eBook

jumpcloud™

State of IT 2024:

The Rise of AI, Economic Uncertainty, and Evolving Security Threats

Executive Summary

Managing IT has never been easy. But today's organizations face extraordinary challenges when it comes to securing corporate resources and employee identity. The model that provided a foundation for decades—centralized IT within corporate offices, across corporate networks, and on identical company-issued devices—no longer adequately covers today's workplace models. Now workers are digital natives who use a variety of devices to access IT resources whenever and wherever they need to. Managing these new IT complexities is difficult enough; add in the growing number and sophistication of external actors means IT teams must protect against threats that can damage an organization's business and economic interests at unprecedented levels.

Today IT admins face a tall task: securing employees and their work, wherever it happens, and enabling productivity and growth while managing rising threats, evolving global economic trends, and the growing impact of artificial intelligence (AI). These factors and others, accelerated by cloud innovation, have transformed the way organizations need to approach identity.

JumpCloud's sixth edition of its biannual small to medium-sized enterprise (SME) IT Trends Report evaluates the state of IT and offers guideposts on where it's headed. This most recent edition of the SME IT Trends survey shows how quickly AI has impacted identity management and highlights that IT professionals have both big hopes and big fears in their response to it. Surveyed admins widely consider AI positively in some regards—nearly 80% report that AI will be a net positive for their organization, and only one-fifth believe their organizations are moving too slowly with respect to AI initiatives. But despite IT teams' general positivity toward adopting AI, concerns about its negative impacts loom large. Nearly six in ten (62%) agree that AI is outpacing their organization's ability to protect against threats and nearly half (45%) agree they're worried about AI's impact on their job.

The report also reveals how IT admins are embracing identity transformation by adopting approaches that streamline and centralize identity with an open, cloud-based framework. This strategic shift is empowering IT teams to cater to employees' changing needs and evolving IT environments without adding unnecessary friction, cost, or complexity.

Identity is at the core of IT. It's the modern security perimeter. It controls access to sensitive data, devices, and applications. It makes work *work*. IT teams are looking for an open IT approach that streamlines and centralizes identity to meet increasingly challenging workplace needs. This approach is especially critical given that 57% of organizations have experienced layoffs over the last year and 51% expect to see them in the next six months. A unified, open identity and IT management approach can prevent operational disruptions and admin burnout amidst economic uncertainty—especially critical given the significant time and budget constraints under which IT teams generally operate.

JumpCloud commissions the SME IT Trends Report to highlight the challenges and opportunities facing these IT experts as they work to fortify organizational security, optimize operations, and foster sustainable growth. It gives organizations the insights to strengthen their IT foundation, creating a secure, efficient, and highly productive environment for long-term success.

This Q1 2024 edition of the SME IT Trends Report suggests:

- IT optimism around AI adoption is tempered by significant fear around the unknown. With a strong majority of respondents both planning or actively implementing within the next year and advocating for AI investment, IT leaders clearly see potential benefits from deploying AI in their workplaces. But IT admins report notable concerns around their organizations' current ability to secure against related threats—and personal concerns about AI's impact on their career.
- Security remains a paramount concern for SME IT teams, given the increasing sophistication of external threats and rising regulatory pressures. As IT admins work to integrate new technologies like biometrics and passkeys, password-based systems continue to dominate and necessitate extra effort to secure.
- Device, identity, and access environments in SMEs continue to be overly complex and burdensome for IT administrators. Despite the higher cost, complexity, the availability of alternatives, and IT teams' continued preference for consolidated IT management, most IT professionals still juggle an extraordinary number of IT solutions.
- Managed service providers (MSPs) continue to be integral to SME IT operations, with a strong focus on providing expertise, user-friendly experiences, and cost-effective solutions. Nearly half (42%) of respondents rely on an MSP for total IT management, a 56% increase from Q2 2023.
- Despite positive industry projections for 2024, IT teams are bracing for the unknown. Over half of respondents expect additional layoffs at their organization, nearly half worry about AI's impact on their job, more than half are more worried about their organization's security posture, and nearly three-fourths agree that any future budget cuts will put their organization at risk.

The Q1 2024 SME IT Trends Report affirms that IT teams are aware of the need for smart AI integration and enhanced security measures, and are committed to delivering operational efficiency and employee productivity—even as they anticipate continued turbulence and uncertainty. Broader challenges like economic uncertainties, complex device ecosystems, and a wide range of work responsibilities are leading IT teams to embrace identity-focused, open IT solutions that strike a balance between robust security and user-friendliness.

IT teams continued to demonstrate ingenuity and grit in 2023, and have proven themselves remarkably resilient. IT administrators are at the forefront of navigating these transformations with agility and an unwavering commitment to openness.

The SME IT Landscape

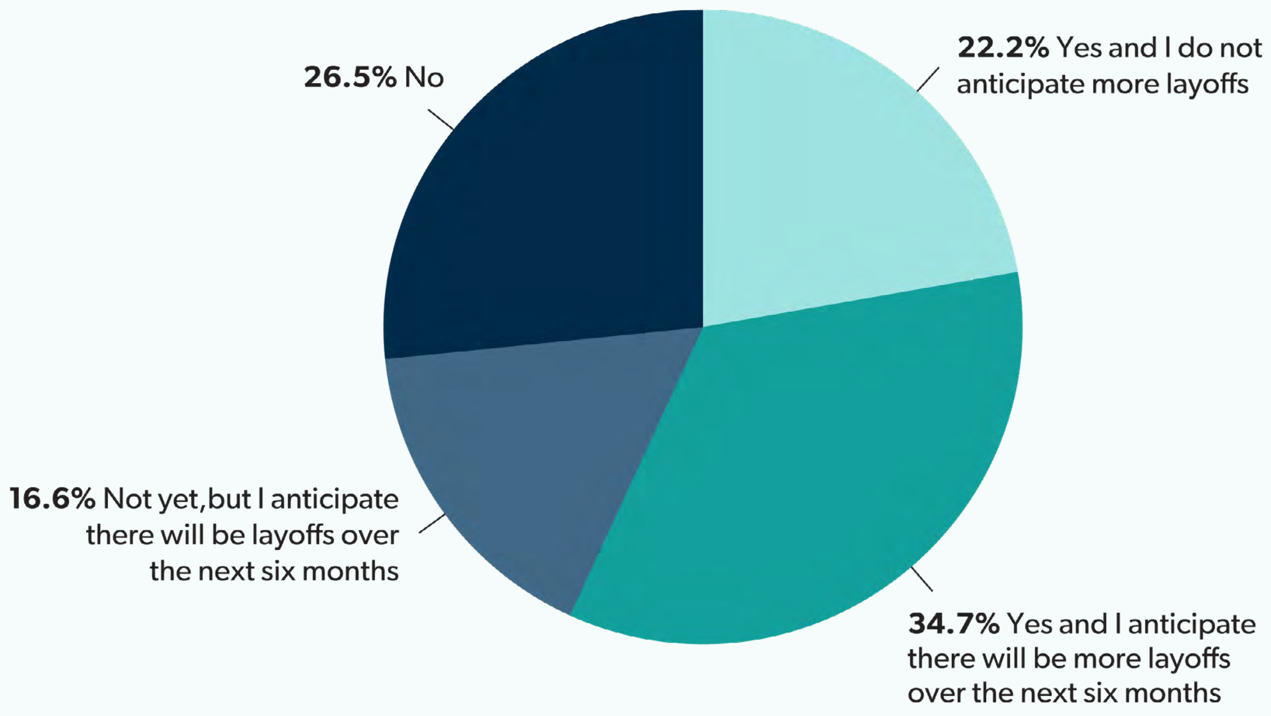
The Hard Economic Reality

Globally, IT admins have had to navigate turbulent economic realities. Over half (57%) have experienced layoffs, up from 30% in early 2023, and over half (51%) expect to see additional layoffs over the next six months.

A plurality of admins (35%) have gone through layoffs and anticipate there will be more over the next six months; 22% have gone through layoffs and don't anticipate additional ones; 17% haven't experienced them but anticipate them over the next six months, and 27% don't expect any.

This outlook is a bit more optimistic than earlier in 2023, when 77% of admins expected layoffs in their organization within the next six months.

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



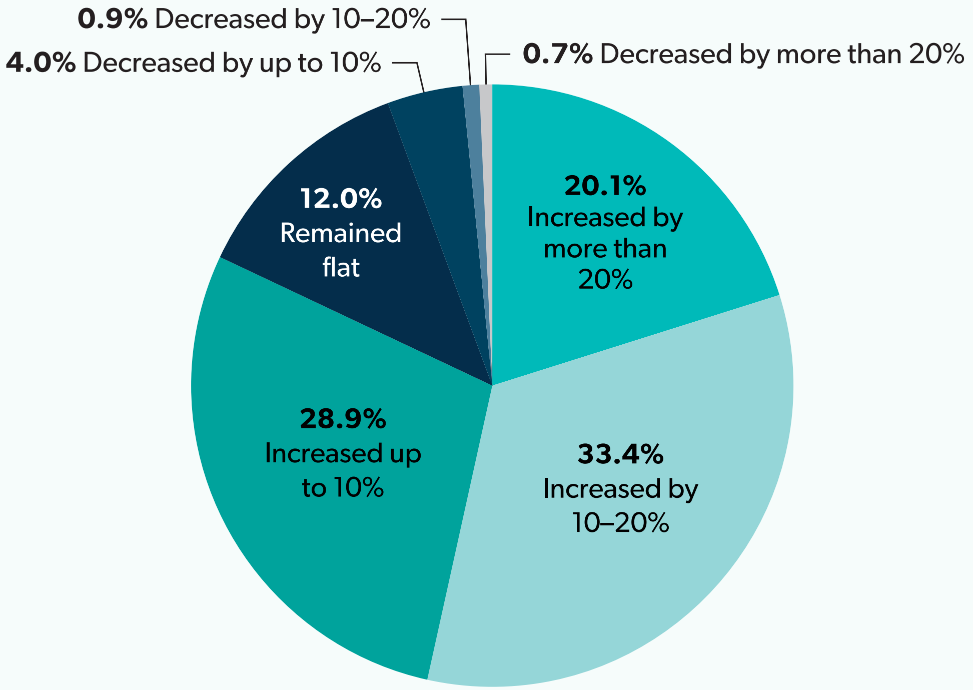
The SME IT Landscape

Budgets Increasing Amid Broader Economic Uncertainty

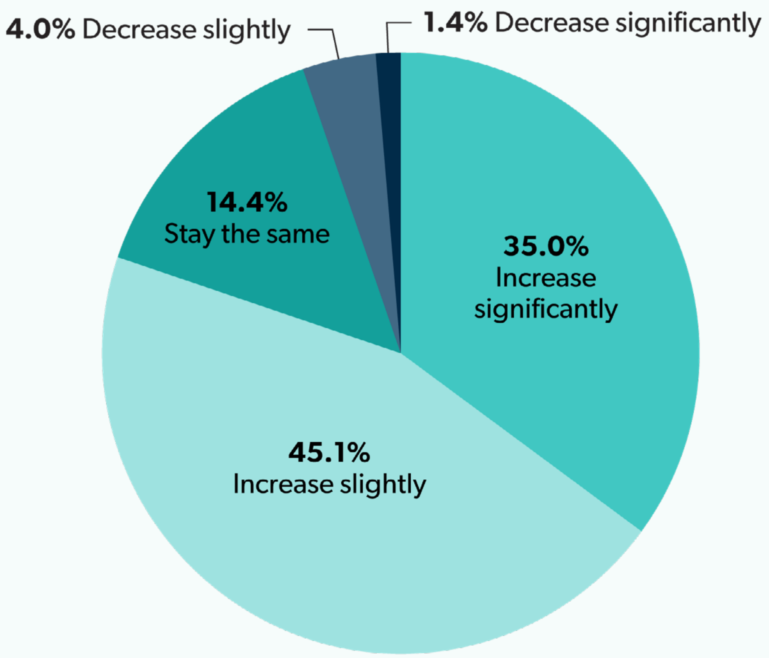
IT budgets are up over the past 12 months, continuing the trend seen in early 2023. Over eight in 10 organizations report an increase in IT budgets (82%) and 20% report an increase of more than 20%, compared with 80% who had seen an IT budget increase and 13% who had seen an increase of over 20% in early 2023. While the World Bank projects the global economy to slow for the third year in a row and is on course for its worst half-decade of growth in 30 years, only 6% of SMEs report a decrease in their IT budget.

IT admins are also more optimistic about IT spending than six months ago. Now 80% expect IT budgets to increase in 2024 versus 64% who responded the same in April 2023. (35% expect significant increases, versus 19% who answered the same in April 2023.)

Over the past year, my IT budget:



In 2024, I expect our IT budget to:



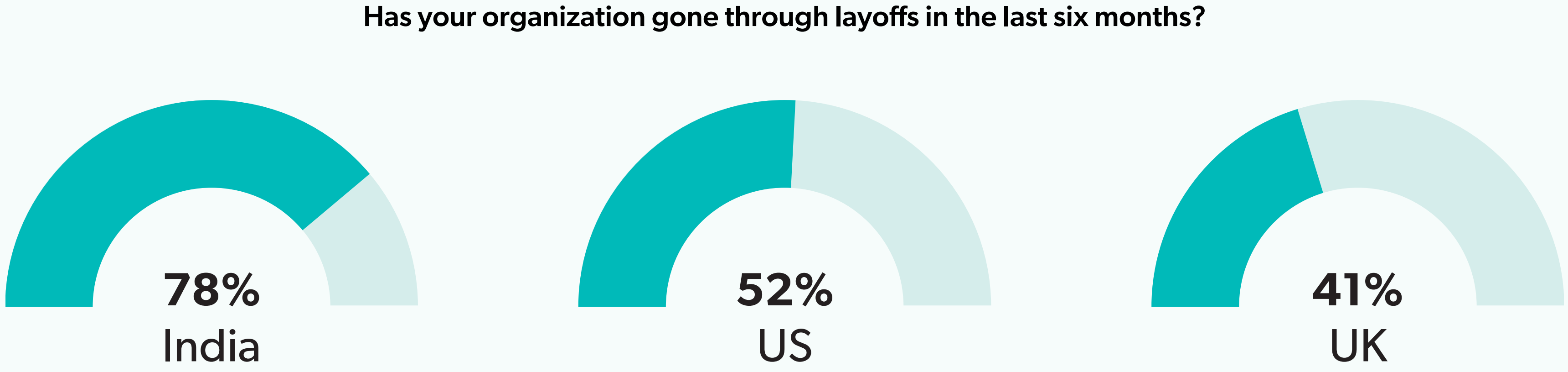
The SME IT Landscape

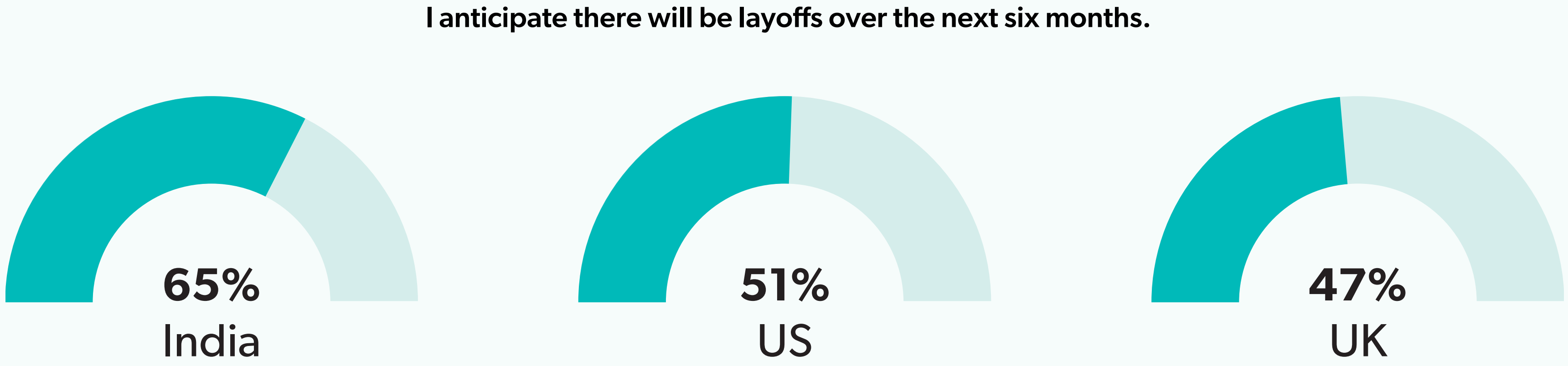
Layoffs Looming Across the Lands

2023 revealed organizations leaned into widespread layoffs and that IT admins aren't convinced the worst is over.

India has been the hardest hit with 78% having experienced layoffs in the second half of 2023, and 13% who haven't experienced layoffs yet but expect them over the next six months. In total, 65% of Indian admins are expecting layoffs in the next six months.

The U.S. saw 52% of respondents reporting layoffs, and 51% expecting more layoffs over the next six months. The U.K. saw 41% of respondents experiencing layoffs, and 47% expect layoffs over the next six months.



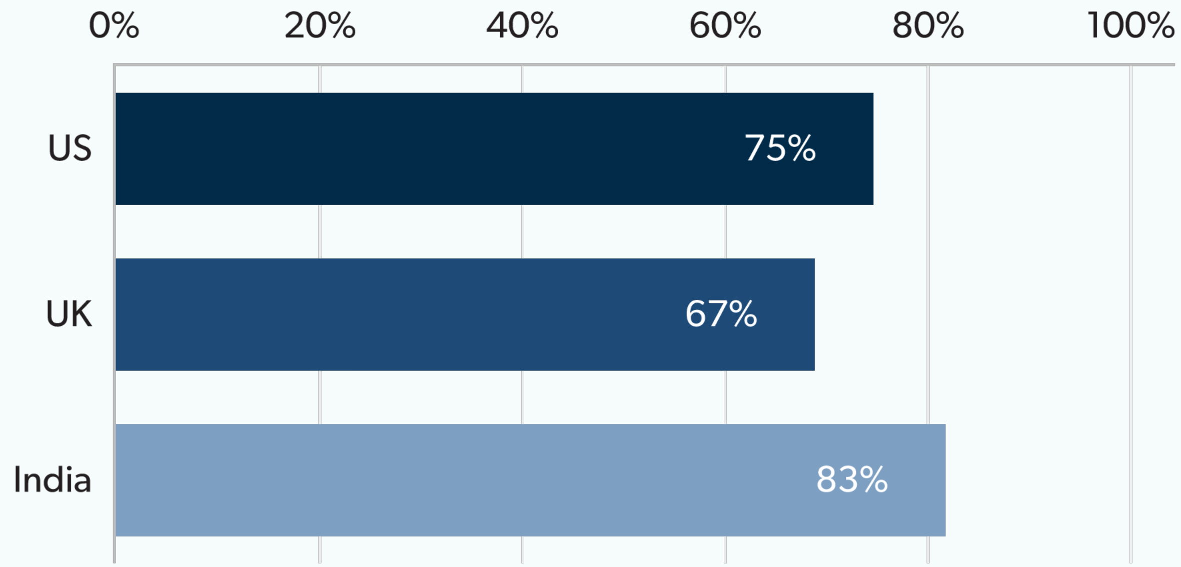


The SME IT Landscape

Compliance Pressure

Amid distributed workforces, there's additional pressure on IT teams around compliance and regulation requirements. Over two-thirds (75%) agree that more compliance and regulation requirements have been mandated in their region. India reports the highest shift toward compliance and regulation, with 83% reporting additional compliance and regulation requirements, versus 75% in the U.S. and 67% in the U.K.

Over the past year, more compliance and regulation requirements have been mandated in my region.



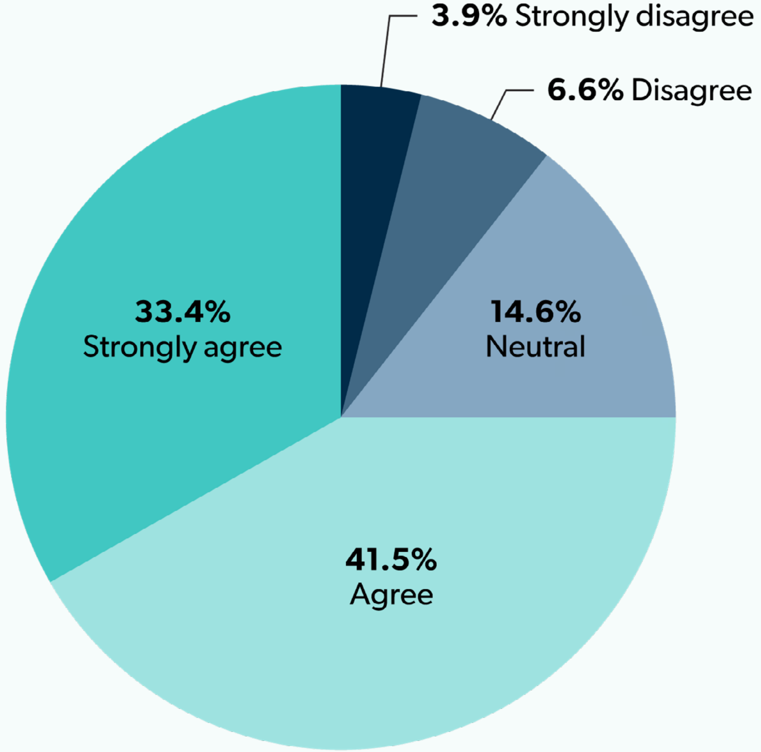
The SME IT Landscape

Despite Demand for Consolidation, Tool Sprawl Continues to Vex IT Admins

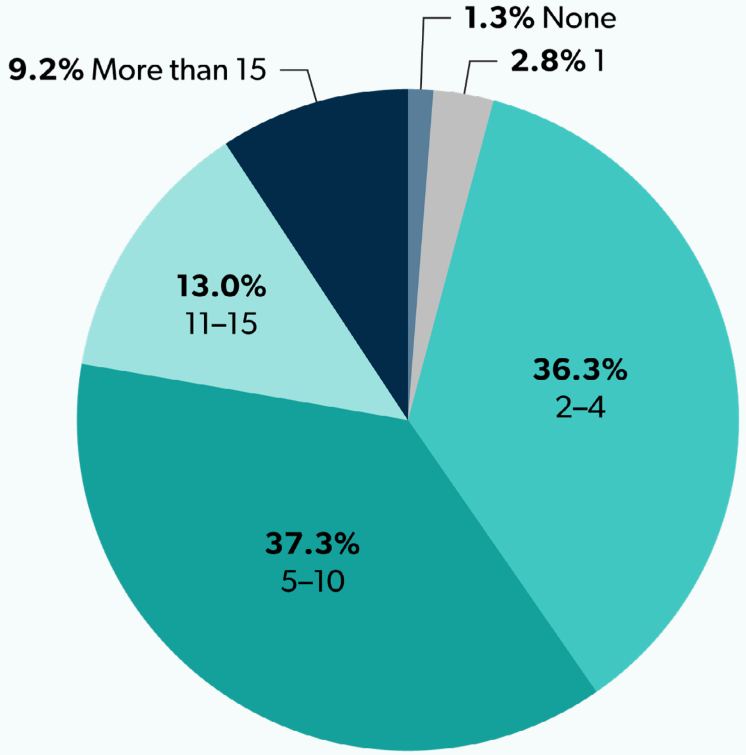
IT teams continue to shoulder the incredible responsibility of securing workers' access to all IT resources without adding friction to their individual or employees' experience. A large majority (75%) continue to prefer a single tool to do their job rather than a number of point solutions, roughly the same as the 77% who said the same in April 2023.

Despite their preference for centralized IT management, 60% of respondents need five or more tools to manage the employee lifecycle and the applications they need to do their job—and almost one in 10 (9%) need more than 15.

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



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.)?



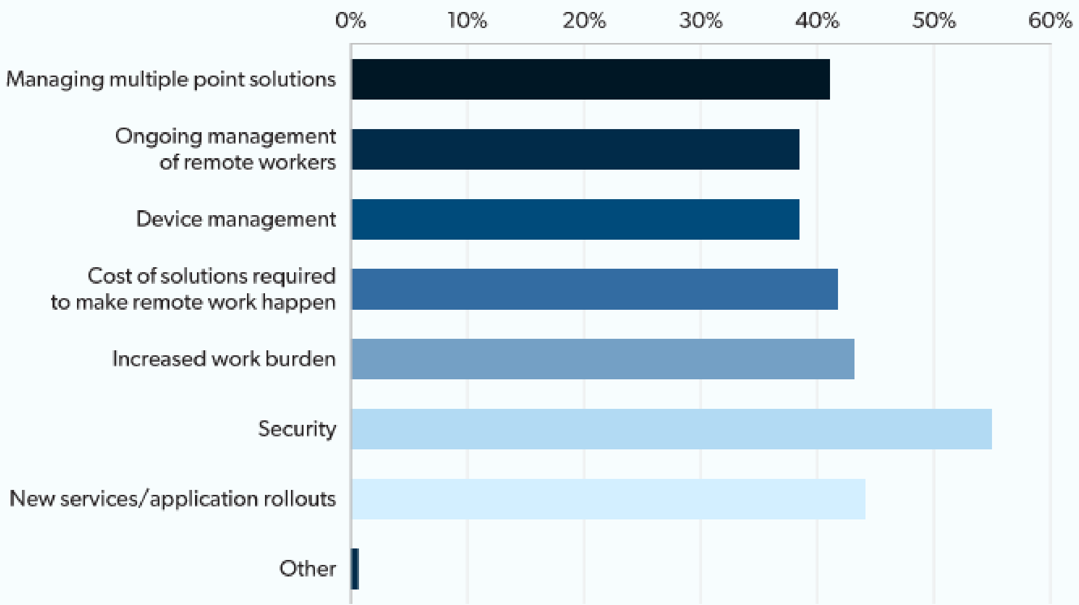
Security and SMEs

Rising Challenges on Every Front

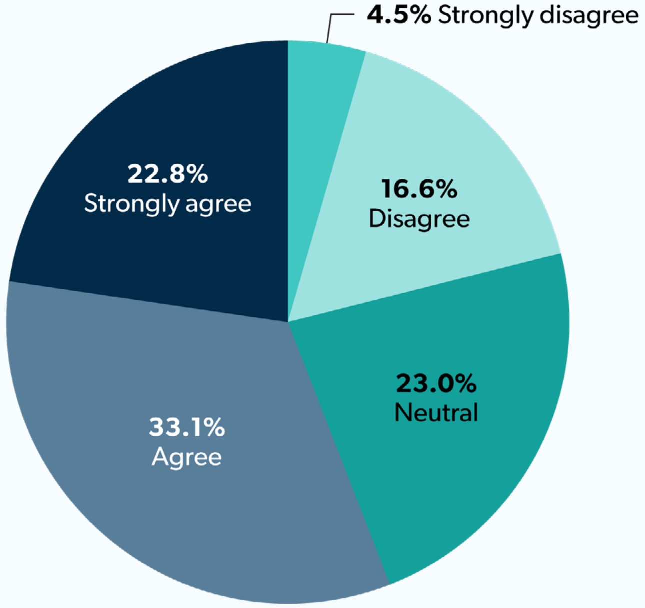
Security continues to be the top challenge facing a majority of IT admins (56% versus 59% in April 2023). The second and third biggest challenges were new services and application rollouts (45% versus 43% in April 2023) and the increased work burden (44%), which displaced the cost of remote work solutions, now the fourth largest concern (42% versus 43% in April 2023).

Security concerns are on the rise, as 56% of admins agree that they're more concerned about their organization's security posture now than they were six months ago, up from 49% in April 2023.

What was been the biggest challenge to your IT team in 2023?



I am more concerned about my organization's security posture than I was 6 months ago.



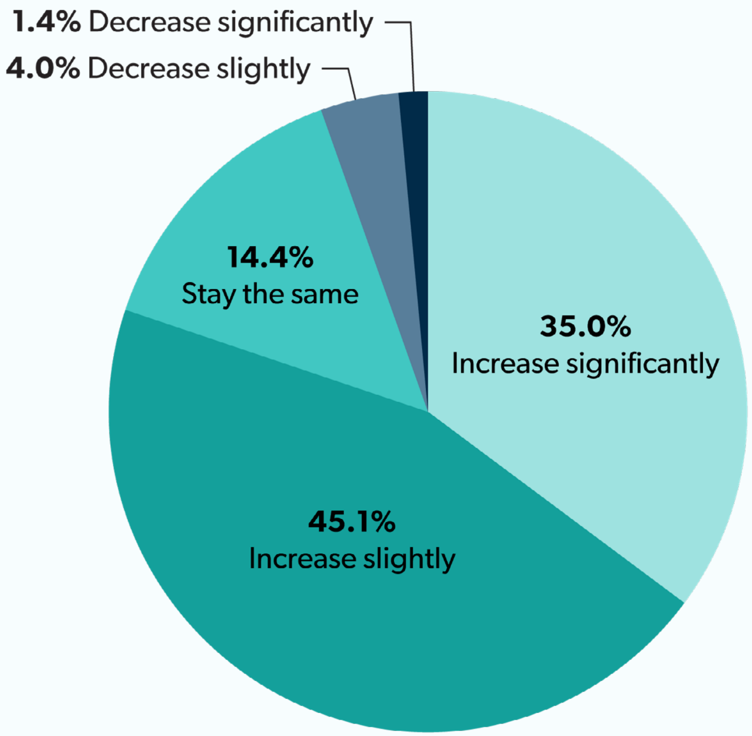
Security and SMEs

IT Spending Holds Steady

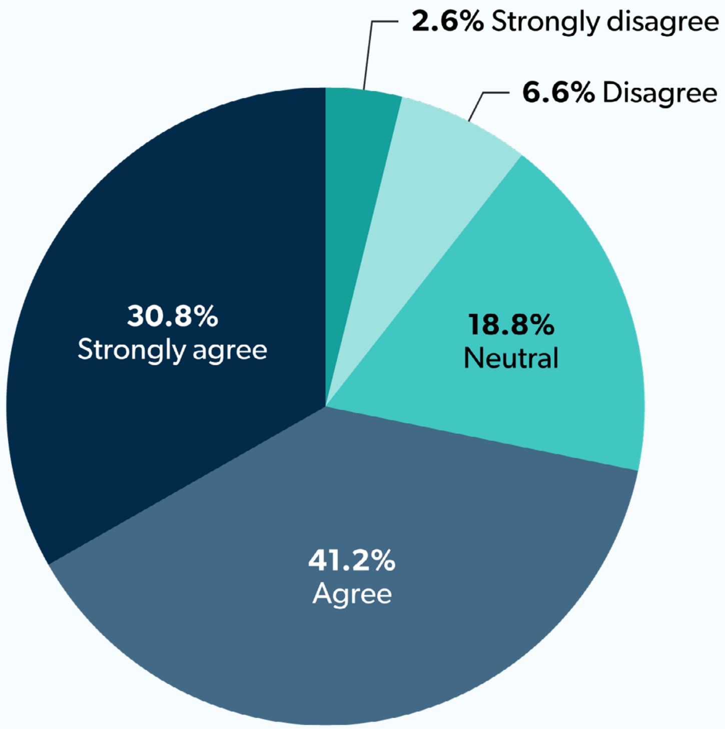
While there's uncertainty around the broader economic outlook, organizations continue to prioritize IT spending. A significant percentage of admins (80%) expect their IT budget to increase in 2024; 35% expect a significant increase and 45% expect a slight increase.

For admins facing increasingly sophisticated threats, budget cuts are a concern as 72% agree that any cuts to their security budget will increase organizational risk, up from 68% who shared that concern in April 2023.

In 2024, I expect our IT budget to:



Cuts to our security budget will increase our organizational risk.



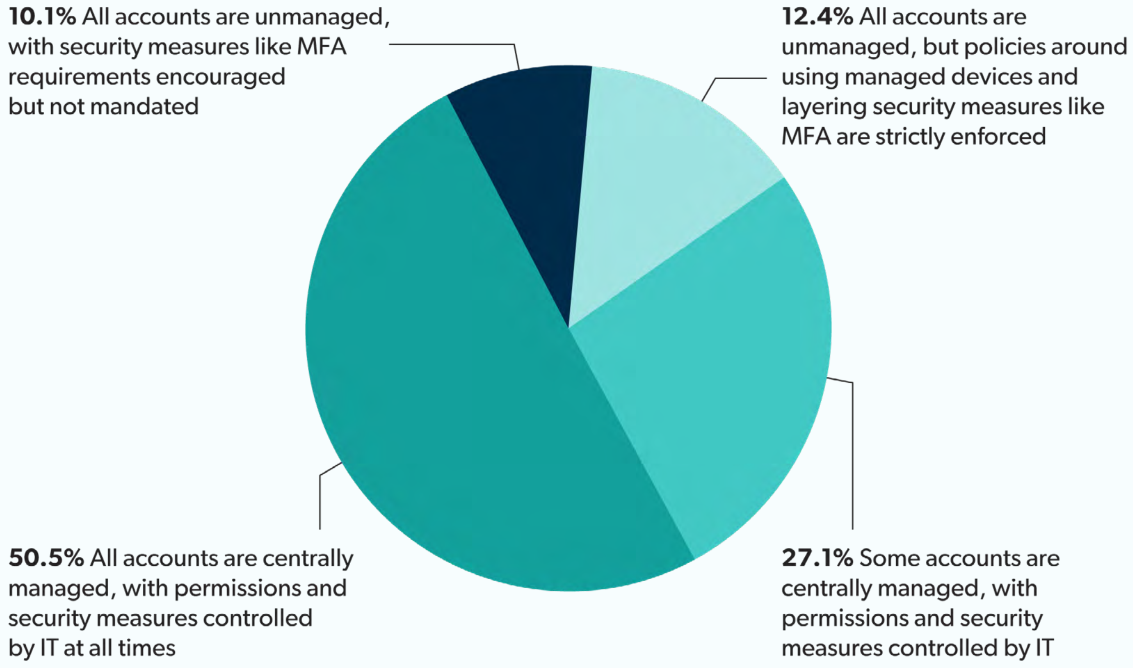
Security and SMEs

Taking Over the Security Reins

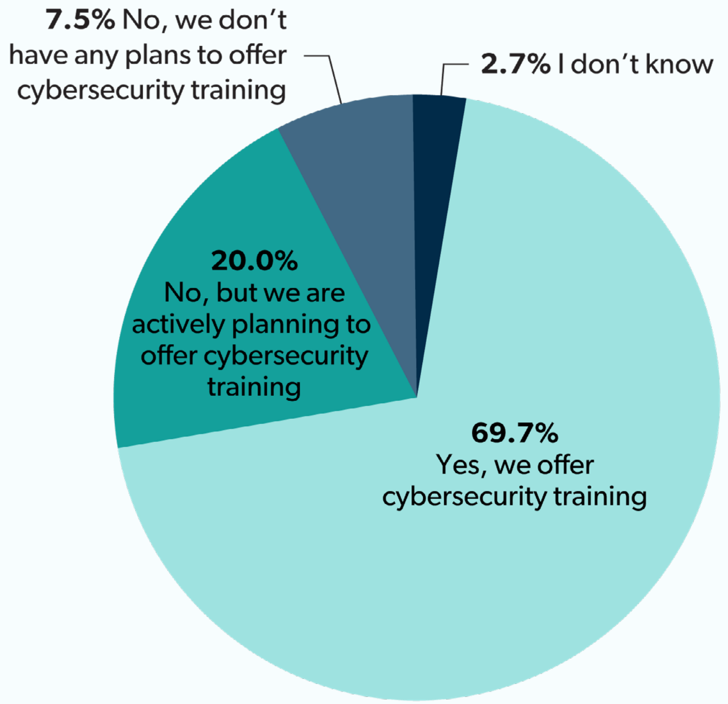
Organizations have significantly fortified their security stance through IT centralization. Over half of organizations (51%) centrally manage employee access to all accounts, with permissions and security measures controlled by IT at all times, up from 31% who reported the same in April 2023. Only 10% leave accounts entirely unmanaged by IT with security practices like multi-factor authentication (MFA) encouraged but not mandated.

Along with centralized IT management, organizations are investing in making sure their employees are aware of security issues. Almost 70% of organizations currently offer formal cybersecurity training for employees, and 20% are actively planning to offer it.

In terms of employees accessing their IT resources, which of the following most resembles your organization's processes?



Does your company currently offer, or have plans to offer, formal cybersecurity training for employeees?

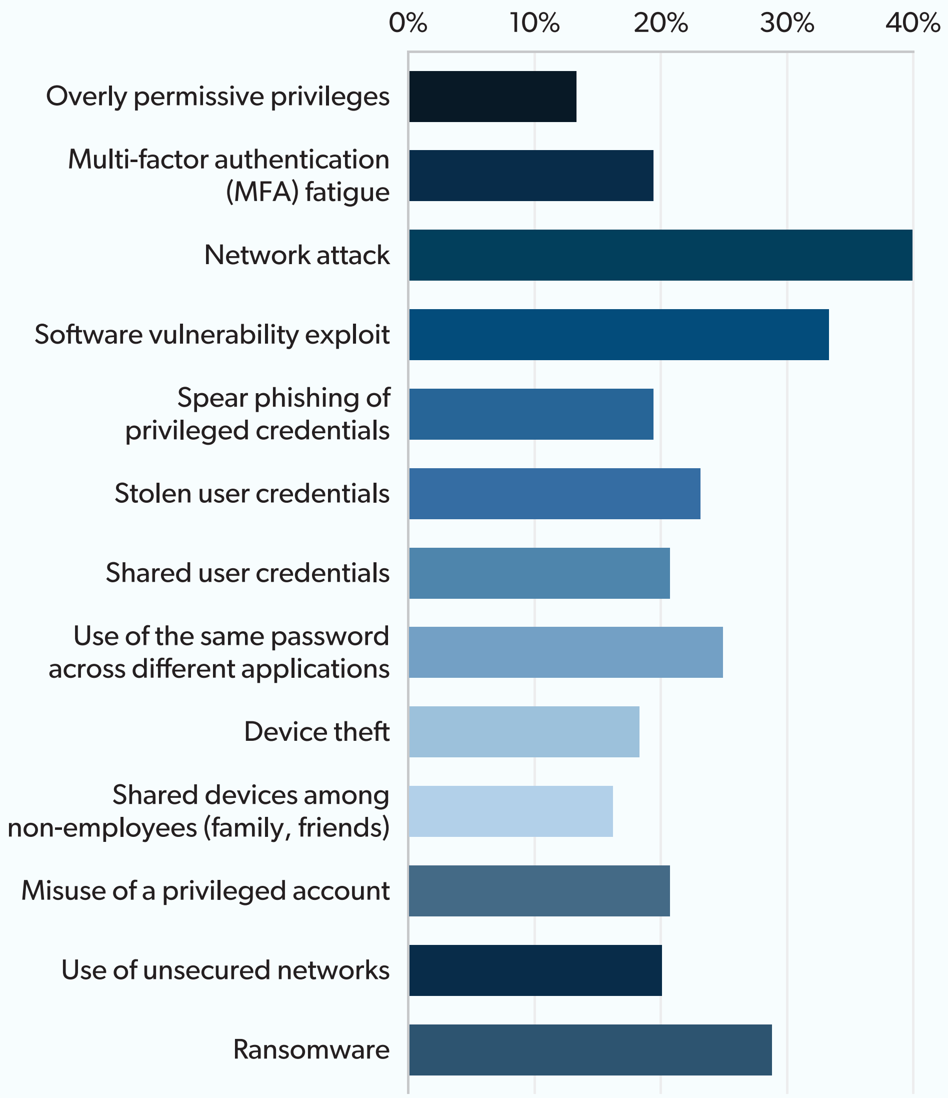


Security and SMEs

Fortifying Against External Threats

The top three security threats remain consistent with what was reported in April 2023. Network attacks topped the list (40%, up from 38% in April 2023), followed by software vulnerability exploits (34%, up from 27% in April 2023), and ransomware (29%, down from 33% in April 2023). The three lowest-ranked security concerns were overly permissive privileges (14%), shared devices (17%), and device theft (18%).

Of the following, please select three that are your biggest security concerns.



Security and SMEs

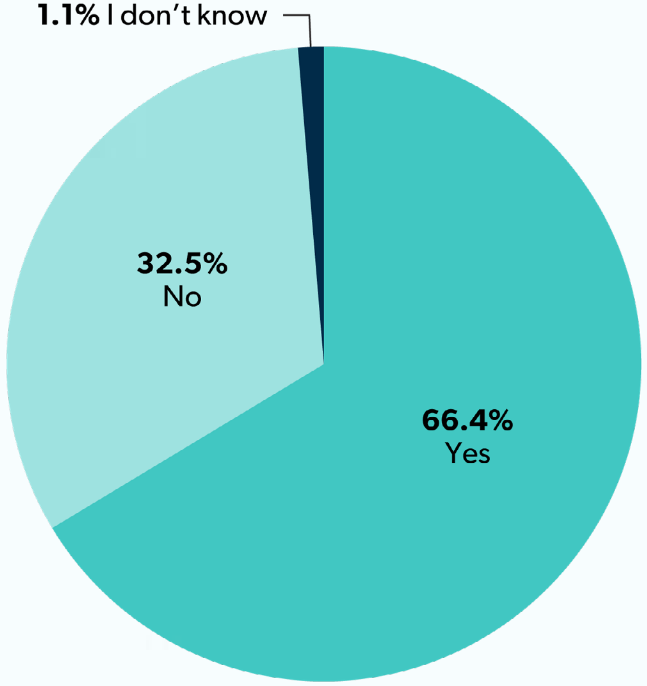
Biometrics Get a Big Thumbs Up

The number of organizations adopting biometrics is swiftly increasing. Two-thirds of organizations require the use of biometrics for employee authentication (66%, up from 55% in April 2023).

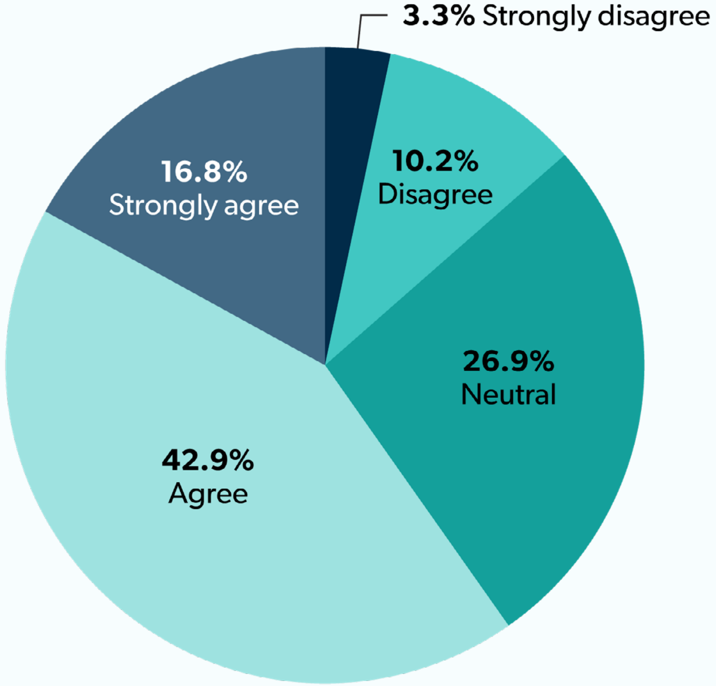
Nearly three of five organizations (60%) agree that adopting biometrics would make their organization's security posture stronger.

Biometrics is seen as the most secure authentication method for MFA (33% rank it as most secure), followed by one-time passcodes (25%), verification app (23%), keys (11%), and mobile push (8%).

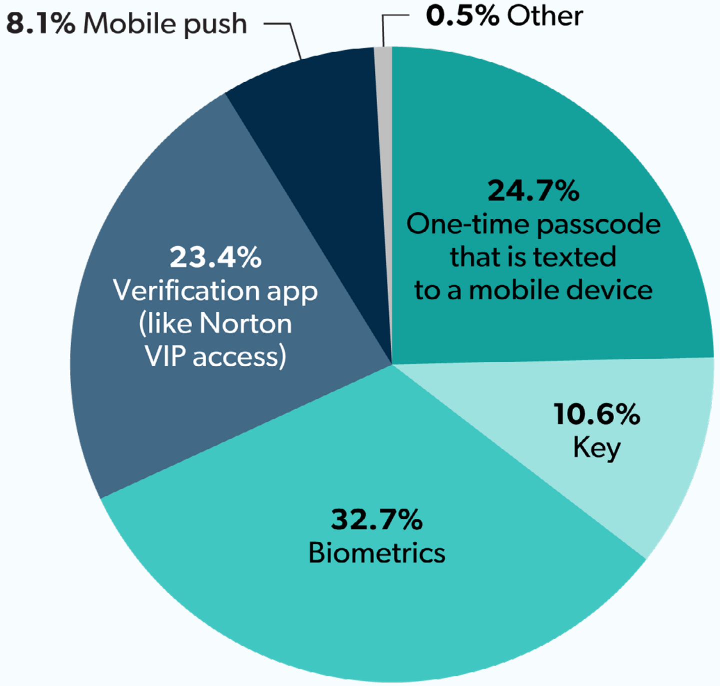
Does your organization require the use of biometrics for employee authentication?



My organization's security posture would be stronger if they required biometrics.



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

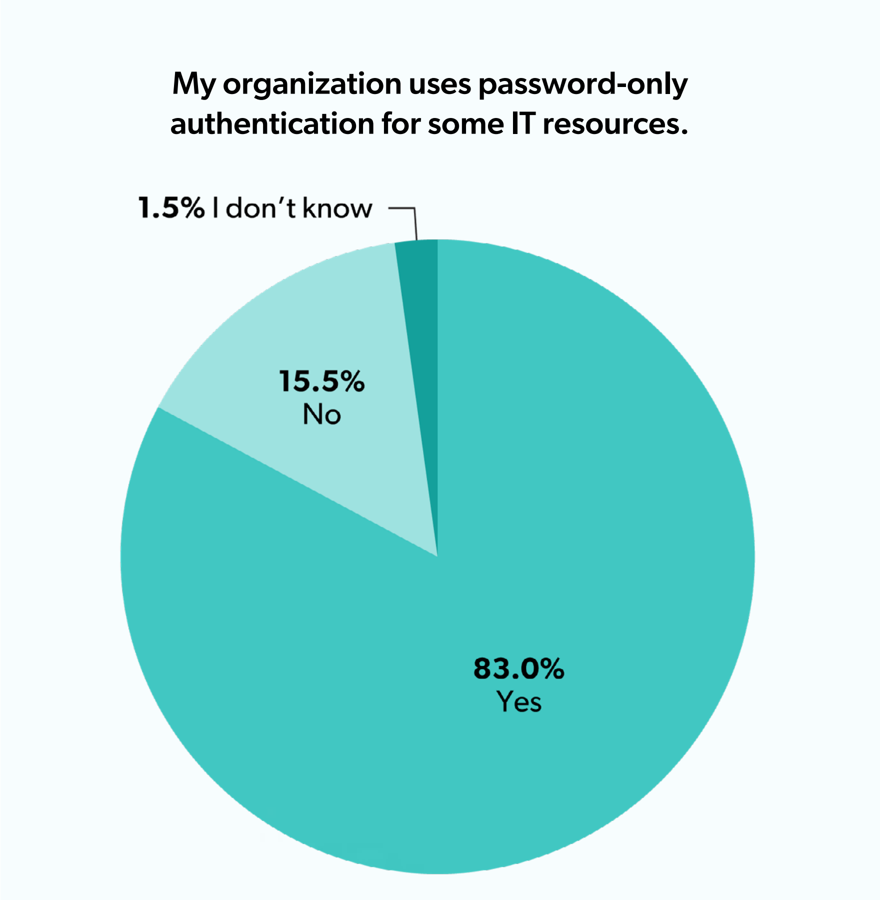


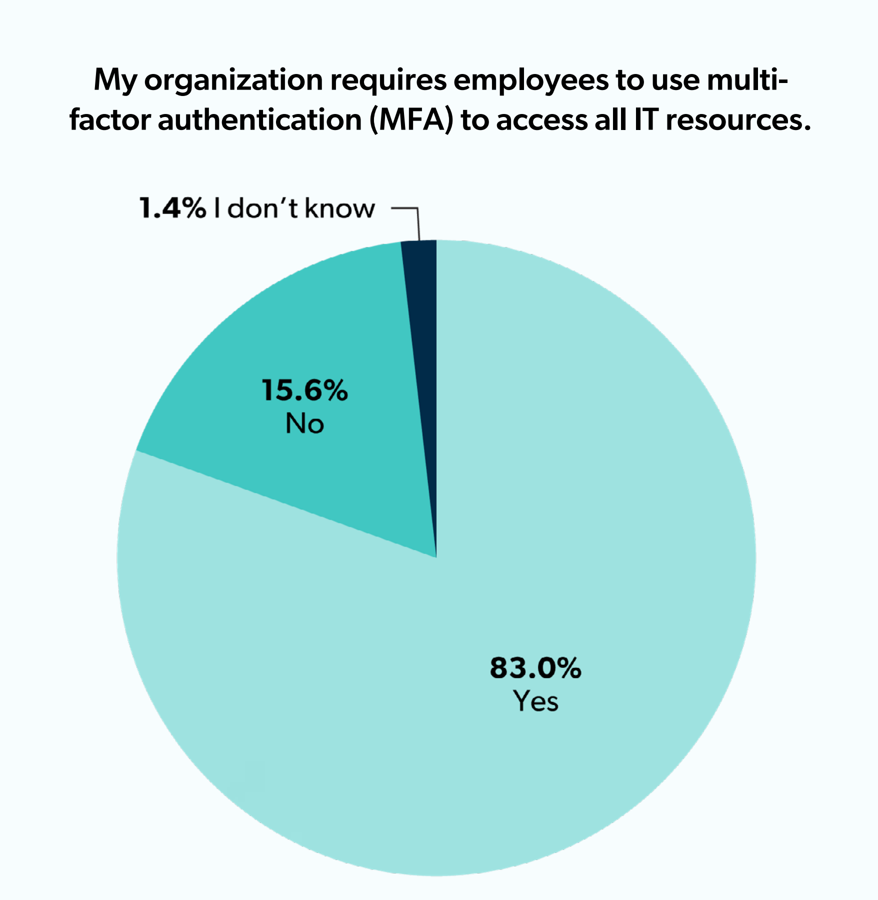
Security and SMEs

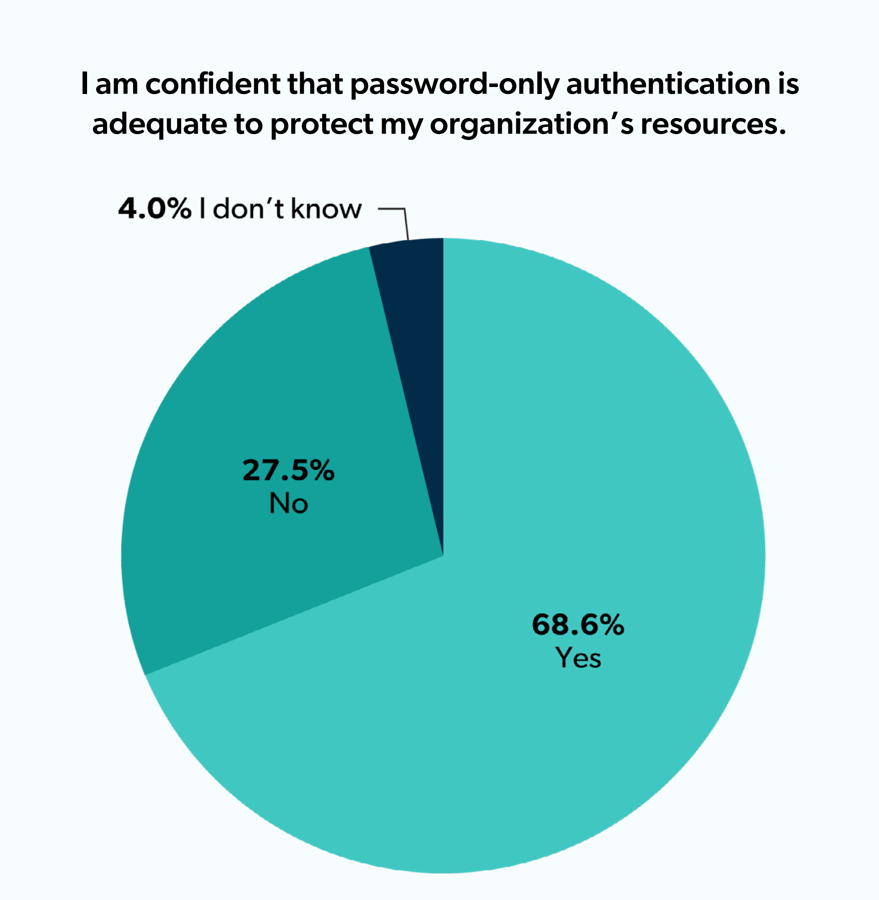
The Staying Power of Passwords

Though passwordless authentication is a stated priority for many, passwords are still a big part of organizational security. Currently, 83% of organizations use password-only authentication for at least some IT resources. Organizations are looking to make password-based authentication as secure as possible, as 83% also require employees to use MFA to access all IT resources.

Despite the broad use of passwords, IT admins have much less confidence in passwords' ability to protect company resources. Over one in four (28%) say password-only authentication is not adequate to protect their organization's resources.


My organization uses password-only authentication for some IT resources.


My organization requires employees to use multi-factor authentication (MFA) to access all IT resources.


I am confident that password-only authentication is adequate to protect my organization's resources.

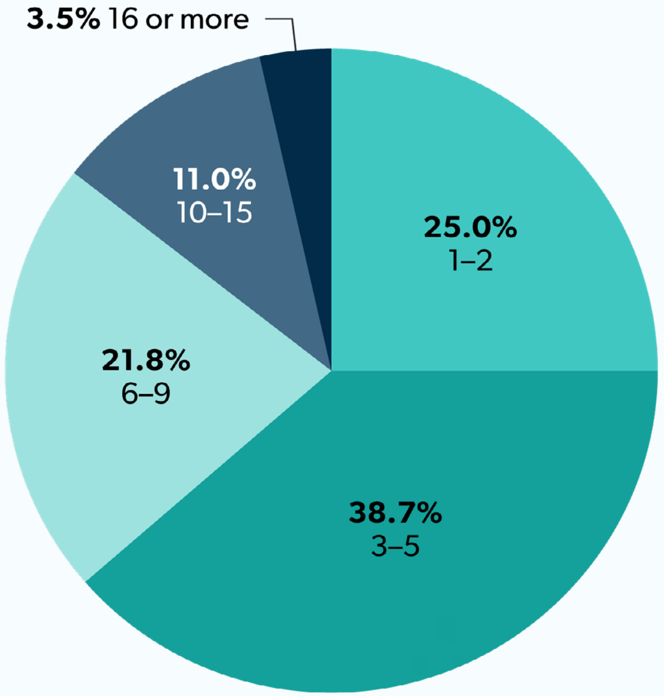
Security and SMEs

Coping with Credential Chaos

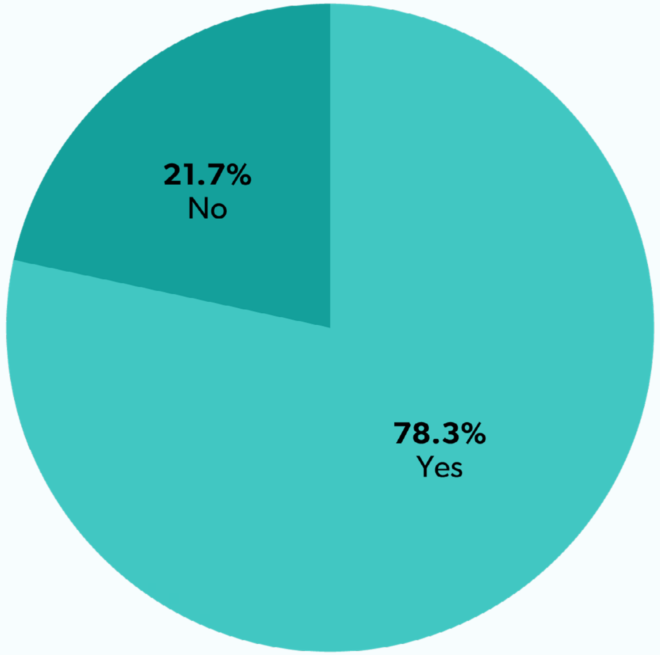
Despite the industry discussions around passwordless authentication, employees continue to juggle a number of different credentials. On average, employees need to manage three to five passwords to log into their resources, though 15% average 10 or more passwords.

Password management systems are a popular tool to help IT teams manage employee access. Nearly eight in 10 (78%) organizations rely on an organization-wide password management tool or software, an increase from 64% in April 2023.

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



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



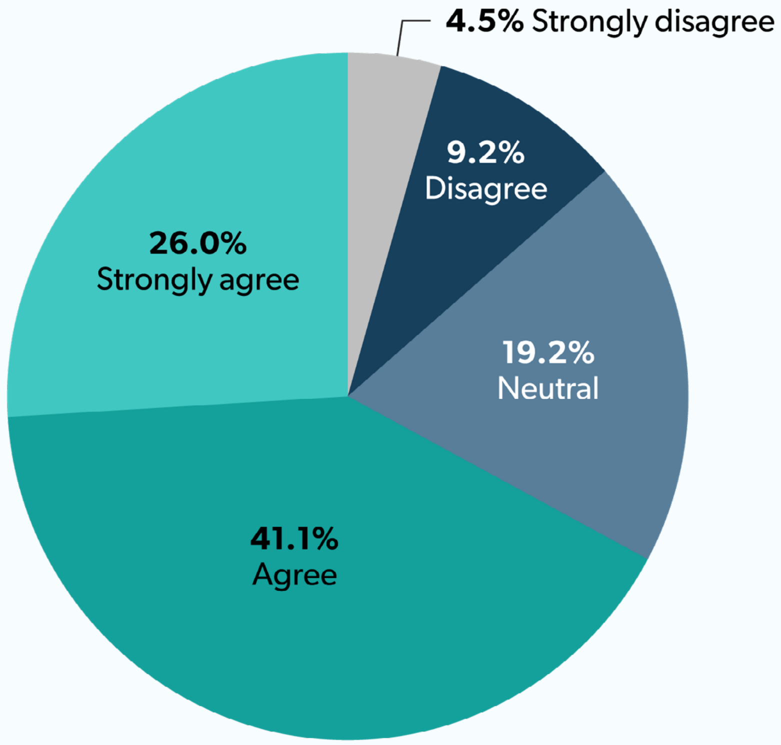
Security and SMEs

Security versus Convenience: Solving Through SSO

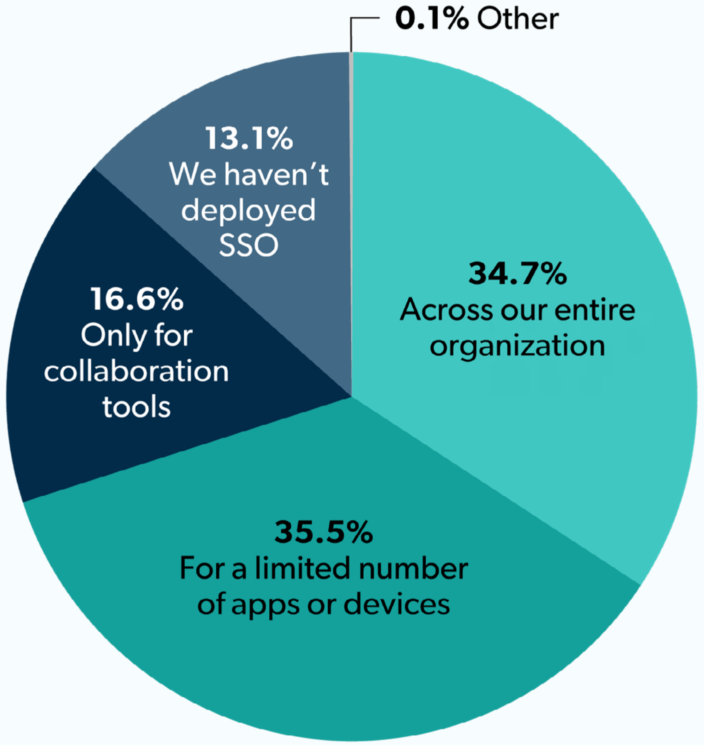
As IT teams survey security options, balancing security and convenience is a growing concern. Over two-thirds of IT admins (67%) agree that adding additional security measures generally means a more cumbersome experience, up from 60% in April 2023.

To help solve the friction issue, IT admins are relying on single sign-on (SSO). SSO adoption remains steady as 87% of organizations have adopted SSO for some resources (versus 88% in April 2023) and 35% have deployed it across the entire organization versus the 26% who reported the same in April 2023.

Additional security measures generally mean a more cumbersome user experience.



We have deployeed single sign-on (SSO):



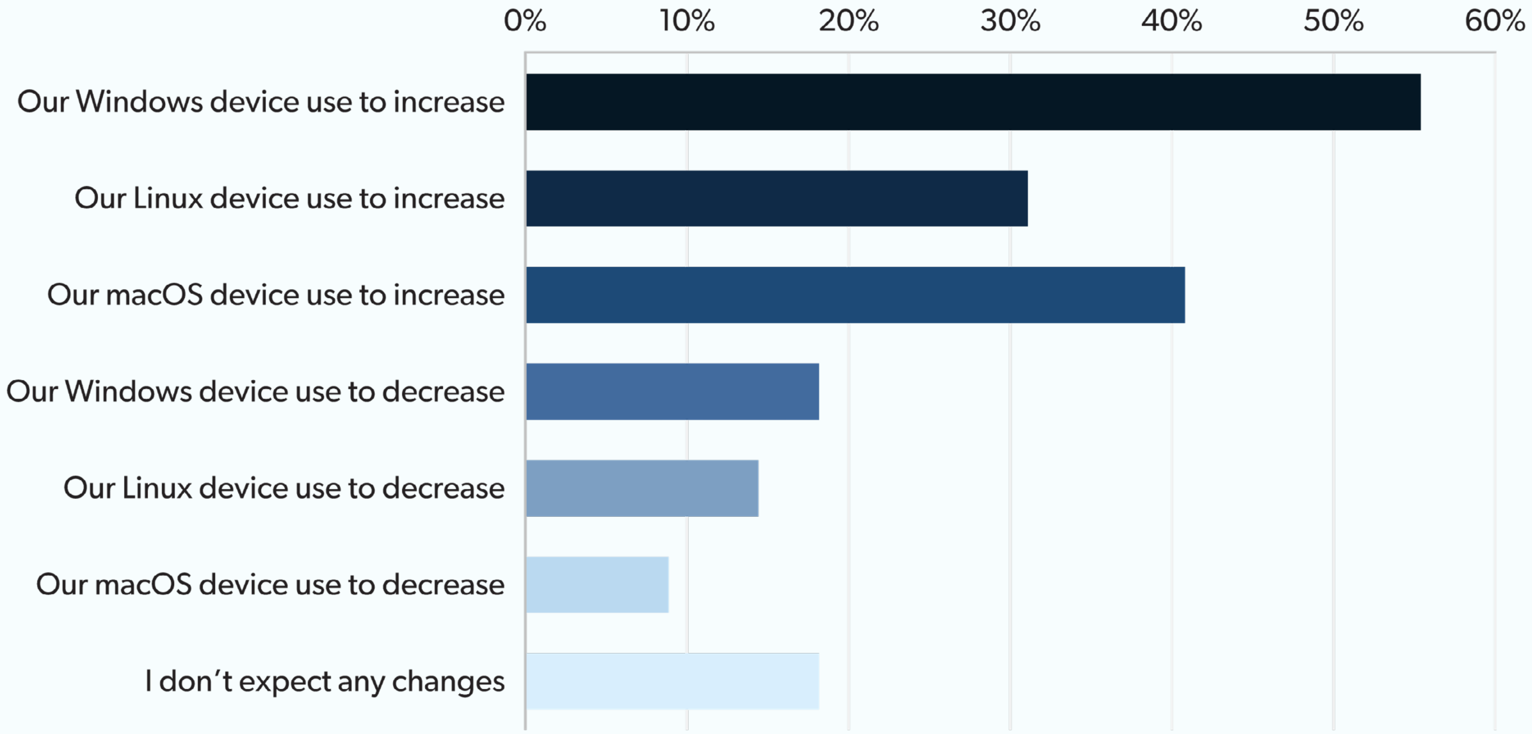
Security and SMEs

Devices: Managing a Mixed Bag

IT teams have adapted with flexibility by supporting a combination of device types. A heterogeneous model (a mix of Windows, macOS, and Linux operating systems) of device environments is the most common. In organizations, the average device type breakdown is Windows 60% (down from 64% in April 2023), macOS 22% (up from 20% in April 2023), and Linux 22% (up from 16% in April 2023).

macOS device use is expected to see the highest percentage increase, with 41% anticipating an increase in macOS use (up from 26% in April 2023), 56% anticipating a Windows increase (up from 46% in April 2023), followed by 31% who anticipate Linux use to increase (up from 26% in April 2023).

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



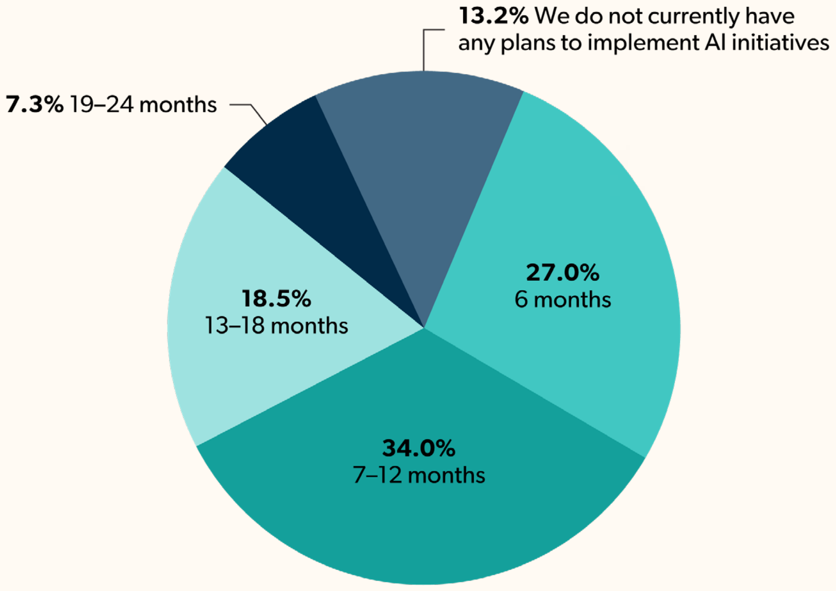
AI and SMEs

Eager to Adopt AI

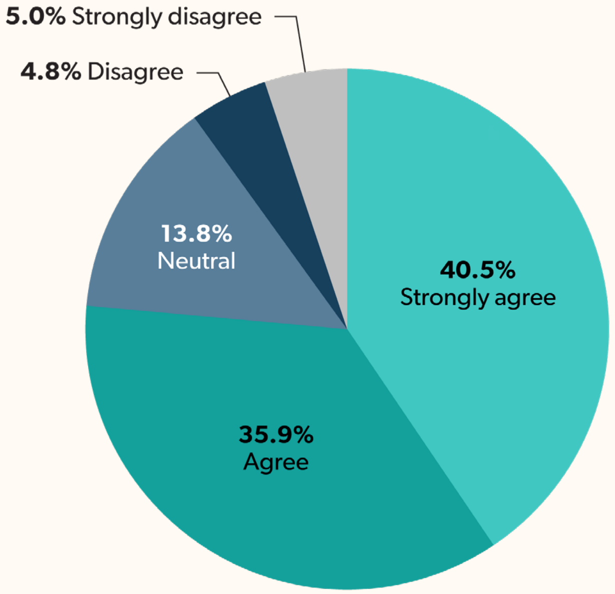
Organizations are actively planning for AI as only 13% of organizations do not currently have any plans to implement AI initiatives. Well over half (61%) expect their organizations to implement AI initiatives within the next year.

IT admins are eager for their organizations to integrate AI. Over three-fourths (76%) agree their organization should be investing in AI, and over half of organizations (63%) have already developed an AI policy.

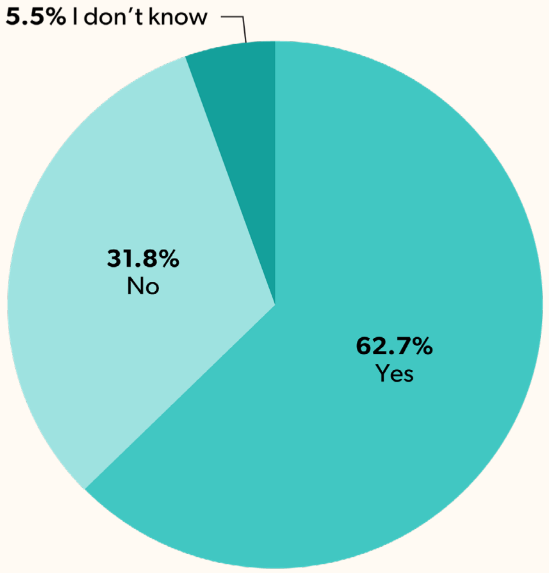
Our organization has plans to implement AI initiatives over the next:



Our organization should be investing in AI initiatives.



Does your company have a policy around AI?



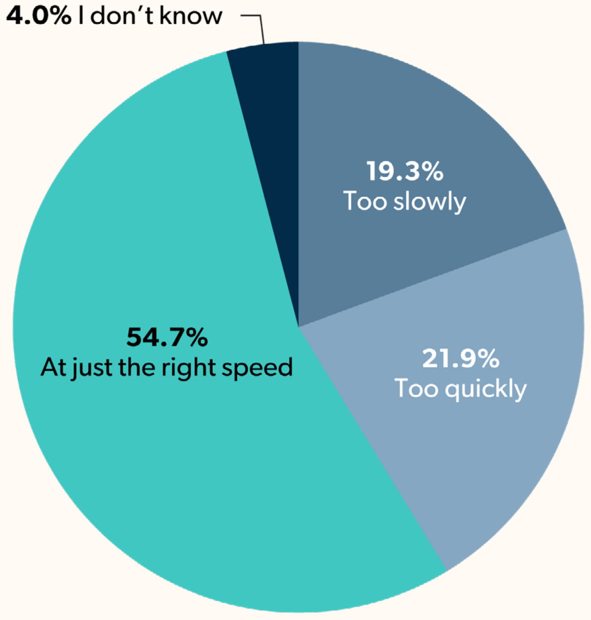
AI and SMEs

Balancing Excitement and Anxiety Around AI

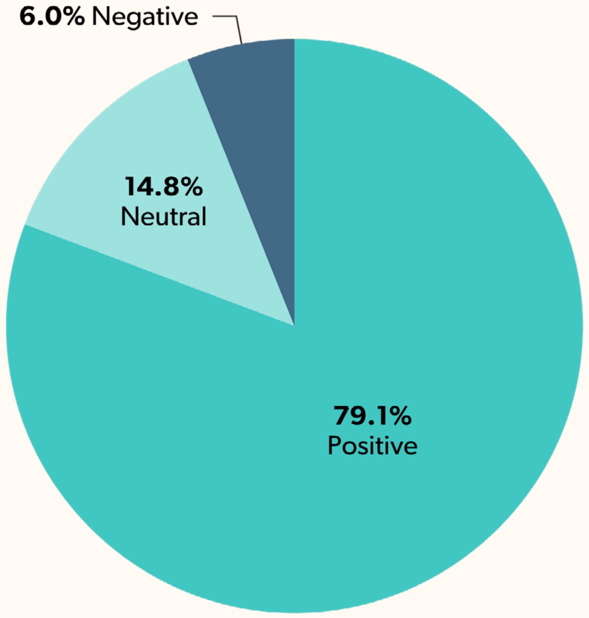
The majority of admins are comfortable with their organization’s approach to AI. Most admins agree their organizations are approaching AI adoption at exactly the right speed (55%). Roughly equal amounts think they are moving too quickly (22%) or too slow (19%).

When asked about the impact of AI on their organization, a vast majority (79%) say AI will be a net positive for their organization versus only 6% who see it as a net negative. But not all is rosy for the AI outlook. Admins are wary about what AI means for their career: nearly half (45%) agree they’re worried about AI’s impact on their job.

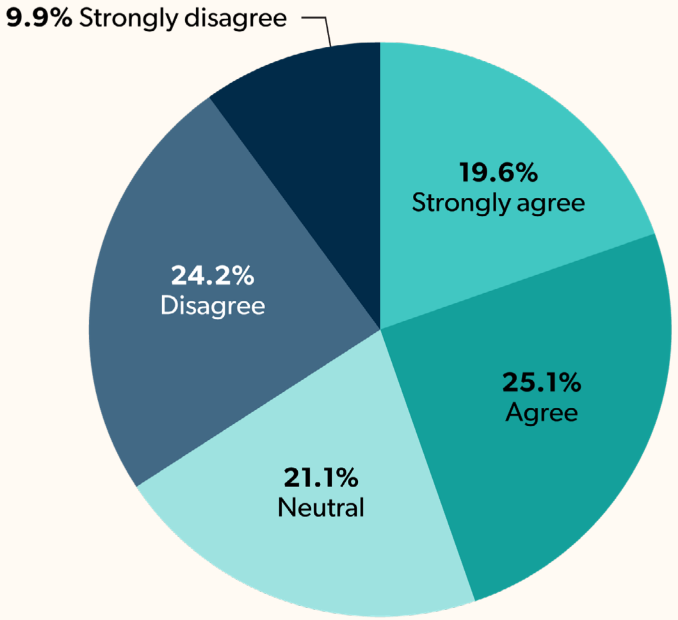
My organization is moving ________________ around AI.



AI will be a net ________ for my organization.



I am worried about AI’s impact on my job.

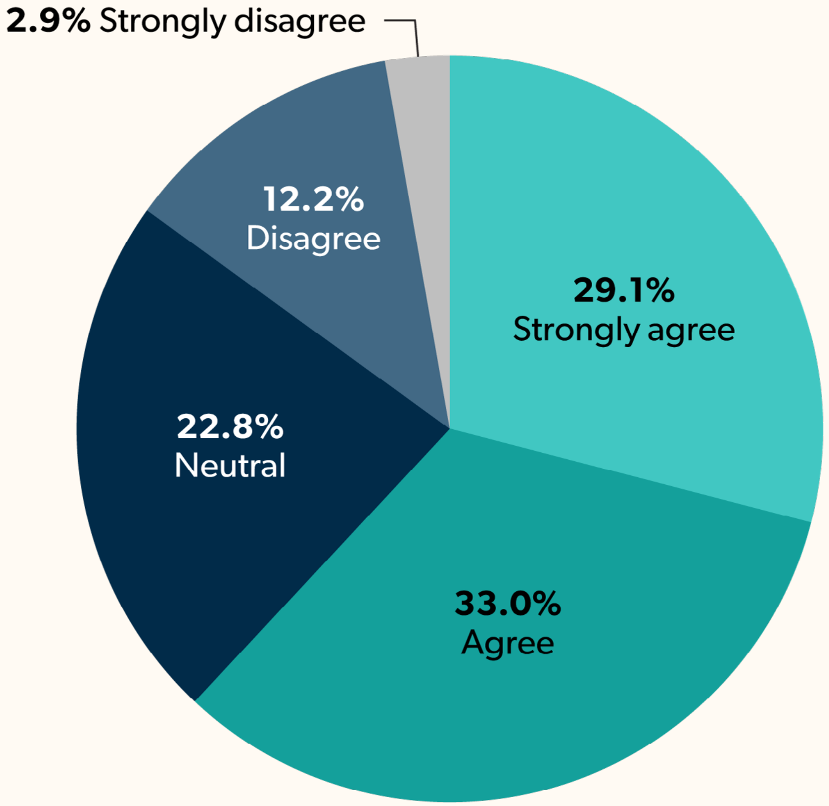


AI and SMEs

AI and Security – More Foe Than Friend

Despite their proactive posture toward AI in their organization, admins also report significant unease around AI's impact on organizational security. Nearly two-thirds (62%) agree that AI is outpacing their organization's ability to protect against threats overall.

AI is outpacing my organization's ability to protect against threats.

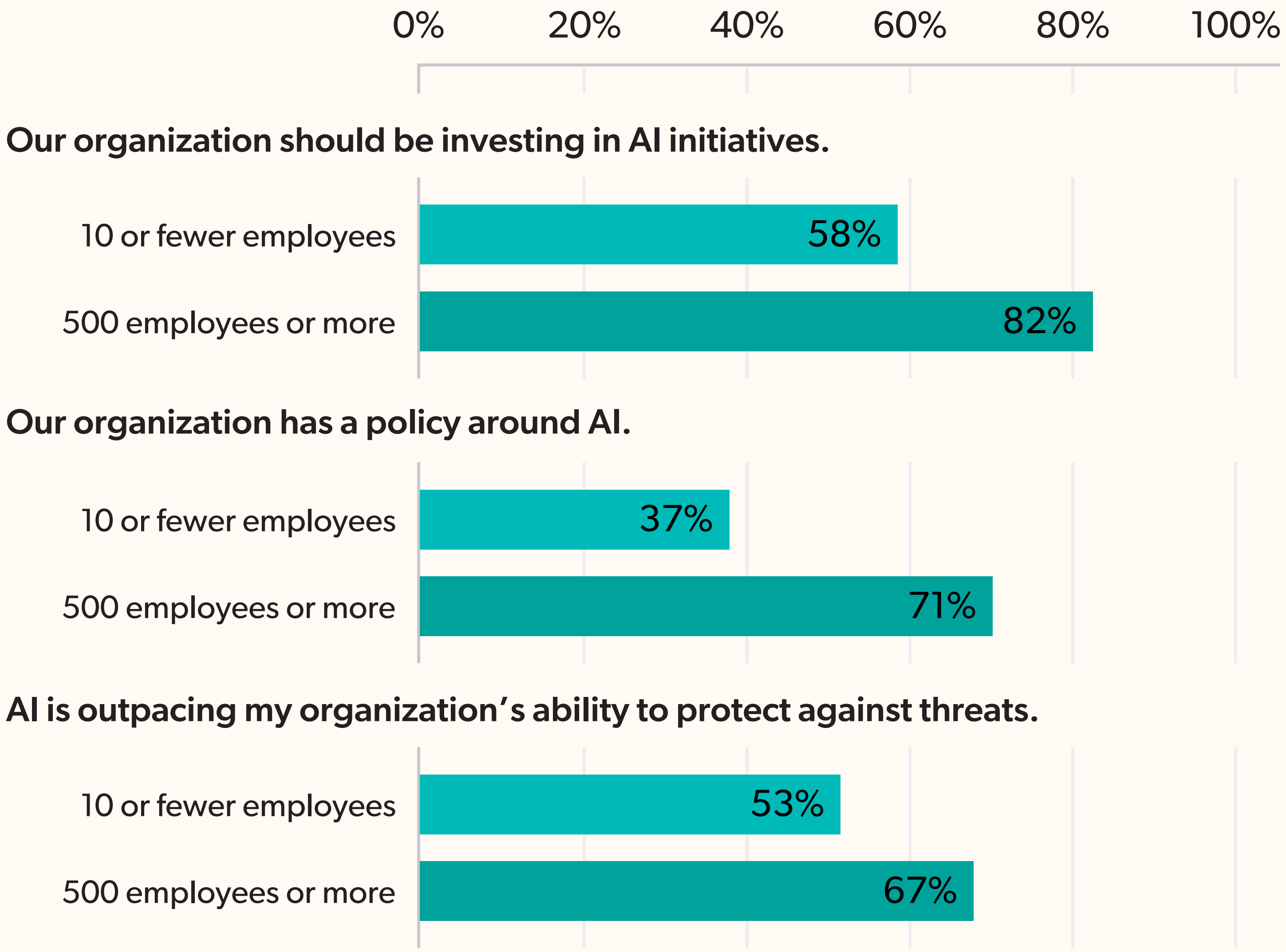


AI and SMEs

Size and Scale Determines AI Approach

Smaller firms are notably less likely to be leaning into AI as aggressively as larger organizations. For admins in organizations with 10 or fewer employees, 58% agreed when asked if their organization should be investing in AI initiatives, versus 82% of organizations with 500 employees or more.

Larger organizations are also more likely to have existing policies around AI. In organizations with 500 or more employees, 71% have developed company-specific AI policies, versus 37% of organizations with 10 or fewer employees. Bigger firms (500+) also have stronger concerns about AI security, with 67% agreeing that AI is outpacing their organization's ability to protect against threats, versus 53% of those with 10 or fewer.



AI and SMEs

How Age and Experience Impact AI Attitudes – Globally

Globally, younger admins are optimistic about the impact of AI on their organization. 82% of admins aged 34 and younger think AI will be a net positive for their organization, versus 64% of admins aged 45 and older. Personally, younger admins are less optimistic than their older counterparts about AI and their career, as

46% of admins 34 and younger agree they're worried about AI's impact on their jobs,

versus just 32% of admins aged 45 and older who agree.

Mid-career U.S. admins are the most eager to adopt AI initiatives:

52% of 35 to 44-year-olds strongly agree that their organizations should invest in AI initiatives

versus 34% of 18 to 25-year-olds and 17% of admins 65 and older.

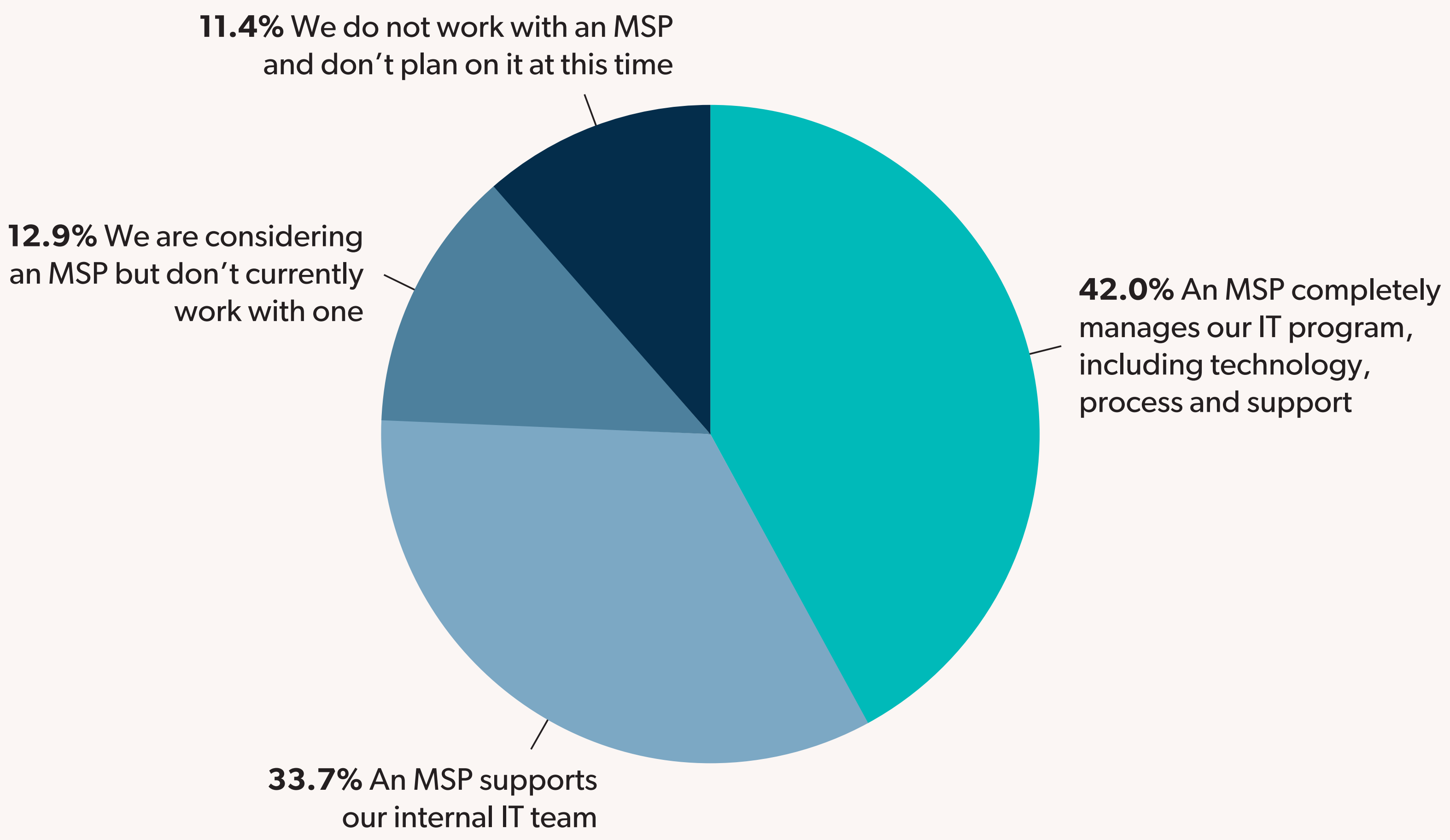
U.S. admins are also more confident about their organization's security posture concerning AI.

When asked whether AI is outpacing their organization's ability to protect against threats, 64% of 18 to 44-year-olds agree or strongly agree versus only 32% of those 45 and older.

MSPs and SMEs

MSPs Stepping Up to the Plate

MSPs continue to be a go-to resource for organizations. Nearly 76% rely on an MSP for some features. Organizations are leaning on MSPs for increased responsibilities. An MSP completely manages the IT environment for 42%, versus 27% in April of 2023—a 56% increase over 12 months.



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

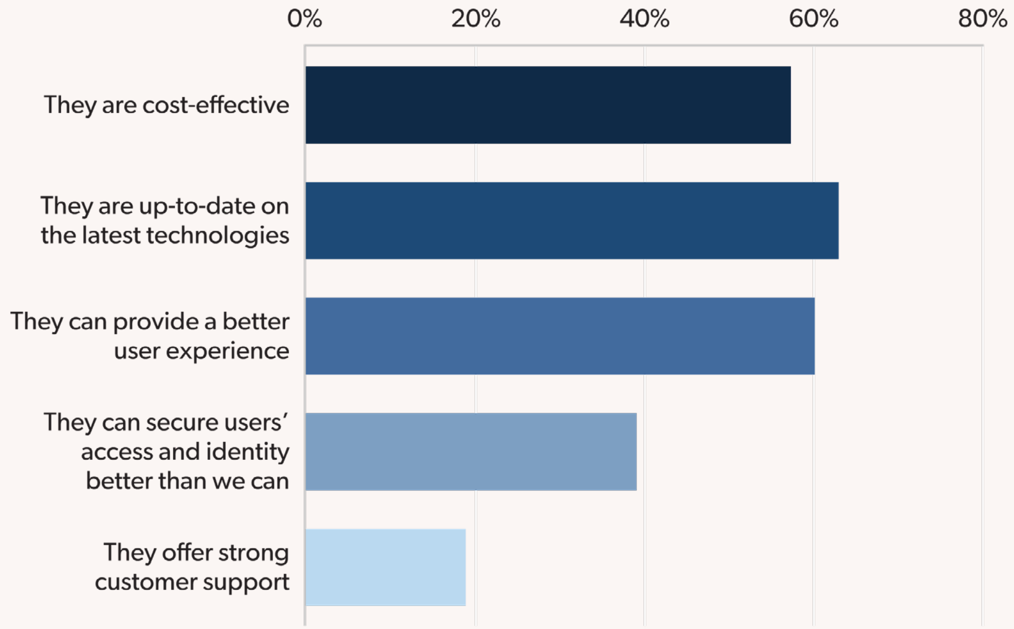
MSPs and SMEs

Functions and Features

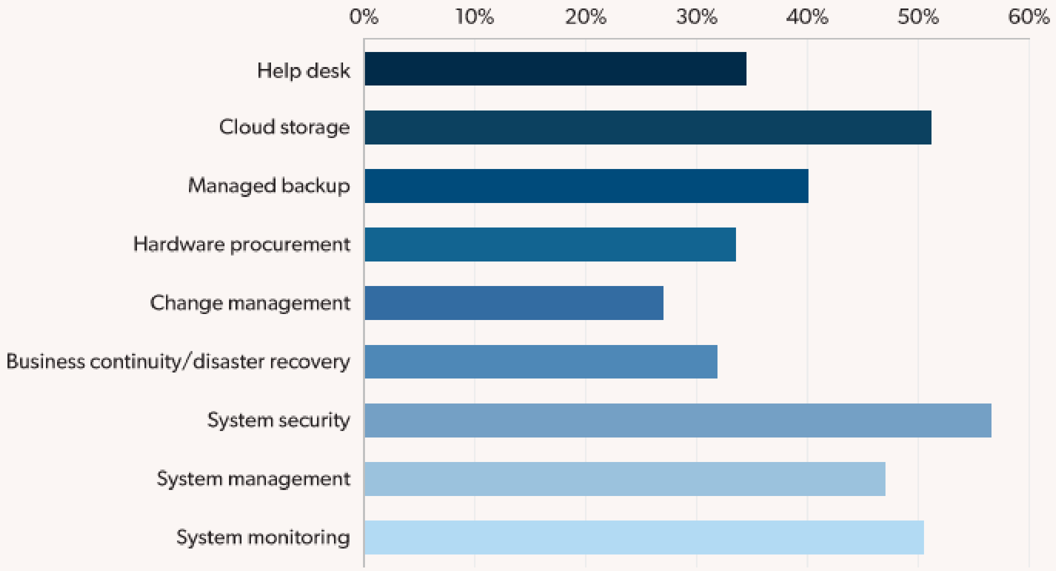
For SMEs working with MSPs, the most popular reason is that they are up to date on the latest technologies (65%, up from 61% in April 2023), they can provide a better user experience (60%, up from 55% in April 2023), and they are cost-effective (56%, up from 50% in April 2023).

System security is the most common area for which organizations use MSPs (57% versus 53% in April 2023), followed by cloud storage (52% versus 53% in April 2023), system monitoring (51% versus 47% in April 2023), system management (47%, same as in April 2023), managed backup (40%, same as in April 2023), hardware procurement (34% versus 33% in April 2023), business continuity/disaster recovery (32% versus 30% in April 2023), help desk (35% versus 30% in April 2023), and change management (27% versus 26% in April 2023).

We use MSPs because (select all that apply):



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



Final Thoughts

IT management for organizations has been undergoing a seismic shift, especially in the wake of recent global events and technological advancements. The sixth edition of JumpCloud's biannual SME IT Trends Report illuminates these changes, emphasizing the significant role of IT professionals in adapting to and shaping the future of the workplace.

The rapid advancement and integration of AI into identity management have brought both optimism and concerns. While there's a strong belief in AI's positive impact on organizations, there's also an awareness of the need for enhanced security measures to keep pace with these technological developments.

IT teams are progressively embracing strategies that streamline and centralize identity management within a flexible, cloud-based framework. This approach is vital in addressing the evolving needs of employees and the complexities of modern IT environments without introducing additional friction or complexity. IT admins have repeatedly shared their wish for a single tool to help manage users' identities and access; this most recent edition of the report reminds us that despite those repeated demands, organizations have been slow to respond. As AI has introduced additional complexities to identity and access management, organizations would be smart to listen to their IT teams and their needs—they know well what security threats exist and how best to manage them.

Other lessons organizations can take from the Q1 2024 SME IT Trends Report:

— **Embrace AI with a balanced approach:** While AI is recognized for its potential to revolutionize IT, it also presents new security challenges. Organizations should adopt AI technologies thoughtfully, ensuring they are complemented by robust security measures to protect against emerging threats. It's about finding the right equilibrium between leveraging AI's benefits and maintaining a secure IT environment.

— **Streamline and centralize identity management:** The complexity of managing diverse devices and identities can be overwhelming. To reduce this complexity, organizations should look toward solutions that offer streamlined and centralized identity management. This approach not only simplifies IT administration but also enhances security by providing a unified overview of all devices and access points.

— **Leverage the expertise of MSPs:** The increasing reliance on MSPs is a testament to their value in contemporary IT operations. Organizations should consider partnering with MSPs to gain access to specialized expertise, user-friendly experiences, and cost-effective solutions. MSPs can play a critical role in managing IT complexities and driving efficiency.

— **Prioritize flexibility and simplicity:** In response to the rapidly changing IT needs and the blurring lines between personal and work devices, organizations should prioritize flexible, open IT solutions. These solutions should be capable of adapting to evolving workplace models and employee needs without adding unnecessary friction or complexity.

As we move forward, it's clear that SME IT teams must continue to be agile, innovative, and forward-thinking. The challenges they face, from economic uncertainties to complex device ecosystems, necessitate a balanced approach that prioritizes both security and usability. The Q1 2024 SME IT Trends Report reinforces the importance of intelligent AI integration, robust security measures, and operational efficiency to foster a productive and secure working environment.

JumpCloud's mission, to Make Work Happen®, resonates strongly in this context. By providing an open directory platform that offers enterprise-level IT management without the associated costs or complexities, JumpCloud is uniquely positioned to support organizations in these challenging times. For those looking to explore JumpCloud's solutions and start immediately, visit **console.jumpcloud.com/signup**.

Methodology:
JumpCloud surveyed 1,213 SME IT decision-makers in the U.K., U.S., and India, 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, from November 14, 2023 to November 27, 2023.

jumpcloud™

JumpCloud® helps IT teams and managed service providers (MSPs) **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 been used by more than 200,000 organizations, including GoFundMe, Grab, ClassPass, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

Learn more at jumpcloud.com

Follow us: Blog | Community | Twitter | LinkedIn | YouTube

Click here to get started with JumpCloud