eBook

jumpcloud™

Managing IT Amidst Rising Security Threats and Global Turbulence for Small to Medium-Sized Enterprises

Small to medium-sized enterprise (SME) IT admins remain committed to delivering a secure and solid experience as they navigate additional responsibilities and impacts of internal and external change

Executive Summary

Nearly three years after the onset of the pandemic, businesses are facing additional challenges and increasing disruption caused by world events. Inflation, labor shortages, recession talks, market volatility, and global conflicts are just a few of the external impacts companies are absorbing. Internally, there's not a lot of respite. Staff fatigue, increased job pressures, budget concerns, and rising security risks add pressure to operations, introducing uncertainty for companies of all sizes, especially SMEs. Despite the challenges, SMEs retain their optimism, with two-thirds **expecting** to see revenue increases over the next year, and over half planning to expand their business.

Taking a closer look at SMEs may reveal a bit about why these companies are feeling more hope than gloom about their future. Behind the scenes are IT departments that continue to power day-to-day operations after migrating whole workforces to entirely new models. They are protecting company resources and making employees' day-to-day experience pleasant and productive.

Despite both internal and external events, SMEs are positioning themselves for success in large part due to the achievements of the IT teams that make it possible. For connected SMEs, the simple-sounding charge of IT teams — to enable users to securely access what they need — belies an almost Herculean level of responsibility. IT professionals are successfully managing complicated tech stacks, balancing complex device environments, and fending off ever-evolving security threats from all directions.

Today's IT teams are bearing these responsibilities and keeping an eye on what's coming next. For the past three years, IT teams have learned to adapt quickly to new information, new technologies, and new global developments. Our most recent edition of the *SME IT Trends* report highlights that IT teams in today's SMEs are dedicated and agile, prepared for the unexpected, and passionate about securing their organizations' employees, devices, and data. They're overwhelmed but happy, working overtime though they're pursuing better work-life balance, and they're more committed than ever to delivering a premium user experience.

IT teams are often the engine that powers everything for SMEs. Because their role and value cannot be overstated, JumpCloud commissions this ongoing research to gain critical visibility into the lives, responsibilities, and work of these professionals.

The Q4 2022 edition finds:

- Growing complexity of internal and external environments is putting pressure on modern workplaces.
- How IT is responding with flexibility, agility, and adaptability in the face of rising security risk and market uncertainty.
- The tools and approaches IT wishes they had and how organizations can better support them.
- How teams are meeting today's security challenges and how they're preparing for tomorrow's.

The end of 2022 reveals incredible resilience and innovation at the core of today's SMEs, and great innovation, adaptability, and tenacity at the heart of SME IT operations.

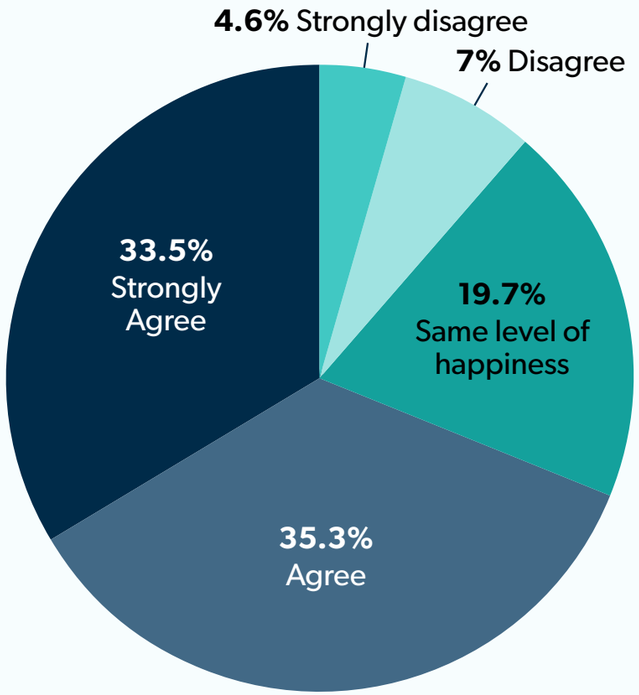
The Modern SME Landscape

IT Admins Overwhelmed but Happy

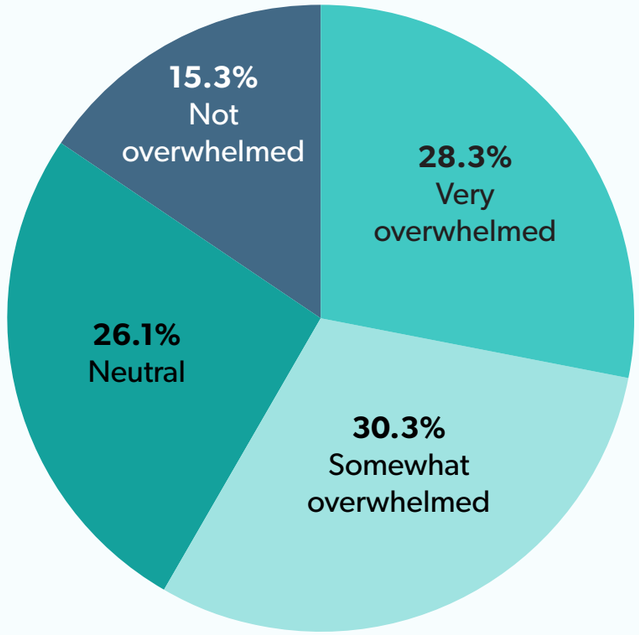
Despite all of the unexpected disruptions, most IT pros are happy, as 88.5% of admins say they are as happy, or happier in their job now compared with one year ago.

As IT admins' responsibilities cover fully remote, in-person, and hybrid models, the job still isn't an easy one. Now, 58.6% report feeling somewhat or very overwhelmed, compared to 56.3% in October 2021. And more (28.3%) are feeling very overwhelmed compared to 14.4% who reported feeling so in October 2021.

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



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



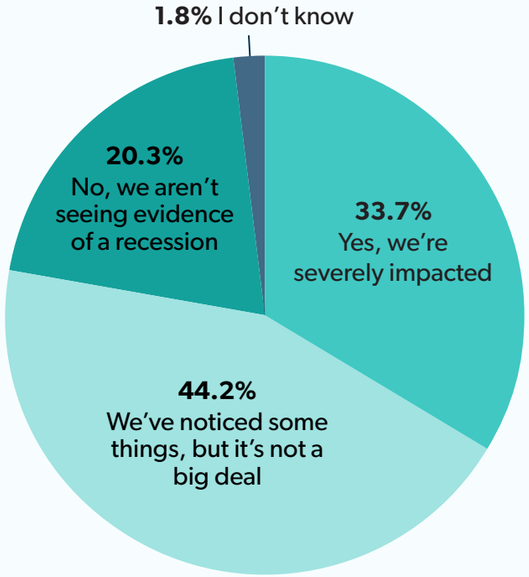
The Modern SME Landscape

Uncertainty Everywhere

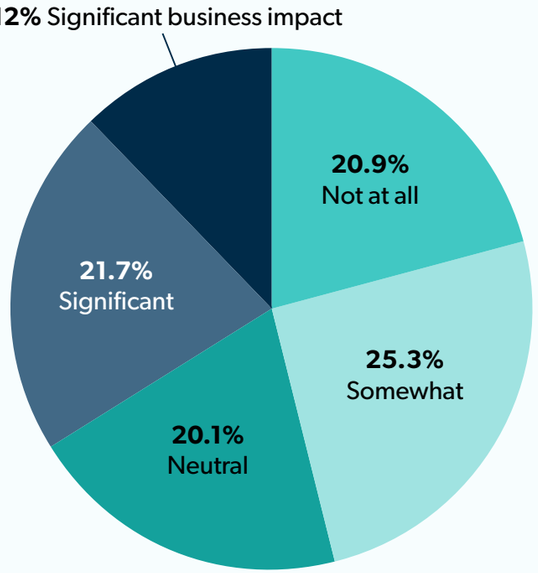
Market and global turbulence was present six months ago, but recent disruptions have been more acute. Recession worries aren't sparing SMEs as 77.9% report seeing evidence of a recession in their business, and 33.7% say their organization is severely impacted.

Despite increased economic worries and the potential for a weak labor market, over one-third (33.7%) of IT admins report that labor shortages are making a significant business impact or are a serious business limiter.

Is your business seeing evidence of a recession?



Have labor shortages been an issue for your business?



The Modern SME Landscape

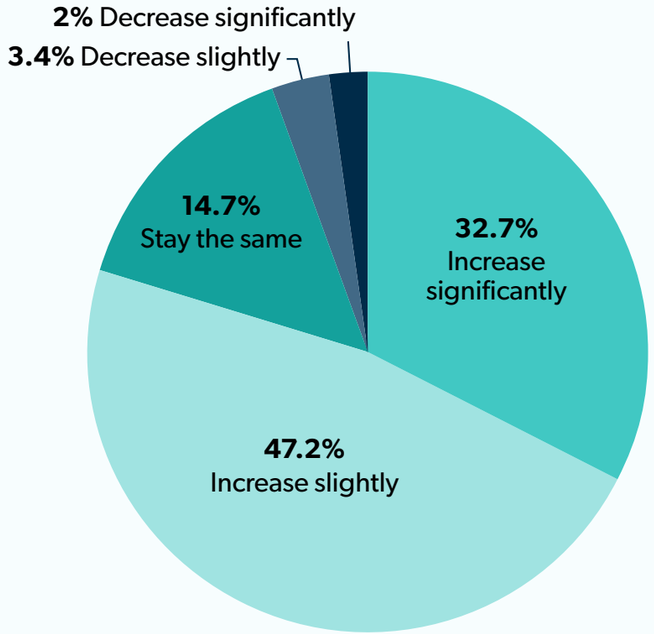
Stability in the Chaos

Though labor and recession worries are creeping up, IT spending has been strong and IT admins expect it to continue. Overall, 79.9% of general IT budgets are expected to increase, and only 5.4% expect to see budget decreases. 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.

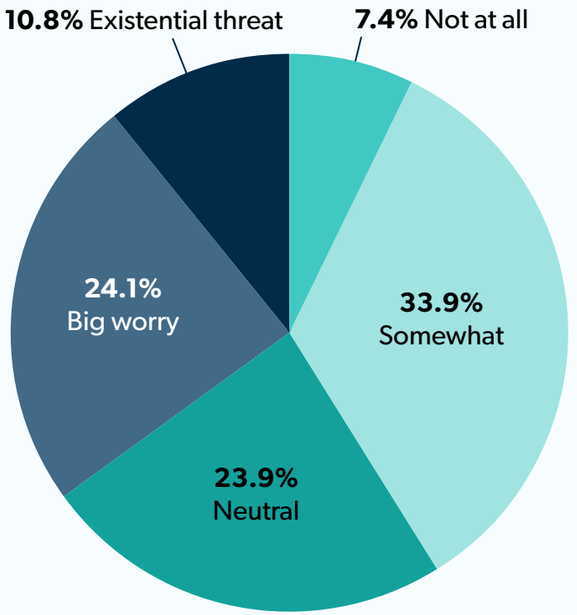
Inflation isn't as concerning for IT, as 7.4% say they're not at all worried about inflation compared to 4.2% who said the same in April 2022, and fewer are reporting it's a big worry (24.1% now vs. 28.9% in April). To make sure your business is set for whatever 2023 may bring, check out our IT Admin's 2023 Planning Kit.

To make sure your business is set for whatever 2023 may bring, check out our IT Admin's 2023 Planning Kit.

In 2023, I expect our IT budget to:



How big a worry for your business is inflation?

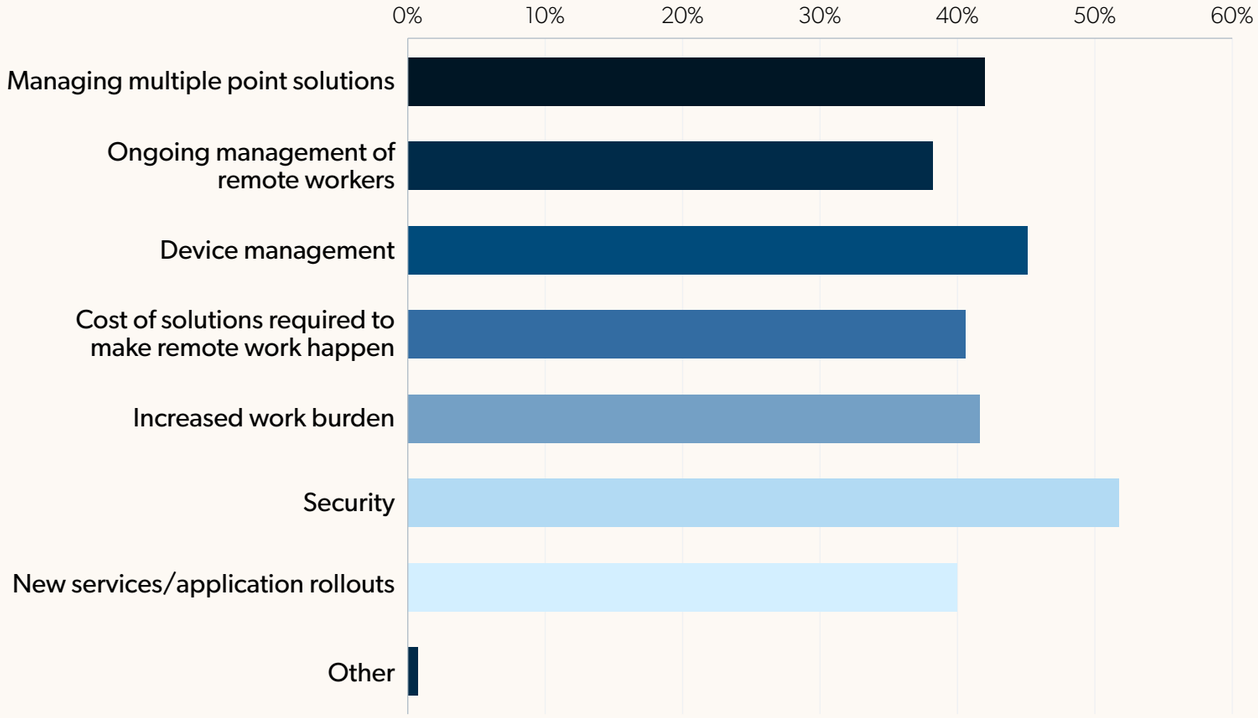


Securing the SME

Rising Security Threats Cause for Concern

Security continues to be the top concern for SME IT admins, with 52.4% saying it's their biggest challenge over user management, budget, and workplace concerns.

What have been the biggest challenges to your IT team since April of 2022? (select all that apply):

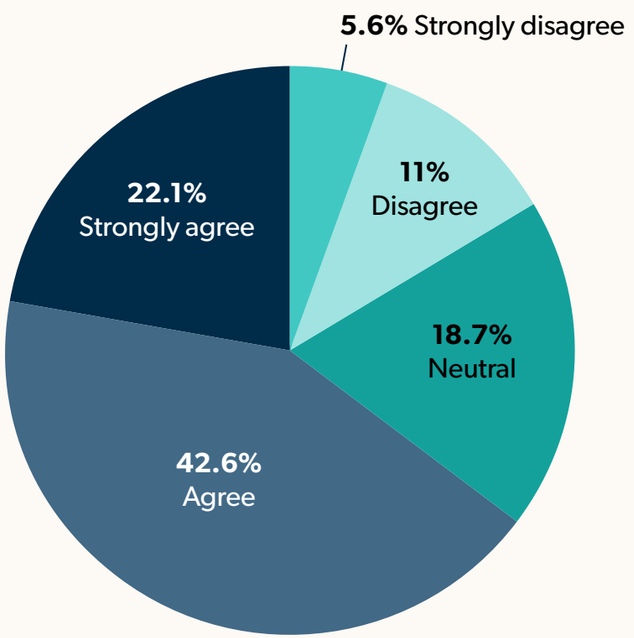


Securing the SME

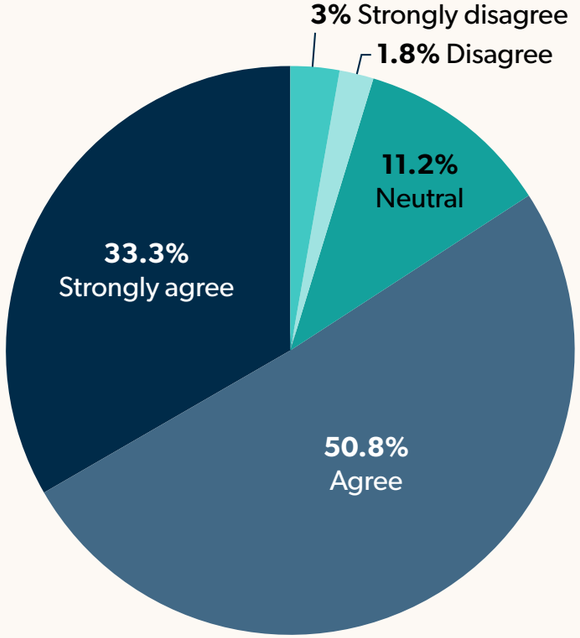
Rising Security Threats Cause for Concern

Part of the challenge is the balance between security and user experience. More admins (64.7%) agree that additional security makes a more cumbersome experience, up from 54.2% in October 2021. And the number of admins who *strongly* agree that additional security makes a more cumbersome experience is up to 22.1% from 18.2% in April 2022. Despite this, IT admins aren't simply allowing their employees to suffer with friction: a vast majority (84.1%) agree that employee experience is an important factor in making IT purchasing decisions.

Additional security measures generally mean a more cumbersome user experience.



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

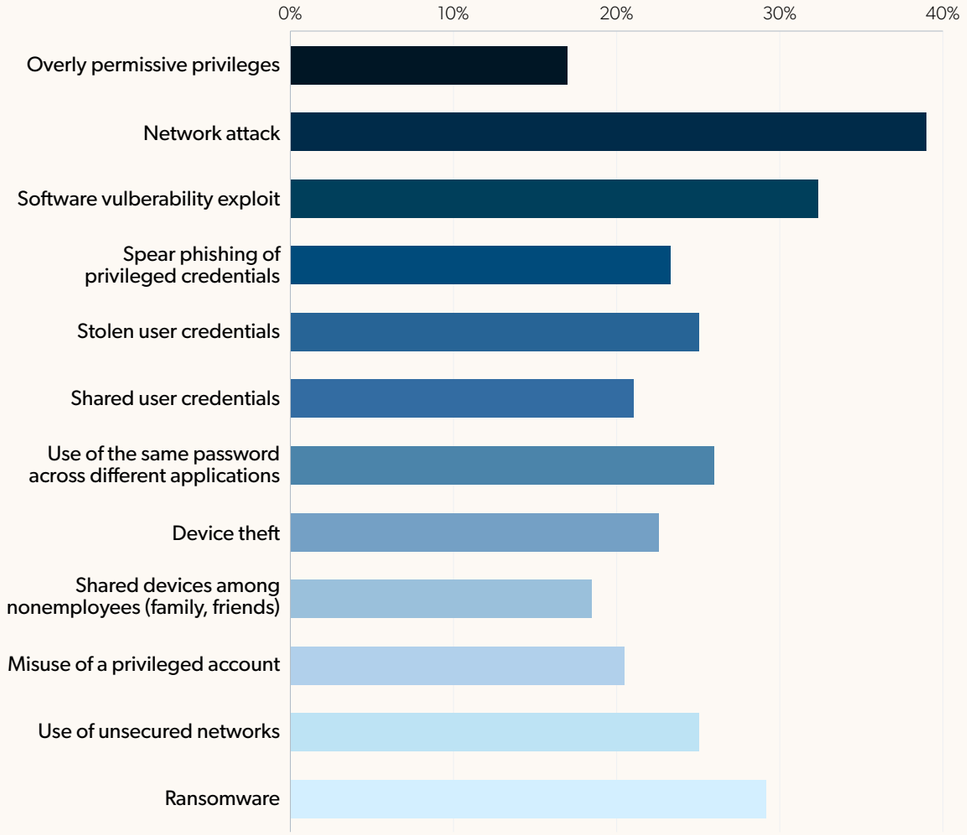


Securing the SME

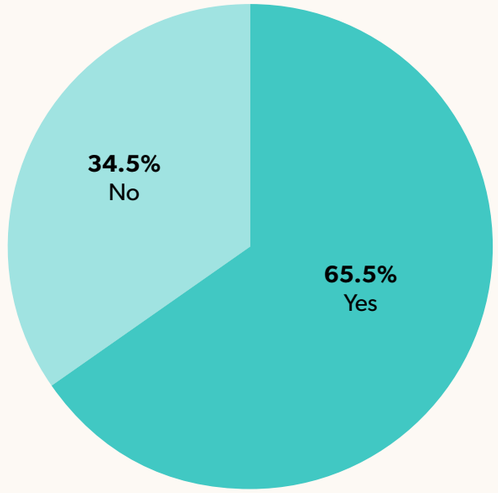
Continued Concern About External Threats

It's no surprise to learn that security concerns plague so many IT admins when we look at the number and variety of threats coming from every direction. The top three security concerns are a network attack (39.6% now vs. 40.1% in April 2022), software vulnerability exploit (32.1% now vs. 29.2% in April 2022), and ransomware (29.3% now vs. 28.3% in April 2022). Nearly 66% report concerns about multi-factor authentication (MFA) fatigue attacks, a process that exploits one-time passwords and push notifications.

Of the following, please select three (3) that are your biggest security concerns:



Are you concerned about MFA fatigue attacks?



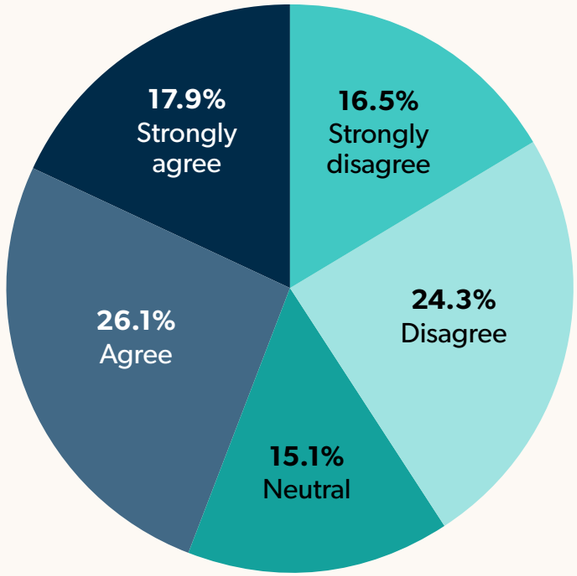
Securing the SME

Internal Issues

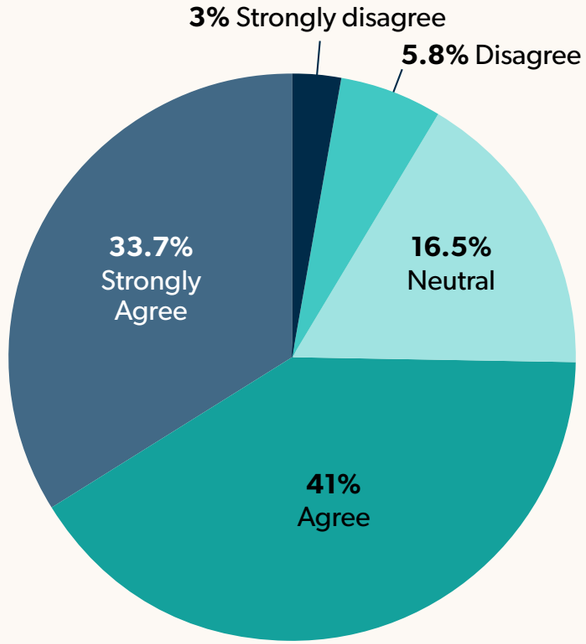
Despite IT admins' confidence in organizational financial support of their department, a plurality worry that cybersecurity-specific funding might be at risk: 44% agree their organization will cut spending on cybersecurity in the next year compared with 40.8% who disagree.

With the accelerated rate of attacks on SMEs and the **sophisticated evolution** of external threats, IT admins are concerned that such cuts will make organizations more vulnerable: 74.7% say cuts to their organization's security budget will increase organizational risk.

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



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

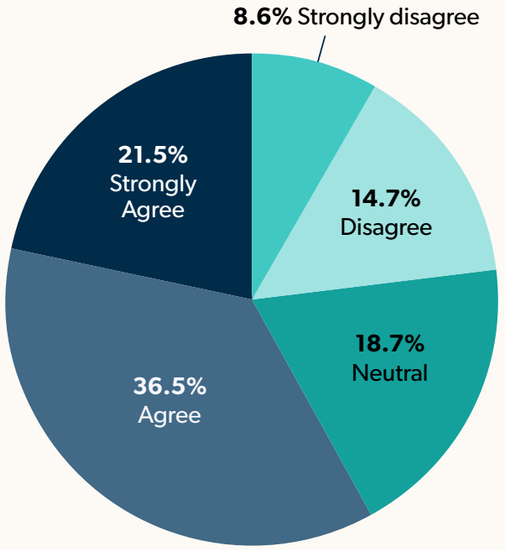


Securing the SME

Internal Issues

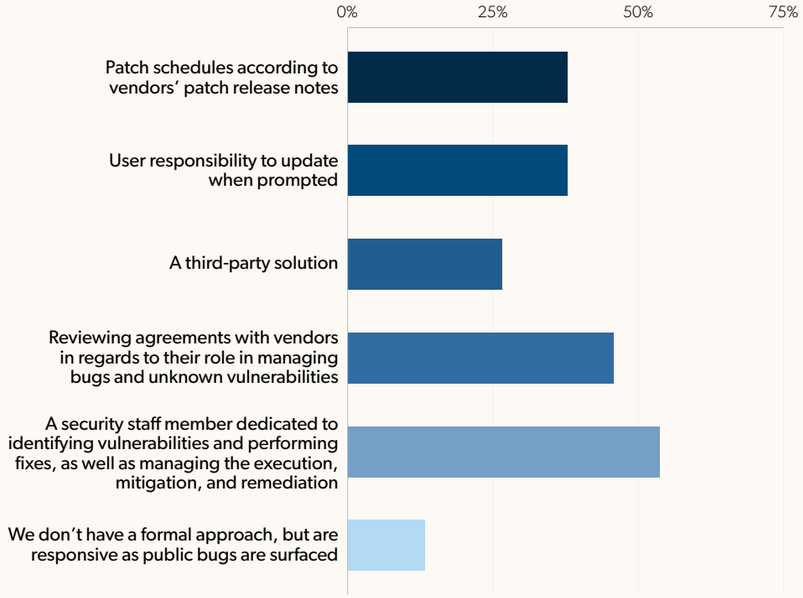
Though hybrid and remote workplace models are well established, and employees have had a chance to adjust, IT teams are still concerned about the potential risk that employees may inadvertently introduce. Fifty-eight percent agree that hybrid work makes it harder for employees to follow good security practices, which hasn't changed much from the 60.1% who agreed in October of 2021 or the 58% who agreed in April of 2022.

I think that hybrid work makes it harder for employees to follow good security practices.



Possibly to address these vulnerabilities, IT admins are integrating software and systems to mitigate such risk. One such example is patch management, where now a majority (56.8%) employ a security staff member dedicated to identifying vulnerabilities and performing fixes, as well as managing execution mitigation and remediation, up from 45.8% in April 2022.

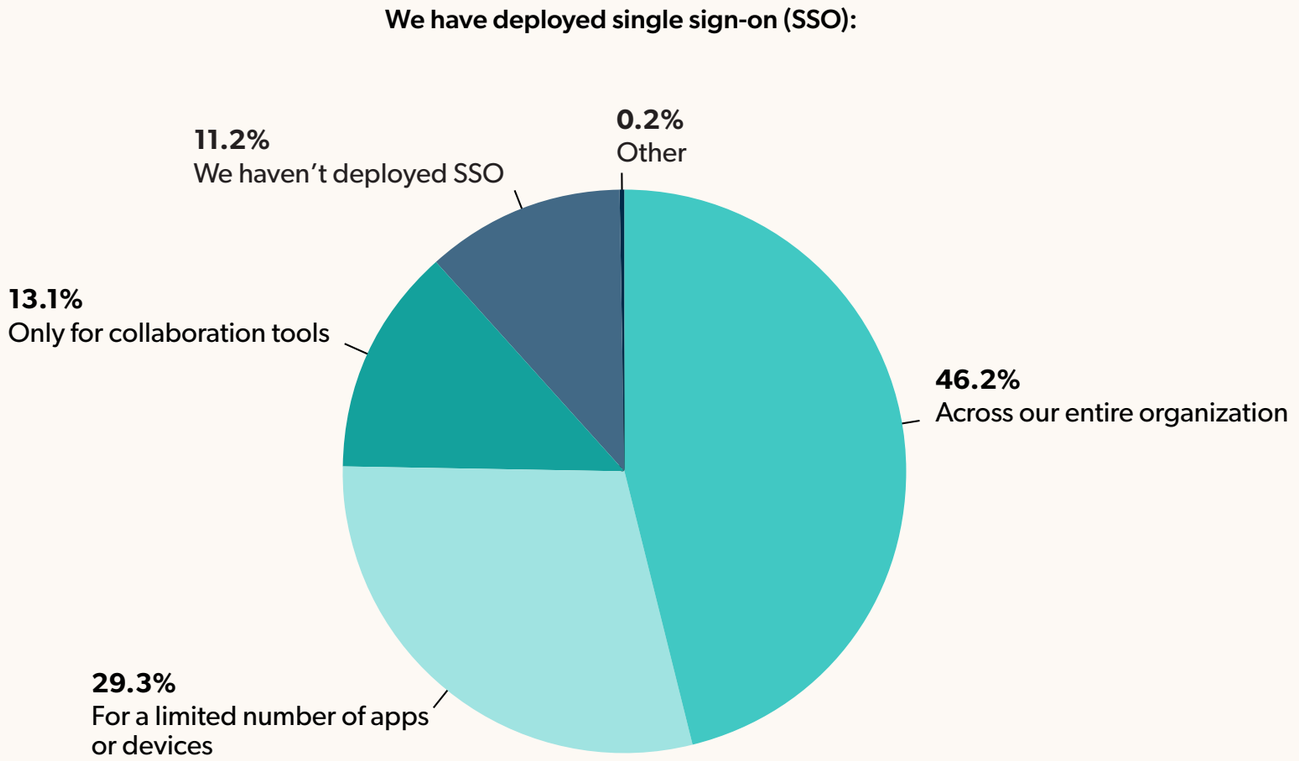
My organization uses the following for patch management (select all that apply):



Securing the SME

Centralizing Authentication

Single sign-on (SSO) adoption continues to increase as SMEs look to simplify and streamline the login process. Consider that in April of 2021, only 20.4% had implemented SSO. Now, eighteen months later, only 11.2% say they haven't deployed SSO at all, and 46.2% report that SSO is required across the entire organization, up from 33.9% in April of 2022.



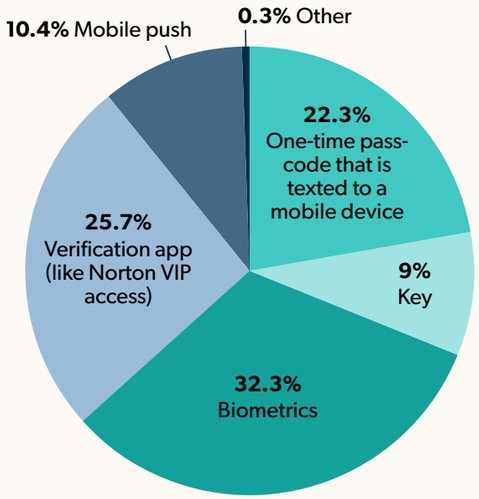
Securing the SME

Multi-Factor's Many Factors

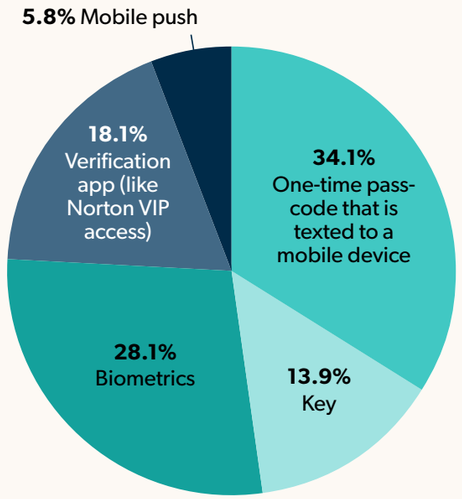
IT admins are regularly evaluating and updating based on perceived pros and cons of different MFA methods. One-time passwords (OTP) are no longer seen as most secure but still the easiest for end users; in April 2022, 31.4% said it was the most secure MFA method, now only 22.3% agree. But OTP is still seen as the easiest for users (34.1% vs. 37.9% in April 2022).

Biometrics secure the top spot for MFA methods, seen as the easiest to use, but still viewed as the most complicated for admins to implement. Thirty-two percent agree (up from 28.5% in April 2022) that biometrics are the most secure MFA method, though they're still seen as the most complicated MFA method for IT admins to implement (34.3% agree, down from 35% in April 2022). Biometrics are now seen as the second easiest MFA method for users (28.1% agree it's the easiest now vs. 24.1% in April 2022), bested only by OTP.

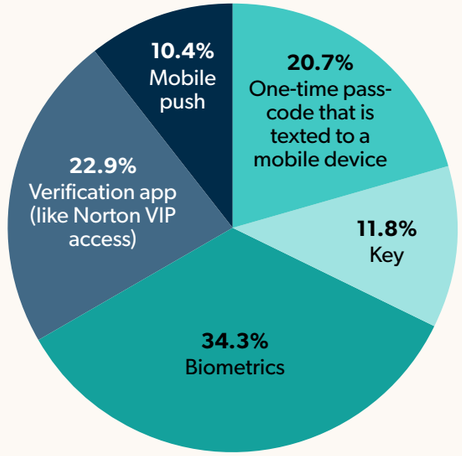
In your opinion, the most secure step for multi-factor authentication (MFA) is:



The easiest step for users for MFA is:



The most complicated MFA to integrate for IT admins is:



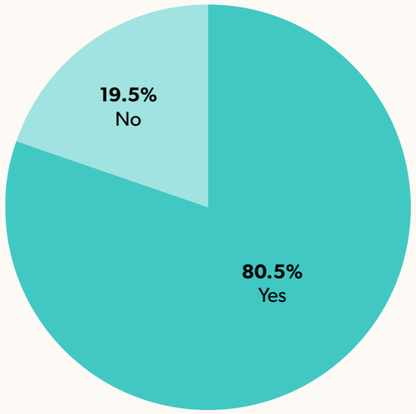
Securing the SME

Biometrics are Big

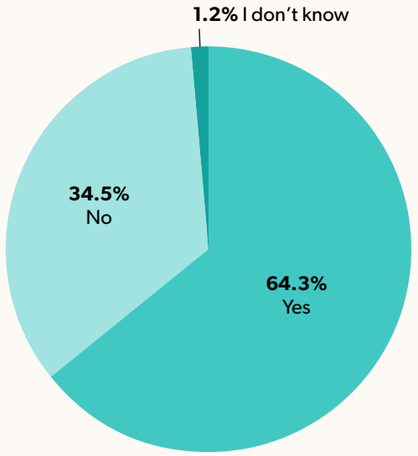
Biometrics continue to increase in their popularity among SME IT admins, who overwhelmingly use biometrics for personal devices: 80.5% use biometrics to secure personal devices, up from 73.9% in April 2022. Fingerprint recognition is the most commonly used (76.7%) followed by face recognition (74.5%), voice (48.5%), and liveness detection (23.8%).

Organizational use of biometrics is on the rise with 64.3% who say their organizations require biometrics for employee authentication, up from 58.5% in April 2022.

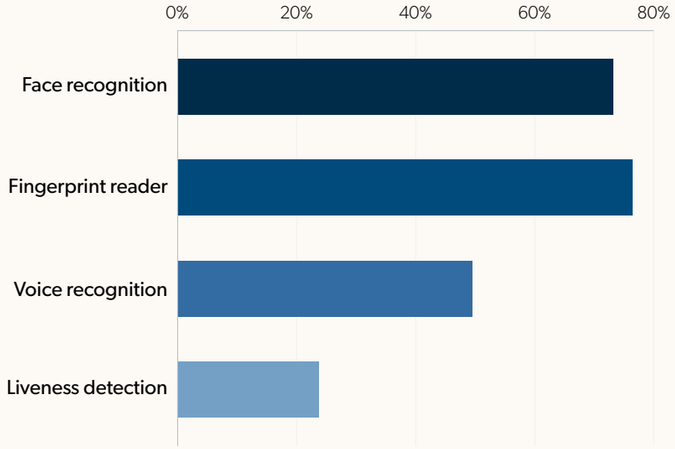
I use biometrics to secure my personal devices.



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



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



Securing the SME

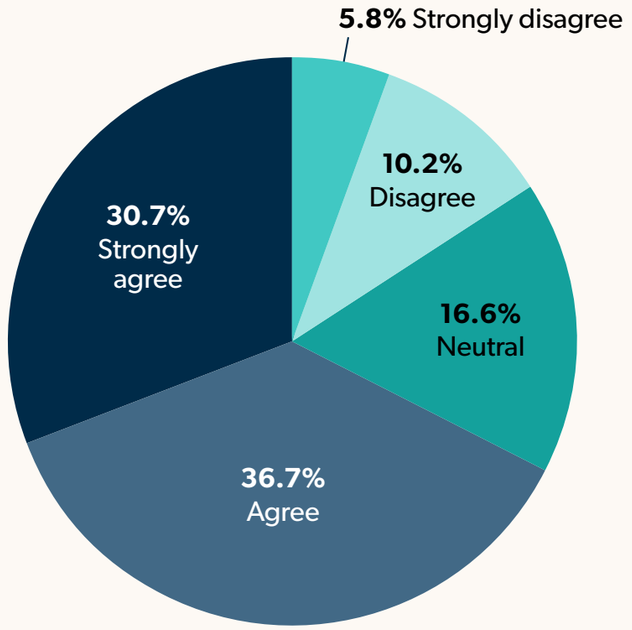
The Journey to Passwordless

The rise in adoption of biometrics in authentication may be a solution for better balancing the employee experience and security, especially as the push toward passwordless authentication has commanded center stage for much industry discussion.

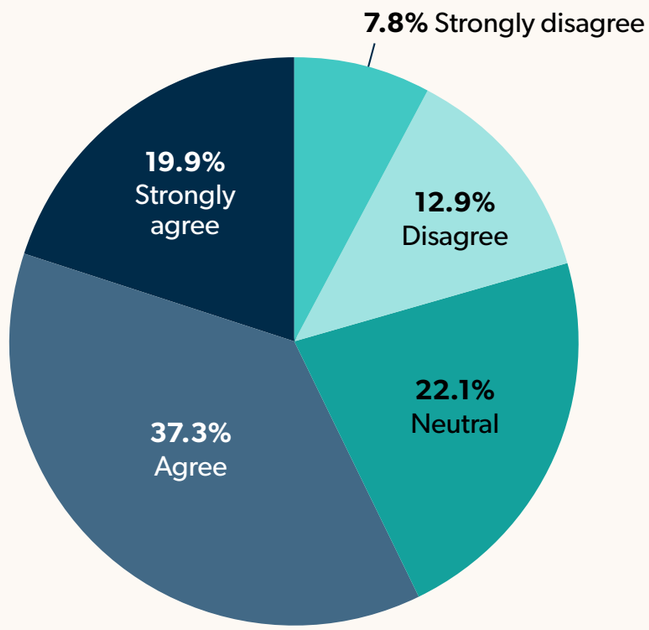
Passwordless is getting more popular across the SME, with 67.4% reporting that passwordless authentication is a priority for their organization, up from 64% in April 2022.

At the same time, IT admins remain skeptical of passwordless. Fifty-seven percent view passwordless as more of an industry buzzword than an IT priority, which is a slight increase of those who agreed when asked the question in April 2022 (52.6%).

Passwordless authentication is a priority for our company.



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

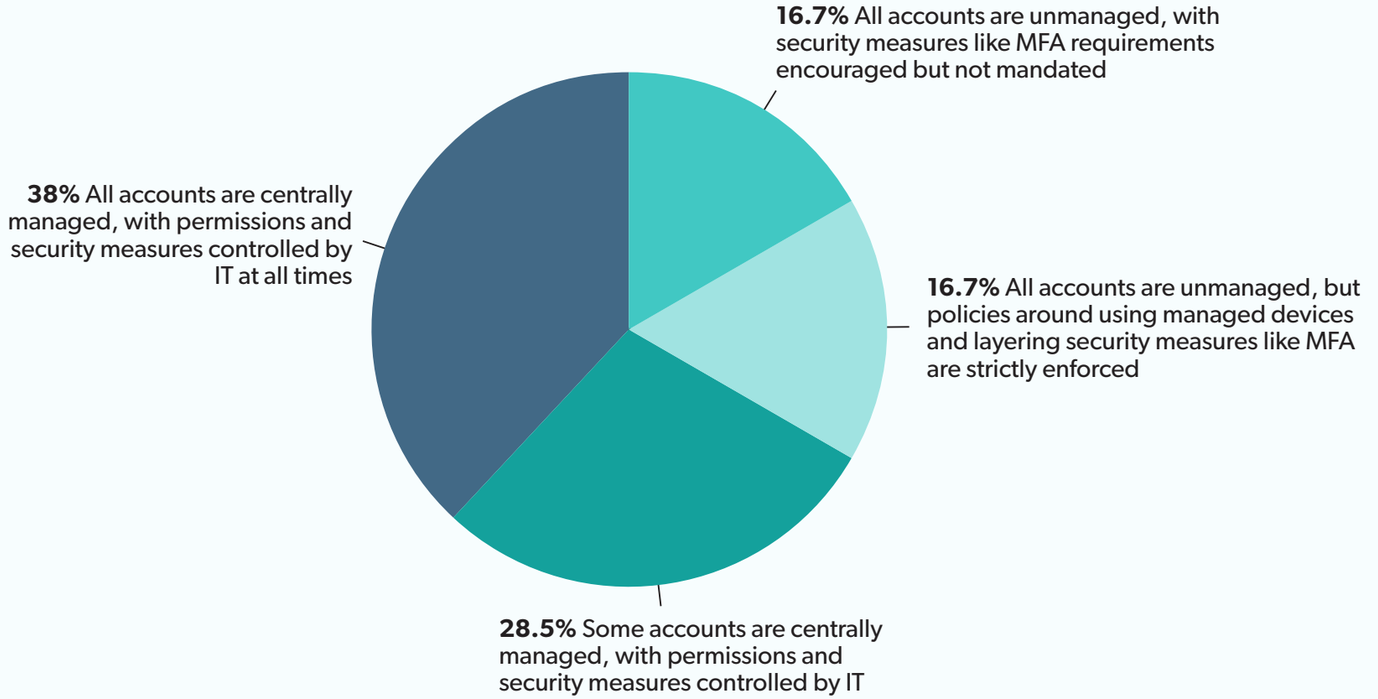


The IT Landscape

Tool Sprawl and Central Management

IT admins are tasked with making work *work*, and there is significant variation in what each organization's user management looks like. When asked how "easy" it is for employees to access what they need, the IT environment looks very different across different SMEs. Around 17% report that accounts are entirely unmanaged, 17% report that accounts are unmanaged but policies around managed devices and security measures like MFA are strictly enforced, 28% report that some accounts and permissions and security measures are centrally managed, and 38% report that all accounts, permissions, and security logins are centrally managed.

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

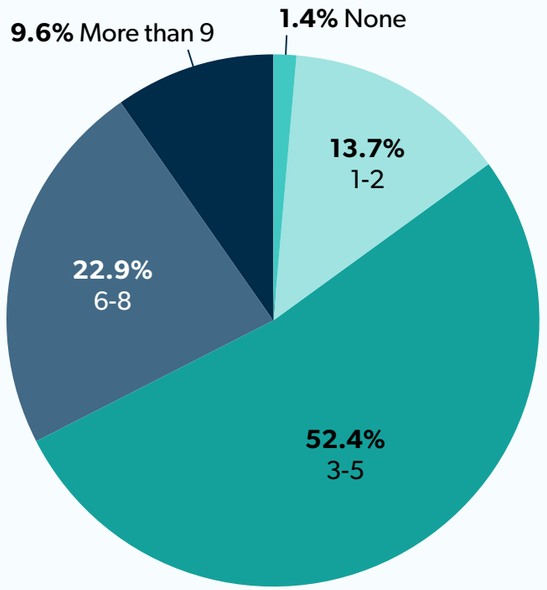


The IT Landscape

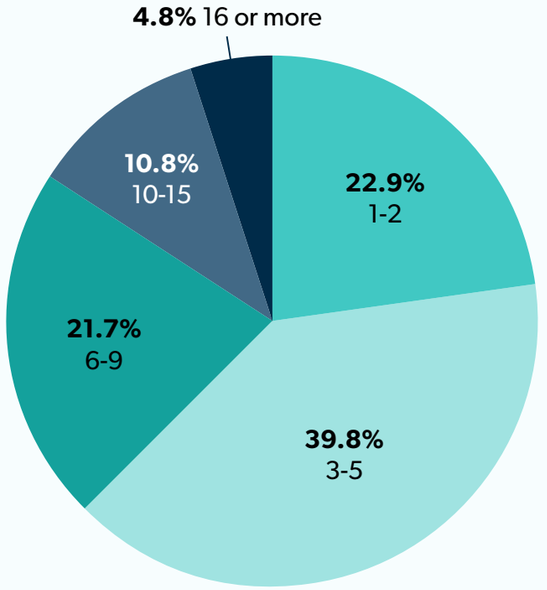
Tool Sprawl and Central Management

Tool sprawl continues to be an issue. Nearly one in 10 IT admins (9.6%) report needing nine or more tools to manage employee lifecycle. It's similarly complicated for employees, with 15.6% of admins estimating employees use 10 or more passwords to do their jobs, and only 22.9% of admins estimating employees need only one or two passwords.

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.)?



On average, how many different passwords do your employees have to log into their resources?

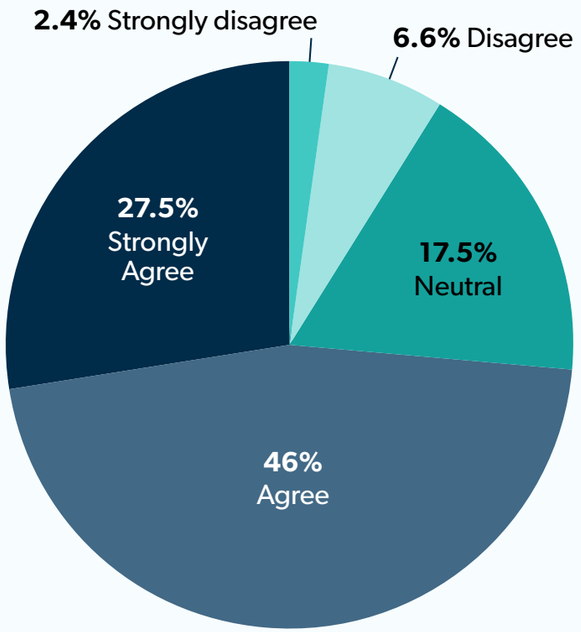


The IT Landscape

Tool Sprawl and Central Management

Tool sprawl doesn't just impact end users, IT admins are juggling a number of solutions and tools despite an interest in consolidating. When asked if they would prefer to use a single solution to do their job, 73.5% agree, virtually the same percentage as those who expressed the preference in April 2022 (75.1%). It's not cost that is holding organizations back from consolidation, as only 18.8% cite a lack of budget as a reason for not consolidating, down from 23.8% in April 2022.

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

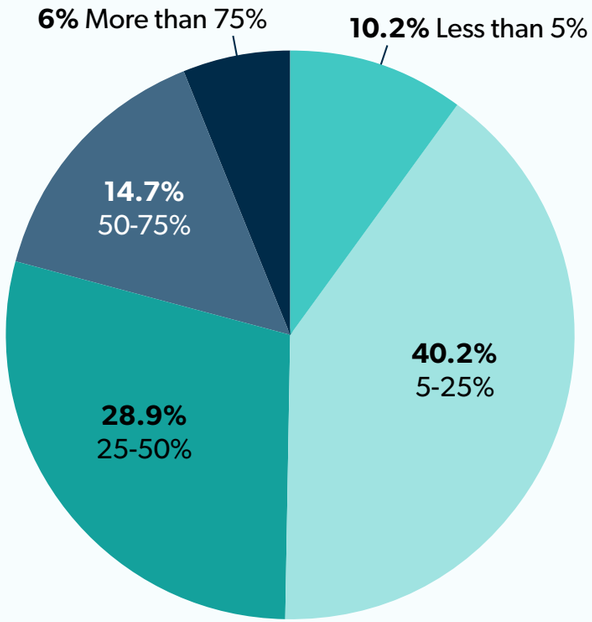


The IT Landscape

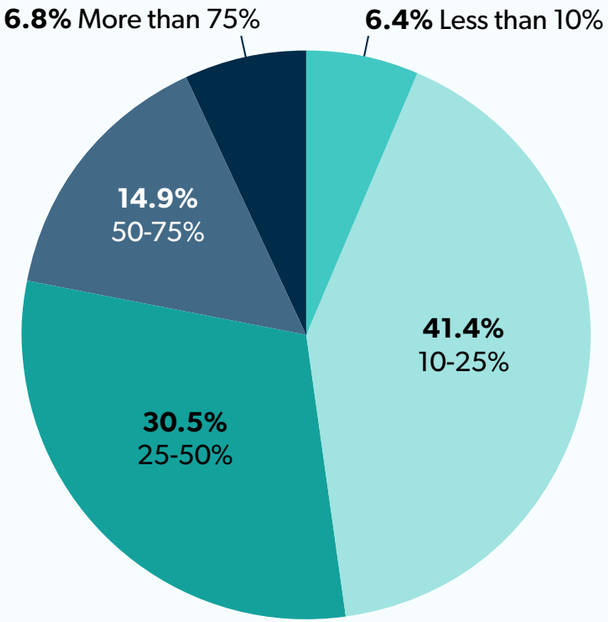
Tool Sprawl and Central Management

Tool sprawl and tech creep has left IT teams dedicating a lot of their time to vendor relations. Nearly half (49.6%) report spending 25% or more of their time communicating with vendors. SME IT admins are also having to dedicate a significant amount of their budgets on licensing costs, with 21.7% who expect to spend 50% or more of their budget on licensing in the coming year, up from 16.6% in April 2022.

About what percentage of your work hours are spent communicating with vendors?



About what percentage of your yearly IT budget goes toward software licensing?

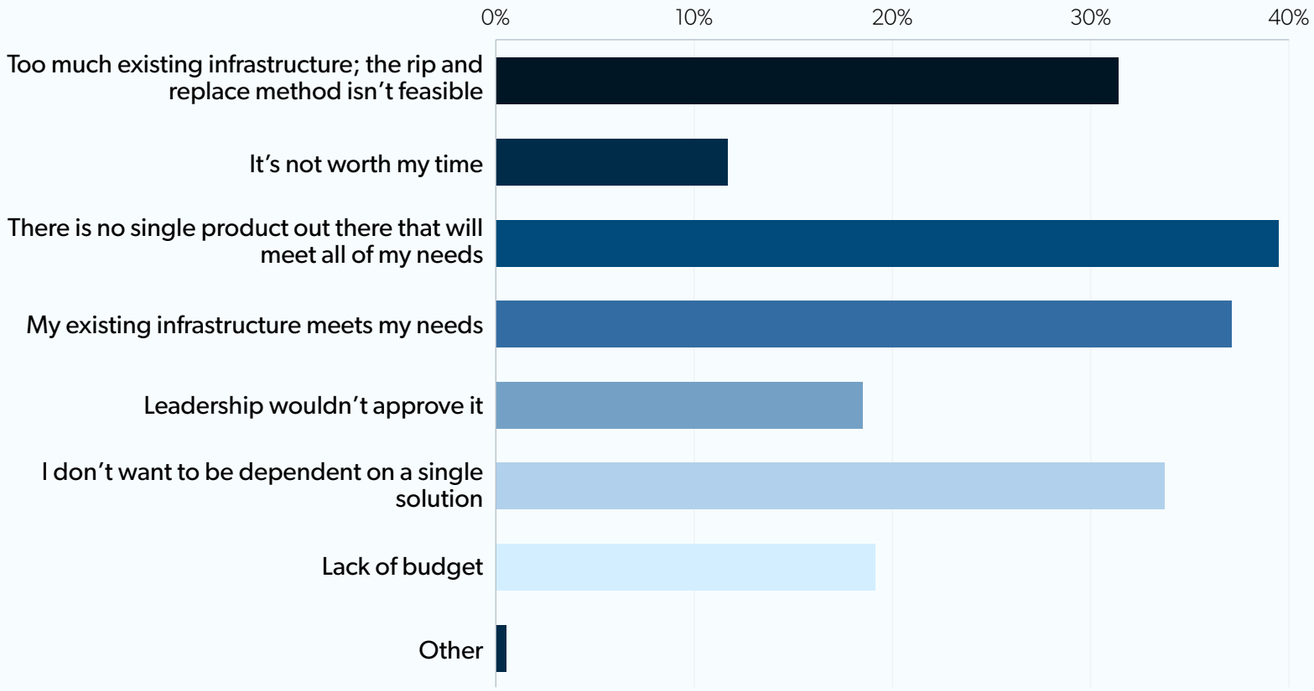


The IT Landscape

Tool Sprawl and Central Management

Despite 73.5% of IT admins preferring a single solution, IT individualism and perceived effort of consolidating are the biggest roadblocks to consolidation. When asked the reasons that prevent admins from consolidating IT products, their top reasons are that there is no single product that will meet all needs (39.8%), their existing infrastructure meets existing needs (36.8%), a preference to not be dependent on a single solution (33.8%), and that rip and replace isn't feasible (32.3%).

What reasons keep you from consolidating IT products? (select all that apply):



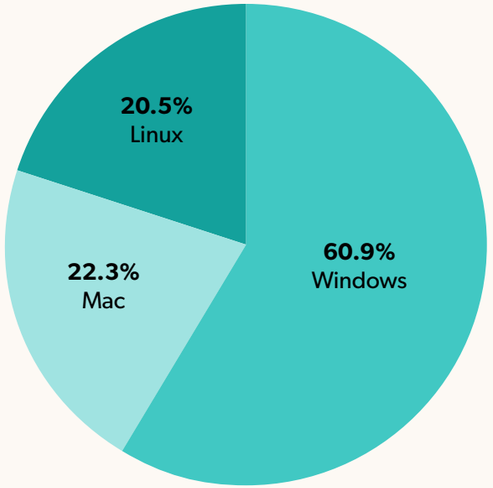
The Device Landscape

Heterogeneity Rules

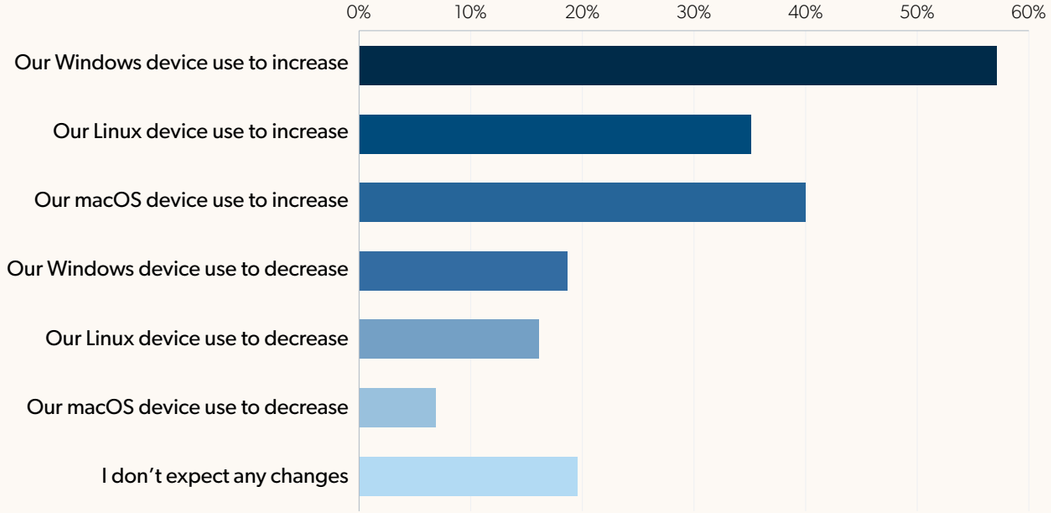
SMEs are continuing to allow flexibility in device environments, with the average workplace made up of 60.9% Windows devices (vs. 65% in April 2022), 22.3% macOS devices (20.9% in April 2022), and 20.5% Linux devices (18.8% in April 2022).

Admins expect to see continued heterogeneity in device landscapes as they project increases in device use across all three OSs, increasing most for Windows (56.8%), followed by macOS (40.2%), and Linux (35.3%).

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



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

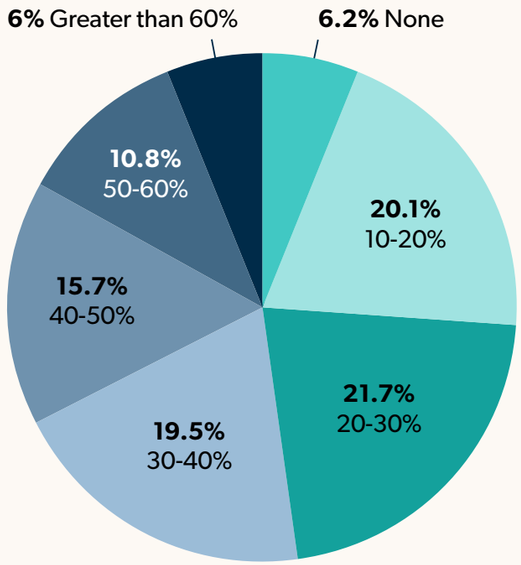


The Device Landscape

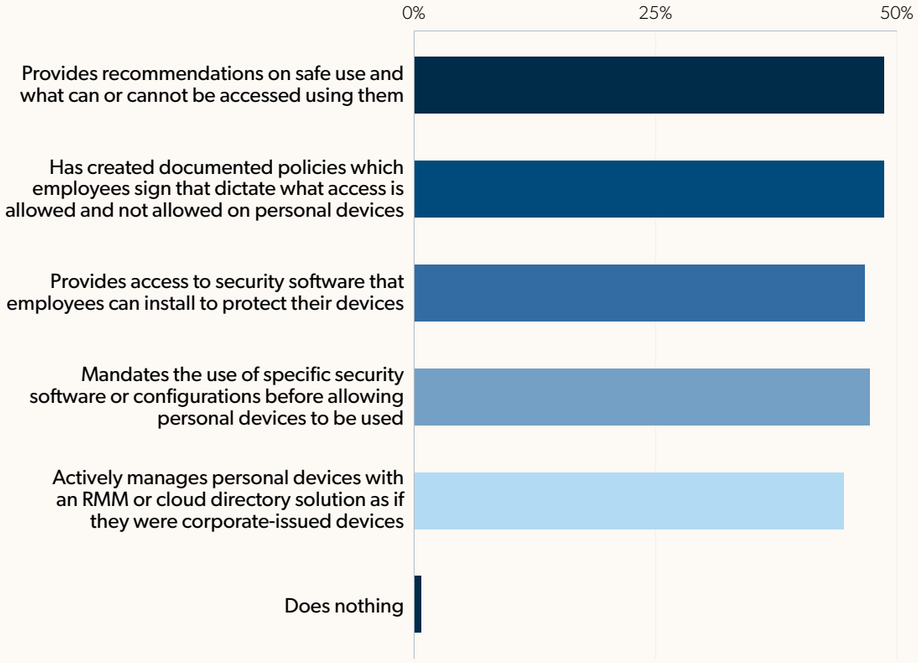
Managing Diverse Devices

The rise of bring your own device (BYOD) environments is evident in SMEs. Only 6.2% of admins estimated that none of their employees used their personal device for work, with most admins estimating that 20-30% of employees do. To address potential risks, IT teams have adopted policies, procedures, and tools to better centrally manage remote devices. Forty-nine percent provide recommendations on safe use and access, 49% have created documented policies to dictate allowed access, 46% offer security software for personal devices, 47% mandate security software or configurations before allowing personal device use, and 41% use a device management platform. Only 1.5% do nothing to manage employees' personal device use.

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



For employees using their own devices, our organization (select all that apply):

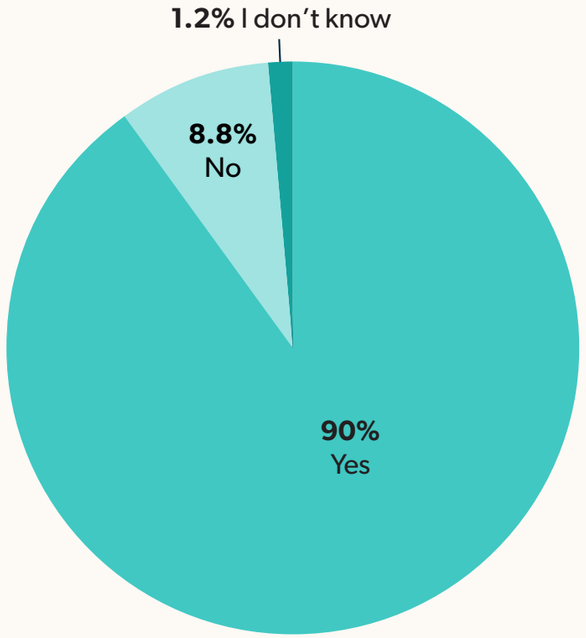


The Device Landscape

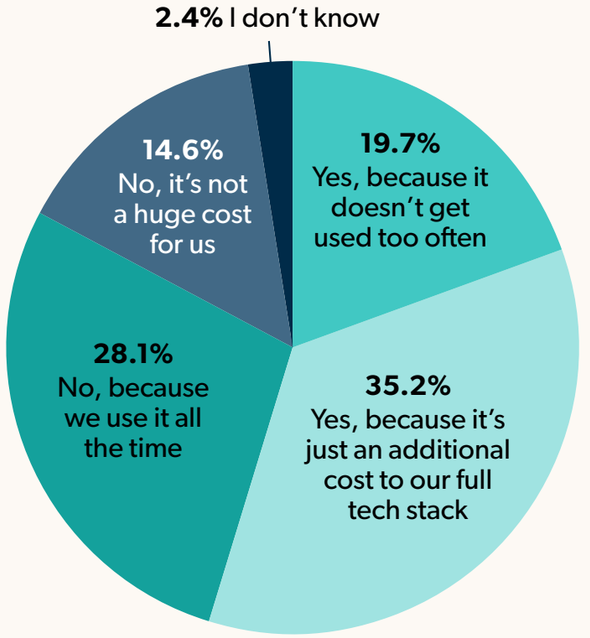
Remote Access

While the days of open door IT in physical offices may no longer be the norm, admins are working to be just as helpful from afar, and privilege the possibility they might be needed over cost. When asked, 90% of admins reported using a remote access solution, though 55% say they spend too much on it.

My organization currently uses a remote access software solution.



I feel like my organization spends too much money on our remote access software solution.

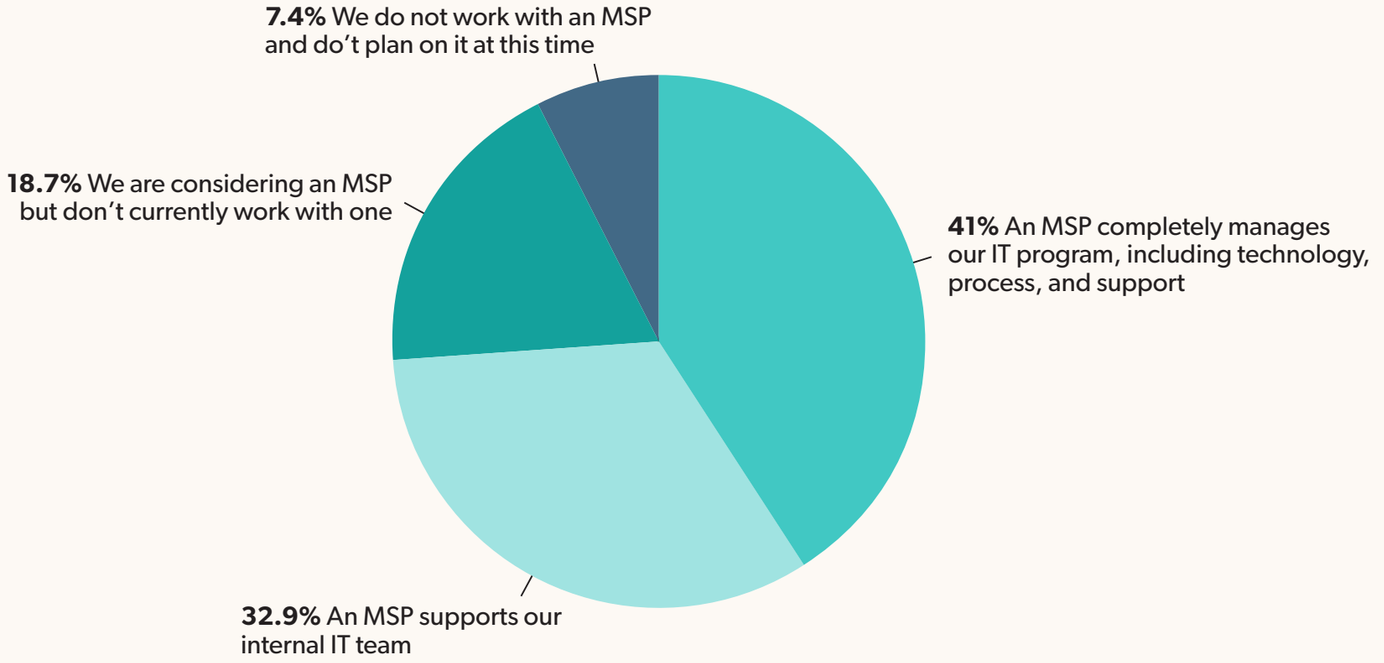


SMEs and Managed Service Providers (MSPs)

SMEs Relying Heavily on MSPs

MSPs continue to be an essential partner for SMEs. Today, 92.6% say they are considering or already work with MSPs, up from 88.9% in October 2021. Forty-one percent say an MSP completely manages their IT program, including technology, process, and support, up from 34.2% in April.

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

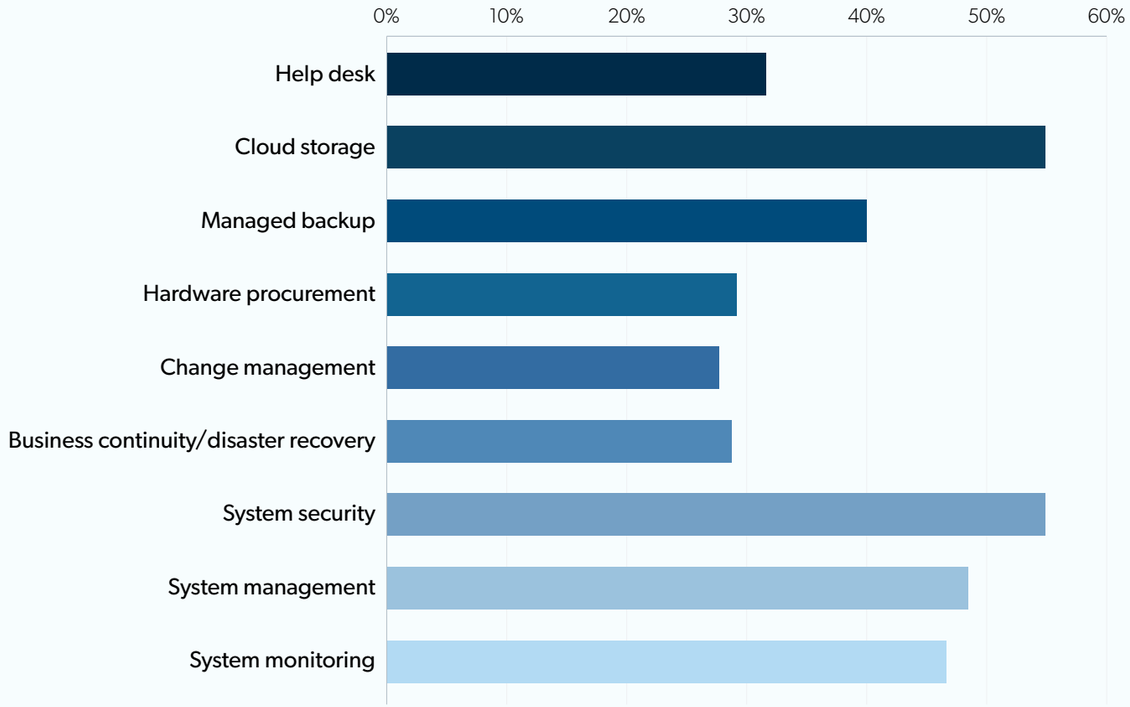


SMEs and MSPs

SMEs Relying Heavily on MSPs

In order, MSPs are used most heavily for cloud storage (55.8%), system security (55.5%), system management (48%), system monitoring (46.4%), managed backup (40.2%), help desk (32.9%), hardware procurement (29.4%), business continuity and disaster recovery (29.1%), and change management (27.5%).

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



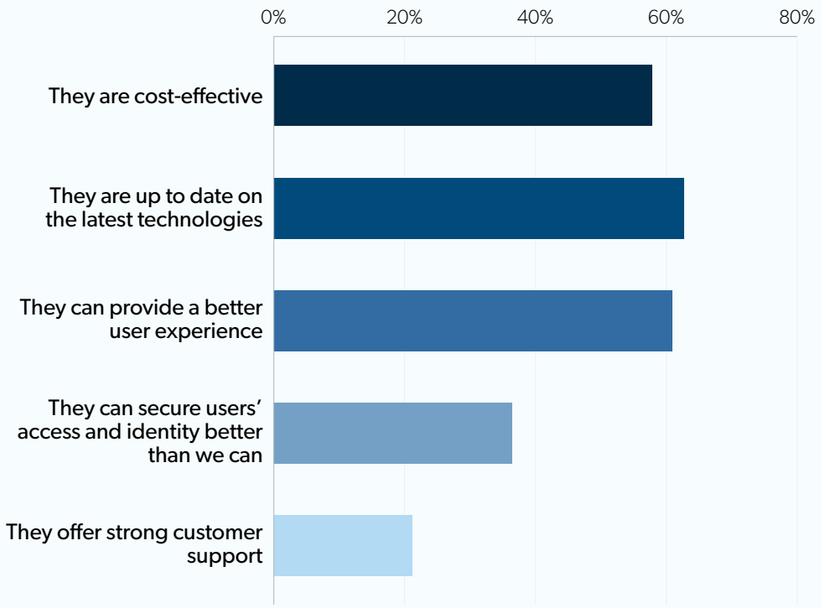
SMEs and MSPs

Goals and Results

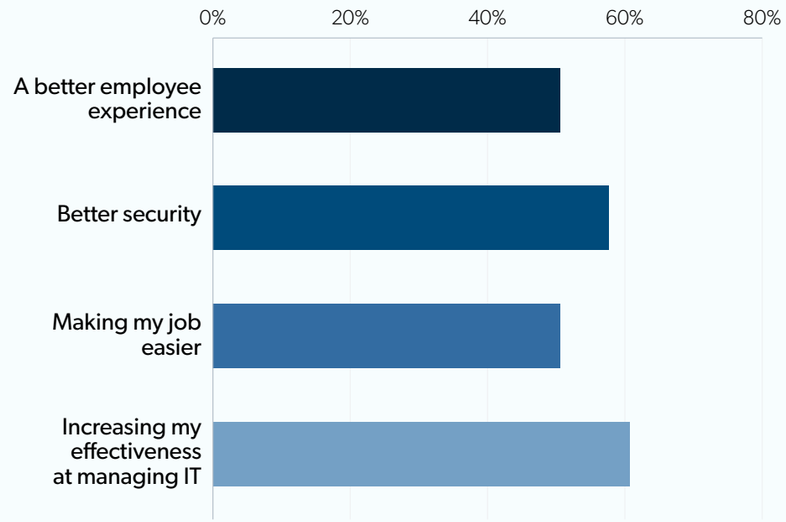
MSPs are seen as valuable across a number of functions. On nearly every metric, IT admins rated MSPs higher across a variety of reasons versus six months ago. The top reasons for MSP use are that they: are up to date on latest technologies (65.2% vs. 63.5% in April 2022), offer a better user experience (62% vs. 52.2% in April 2022), are cost-effective (57.4% vs. 53.8% in April 2022), better secure identity and access management (35% vs. 33.8% in April 2022), and offer customer support (21.8% vs. 20.3% in April 2022).

The biggest impact MSPs are making is seen as improving IT's day-to-day experience. While fewer report better security as a result of their MSP use (down to 56.6% from 70.3% in April 2022), 51.2% report their job is easier due to MSP use (up from 35.7% in April 2022), and 60.4% report their effectiveness has increased, nearly doubling from from 32.1% in April 2022.

We use MSPs because (select all that apply):



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



SMEs and MSPs

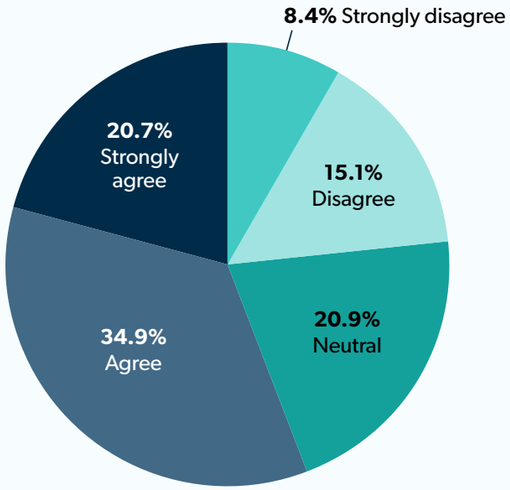
Concerns that Block Adoption

Check out **The MSP's 2023 Planning Kit** for tools to kick-start 2023 business planning

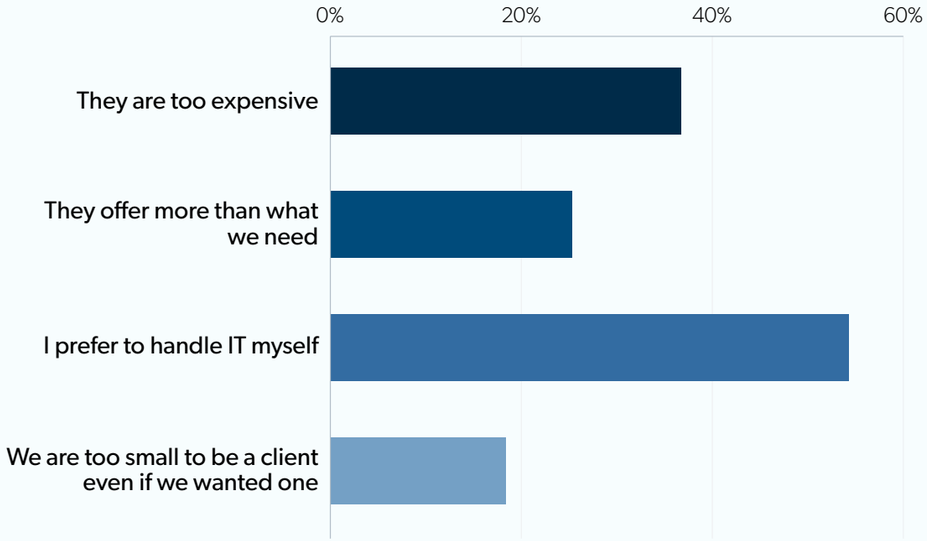
However, concerns about MSPs maintaining robust security are rising. Now, 55.6% agree that they have concerns with how MSPs manage security, up from 41.5% in April 2022, and 36.9% in October 2021.

IT individualism and cost are still the biggest blockers to MSP adoption. When asked, 53.4% of IT admins said they prefer to handle IT themselves over using an MSP (down from 56.3% in April 2022) and 35.9% say MSPs are too expensive (up from 28.9% in April 2022). Other cited reasons for not working with an MSP is that MSPs offer more than what the admins' organizations need (26.7%) and that organizations are too small to be a MSP client (17.6%). Check out **The MSP's 2023 Planning Kit** for tools to kick-start 2023 business planning — and ensure your selling, technical, and support strategies are set for the year.

I have concerns about how MSPs manage security:



We don't use MSPs because (select all that apply):



Final Thoughts

There's no question that over the past year, IT teams have managed to navigate uncertain waters by pursuing innovative solutions, adopting a good attitude, and jumping in to solve problems no matter where they surface. These overworked but happy professionals have kept workplaces productive and secure in the face of unprecedented change, both external and internal.

Despite IT's success in ensuring operational stability in these interesting times, the outlook for the next 12 months suggests that accepting the unknown and unpredictable may be the state of the industry (and world) for the foreseeable future.

As security continues to be the top challenge and priority for SMEs, there are a number of ways organizations can better let IT lead based on the findings of our research.

- **Consider consolidation:** Seventy-five percent of admins prefer a single solution to manage IT. Cost is a roadblock for only 18.8% of admins, suggesting that there may be ample opportunity to convince reluctant stakeholders that the time for consolidation is now. With 84% of admins agreeing that employee experience is a top consideration, decision makers should empower those most capable and knowledgeable to determine how to deliver it.
- **Evaluate MFA for improvements:** As an industry, not every organization even deploys MFA. Now with MFA fatigue attacks, those who have deployed it can't be complacent that MFA is adequate without establishing that MFA steps are as secure as possible. That 80% of admins use biometrics on their personal devices, taking advantage of native device features like fingerprint readers and front-facing cameras, should make clear that biometrics is, and should be, a leading contender for MFA in any size of organization.
- **Look at mobile device management (MDM):** The current device breakdown in SMEs continues to be a mix of macOS, Windows, and Linux devices. IT admins are telling us they project that organizational use will mirror that moving forward. At the same time, personal device use in SMEs continues to increase, transferring much security responsibility to users who may or may not know or follow best practices. Mixed device environments and distributed workforces have put an extraordinary amount of pressure on IT to both enable — and secure — work. Taking into account admin preference for consolidation, looking at MDM solutions is one critical way that organizations can centralize IT management, take the burden off of admins, and guarantee that secure procedures and policies are followed.
- **Spend wisely:** IT admins are telling us that they know how to be smart with their budget. Whether it's a reluctance to sign with an MSP due to cost or acknowledging that existing solutions like remote access cost more than they're worth, these professionals know what features should be prioritized and are wary of spending money without understanding the return on investment. If admins are telling us they're overspending on too many tools and worried about cutting budget on cybersecurity, organizations would be smart to listen.

As we round into 2023, IT teams have more than proven they're capable, competent, and adaptable. SMEs have the opportunity to be guided by practitioners who keep the organization operational, and who regularly demonstrate a passion for making it run better and making it more secure.

JumpCloud's commitment is to Make Work Happen®. Designed and built for SMEs, JumpCloud's directory platform delivers enterprise-level IT management without enterprise-level cost or complexity. The entire platform follows a product-led growth (PLG) model to ensure its delivering instant value to IT teams and MSP partners, anticipating their needs, and offering a solution based on their feedback.

To get started with JumpCloud immediately, for free, visit console.jumpcloud.com/signup.

Methodology:

JumpCloud surveyed 502 US-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 online survey was conducted by Propeller Insights, October 11-14, 2022.

jumpcloud™

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 →