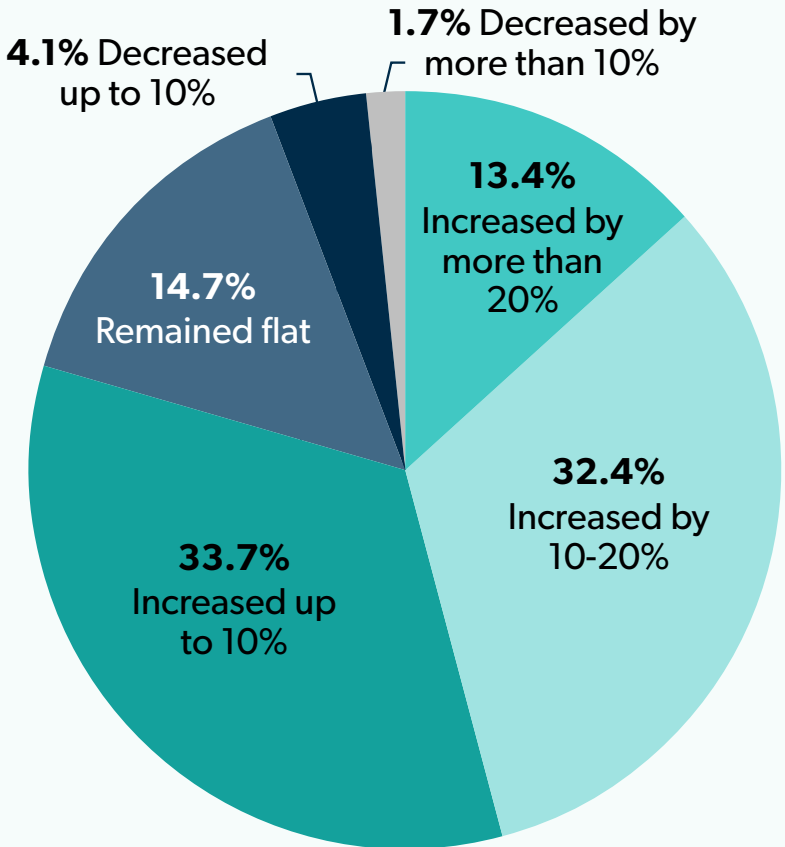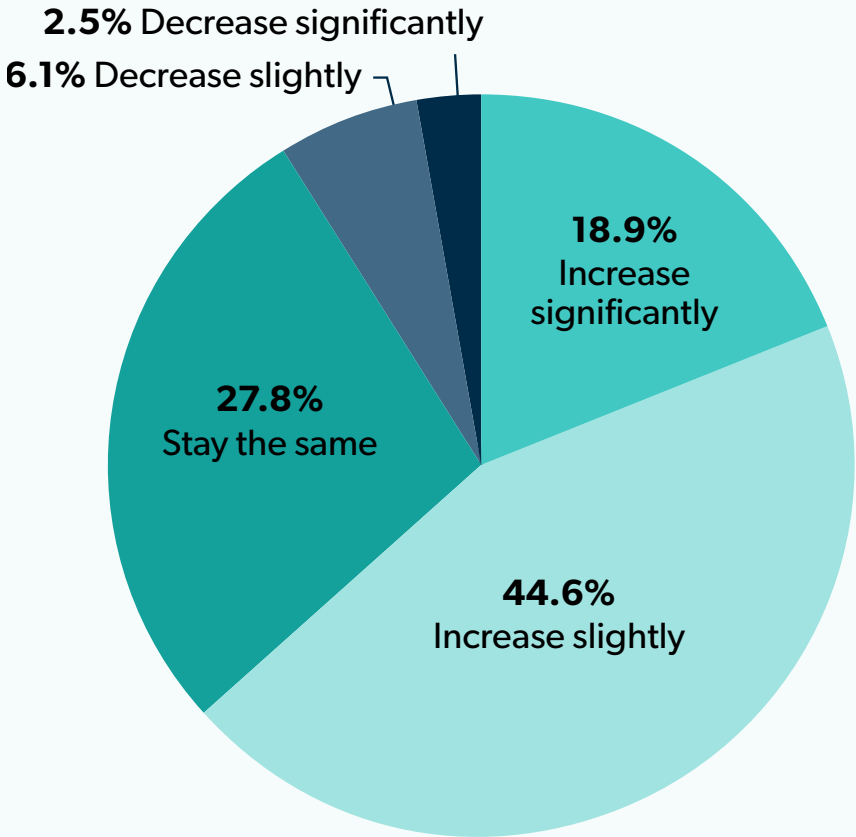
The SME IT Landscape

Budgeting Realities

In spite of choppy economic waters for the tech industry during the first half of the year, IT budgets have continued to rise and SMEs have largely avoided budget cuts, as 80% of SMEs report their IT budgets have increased over the past year, and 13% have seen an increase of over 20%.

Overall, IT admins are optimistic about future SME spending with 64% expecting their IT budget to increase over the second half of 2023, while just 9% expect their IT budgets to decrease.

Over the past year, my IT budget:

- 1.7% Decreased by more than 10%
- 4.1% Decreased up to 10%
- 13.4% Increased by more than 20%
- 14.7% Remained flat
- 32.4% Increased by 10-20%
- 33.7% Increased up to 10%

In the second half of 2023, I expect our IT budget to:

- 2.5% Decrease significantly
- 6.1% Decrease slightly
- 18.9% Increase significantly
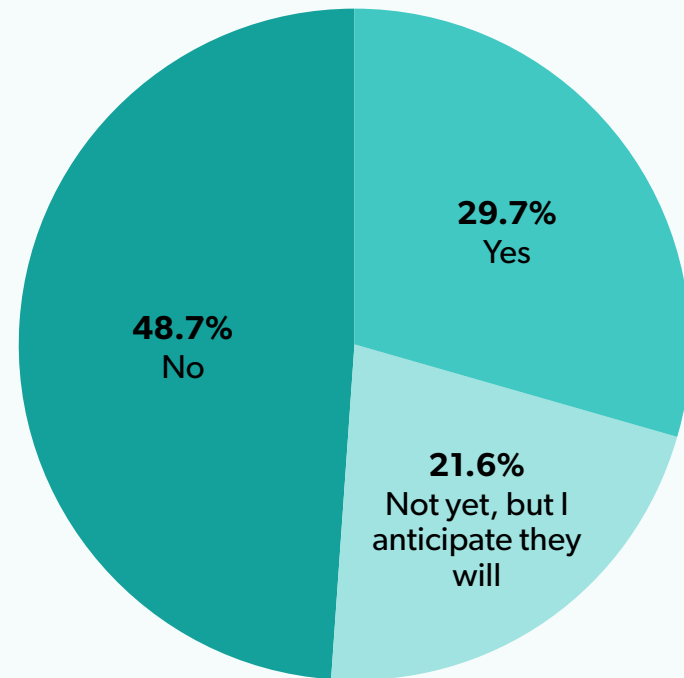- 27.8% Stay the same
- 44.6% Increase slightly
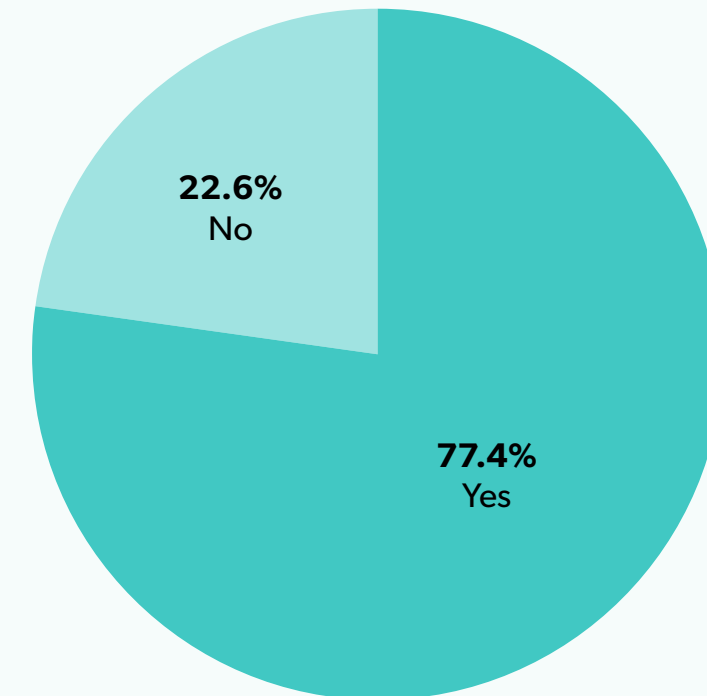
The SME IT Landscape

Layoffs and Outlook

While budgets on spending may have increased, SMEs haven't avoided all of the impacts of the year's turbulent market conditions—specifically the rash of layoffs that have swept through the entire tech industry. 30% of all surveyed admins reported their organization had gone through layoffs within the last six months.

And while admins were optimistic about IT budgets in the second half of 2023, they don't have similar optimism about organizational staffing. Over three-fourths (77%) of admins anticipate more layoffs in their organization within the next six months.

Has your organization gone through layoffs in the last six months?

- **29.7%** Yes
- **48.7%** No
- **21.6%** Not yet, but I anticipate they will

Do you anticipate more layoffs in the next six months?


- **22.6%** No
- **77.4%** Yes

The SME IT Landscape

The Employee Experience

The uncertainty around the modern workplace model has largely settled as SMEs have adjusted to distributed workforces. Nearly half of workers (47%) have returned to the office, with 33% working in a hybrid model and 20% working remotely.

IT admins have been keen to ensure that the employee experience is a good one, no matter where users are working, or what applications they're using to do their job. 84% agree that employee experience is an important factor in making IT purchasing decisions.

What is the percentage breakdown of employees working in the office, hybrid, or working remotely full-time?

- **20%** Remote
- **33%** Hybrid
- **47%** Office
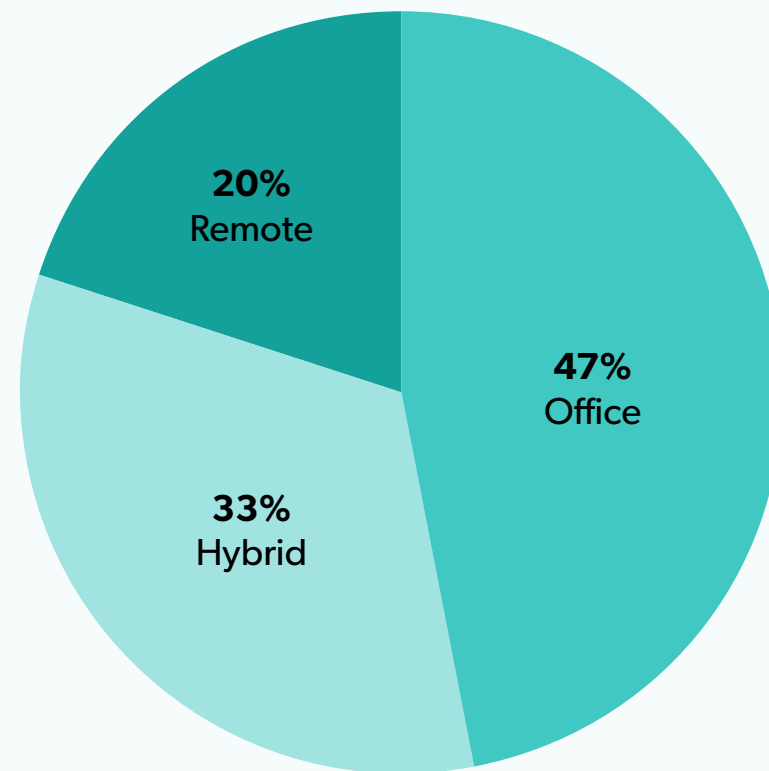
I consider employee experience to be an important factor in making IT solutions purchasing decisions.

- **1%** Strongly disagree
- **3.2%** Disagree
- **11.8%** Neutral
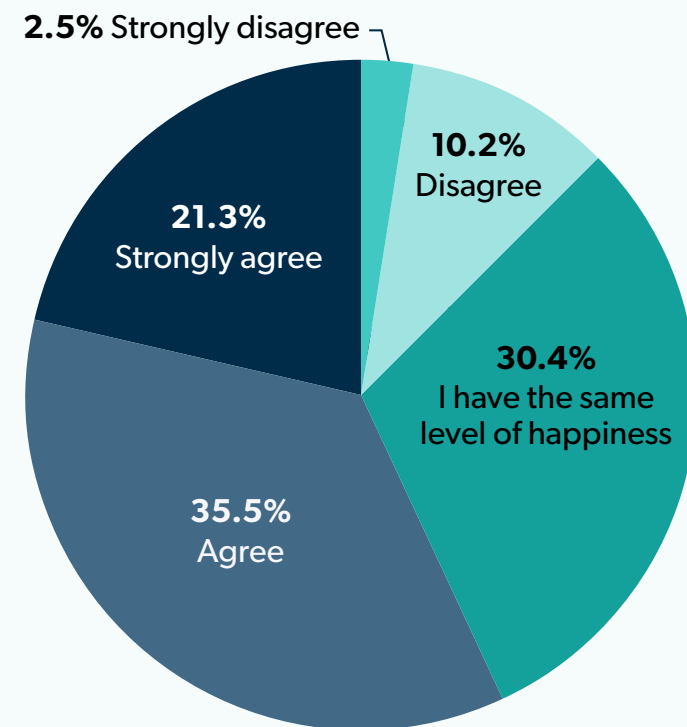- **30.9%** Strongly agree
- **53.2%** Agree
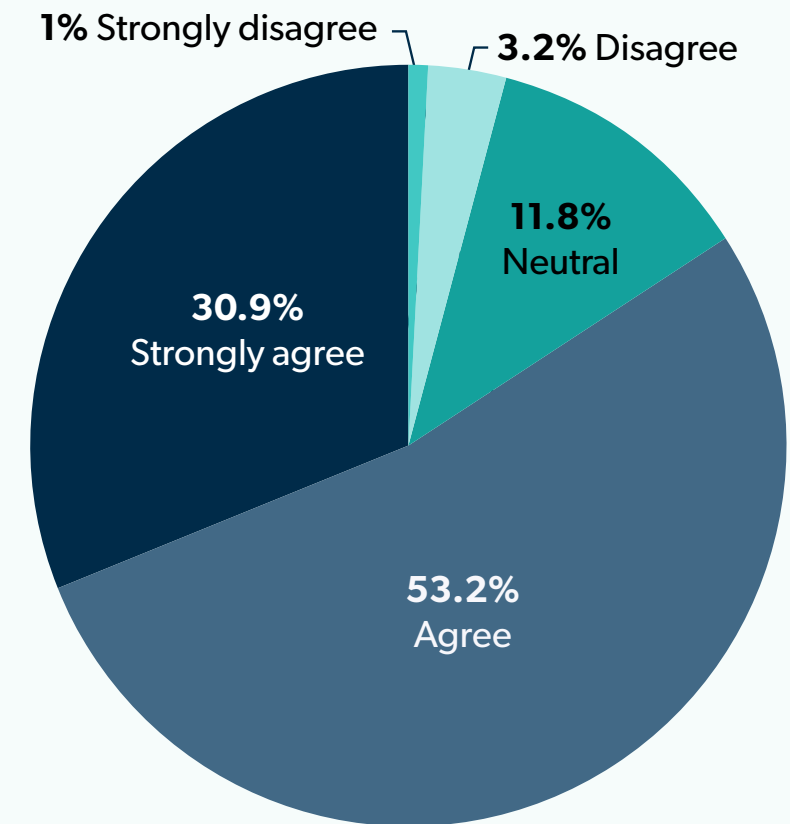
The SME IT Landscape

Job Satisfaction of IT Admins

Despite facing continued challenges that have been outside of IT control, and the resulting responsibilities that IT teams have had to shoulder, overall, SME IT admins are happier in their job than a year ago. 57% agree or strongly agree that they are happier in their job than a year ago and 30% report the same level of happiness. Only 13% report they are unhappier now than in April 2022.

Increased and evolving stressors may not be impacting happiness, but IT admins are definitely feeling the weight of their job. Now nearly half (48%) say they are somewhat overwhelmed in relation to their jobs and expectations, and 16% say they are very overwhelmed.

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

2.5% Strongly disagree

21.3% Strongly agree

10.2% Disagree

30.4% I have the same level of happiness

35.5% Agree

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

12% Not overwhelmed

16.4% Very overwhelmed

23.5% Neutral
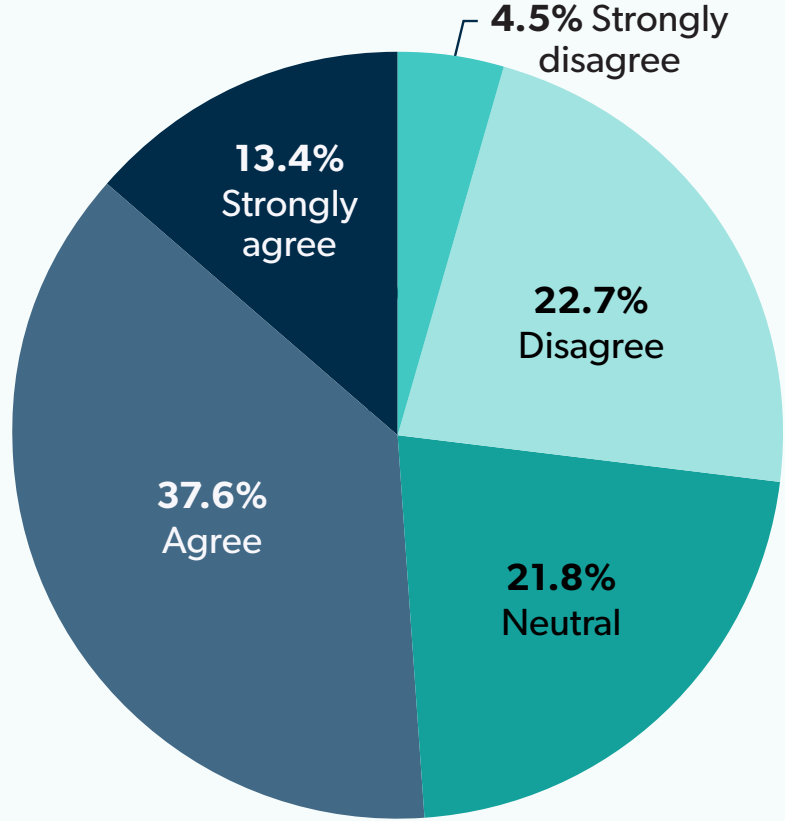
48.1% Somewhat overwhelmed
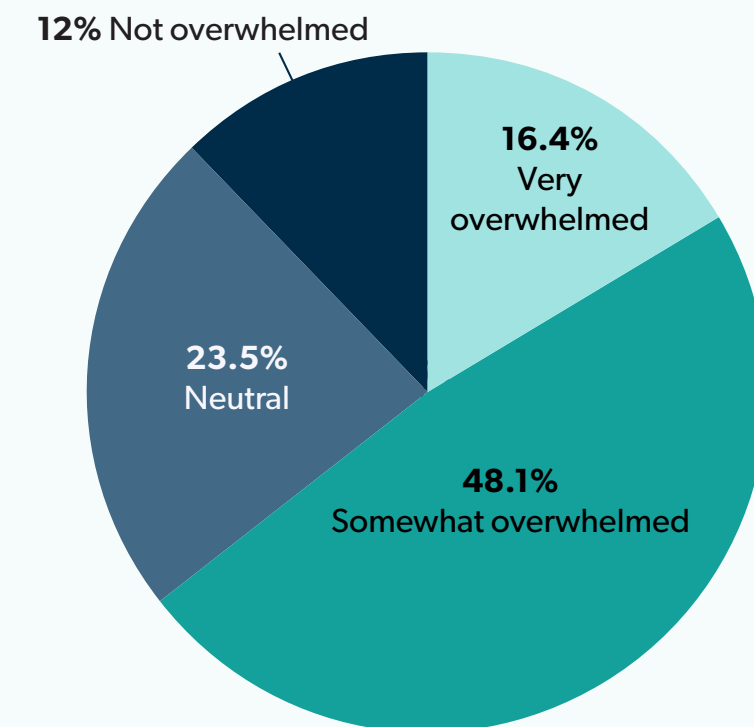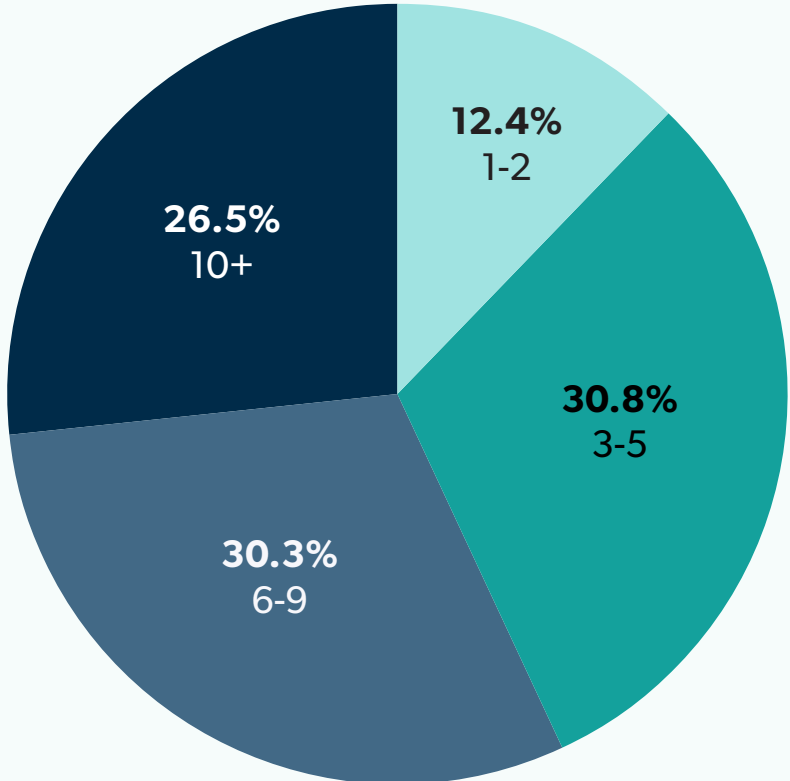
The SME IT Landscape

Life of an IT Admin

Amid industry conversations about layoffs, inflation, budget cuts, and recessions, IT admins are making efforts to avoid burnout. 51% of all surveyed IT admins report having purposely reduced their workload in order to achieve a better work-life balance in the last six months.

This reduction in hours hasn't translated into quiet quitting or a shirking of responsibilities—in fact, IT admins continue to be overworked. Over a quarter (26%) of IT admins report working 10 or more hours per week more than their job description requires, and 100% of admins report working at least an hour more per work than their job description.

Over the last six months, I have purposely reduced my workload in order to achieve a better work-life balance.

- **4.5%** Strongly disagree
- **22.7%** Disagree
- **21.8%** Neutral
- **37.6%** Agree
- **13.4%** Strongly agree

Each week, the number of hours I work over my job description is:

- **12.4%** 1-2
- **30.8%** 3-5
- **30.3%** 6-9
- **26.5%** 10+
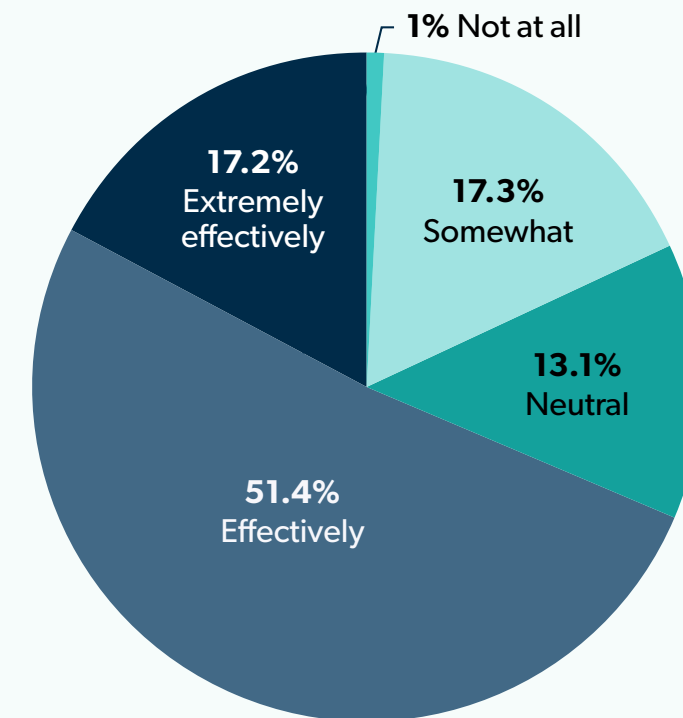
The SME IT Landscape

Compliance and Governance

With employees logging in across distributed workplaces, SMEs are keeping aware and active about **compliance needs**, whether due to increased governmental regulation or the proliferation of new applications and tools. Nearly half of IT admins (45%) are concerned about meeting government compliance IT requirements, and a large majority (69%) believe their existing IT investments and systems meet regulatory and compliance laws effectively or extremely effectively.

How concerned are you about meeting government compliance requirements with your IT?

- **13.7%** Extremely concerned
- **11.8%** Not at all
- **21.7%** Somewhat
- **30.8%** Concerned
- **22%** Neutral
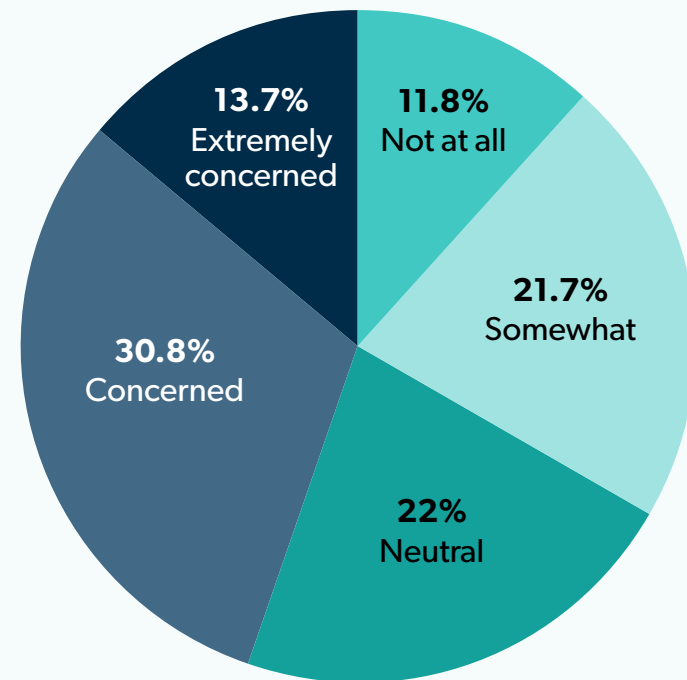
How effectively do you think your existing IT investments and systems meet regulatory and compliance laws?

- **1%** Not at all
- **17.2%** Extremely effectively
- **17.3%** Somewhat
- **13.1%** Neutral
- **51.4%** Effectively

The SME IT Landscape

Tools and Applications

SME IT teams have the incredible responsibility of securing workers' access to all IT resources without adding any adverse impact to the user experience. One consideration that the survey suggests admins think would be helpful is **tool consolidation**. 77% of admins would prefer to use a single tool to do their job instead of a number of point solutions. But centralized IT management has eluded most SMEs, despite admins' preference for it. Only 13% of SMEs use just 1-2 tools to manage the employee lifecycle and the applications they need to do their job—41% say they need eight or more tools.

I would prefer to use a single solution/tool to do my job over managing a number of different solutions.

1.7% Strongly disagree

6.4% Disagree

27.2% Strongly agree

15.2% Neutral

49.5% Agree
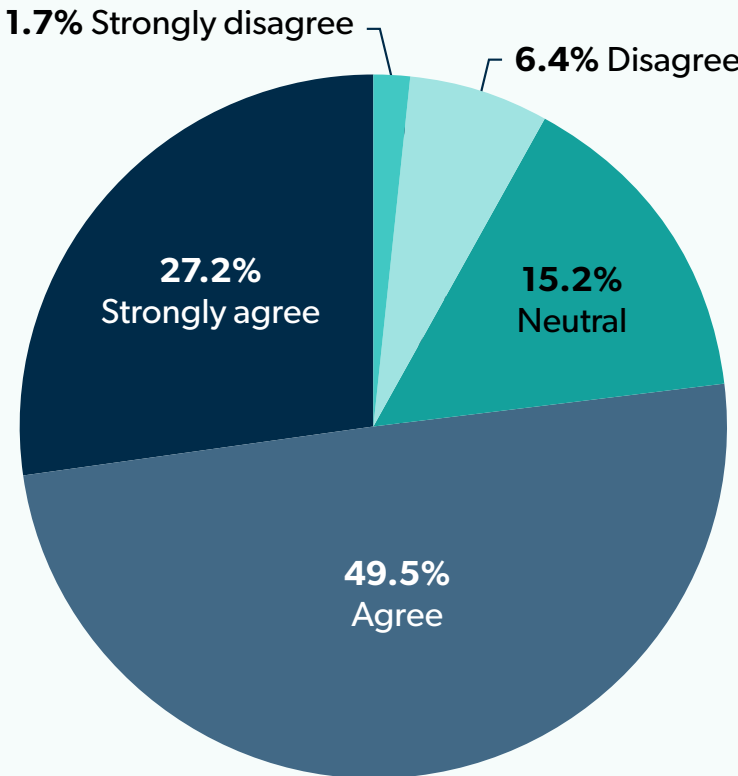
How many tools or applications does your organization use to manage the employee lifecycle and the tools they need to do their job (e.g: onboarding, device management, security tools, directory services, offboarding, help desk, etc.)?

4.8% 19+

2.4% None

7.8% 13-18

12.7% 1-2

28.8% 8-12

**43.6%** 3-7
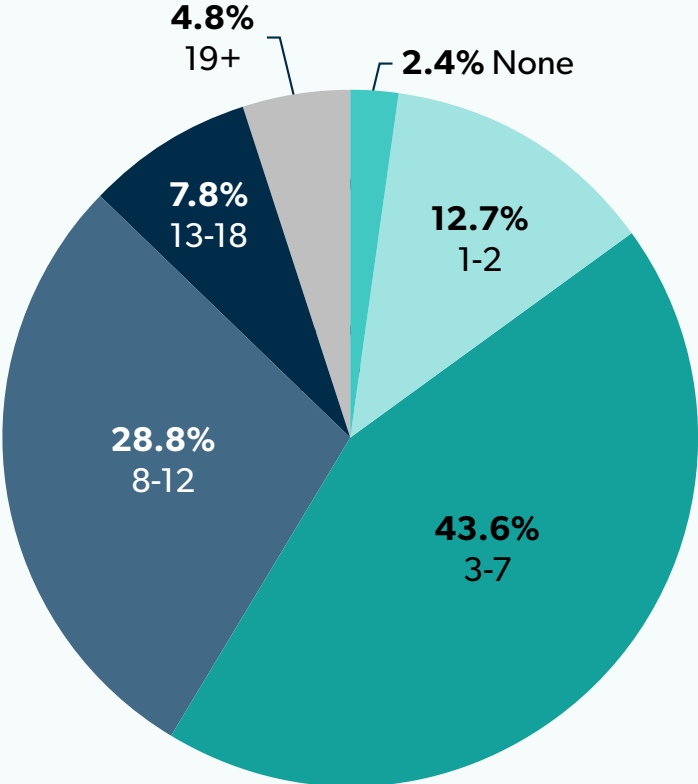
Security and SMEs

Biggest Concerns

With a broad portfolio of responsibilities, admins rank security as their biggest IT challenge in 2023. 59% report it as the biggest challenge, followed distantly by new services and application rollouts (43%) and the cost of remote work solutions (43%).

49% of admins agree that they're more concerned about their organization's security posture now than they were six months ago.

What have been the biggest challenges to your IT team in Q1 2023?
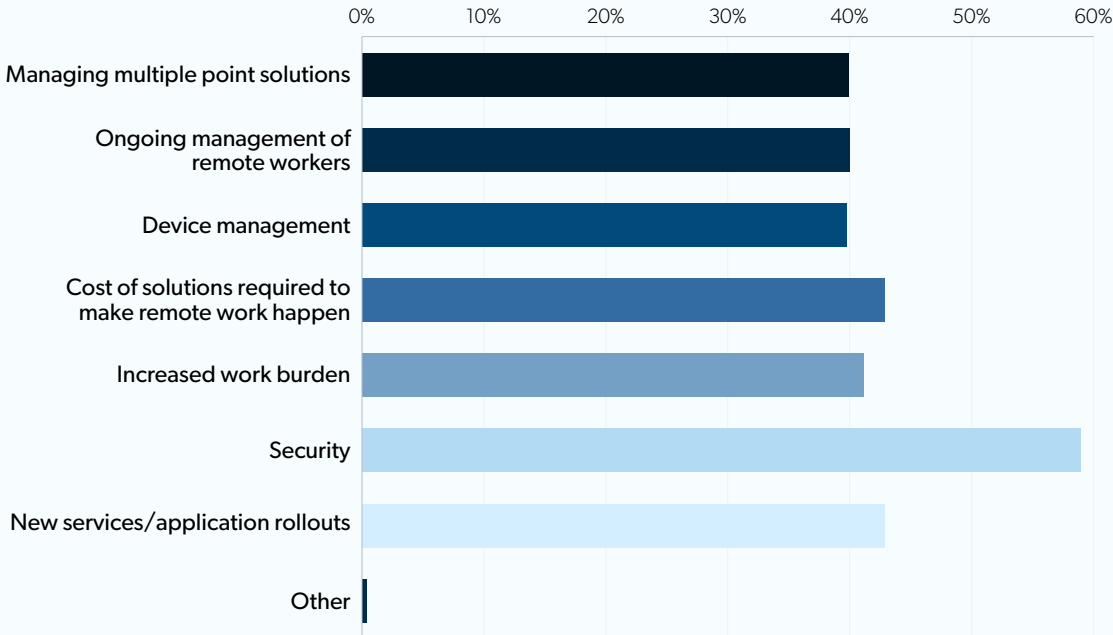
I am more concerned about my organization's security posture than I was 6 months ago.

- **5.8%** Strongly disagree
- **19.8%** Disagree
- **25.1%** Neutral
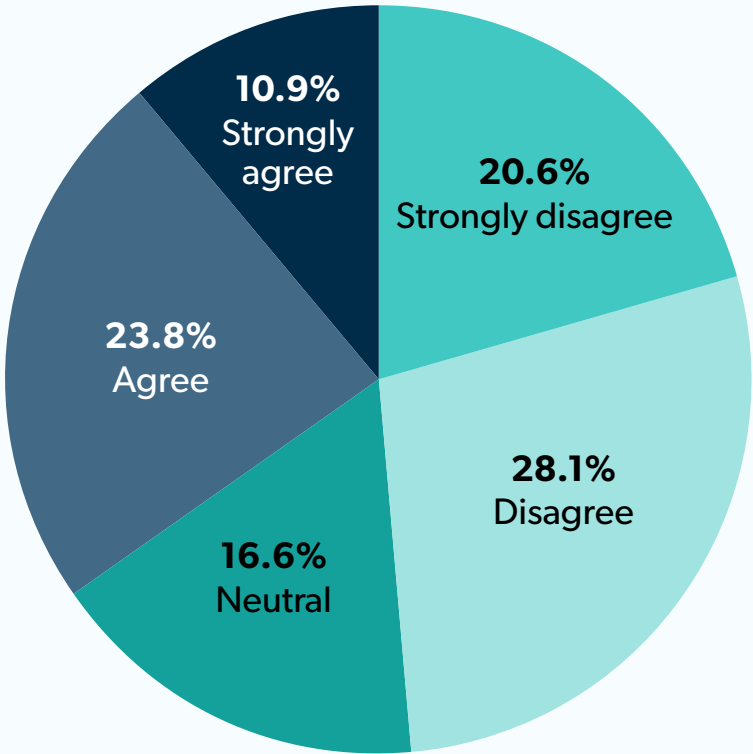- **33%** Agree
- **16.2%** Strongly agree
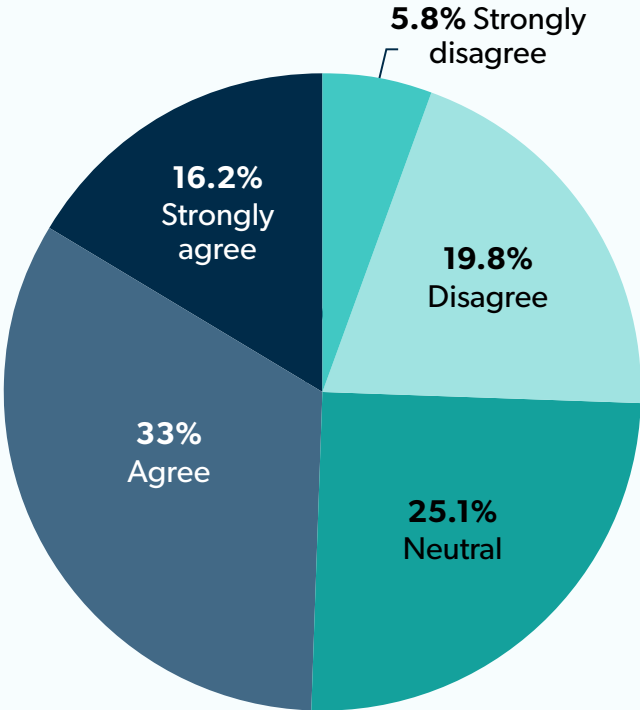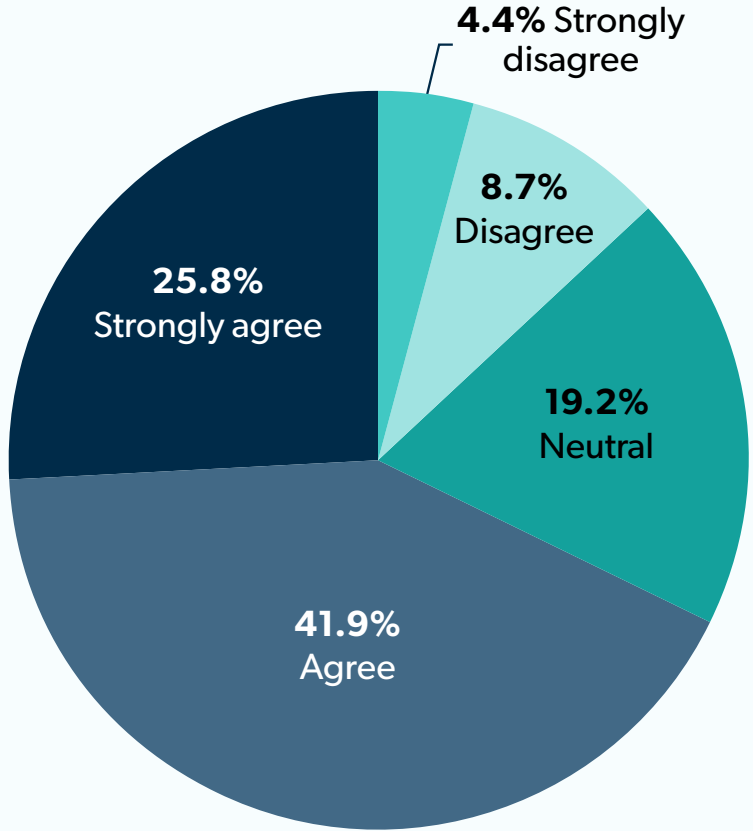
Security and SMEs

Spending

Budgets are a bright spot when it comes to SME IT as the survey suggests organizations prioritize security spending. Only 35% of SME IT admins believe their organizations will cut spending on cybersecurity this year, while nearly half (49%) believe their organizations will not make spending cuts.

It's a measure of relief for admins navigating an ever-evolving security landscape as nearly 68% believe that any cuts to their security budget will increase organizational risk.

I believe my organization will cut spending on cybersecurity in the next year.

- **10.9%** Strongly agree
- **20.6%** Strongly disagree
- **23.8%** Agree
- **28.1%** Disagree
- **16.6%** Neutral

I think any cuts to our security budget will increase our organizational risk.

- **4.4%** Strongly disagree
- **8.7%** Disagree
- **25.8%** Strongly agree
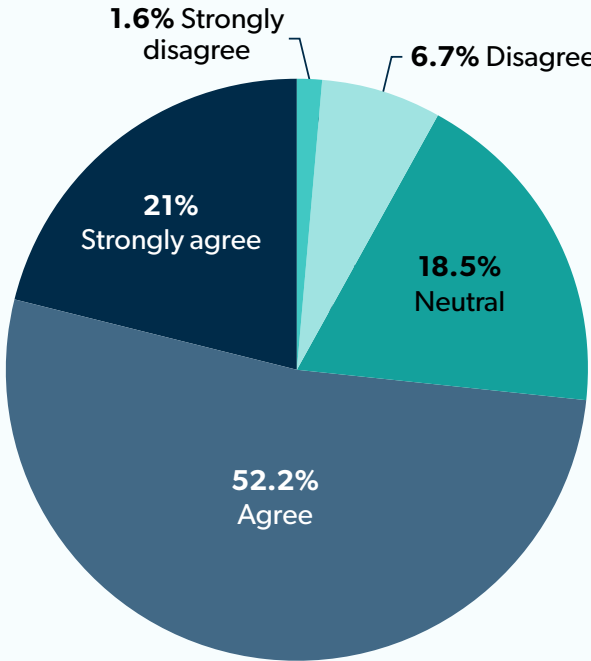- **19.2%** Neutral
- **41.9%** Agree
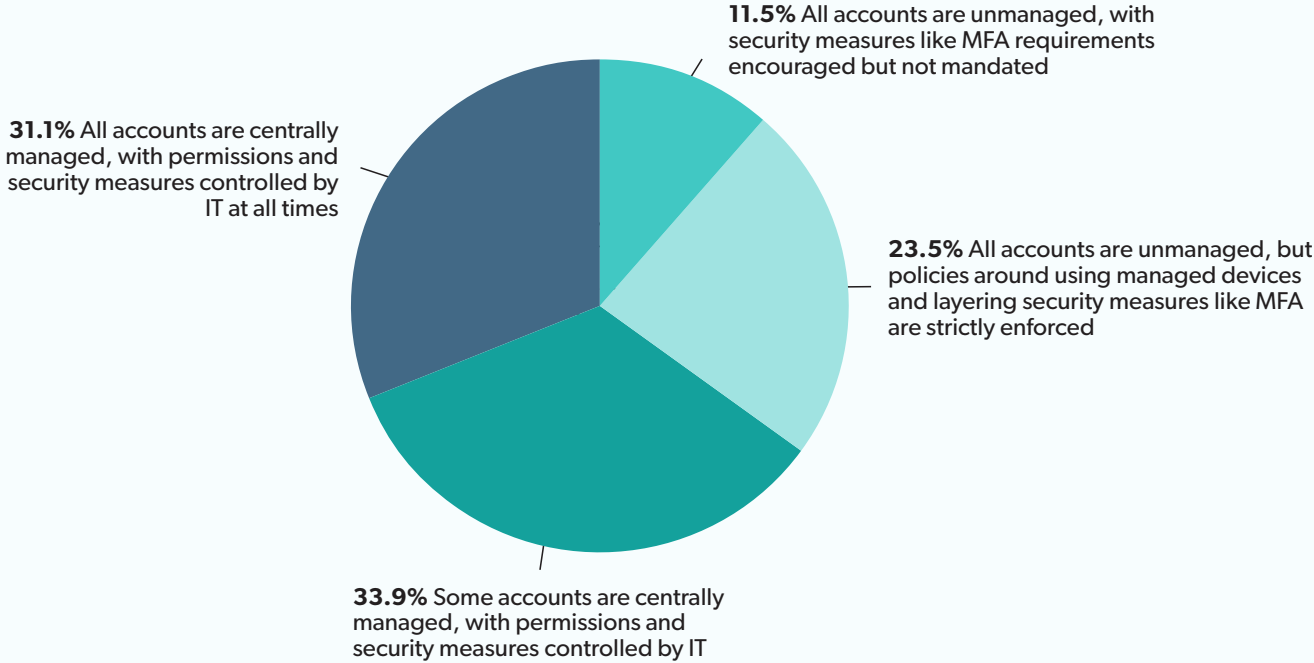
Security and SMEs

Focusing Inward

With workers logging in from around the globe, IT admins can breathe a little easier when it comes to employee education around security practices. With the complex makeup of remote, in-office, and hybrid employees, 73% agree or strongly agree that remote workers are better at following best security practices than they were a year ago. Only 8% disagree.

But despite employee awareness around issues, SMEs may still be placing too heavy of a security burden on employees. When surveyed about specific approaches to employee IT access, 12% leave accounts entirely unmanaged by IT with security practices like multi-factor authentication (MFA) encouraged but not enforced. Just 31% of accounts are fully centrally managed with permissions and security measures controlled by IT at all times.

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

- 1.6% Strongly disagree
- 6.7% Disagree
- 21% Strongly agree
- 18.5% Neutral
- 52.2% Agree

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

- 11.5% All accounts are unmanaged, with security measures like MFA requirements encouraged but not mandated
- 31.1% All accounts are centrally managed, with permissions and security measures controlled by IT at all times
- 23.5% All accounts are unmanaged, but policies around using managed devices and layering security measures like MFA are strictly enforced
- 33.9% Some accounts are centrally managed, with permissions and security measures controlled by IT
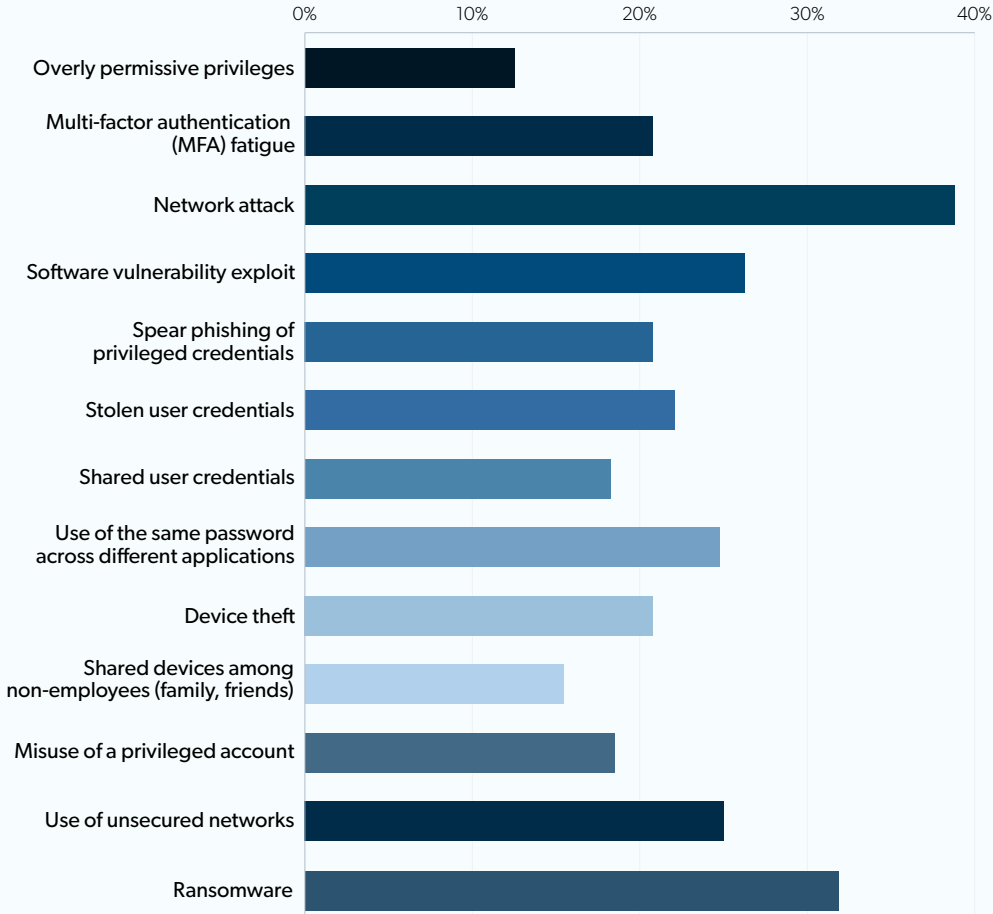
Security and SMEs
Fortifying Against External Threats

The growing sophistication of security threats continue to plague SME IT admins. External threats cause the most alarm. When asked about their biggest security concerns, network attacks topped the list (38%), followed by ransomware (33%), software vulnerability exploits (27%), and the use of unsecured networks (25%).

Of the following, please select three that are your biggest security concerns:
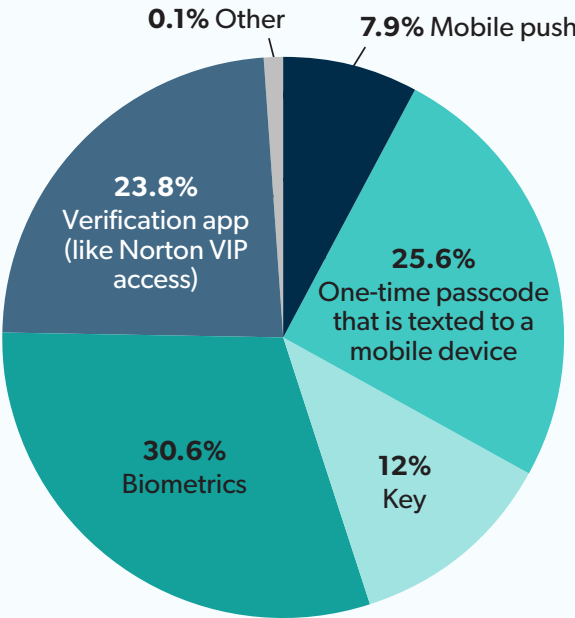
Security and SMEs

Biometrics

As more applications and other IT resources move to the cloud, SME IT admins regularly evaluate the best approaches and tools for security for employee access. For MFA, biometrics tops the list for security and convenience in the eyes of IT professionals. Three in ten (31%) of admins report they consider biometrics the most secure form of MFA, followed by one-time passcodes texted to a mobile device (26%), and a verification app (24%).

Personally, 80% of SME IT admins report using biometrics to secure their own personal devices. Of those respondents, the most commonly used biometrics are fingerprint readers (79%) and face recognition (73%), followed by voice recognition (35%). The survey suggests that admins are maximizing the use of built-in biometric readers increasingly found in devices.

Given the high rate of biometric use among admins on their personal devices, it's no surprise that IT teams are seeing organizational efforts regarding biometric authentication adoption. Over half of all SMEs (55%) say biometrics are required for employee authentication in their organization.

In your opinion, the most secure step for multi-factor authentication (MFA) is:

- **0.1%** Other
- **7.9%** Mobile push
- **23.8%** Verification app (like Norton VIP access)
- **25.6%** One-time passcode that is texted to a mobile device
- **30.6%** Biometrics
- **12%** Key

I use the following forms of biometrics for my devices (select all that apply):

- Face recognition
- Fingerprint reader
- Voice recognition
- Liveness detection
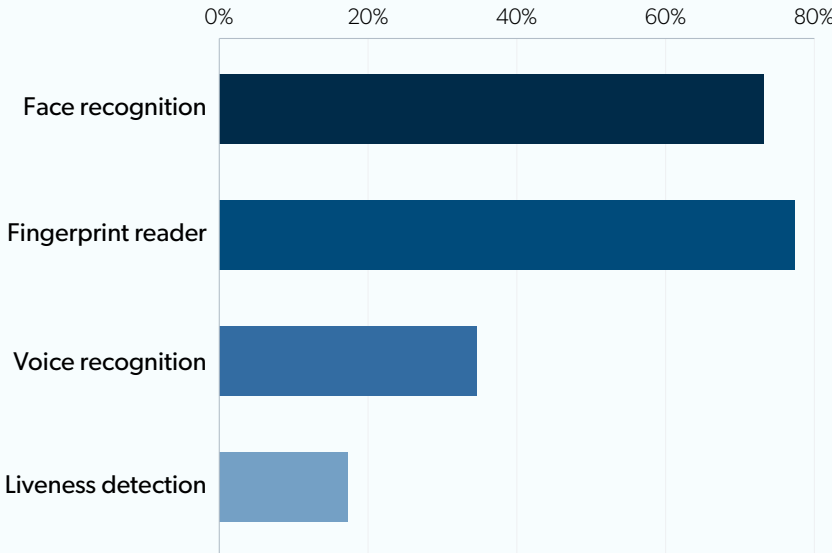
Does your organization require the use of biometrics for employee authentication?

- **1%** I don't know
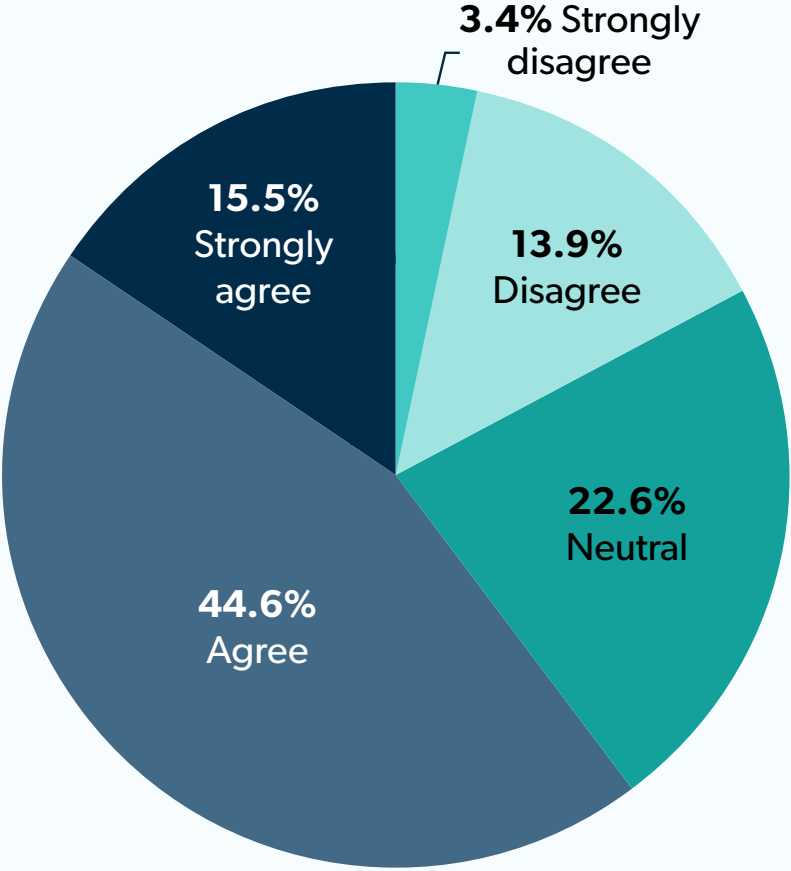- **44.1%** No
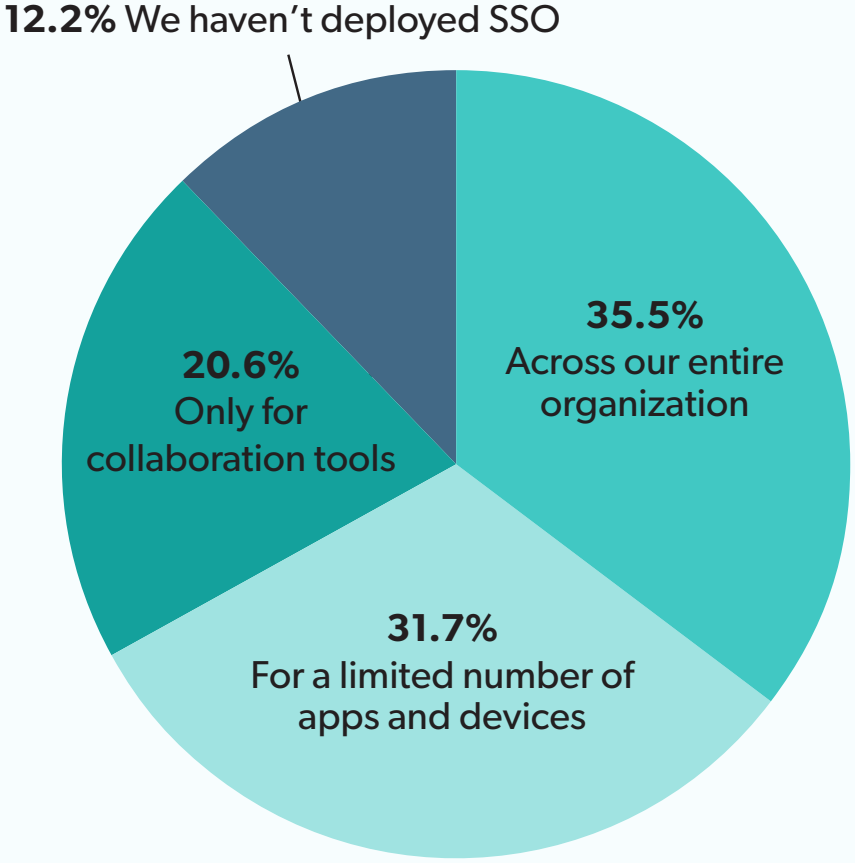- **55%** Yes
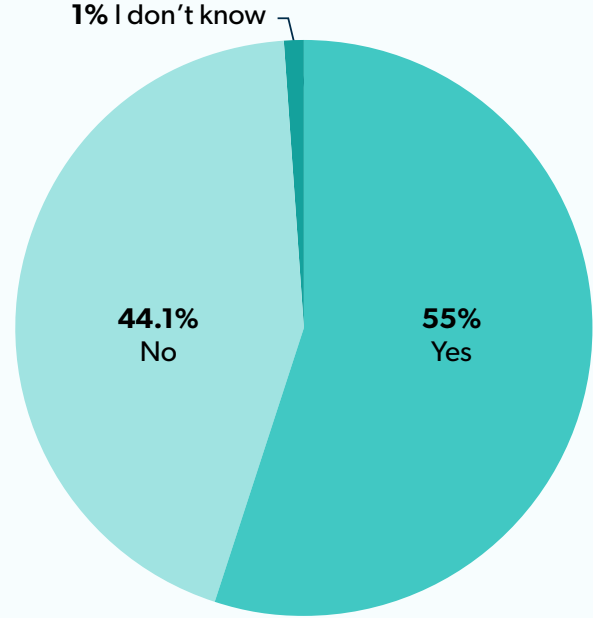
Security and SMEs

Security vs. Convenience

Part of the challenge in managing modern workforces is ensuring worker ease, productivity, and security without introducing unnecessary friction—a challenge that continues to vex many IT admins. Six in ten IT professionals (60%) agree that additional security measures generally mean a more cumbersome experience.

One popular approach IT admins at SMEs are leveraging to reduce such friction while increasing security is single sign-on (SSO). Nearly nine in 10 SMEs (88%) have deployed SSO for at least some apps in their IT stack, and 36% have deployed it across the entire organization.

Additional security measures generally mean a more cumbersome user experience.

- 3.4% Strongly disagree
- 13.9% Disagree
- 15.5% Strongly agree
- 22.6% Neutral
- 44.6% Agree

We have deployed single sign-on (SSO):

- 12.2% We haven't deployed SSO
- 35.5% Across our entire organization
- 20.6% Only for collaboration tools
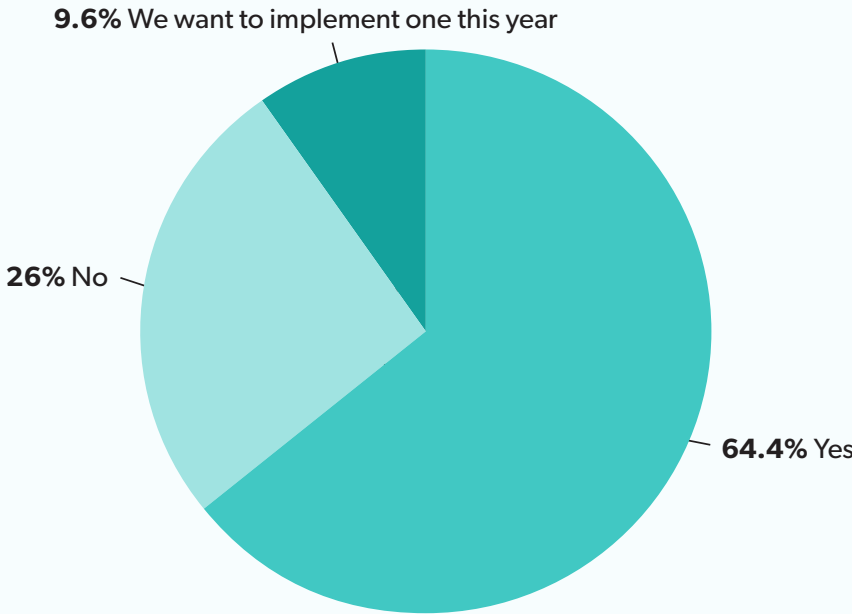- 31.7% For a limited number of apps and devices
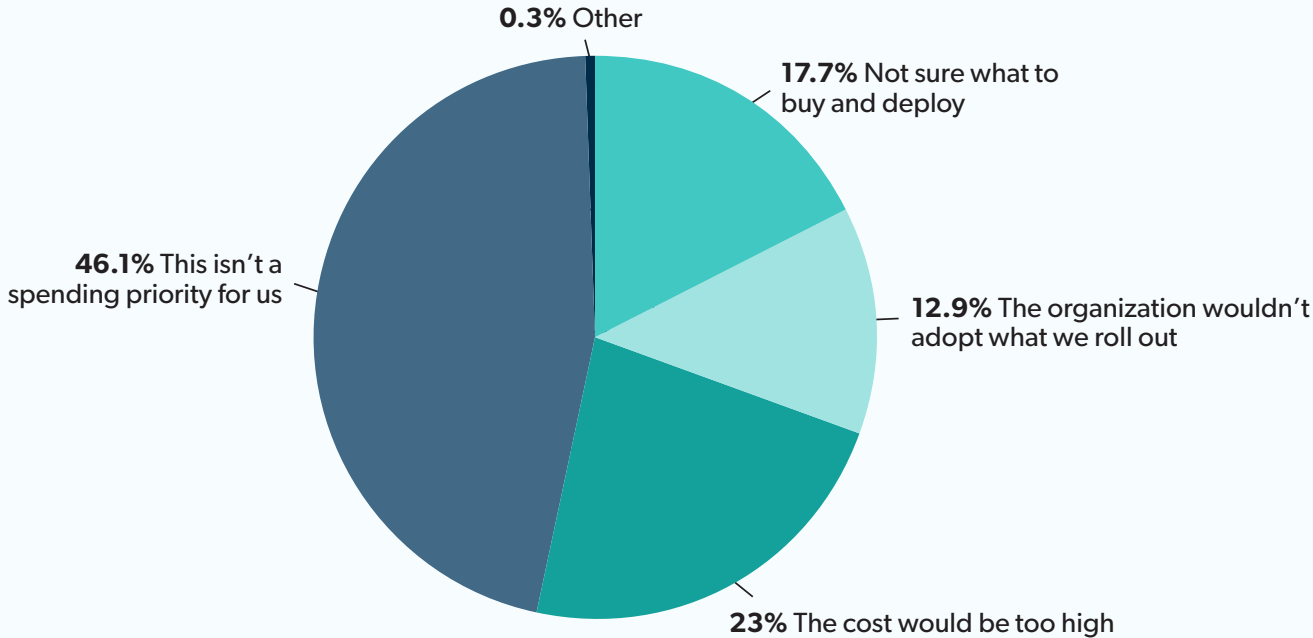
Security and SMEs

Password Management

That balance of security and convenience has led to increased industry conversation around passwordless authentication. Despite the industry chatter, many SMEs still include password-based systems for at least part of their operations and the majority have technology in place to support password management. 64% of SMEs use an organization-wide password management tool or software, and 10% plan to implement one this year.

Cost is the biggest consideration for those who don't have a password management tool and don't plan to use one, as 46% report it isn't a spending priority and 23% report the cost would be too high.

Does your organization use an organization-wide password management tool or software?

9.6% We want to implement one this year

26% No

64.4% Yes

What keeps you from deploying an organization-wide password manager?

0.3% Other

17.7% Not sure what to buy and deploy

46.1% This isn't a spending priority for us

12.9% The organization wouldn't adopt what we roll out

23% The cost would be too high
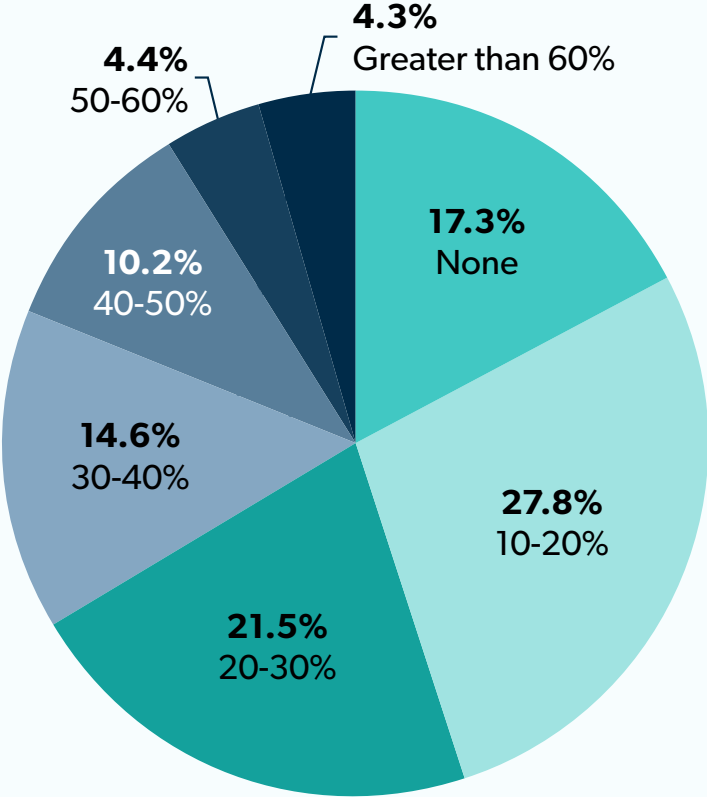
Security and SMEs

Identity and Devices

SMEs, like businesses everywhere, are embracing flexibility when it comes to their device environments. Personal device use is popular among SME IT professionals with 62% saying they use their personal device to access work-related IT resources and perform work-related tasks.

IT admins estimate that the vast majority of employees use their personal devices for work (83%).

Do you use your own, personal device(s) to access work-related IT resources and perform work-related tasks?

37.7%
No

62.3%
Yes
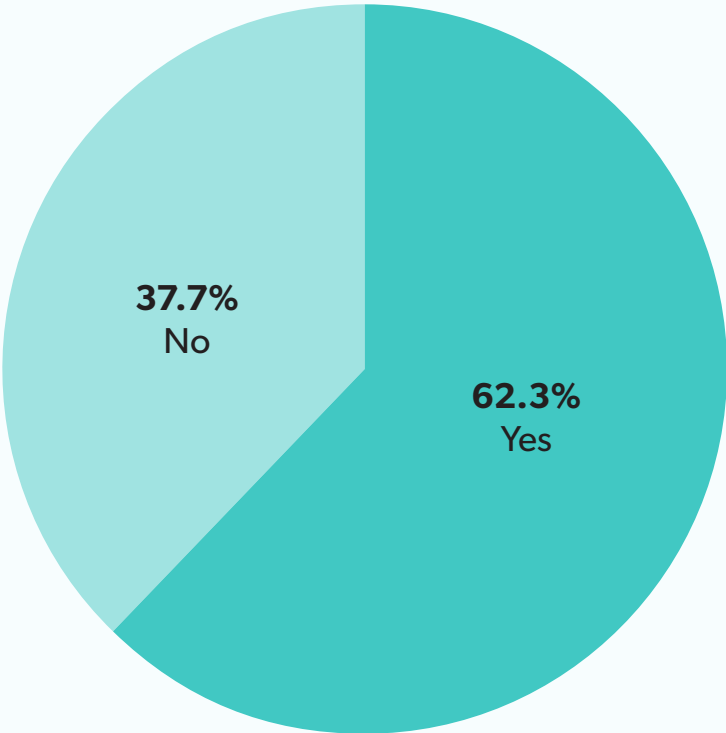
What percentage of employees would you estimate use personal devices to access work-related IT resources and perform work-related tasks?

4.3%
Greater than 60%

4.4%
50-60%

10.2%
40-50%

14.6%
30-40%

21.5%
20-30%

17.3%
None

27.8%
10-20%

Security and SMEs

Identity and Devices

To address the high rate of personal device use and the industry shift toward acceptance of bring-your-own-device (BYOD) environments, SME admins are taking a proactive IT approach. For employees using their own devices, SMEs are deploying a number of approaches to ensure strong security, including providing recommendations on secure use and access (46%), having created documented policies for employees to sign to dictate allowed access (46%), providing access to security software that can be installed on a device (45%), mandating specific security software or configurations (45%), and actively managing personal devices with a remote monitoring and management tool (RMM) or cloud directory (40%).
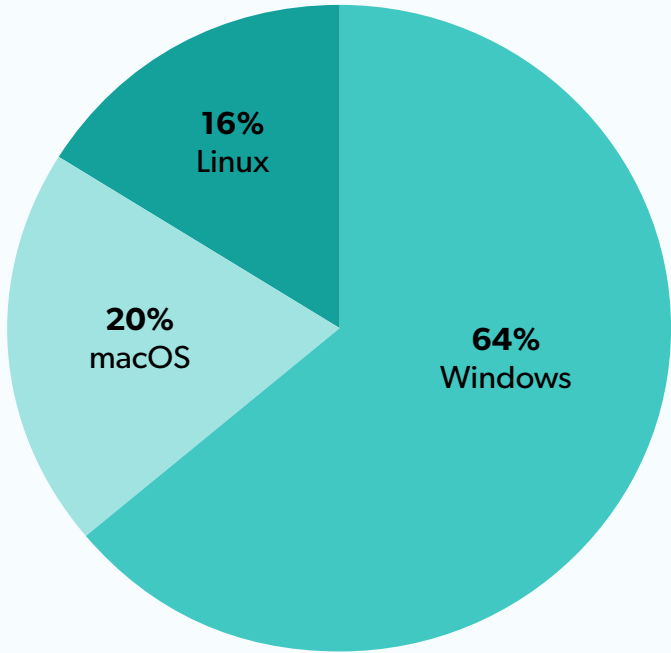
For employees using their own devices, our organization (select all that apply):
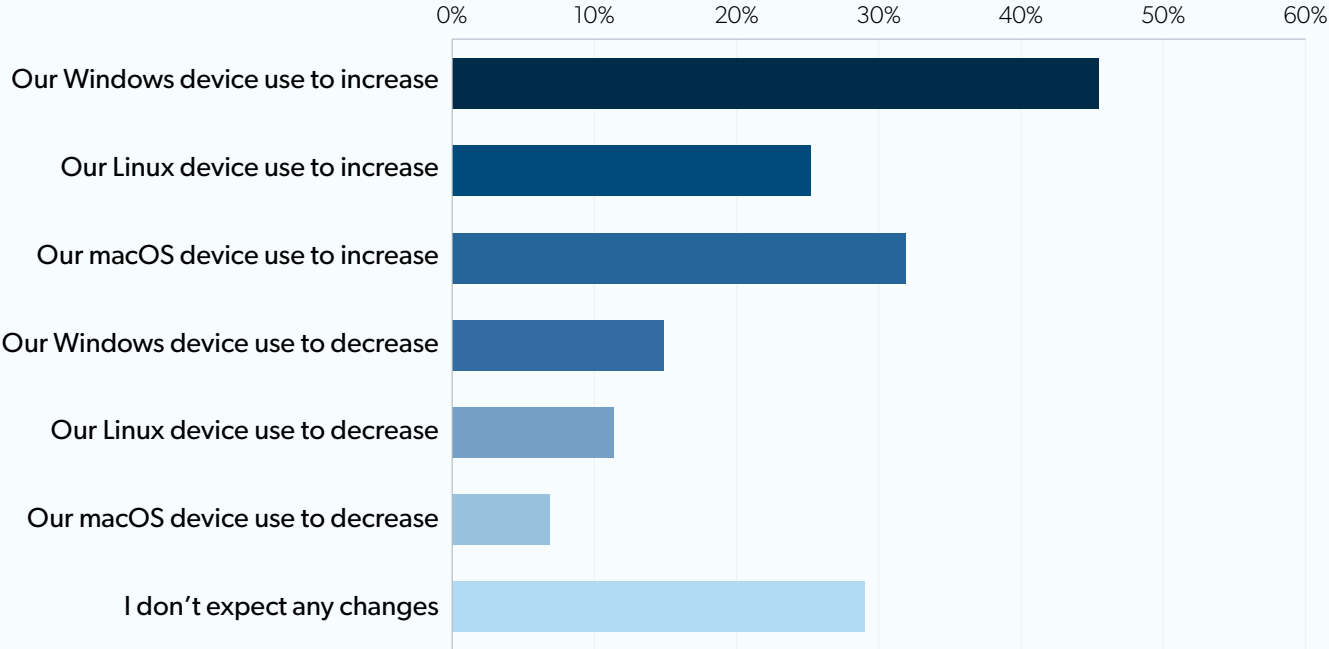
Security and SMEs

Identity and Devices

Device flexibility involves incorporating both personal and corporate devices as well as adapting to a combination of device type and different operating systems. IT admins report that SMEs currently run heterogeneous device environments, with a mix of Windows, Linux, and macOS devices. When asked about the breakdown of device type in their work environment, SME IT admins reported an average of 64% Windows, 20% macOS, and 16% Linux.

SME admins expect that the combination of device types will continue in their workplace. When asked about specific operating systems and expected use, 46% expect their organizations' Windows device use to increase, followed by a 33% expected increase in macOS, and 26% expected increase in Linux.

What is the device type breakdown of Windows/Linux/macOS devices in your workplace?

16% Linux

20% macOS

64% Windows

Over the next year, I expect (select all that apply):

- Our Windows device use to increase
- Our Linux device use to increase
- Our macOS device use to increase
- Our Windows device use to decrease
- Our Linux device use to decrease
- Our macOS device use to decrease
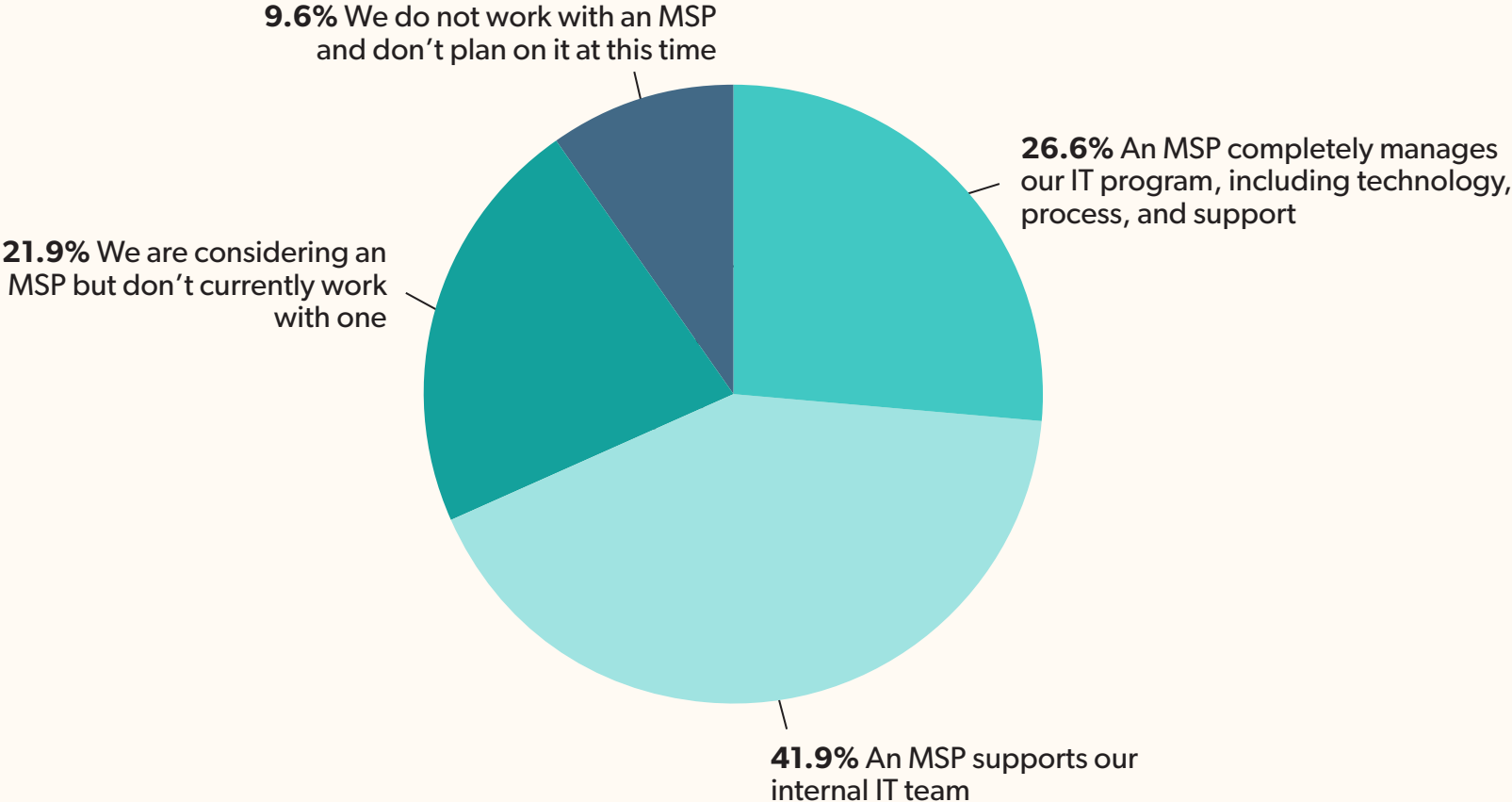- I don't expect any changes

MSPs and SMEs

MSPs Offer Outsized Support

With an increasingly complicated array of IT responsibilities, user identities, and device types, many SMEs are leaning on managed service providers (MSPs) for help. An overwhelming majority of SMEs (90%) are either already working with or considering using an MSP. For almost a third of all surveyed SMEs (27%), an MSP completely manages their IT program.

To what extent does a managed service provider (MSP) play a role in your IT program?

9.6% We do not work with an MSP and don't plan on it at this time

26.6% An MSP completely manages our IT program, including technology, process, and support

21.9% We are considering an MSP but don't currently work with one

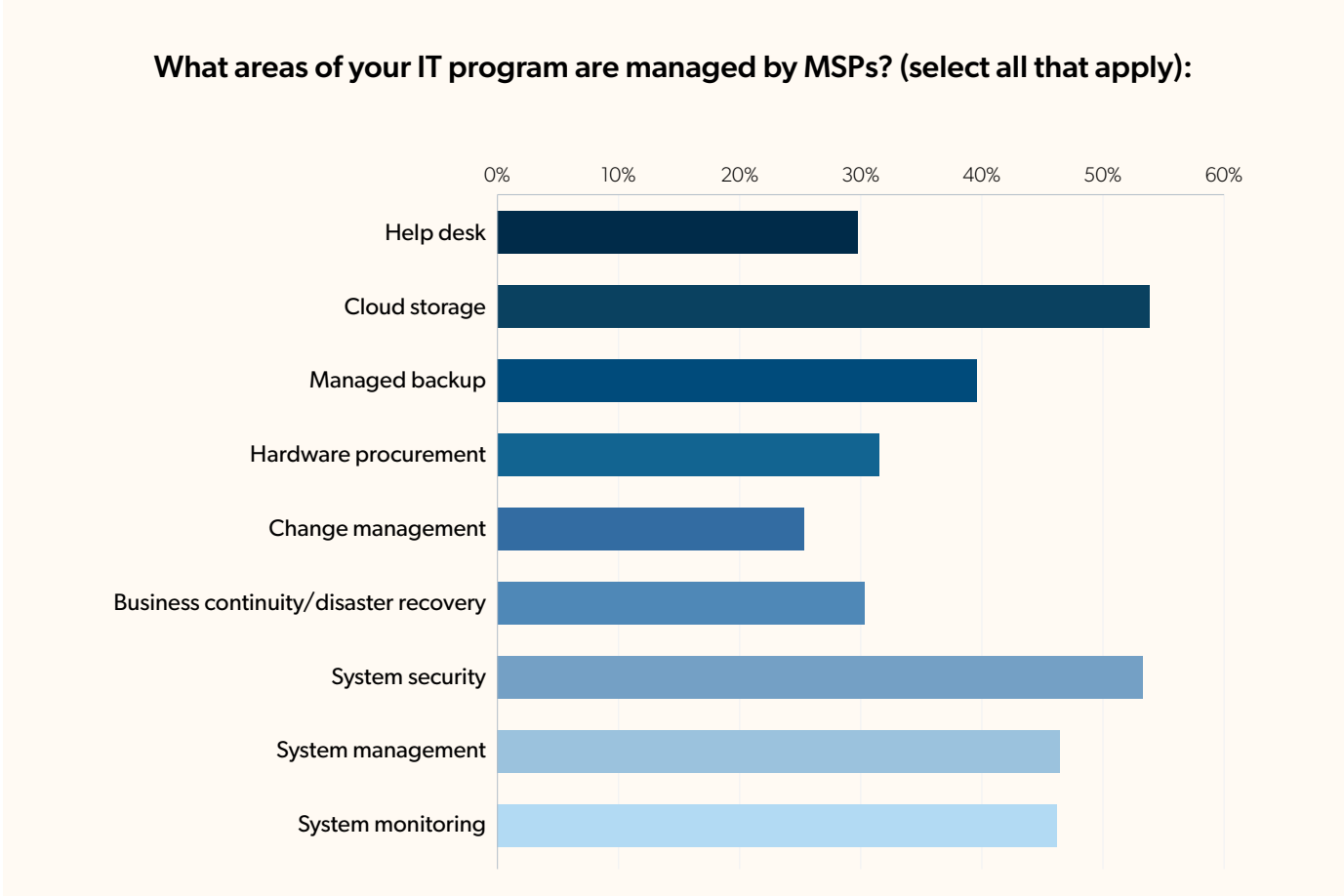**41.9%** An MSP supports our internal IT team

MSPs and SMEs

Functions and Features

For SMEs working with MSPs, the most popular reason is that MSPs are considered up to date with the latest technologies (61%), followed by MSPs providing a better user experience (55%), being cost-effective (50%), better securing users' access and identity than the SME can (41%), and offering strong customer support (22%).
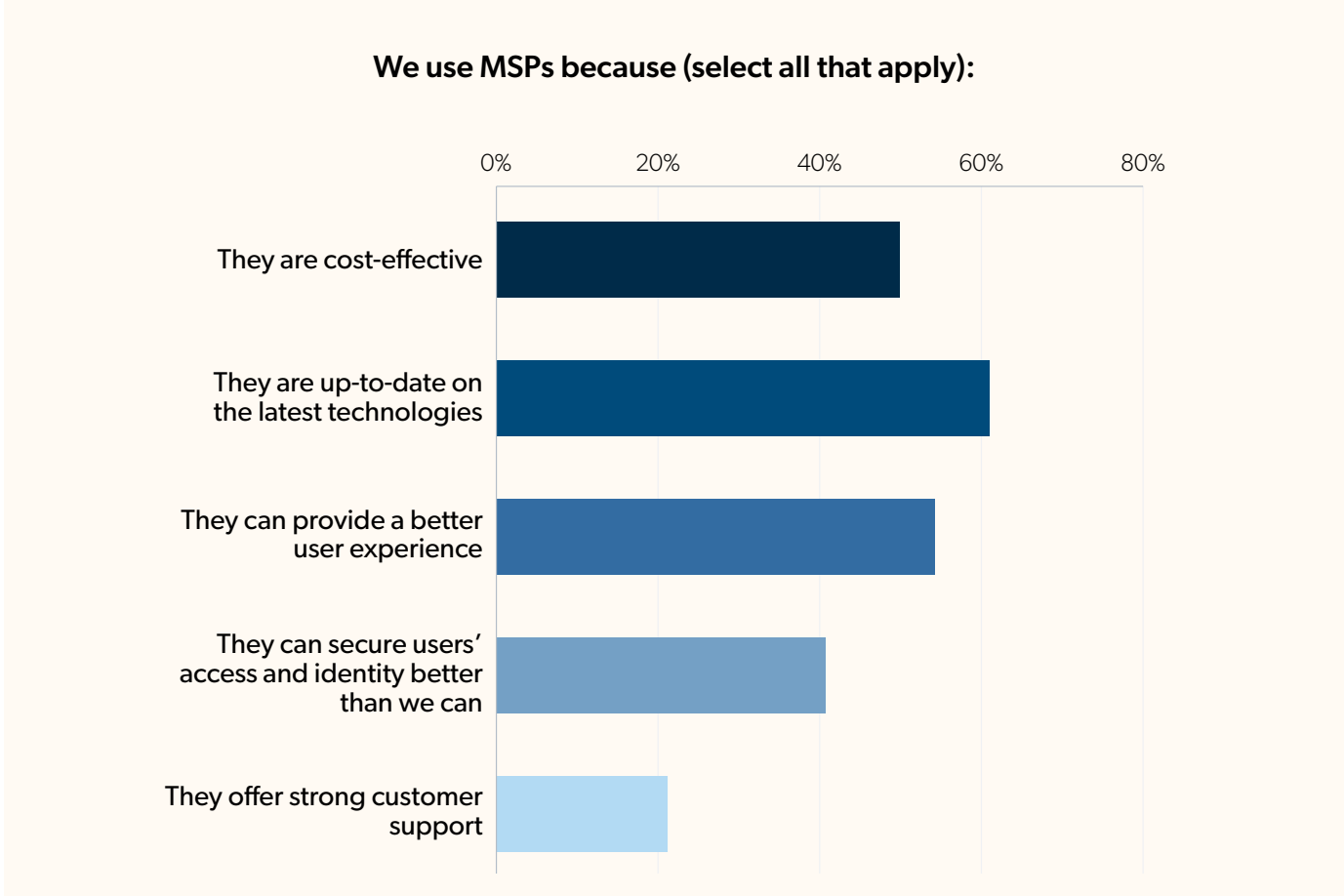
The two most common areas for which SMEs use MSPs are cloud storage (53%) and system security (53%), followed by system management (47%), system monitoring (47%), managed backup (40%), hardware procurement (33%), business continuity/disaster recovery (30%), help desk (30%), and change management (26%).
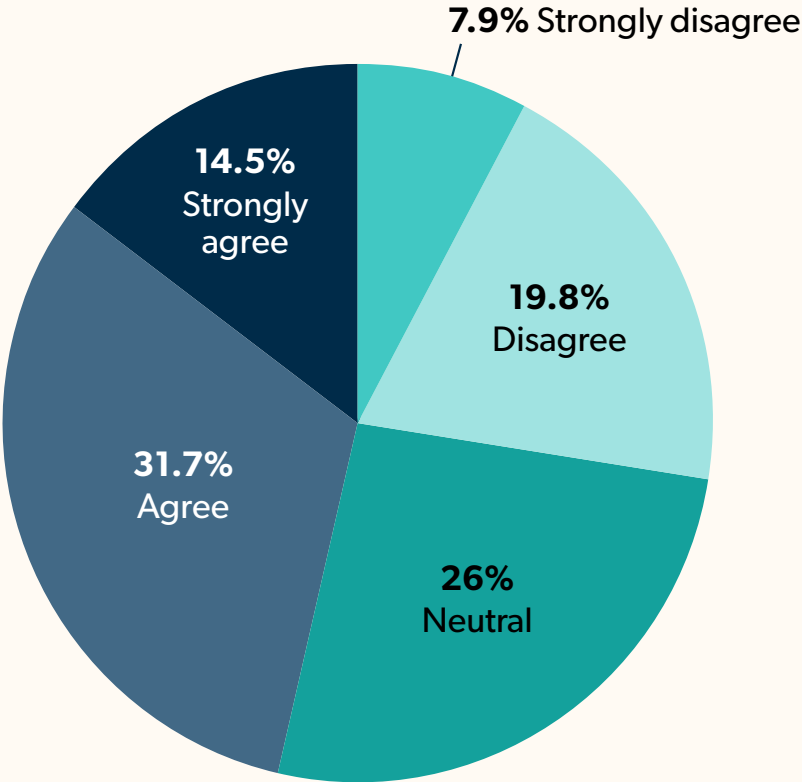
We use MSPs because (select all that apply):

What areas of your IT program are managed by MSPs? (select all that apply):
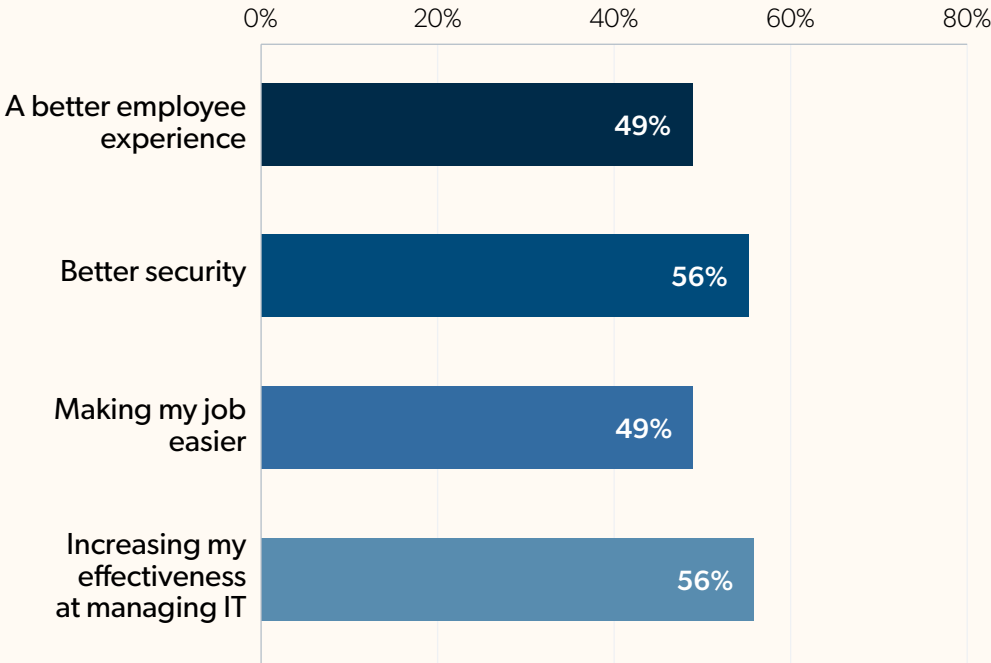
MSPs and SMEs

MSPs and Security

Despite broad use of MSPs, there remain a number of concerns about MSPs' handling of security, even from those who have seen the benefit firsthand. Nearly half of SMEs (46%) have concerns about how MSPs handle security, despite 56% of SMEs reporting that their MSP use has resulted in better security. This is why it is critical for MSPs to **start a good relationship** with their clients early.

I have concerns about how MSPs manage security:

- **7.9%** Strongly disagree
- **19.8%** Disagree
- **26%** Neutral
- **31.7%** Agree
- **14.5%** Strongly agree

Using an MSP has resulted in (select all that apply):

Category	Percentage
A better employee experience	49%
Better security	56%
Making my job easier	49%
Increasing my effectiveness at managing IT	56%

Final Thoughts

The past three years have not been easy for SMEs, and have been especially complicated for the IT professionals who make work *work*. With three years of disruption under their belts, SMEs have navigated the chaos of sudden remote work and settled into the new workplace normal. That's been possible, in large part, because of the agility and commitment of the IT admins powering it.

IT's success in leading organizations through these tumultuous times overshadows the scale of both continuing and novel challenges. These professionals rose to the challenge of completely—and urgently—overhauling organizations' workplace models to meet unforeseen needs. Now these same teams face new uncertainty around external and internal shifts, and are resolute in their commitment to preparing their organizations for whatever comes.

Security continues to be the biggest concern and priority for SMEs. The IT admins in the SME IT Trends Report offer critical insight into how organizations can better support their IT teams in their efforts to combat the challenge.

— **Listen and let IT lead on spending: IT admins are discerning about their spending.** Whether it's sharing their concern that cybersecurity cuts will undermine organizational security, or their hesitancy to spend on non-priority areas, IT teams have an acute understanding of organizational tech needs and an eye for measuring value. When admins share they're spending too much on tools to simply make work happen or that they want to invest in an MSP, organizations would be wise to listen.

— **Accommodate diverse device environments with mobile device management (MDM).** The device environment in modern SMEs requires flexibility and oversight. IT teams require tools or systems to manage Windows, macOS, and Linux devices, especially as the line between personal and work devices is virtually indistinguishable. Despite admin confidence that employees' security hygiene is improving, leaving too much responsibility on end users—whether for patching, password management, or more—leaves organizations' security susceptible to honest oversight or mistakes. A mobile device management tool centralizes device management and can ensure the most stringent security procedures and policies are in place.

— **Consolidate tools.** 77% of SME IT admins want a single tool to do their job, yet organizations continue to force them to use many more. Consolidating tools shifts an enormous tech burden, leveraging technology to manage what is a complicated, frustrating, and time-intensive process for IT admins who are overworked and overwhelmed with job responsibilities. With both security and employee experience top of mind for these admins, heeding IT's call for centralizing operations can result in a better UX for users, increased convenience and effectiveness for admins, and better security for all.

— **Optimize operations with an MSP.** MSPs' ability to deliver significant results is a belief widely shared by IT professionals: 90% of SMEs are either already working with or considering using an MSP. Whether it's better security, a better employee experience, increasing admin efficiency, or making the job of IT easier, SME admins are reporting broad MSP benefits. Now may be the time for organizations to evaluate how they might initialize or deepen their MSP investment to best leverage partner expertise for better overall IT operations.

As we head into the second half of 2023, IT teams remain committed, innovative, and responsive to the evolving needs of today's SMEs. Listening to these practitioners' experiences, wants, and fears offers organizations an incredible opportunity to build an IT environment capable and flexible enough to withstand whatever comes next.

JumpCloud's commitment is to Make Work Happen®. Designed and built for SMEs, JumpCloud offers an open directory platform that delivers enterprise-level IT management without enterprise-level cost or complexity. To get started with JumpCloud immediately, for free, visit **console.jumpcloud.com/signup**.

Methodology:

JumpCloud surveyed 1,221 SME IT decision-makers in the U.K., U.S., and France, 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 online survey was conducted by Propeller Insights, May 12-24, 2023.

JumpCloud® helps IT teams **Make 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.

Try JumpCloud Free →