jumpcloud™

SME IT TRENDS Q1 2025

From Chaos to Control:

Simplifying IT in the Fast Lane of Change

The IT Landscape

Devices

AI

Security

MSPs

Executive Summary

Managing IT today means navigating a minefield of rising costs, fragmented ecosystems, and ever-evolving security threats. IT admins are under constant pressure to juggle complex device environments, shadow IT risks, and the rapid advance of AI—all while delivering a simple and seamless user experience.

The pace of change can feel relentless. Nearly 90% of IT admins worry about unauthorized apps and devices expanding their attack surface, while 67% are concerned that AI's rapid rise outpaces their ability to secure against AI-driven threats. With IT sprawl overwhelming many teams, 85% of admins are calling for a unified platform to manage devices, identities, and access, simplifying their increasingly fragmented environments.

Despite the rapid pace of change, JumpCloud's biannual SME IT Trends Report reveals that IT teams remain remarkably resilient. In response to increasing pressures and rising challenges, IT practitioners continue to seek ways to make it simple for employees to get their job done while securing their organizations. They remain convinced that IT management can be simplified. They are stepping up investments in IT for better security. They are leaning into emerging technologies and determining the best way to support an increasingly complicated device environment.

Key Findings

Shadow IT: A Silent Epidemic

- Nearly 90% of IT admins are alarmed by shadow IT, and estimate most employees use one to five unauthorized applications.
- Lack of IT visibility fuels the chaos. 38% of admins admit they can't even discover all applications in use.

AI: A Double-Edged Sword of Innovation and Fear

- AI's rapid rise sparks both hope and terror. 67% of admins feel AI is outpacing their ability to secure it, while 37% worry it will take their jobs.
- But organizations aren't opting out. 42% of organizations plan to invest in AI-related IT tools within six months and 77% plan to implement AI initiatives within the next year.

Hybrid Work: The Great Divide

- U.S. companies are leading the charge back to offices. 57% mandate full-time in-office work, compared to only 41% in Australia and 42% in the U.K.
- Globally, IT struggles to keep up with this fragmented workforce model while ensuring seamless security and support.

MSPs: From Sidekicks to Superheroes

- Once a cost-savings tool, MSPs are now strategic lifelines. 35% of organizations rely on MSPs to fully manage IT, a significant jump from last quarter.
- The stakes are higher than ever. 44% worry about MSPs' ability to manage security effectively.

Key Findings

IT Sprawl: The Unseen Threat

- Admins are drowning in tools. 26% still require 11+ tools to manage employees' IT needs, while 47% say managing too many point solutions is their No. 1 challenge.
- Rising costs pile on. 39% spend 26-50% of their entire budgets on licensing fees, up from 28% in Q3 2024.

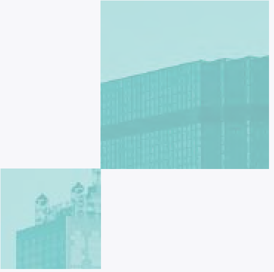
Cybersecurity: The Never-Ending War

- The battlefield intensifies. 46% of organizations have experienced a cyberattack, 33% of which were due to AI-generated attacks. It's no surprise that 55% of IT teams are more concerned about their security posture than they were six months ago.
- Despite rising security concerns, only 30% of admins patch critical systems within hours of them being released.

IT teams are regularly evaluating the tech landscape and what's on the horizon to adjust their approach. These professionals aren't content with their organization simply keeping up, they want to set the pace. JumpCloud's Q1 2025 SME IT Trends Report, *From Chaos to Control: Simplifying IT in the Fast Lane of Change*, dives into how IT teams are conquering these challenges and choosing control over chaos. From securing diverse device ecosystems to balancing AI innovation with caution, the report highlights the approaches admins are adopting to simplify IT and stay ahead.

The IT Landscape

Hybrid or Headquarters: IT’s Role in Shaping Workspaces



IT admins are adjusting to a mix of workplace models: Nearly half (47%) of organizations surveyed have required employees to return to the office 100% of the time, 43% require workers in-office a few days per week, and 9% have no in-person requirements (**Chart 1**).

More U.S. organizations (57%) are requiring workers to return to the office full-time, vs. 42% of U.K. organizations and 41% of Australian organizations who have similar expectations (**Chart 2**).

Is your company requiring employees to return to the office?

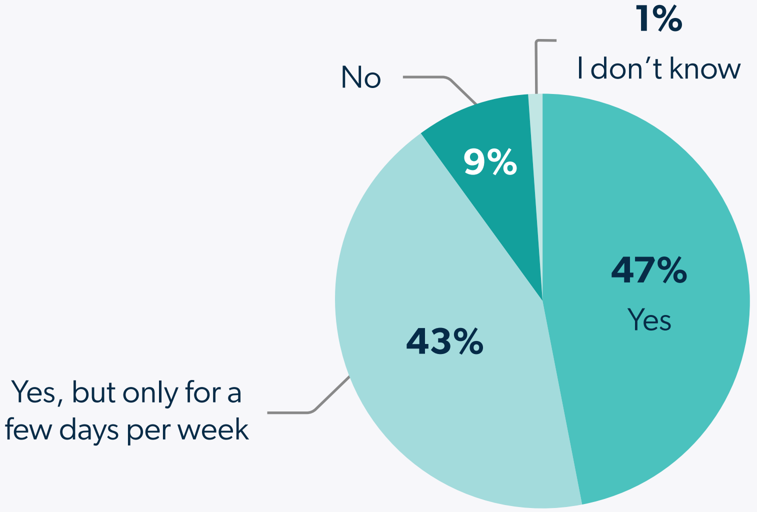


Chart 1

Who’s returning to the office?

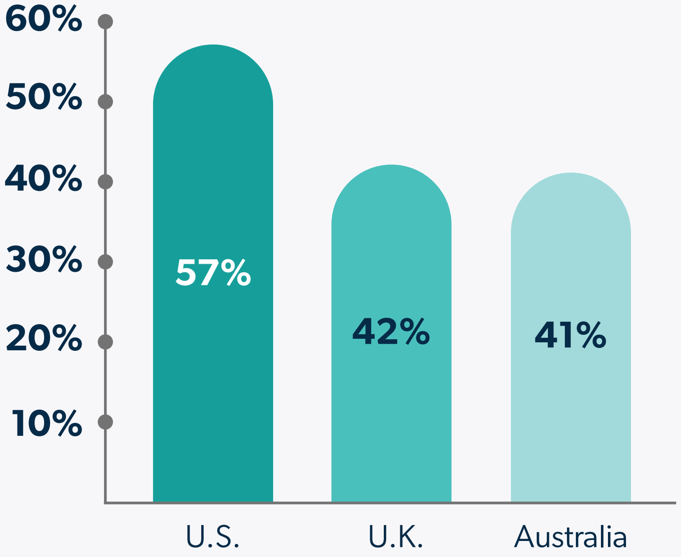


Chart 2

Workforce Woes with Worldwide Layoffs

While IT teams have already navigated much uncertainty over the past few years, the general business outlook remains bumpy, with increased anxieties around job security. 72% of admins have gone through layoffs or anticipate them over the next six months. 30% have already gone through layoffs and anticipate additional layoffs over the next six months (up from 28% in Q3 2024), 23% have gone through layoffs in the last six months and do not anticipate more (up from 21% in Q3 2024), and 19% have not gone through layoffs but anticipate layoffs over the next six months (up from 18%). A little over one-quarter (28%) have had no layoffs and no expectations of them (down from 33% in Q3 2024) (**Chart 3**).

Staffing issues are hitting Australia the hardest, with 81% experiencing layoffs or expecting them over the next six months, with 69% of U.S. and 66% of U.K. firms reporting the same.

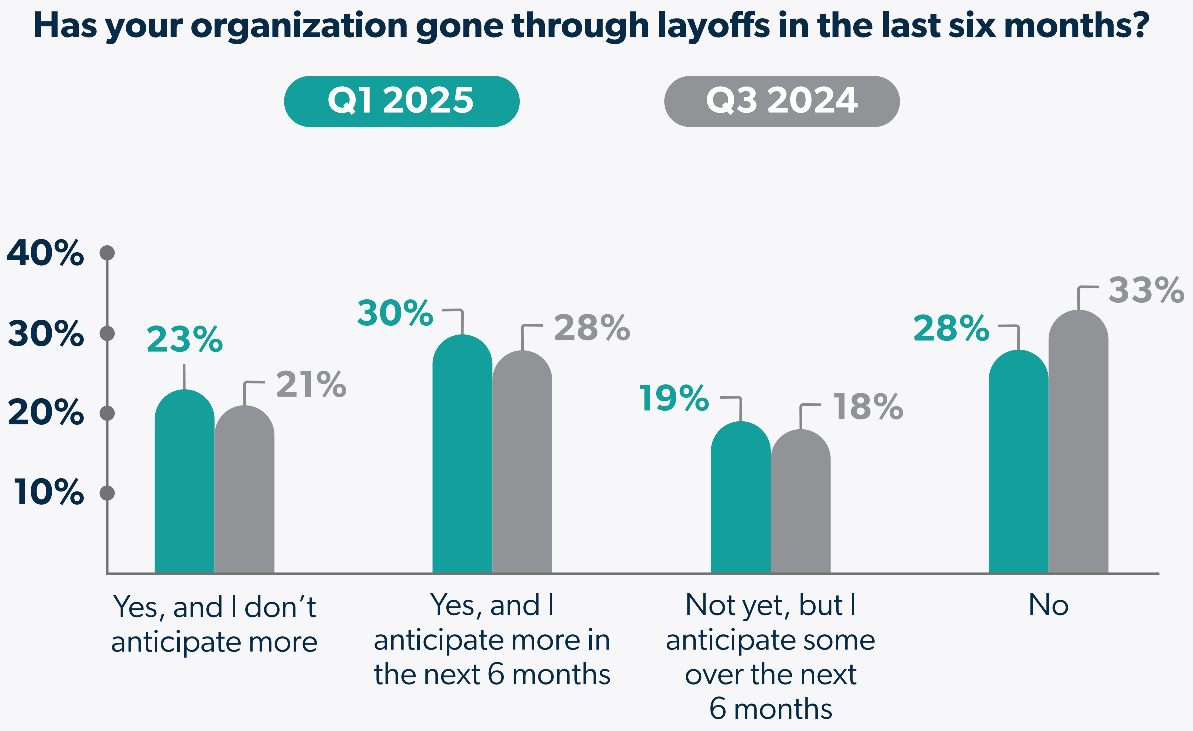


Chart 3

Thriving Budgets in Turbulent Times

Despite staffing uncertainty, attitudes toward general IT budgets remain positive as 77% of admins expect their IT budget to increase over the next 12 months, up from 70% in Q3 2024 (**Chart 4**).

Admins report that the top areas for IT spending are cybersecurity tools and services (48%), AI-related IT tools (42%), cloud infrastructure (40%), IT service providers or MSPs (37%), and IT asset management (ITAM) (35%). The lowest spending priorities are Zero Trust (16%) and additional headcount (22%). These investment priorities suggest that IT teams are seeking to optimize innovation and security and are looking to leverage AI investments for efficiencies (**Chart 5**).

In 2025, I expect our IT budget to:

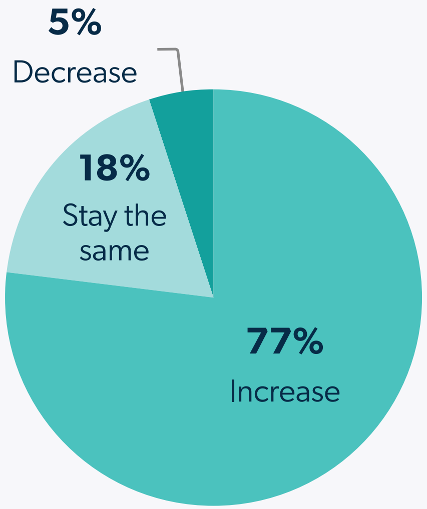


Chart 4

Which areas of IT are you planning to invest in over the next 6 months?

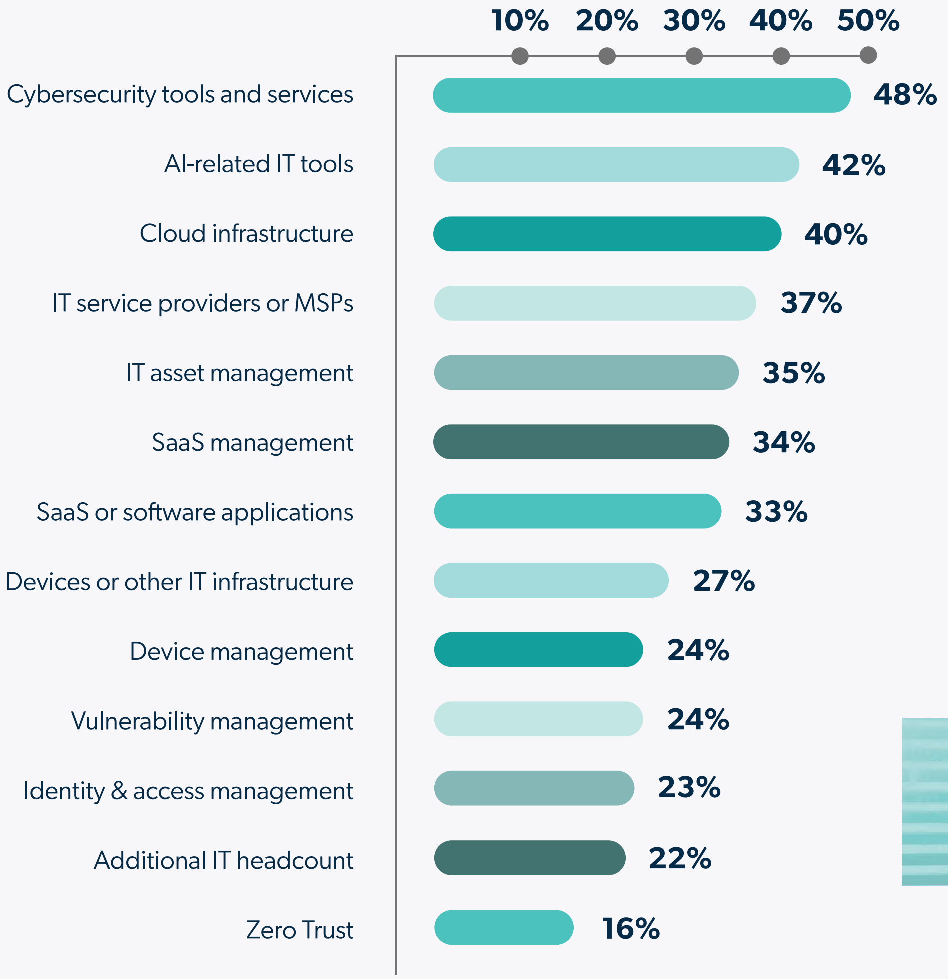
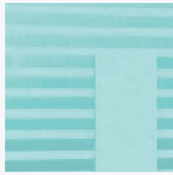


Chart 5



Tool Overload and the Quest for Simplicity

IT admins continue to wrestle with IT sprawl with a continued preference for a single tool for IT management (85%). IT teams most commonly use five to 10 tools for IT management (48%), though over a quarter (26%) use 11 or more, down slightly from 28% in Q3 2024 (**Chart 6**).

How many tools or applications do you/your IT team use to manage the employee lifecycle and the resources they need to do their job?

(e.g., onboarding, device management, security tools, directory services, offboarding, help desk, etc.)

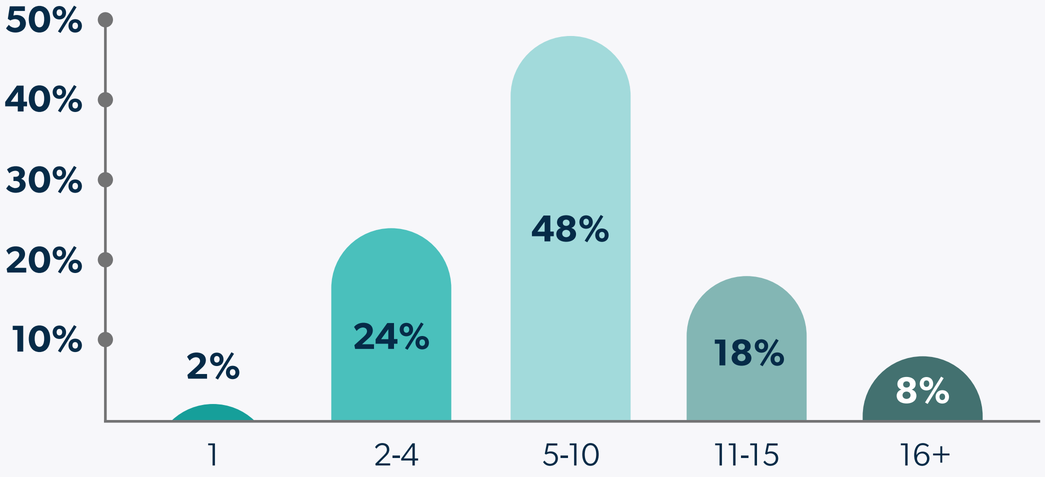
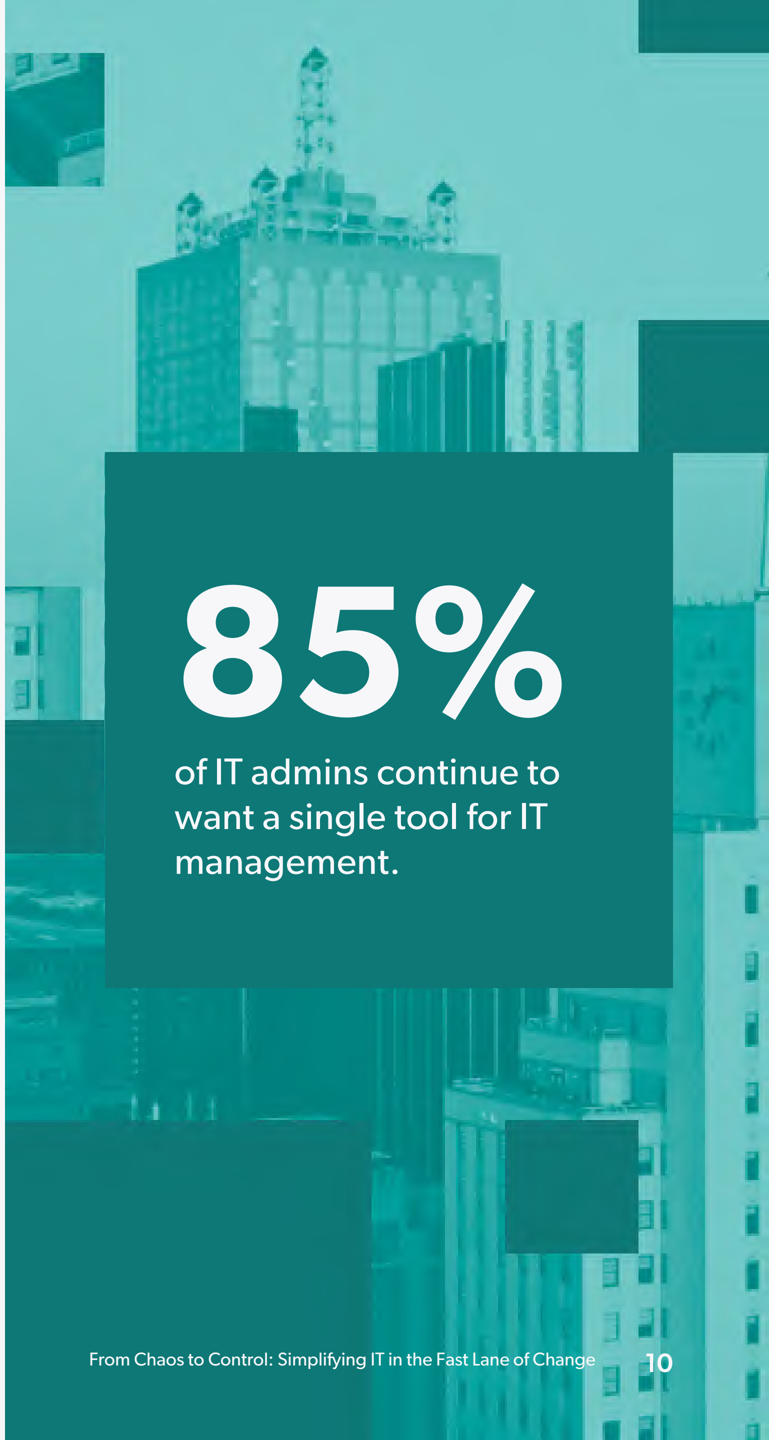


Chart 6



85%

of IT admins continue to want a single tool for IT management.

Tool Overload and the Quest for Simplicity

Managing multiple point solutions is a top-three challenge for nearly half of admins, with 47% of admins reporting it's a top challenge along with 47% who say the same about new services and application rollouts (**Chart 7**).

Adding to the pressure are rising licensing costs. Now only 7% of organizations spend less than 10% of their budget on licensing compared to 11% in Q3 2024, and 39% spend 26-50% of their budget on licensing, up from 28% in Q3 2024.

What have been the biggest challenges to your IT team in Q4 2024?

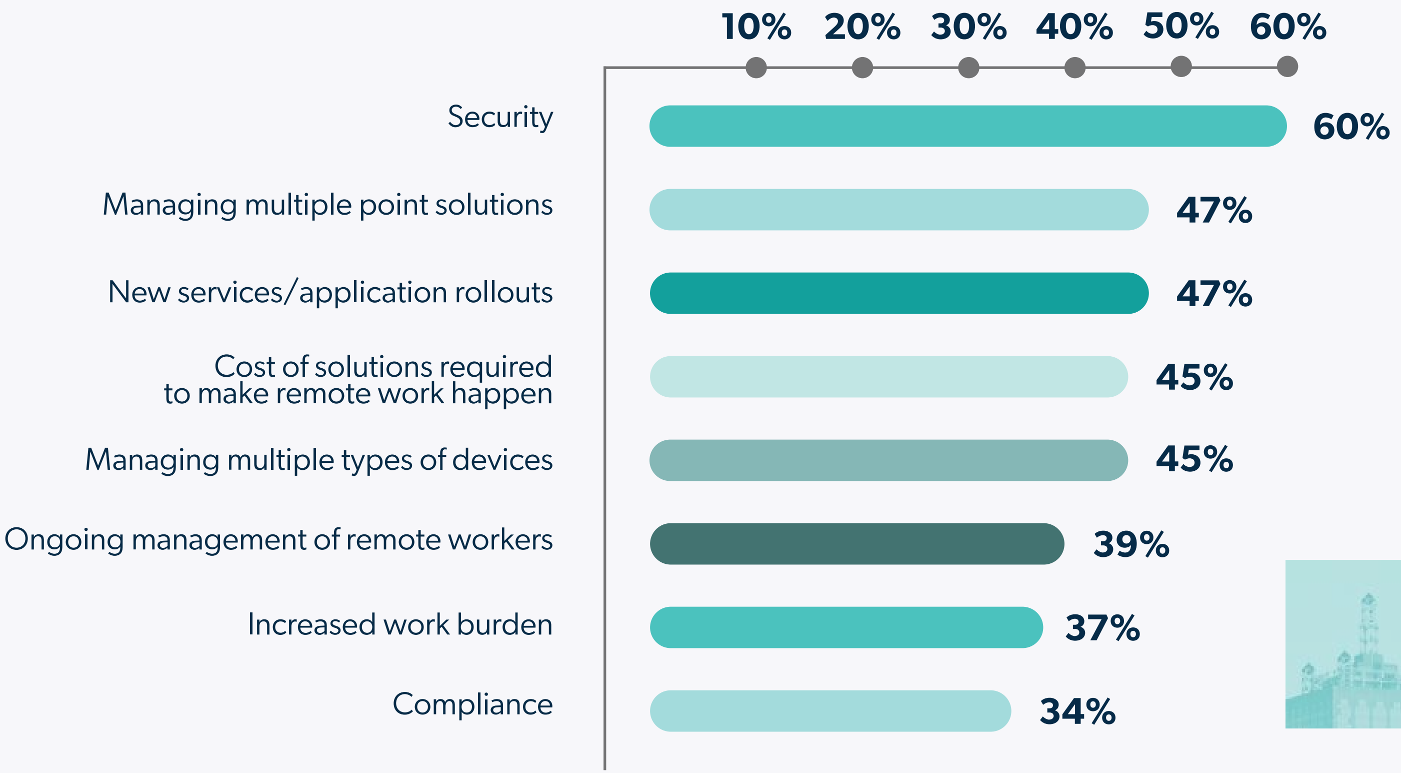
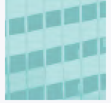
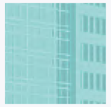


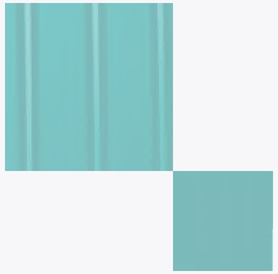
Chart 7

Lockdowns without Logjams





IT teams are wary of adding unnecessary friction to the user experience, and admins report the biggest roadblock to implementing stronger security controls is additional security measures usually mean poor user experience (46%). The other roadblocks cited were having too many tools already (36%), lack of budget (32%), can't hire staff (29%), and teams don't have adequate expertise (20%) (**Chart 8**).



What has prevented you from implementing stronger security controls?

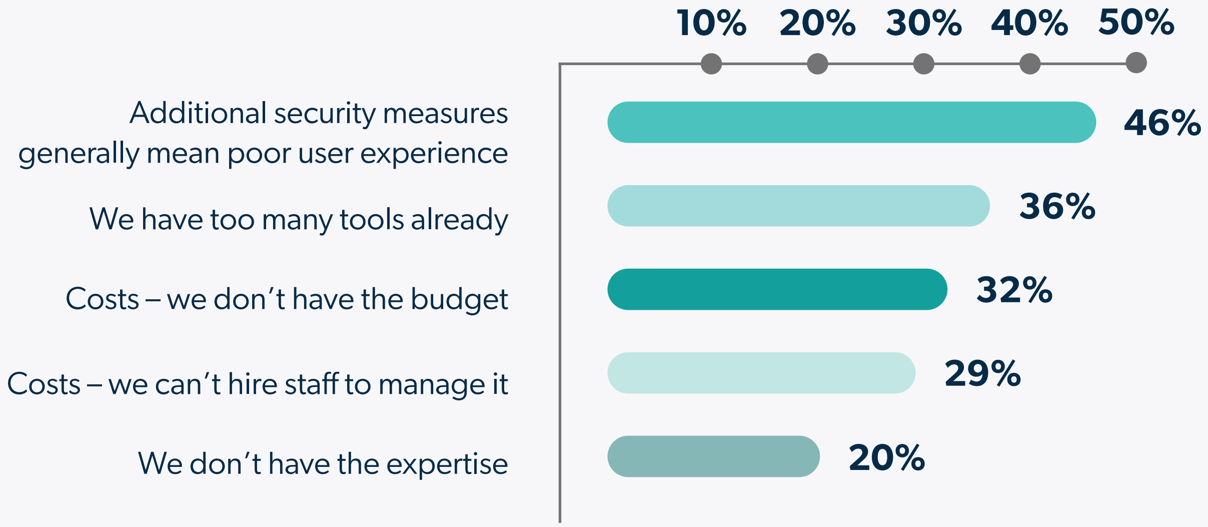
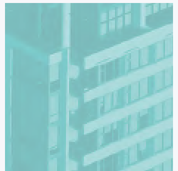


Chart 8



Lockdowns without Logjams

Managing too many solutions may be putting organizations at higher risk. When asked how long it takes to roll out the latest OS patches, 30% say hours, 43% say days, 22% say weeks, and 5% say months (**Chart 9**).

How long does it take you to roll out the latest device OS patches?

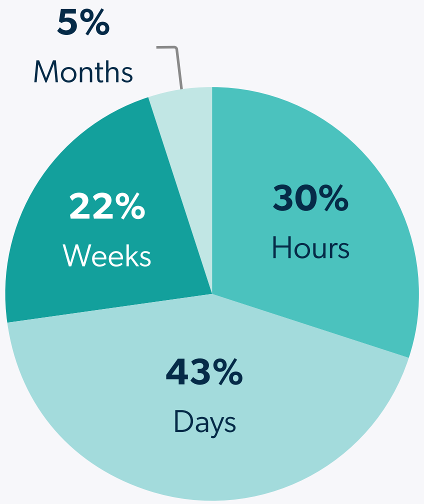


Chart 9

> **"What keeps me up at night is the lack of cohesive information and reliable data on what is actually occurring."**
>
> — Anonymous survey respondent

Security

Security Showdown: Today’s Top Threats

Security continues to be the biggest challenge for IT admins, with 60% of organizations reporting it as their top challenge, followed by new services/ application rollouts (47%) and managing multiple point solutions (47%).

When drilling down on specific security issues, software vulnerability exploits (34%), network attacks (33%), use of unsecured networks (26%), and ransomware (26%) are admins' top security concerns (**Chart 10**).

Admins’ biggest security concerns are:

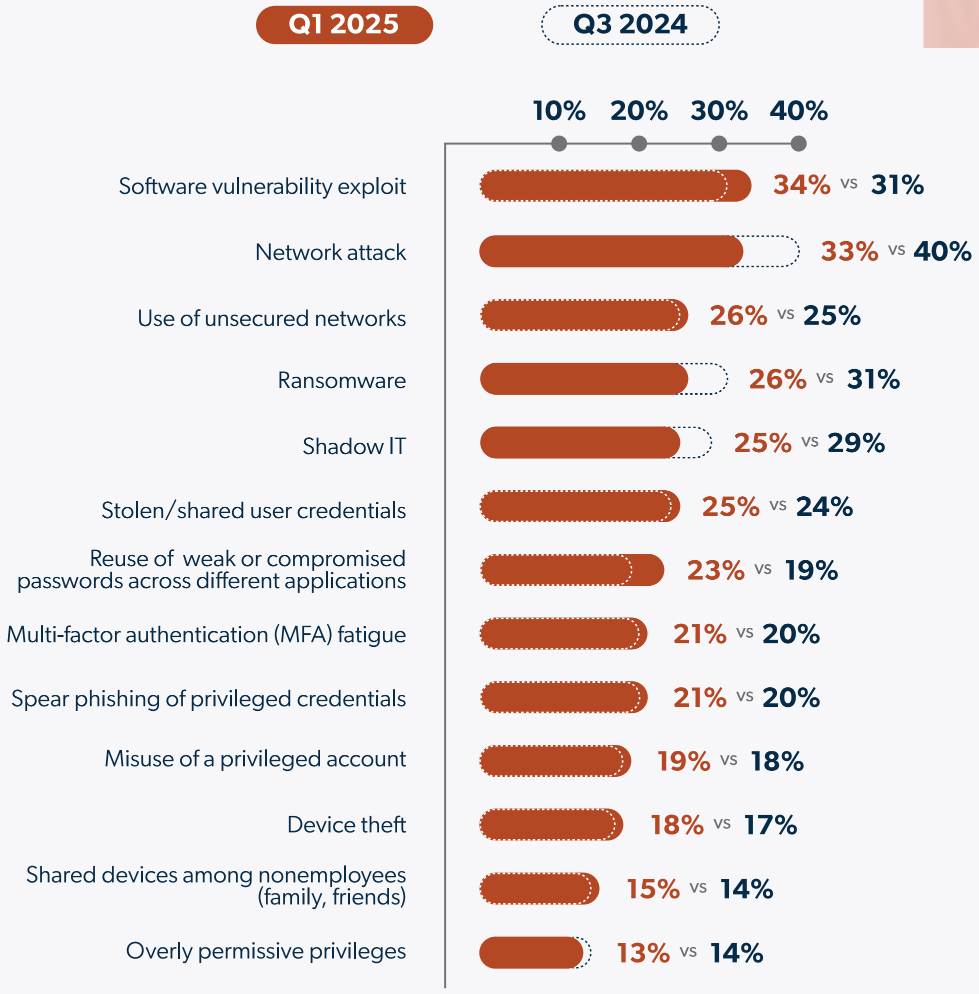


Chart 10

60%

of admins say security is their biggest challenge.

Security Concerns Surge, Organizations Step Up Cybersecurity Staffing

More than half of IT admins (55%) are more concerned about their organization's security posture than they were six months ago, an increase from 50%. Regionally, more Australians report concerns (59%), compared to 53% of U.K. admins and 51% of U.S. admins (**Chart 11**).

Despite security concerns, organizations are staffing to meet the challenge, with 72% reporting they have a cybersecurity staff member on their team and 17% have access to one through their MSP. Only 10% report having neither, down from 15% who said the same in Q3 2024 (**Chart 12**).

Security concerns across regions:

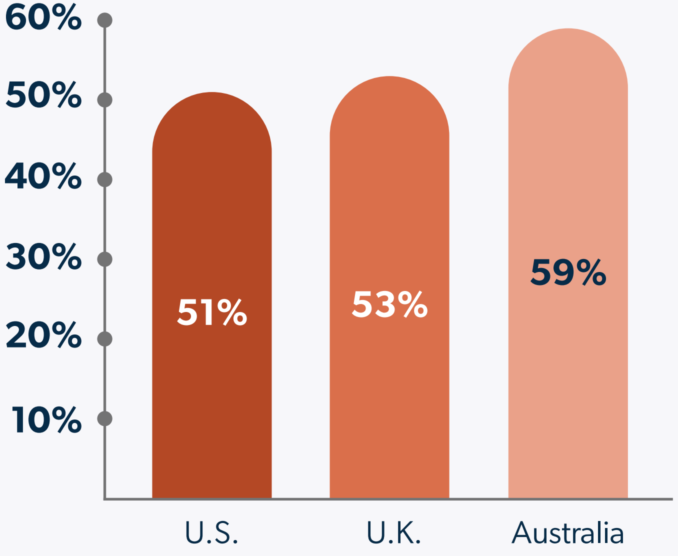


Chart 11

Do you have a cybersecurity expert on staff?

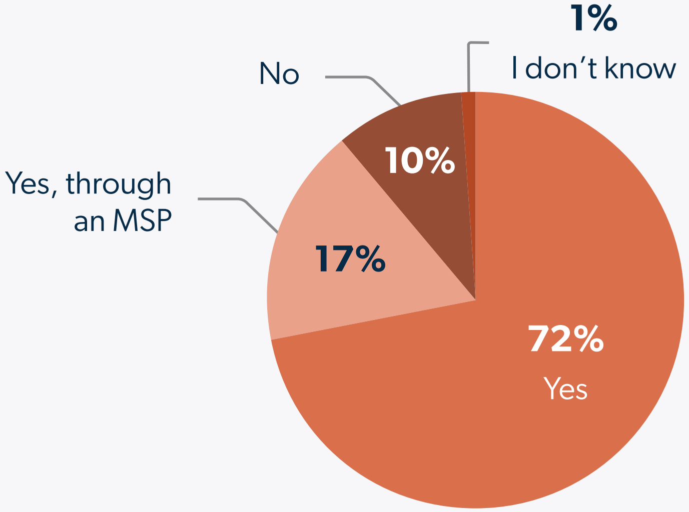


Chart 12

The Hidden Threat of Shadow IT: Reality and Root Causes

Shadow IT is becoming an increasing headache for IT admins. Almost nine in 10 (88%) of admins report concerns about devices or applications managed outside of IT, up from 84% in Q3 2024 (**Chart 13**).

Are you concerned about shadow IT?

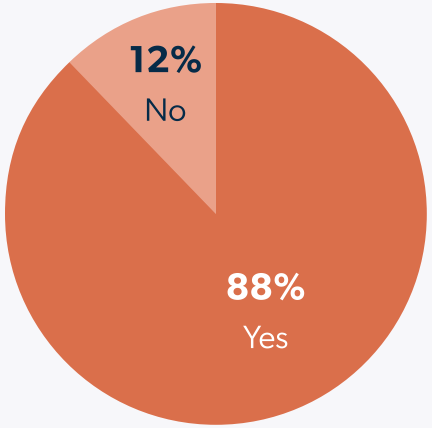


Chart 13

66%

say they lack a SaaS management solution or don't have the ability to discover applications used by employees.

58%

have discovered applications used by employees not officially managed by IT.

60%

estimate employees use six or more unauthorized applications.

The Hidden Threat of Shadow IT: Reality and Root Causes

Despite the growing impact of shadow IT, admins experience significant struggles in their efforts to combat it as many report a lack of visibility into their IT environment. A growing number of admins (38%) report the reason they can't address the issue of shadow IT is because they don't have the ability or visibility to discover all applications (up from 32% in Q3 2024). Roughly the same number (39%) say business users move too fast for IT to keep up with their needs (up from 31% in Q3 2024) and 35% say it's because they have other more important priorities (down from 36% in Q3 2024). Nearly three in 10 (29%) say they lack the partnership and communication with business partners (the same as Q3 2024), and 28% say they don't have a SaaS management or asset management solution (up from 24% in Q3 2024) (**Chart 14**).

Why are you unable to address shadow IT?

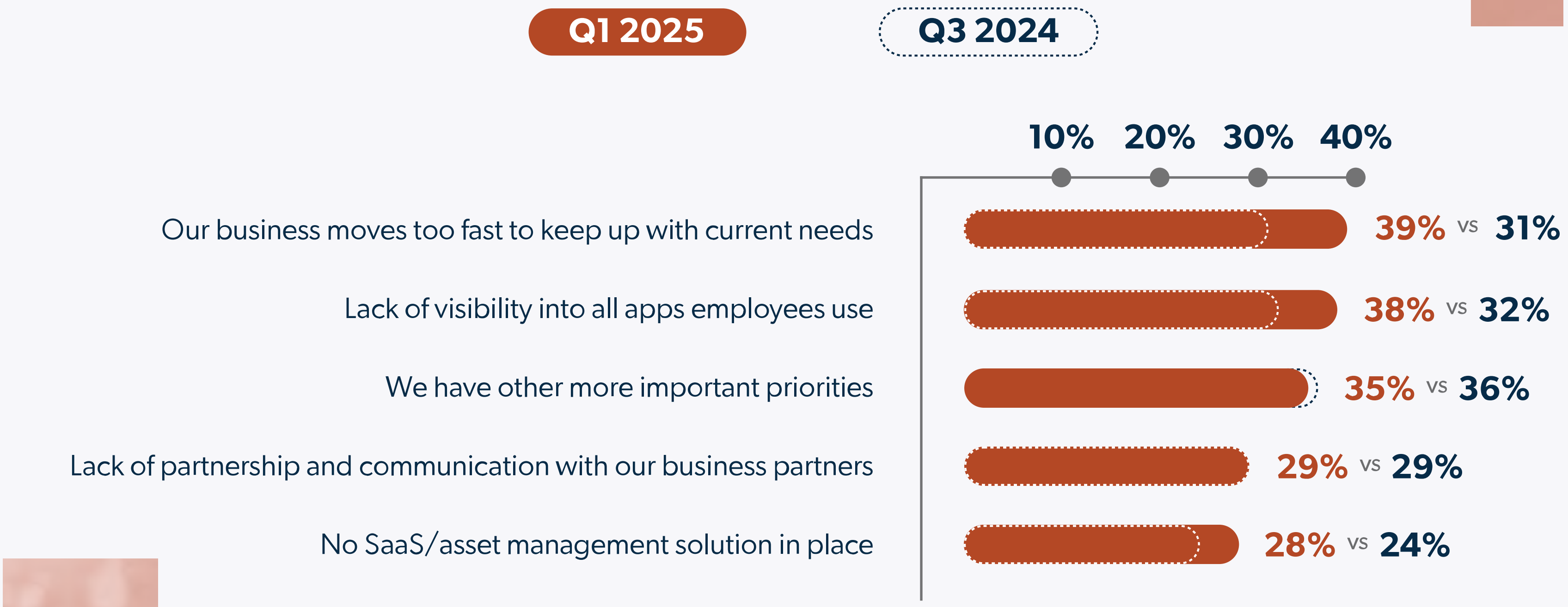


Chart 14

A Shortcut to Productivity or Security Pitfall?

Underscoring that IT teams are investing serious effort to empower employees without sacrificing security, respondents displayed general understanding about why users are turning to unauthorized applications (**Chart 15**).

In my opinion, employees most commonly use applications not officially sanctioned or managed by IT:

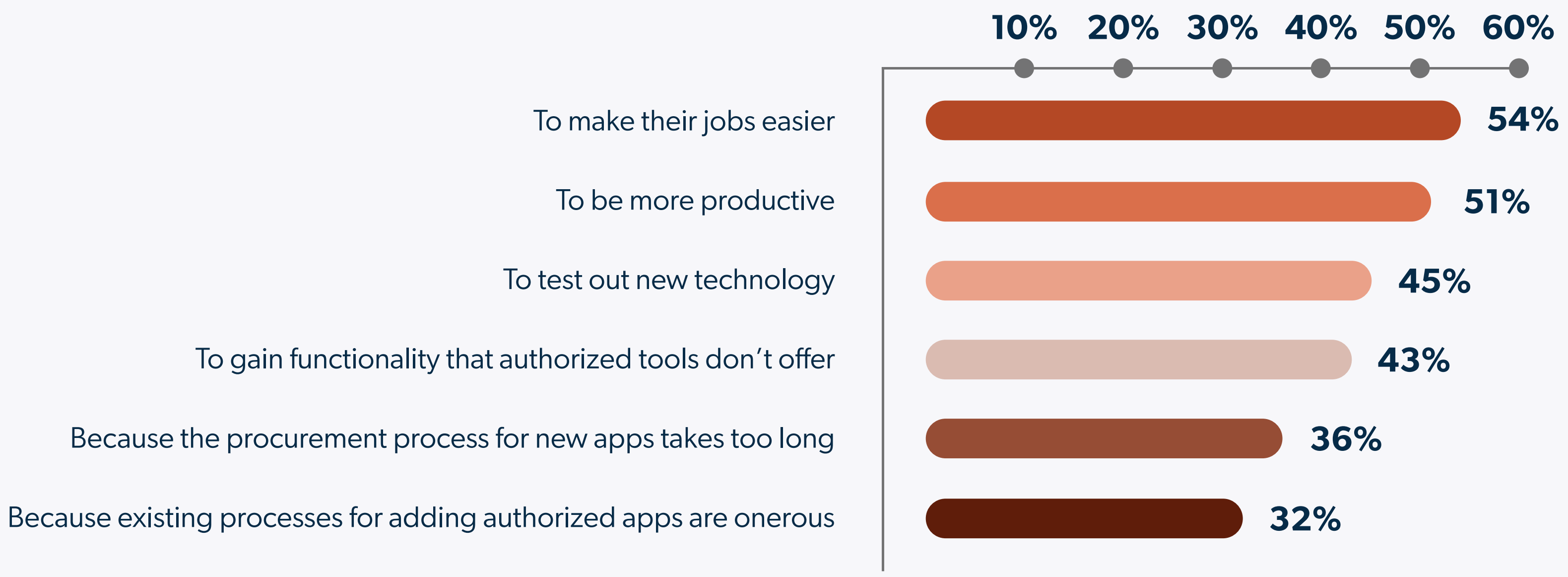


Chart 15

Doubling Down on Digital Defense

When asked which areas of IT respondents plan to invest in over the next six months, cybersecurity tools takes the top spot (**Chart 5**).

A plurality of organizations (47%) spend between 10-25% of yearly IT budget toward cybersecurity. 24% spend 26-50%, 5% spend more than 51%, 19% spend 5-9%, and 4% spend less than 5% (**Chart 16**).

The outlook for future spending on cybersecurity is significantly positive as 75% expect their organization's cybersecurity budget to increase over the next 12 months, and 99% expect it to stay the same or increase, with only 1% expecting a decrease (**Chart 17**).

What percentage of your yearly IT budget goes toward cybersecurity?

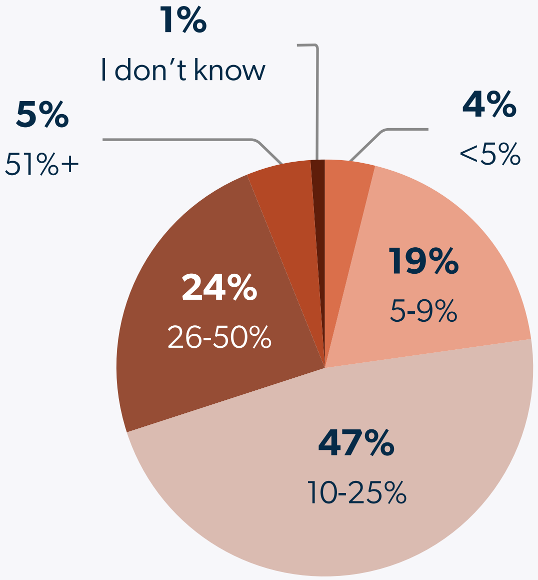


Chart 16

Over the next 12 months, I expect our cybersecurity budget to:

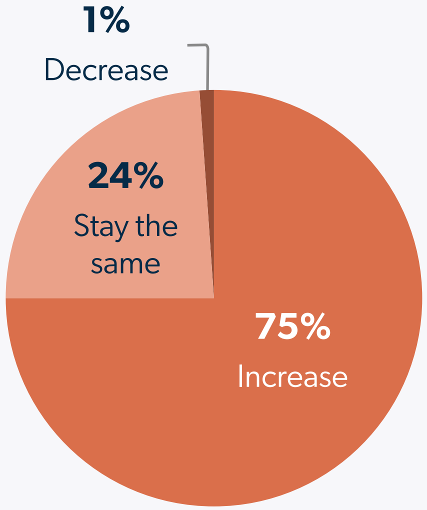


Chart 17

Sticking to Passwords as Biometrics Break Through

Though passwordless authentication has been a point of industry discussion for years, organizations are far from achieving it as reality. Despite widely known weaknesses of credential-based authentication, nearly all (98%) of respondents still use password-based systems for at least some IT resources. Password management will likely continue to be something organizations deal with over the near term as 21% of employees still have to manage 10 or more passwords to log into their IT resources (up from 17% in Q3 2024).

As credential-based and other cyberattacks increasingly threaten organizations, over half (54%) of IT teams say biometrics are the best tool, application, or process for keeping an organization secure (**Chart 18**).

What do you consider the best tools/applications/processes for keeping an organization secure?

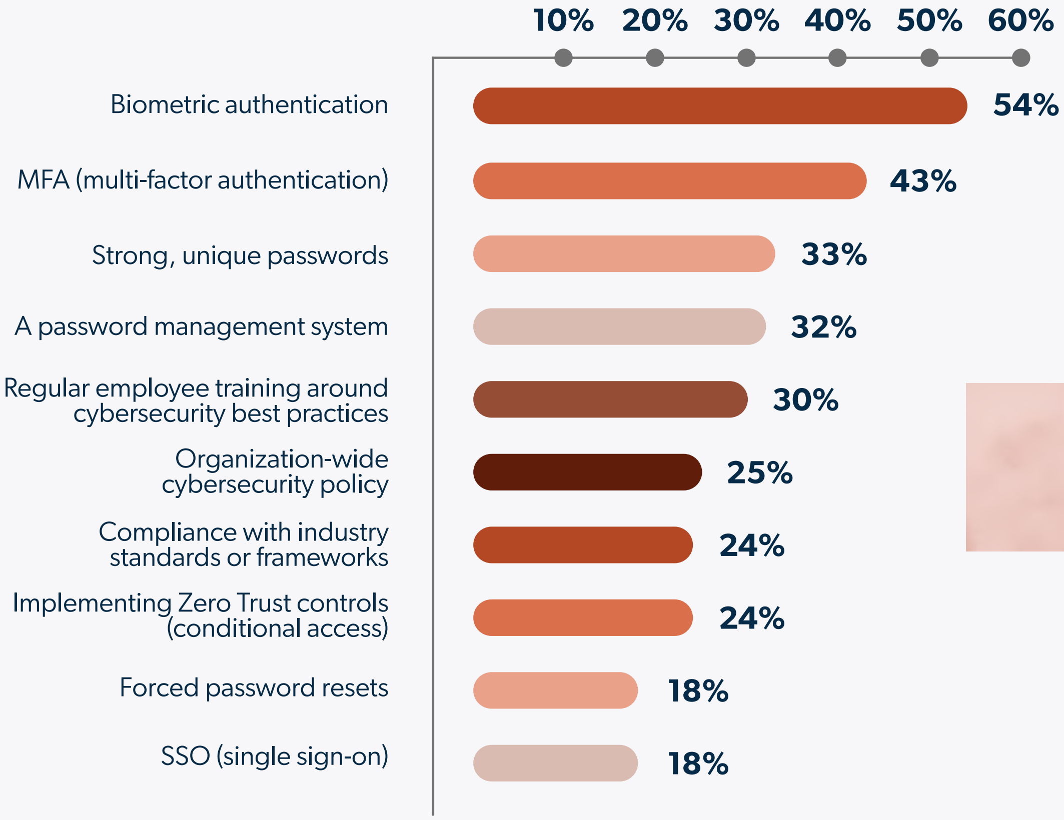


Chart 18

Biometrics Boom: Demand and Device Gaps

The demand for biometrics is driven by a widely shared opinion that their organization's security posture would be stronger if it required biometrics, (85%, up starkly from 67% in Q3 2024), suggesting admins are looking to make security as simple as it is strong (**Chart 19**).

This strong preference for biometrics underscores another challenge for IT teams: 92% of admins say it's important for all new devices to have biometric capabilities, though 68% of admins report that less than half of the devices they currently manage have biometric capabilities. In the U.S., it is very important for new devices to have biometric capabilities (71%) vs. 57% in U.K. and only 46% in Australia. Biometrics are seen as the best tool, application, or process for keeping an organization secure (US=56%, UK=62%, AUS=44%) (**Chart 20**).

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

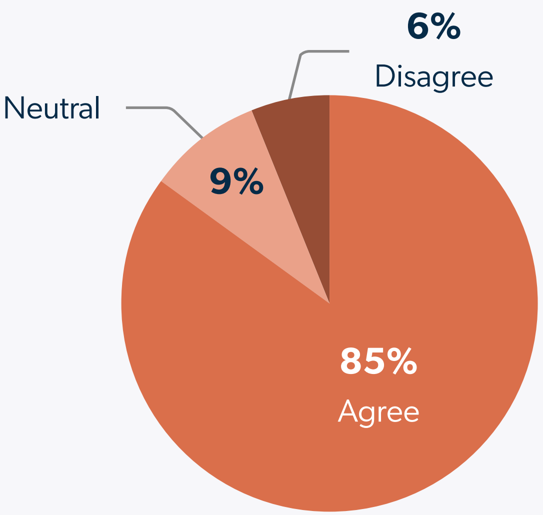


Chart 19

It is important that all new devices have biometric capabilities:

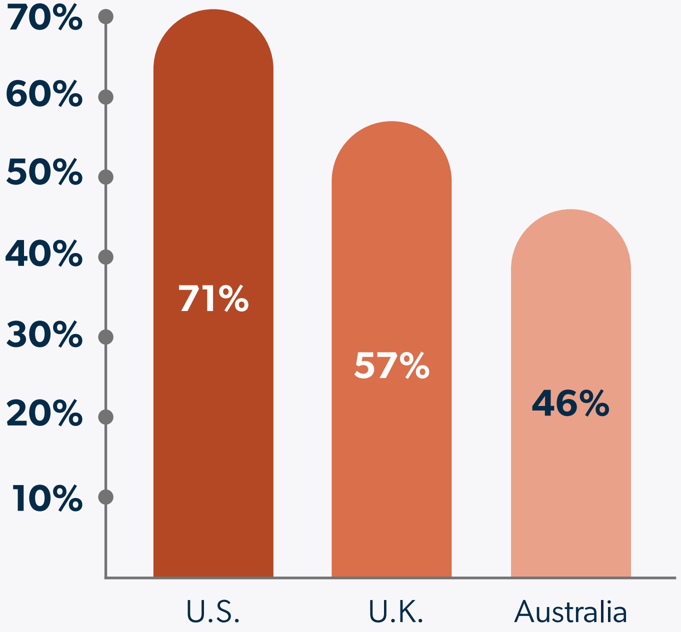


Chart 20

Cyberattacks Spike as Organizations Step Up Their Defenses

As the security landscape continues to evolve, organizations have to remain vigilant to a constant threat from bad actors. Nearly half (46%) report having been the victim of a cybersecurity attack (up from 45% in Q3 2024). Australian firms have fared the worst, with 53% having experienced a cyberattack, compared to 45% of U.K. organizations and 41% of U.S. organizations (**Chart 21**).

My organization has been the victim of a cybersecurity attack:

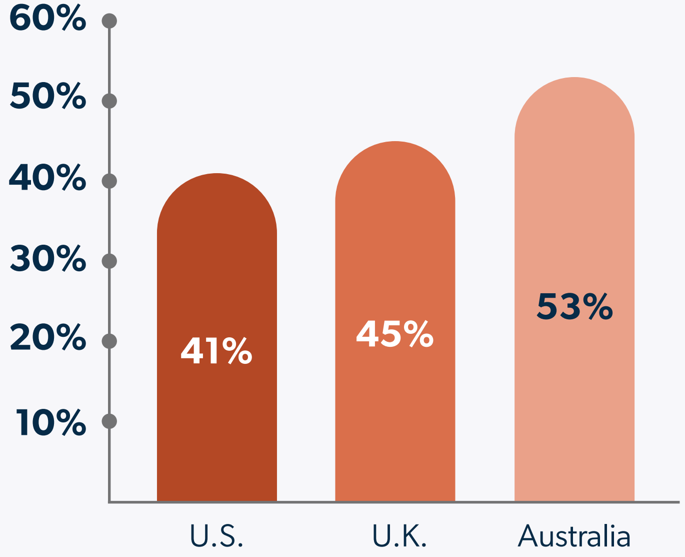


Chart 21

> **"Hackers are getting more brutal with attacks."**
>
> — Anonymous survey respondent

Cyberattacks Spike as Organizations Step Up Their Defenses

AI-generated attacks and attacks resulting from too many permissions have seen the highest increase over the last six months (**Chart 22**).

Despite regular threats, a large majority (81%) of all organizations are confident they're prepared financially to recover from a cyberattack, up from 73% six months ago, including 86% of U.S. firms, 77% of U.K. firms, and 78% of Australian firms.

Admins reported the cause of recent cyberattacks were due to:

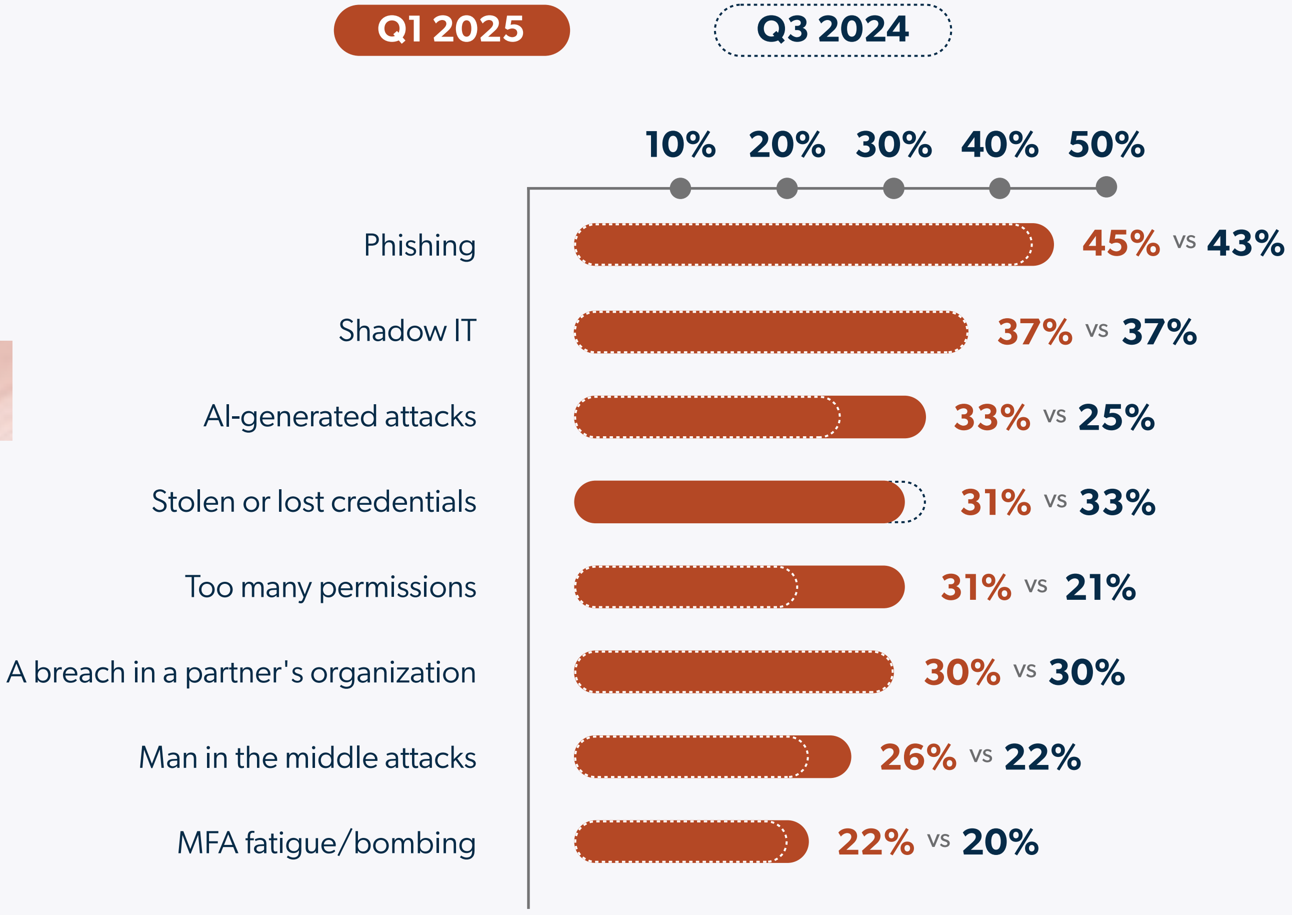


Chart 22

Devices

Diverse Devices and Differentiated Use

For modern organizations, managing a diverse range of devices is the new reality, and one that introduces significant challenges. Properly securing devices, ensuring updates and patches are applied, and troubleshooting across various operating systems all add to the complexity. The average device ownership breakdown in surveyed organizations is 66% corporate-owned devices and 34% personal devices (**Chart 23**).

Windows use has shown the most significant decrease over the last six months, compared to macOS and Linux, which both increased. When asked about the breakdown of their organization's device type, admins reported Windows devices comprise 56% (down from 63% in Q3 2024), macOS 27% (up from 24% in Q3 2024), and Linux 20% (up from 18% in Q3 2024) (**Chart 24**).

What is the device ownership breakdown of devices that are accessing resources?

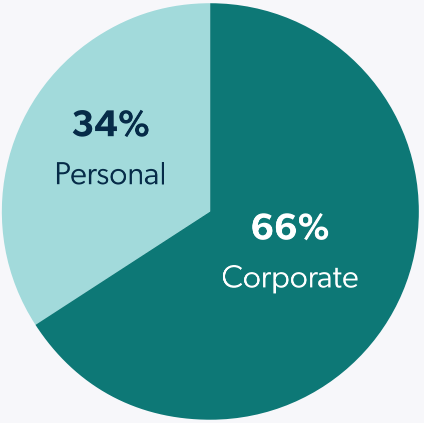


Chart 23

The average breakdown of Windows/Linux/macOS devices in the workplace:

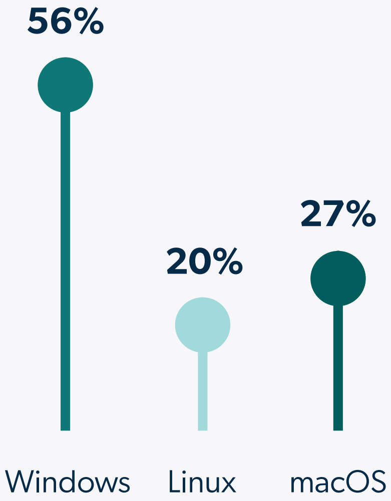
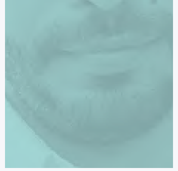


Chart 24

Grappling with Diverse Device Demands



Over the next 12 months, IT teams expect increased use across all device types. When asked about device use over the next year vs. what they expected six months ago, they said: (**Chart 25**).

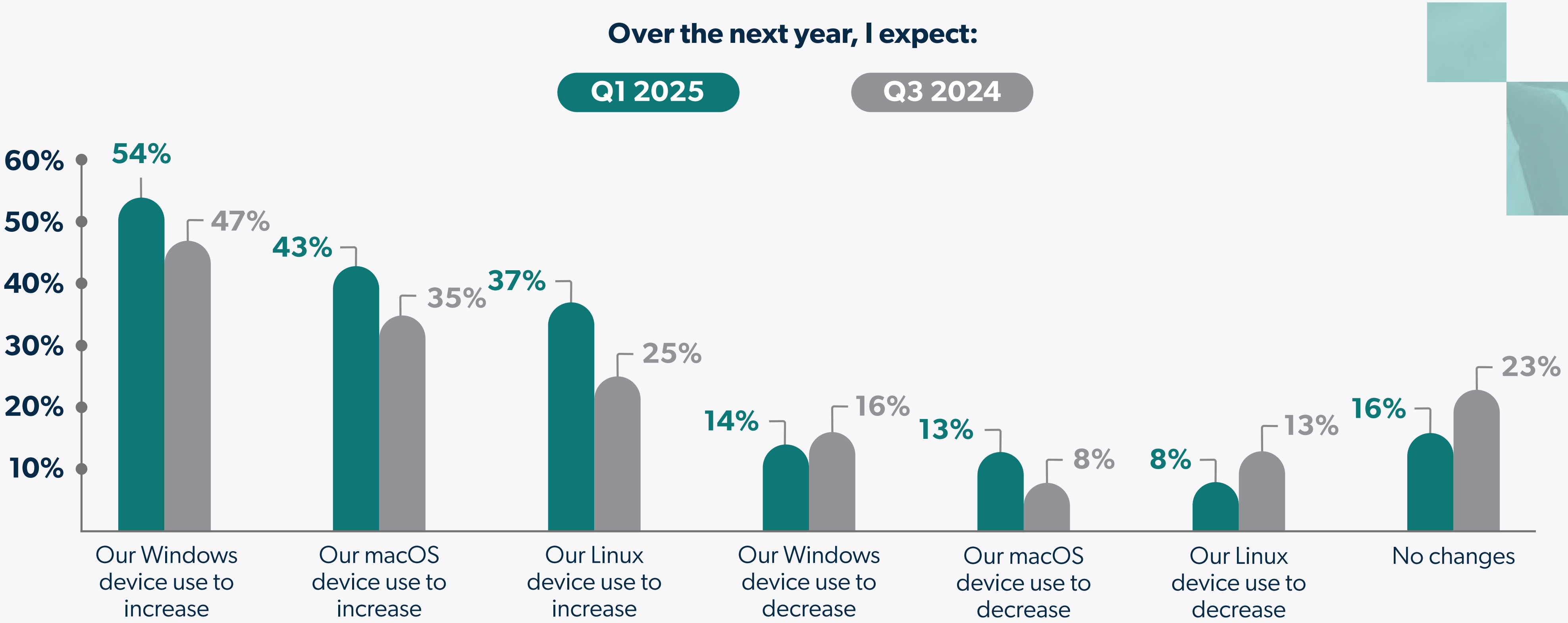


Chart 25

Grappling with Diverse Device Demands

When asked about the most difficult things to manage as an IT admin, the top answer was Windows and other Microsoft devices (23%), followed by cloud infrastructure (22%), macOS and other Apple devices and apps (19%), and Linux devices and applications (14%). 13% said they're equally difficult to manage, and 9% had no opinion as they use what their workplace uses (**Chart 26**).

Which are the most difficult for you to manage as an IT admin?

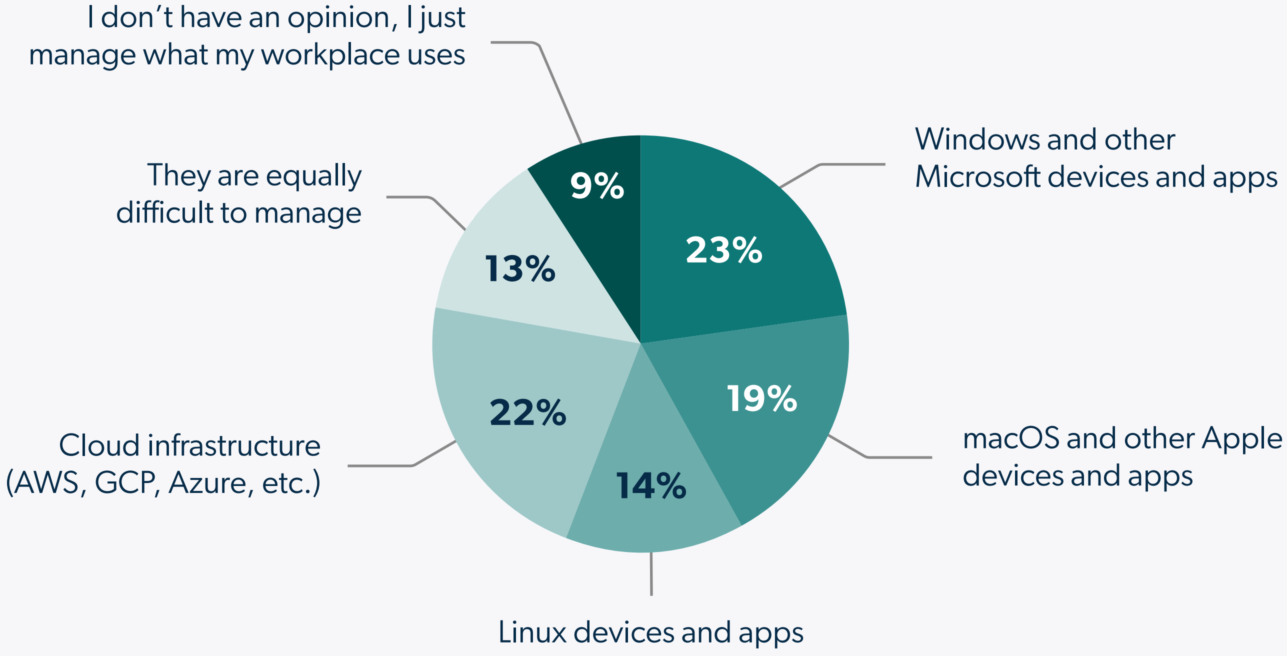


Chart 26

MSPs

From Cost-Cutters to Consiglieres: MSPs as Trusted Advisors

Customers are increasingly viewing MSPs as trusted advisors to help navigate a rapidly changing tech and business landscape, rather than just being a source of cost-savings. Over nine in 10 (93%) of organizations surveyed use or are considering using an MSP, and 35% use an MSP to completely manage their IT program, up from 29% who said the same six months ago (**Chart 27**). The U.S. relies on MSPs significantly more, with 43% using an MSP to completely manage their IT program vs. 31% of U.K. and 31% of Australian organizations.

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

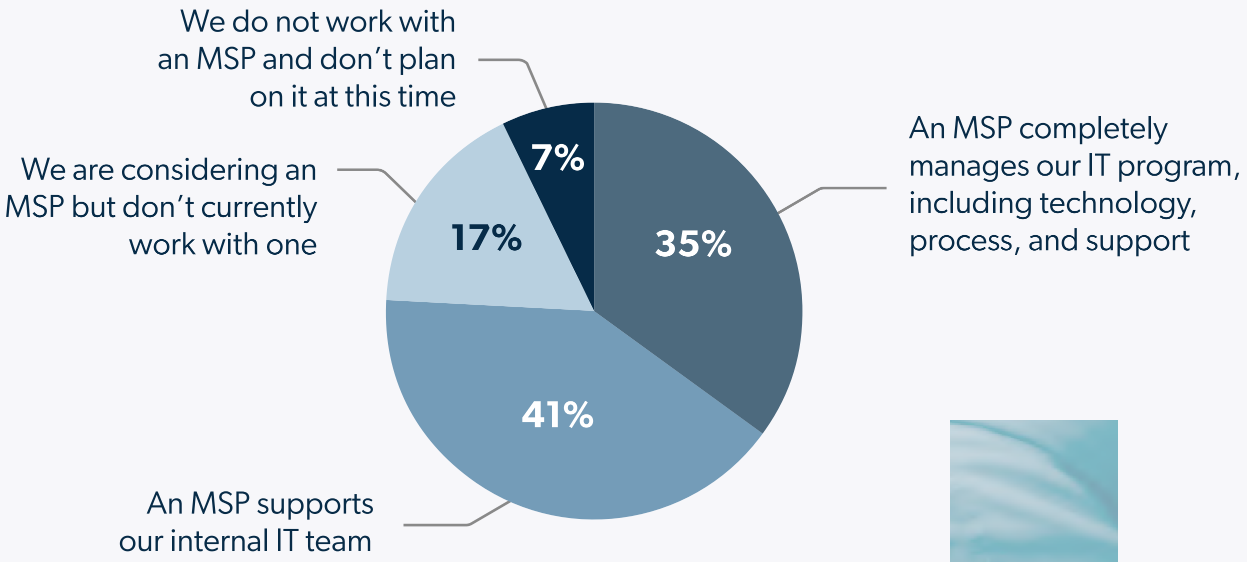


Chart 27

From Cost-Cutters to Consiglieres: MSPs as Trusted Advisors

MSPs are embracing the shift from being viewed as a value provider to one that delivers broader benefits. Increased IT effectiveness is the top reason IT admins use MSPs (54%), followed by MSPs make my job easier (43%), are cost-effective (41%, down from 58% in Q3 2024), offer strong customer support (41%, up from 29% in Q3 2024), are up to date on the latest technologies (40%, down from 56% in Q3 2024), and provide a better user experience (38%, down from 50% in Q3 2024) (**Chart 28**).

We use MSPs because:

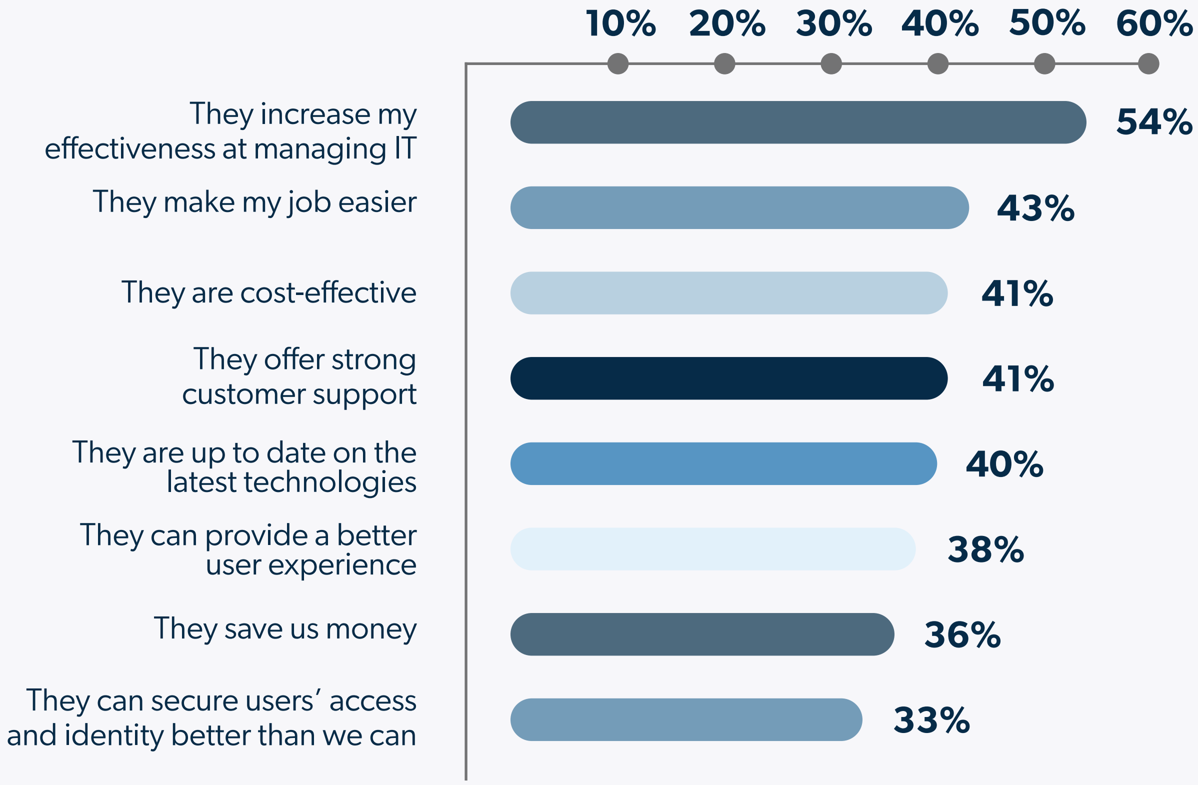


Chart 28

Seizing the Spotlight: MSPs' Time to Shine

The opportunity for MSPs who can successfully demonstrate their value as a partner is big: 76% of organizations plan to increase MSP investment over the next 12 months, up from 67% who said the same six months ago. Most commonly, organizations find their MSP partners through recommendations (45%), followed by an online search (37%), and the MSP reaching out (17%) (**Chart 29**).

How did you find the MSP that you currently work with?

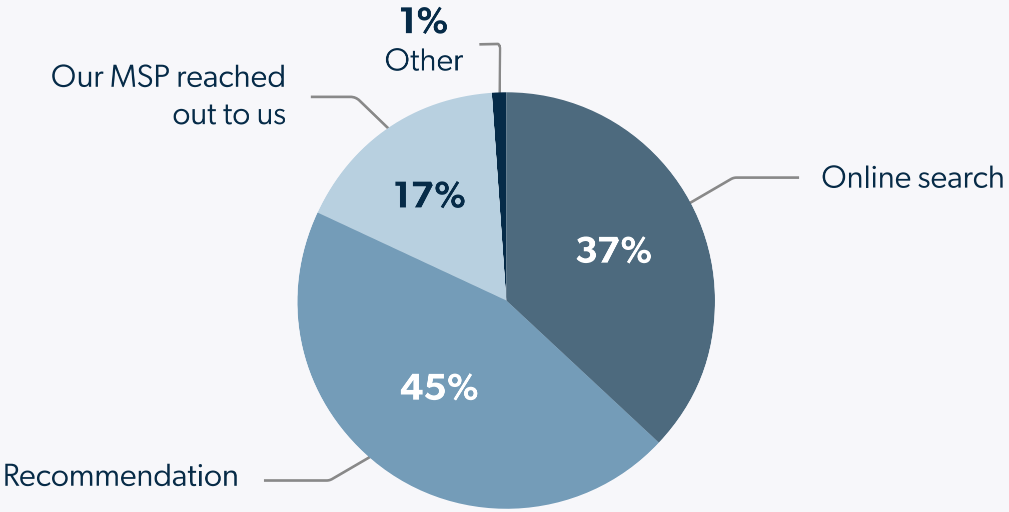


Chart 29

> **"Trying to keep delivering the same level of service with less staff with less experience keeps me up at night."**
>
> — Anonymous survey respondent

Seizing the Spotlight: MSPs' Time to Shine

One in five organizations (21%) don't use an MSP because they don't support the devices, productivity suite, or IT systems that they currently deploy. When asked what tools they would like their MSP to manage that they don't manage today, admins said cybersecurity (63%), SaaS management (53%), Google Workspace (39%), compliance and reporting (37%), and expanded device management (Android, Linux, etc.) (40%) (**Chart 30**).

Compliance is another area of opportunity for MSPs: 34% of organizations surveyed report having failed a compliance audit or are being required to implement additional security controls to pass an audit.

What tools would you like to see your MSP manage that they do not today?

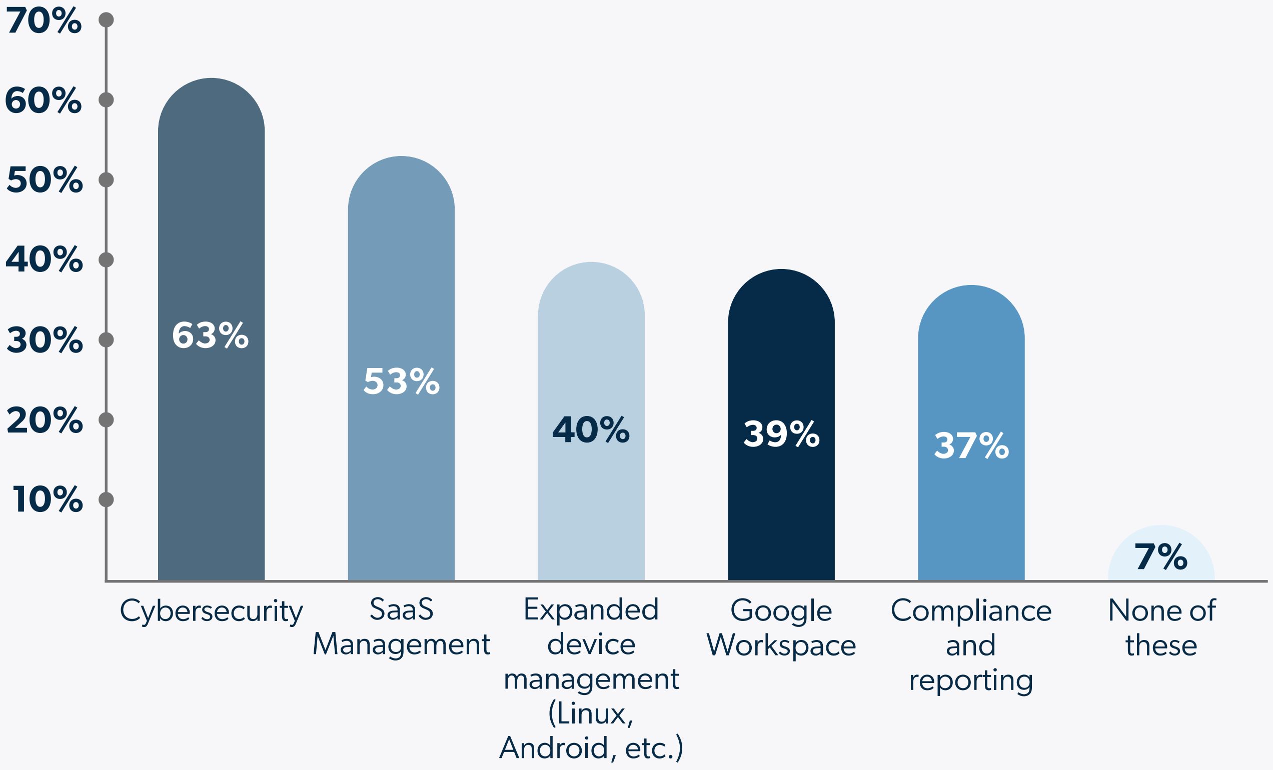


Chart 30

MSPs in the Hot Seat: Security Concerns and Cost Barriers

How MSPs manage security is a rising concern for those using or considering an MSP, with 44% reporting they have concerns about how MSPs manage security, up from 39% six months ago (**Chart 31**).

I have concerns about how MSPs manage security:

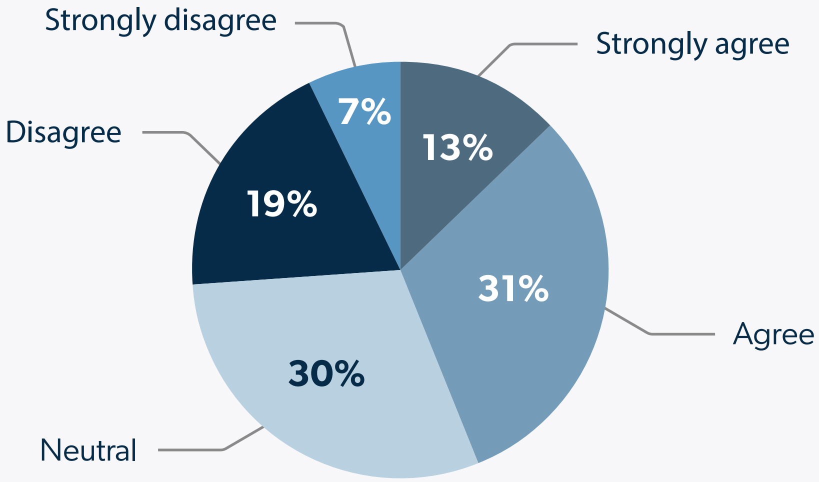


Chart 31

44%

of organizations report they have concerns about how MSPs manage security.

MSPs in the Hot Seat: Security Concerns and Cost Barriers

For those who don't use an MSP, admins cite wanting to handle IT themselves as the biggest reason (38% down from 47% in Q3 2024). Cost is the second reason (35%, down from 39% in Q3 2024). Other reasons admins give for not using an MSP include: they offer more than what organizations need (17%), organizations are too small (13%), they don't support the devices, productivity suite, or IT systems that they currently deploy (21%), and they have had a bad MSP experience (17%) (**Chart 32**).

We don’t use MSPs because:

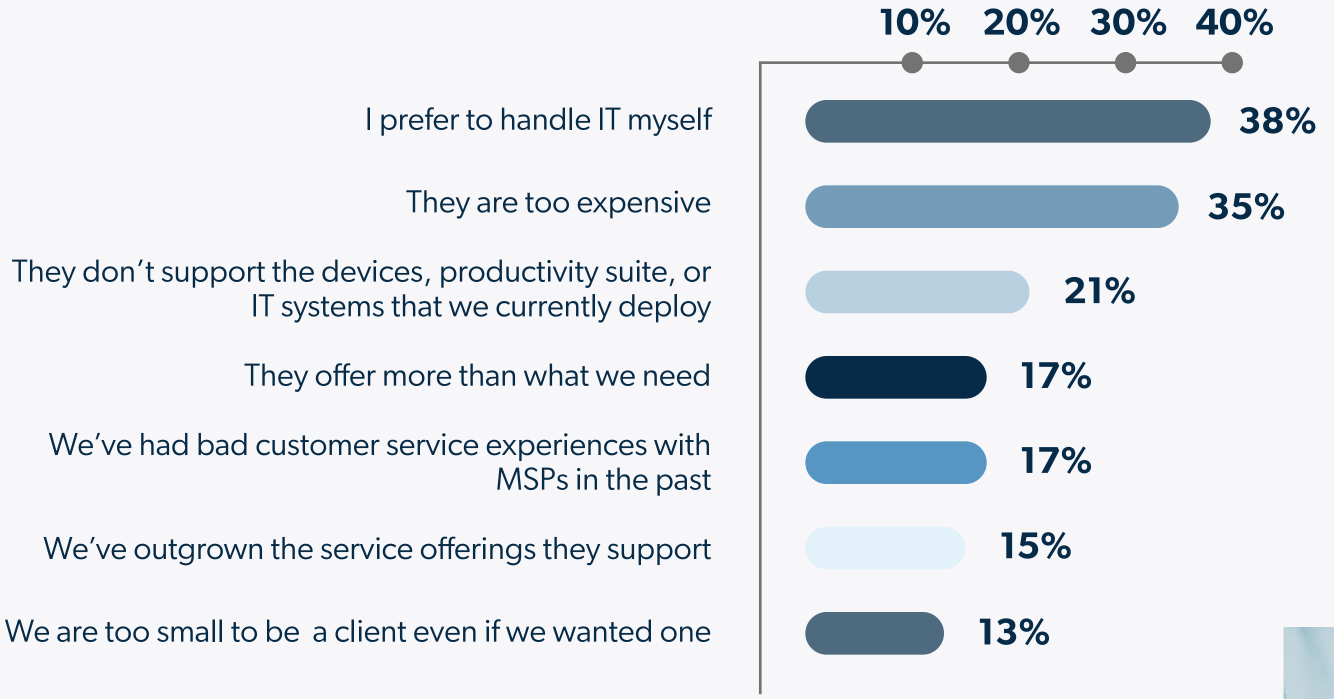


Chart 32

AI

Double-Edged Surge: AI Risk and Reward

AI has become more entrenched in organizations though it's viewed as holding both potential and risk, and admins acknowledge the complexity of integrating it. Organizations are accelerating AI plans when compared to what they reported six months ago (**Chart 33**).

Implementation plans for AI initiatives for IT are within:

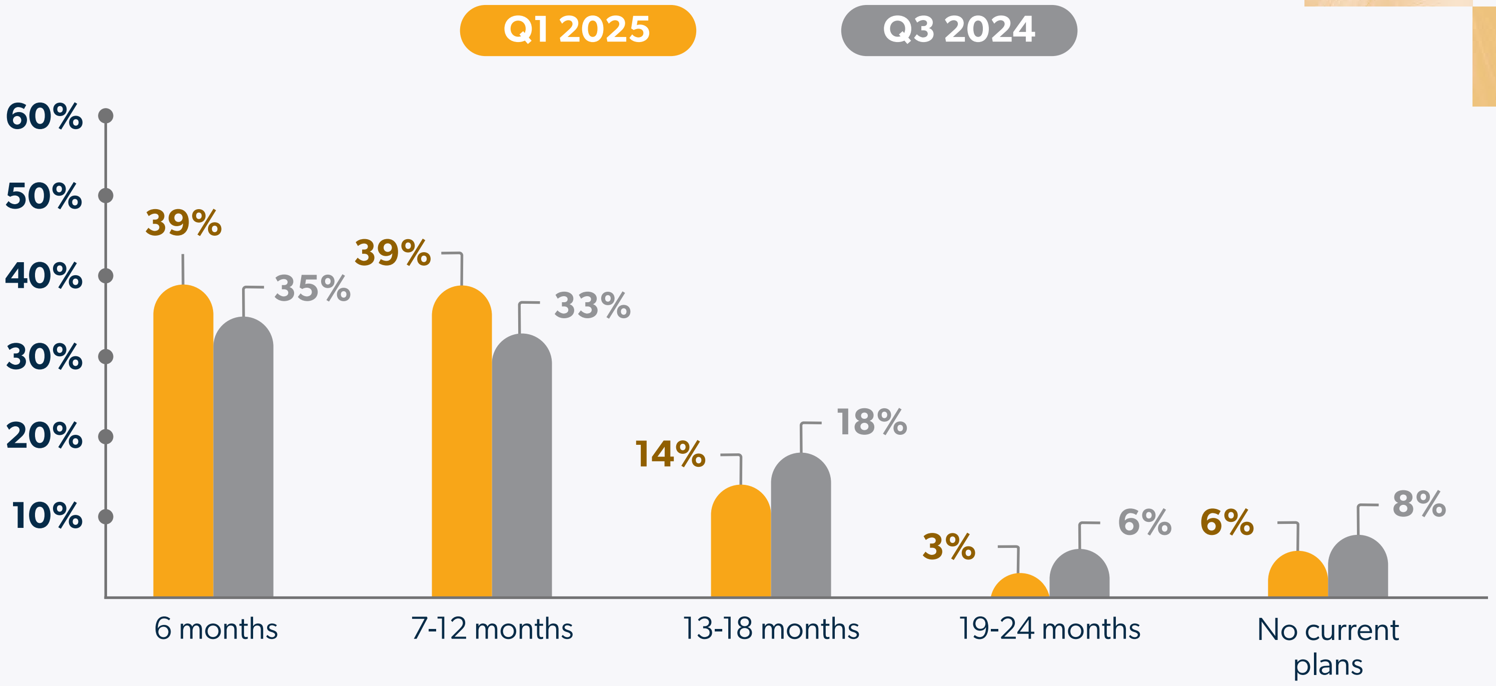


Chart 33

Double-Edged Surge: AI Risk and Reward

Only 6% of organizations report having no plans for AI and 15% (down from 17% in Q3 2024) of admins think organizations are moving too quickly around AI. 67% think their organization is moving at exactly the right speed (up from 60% in Q3 2024) and 17% think the pace is too slow (down from 20% in Q3 2024) (**Chart 34**).

My organization is moving ______ around AI.

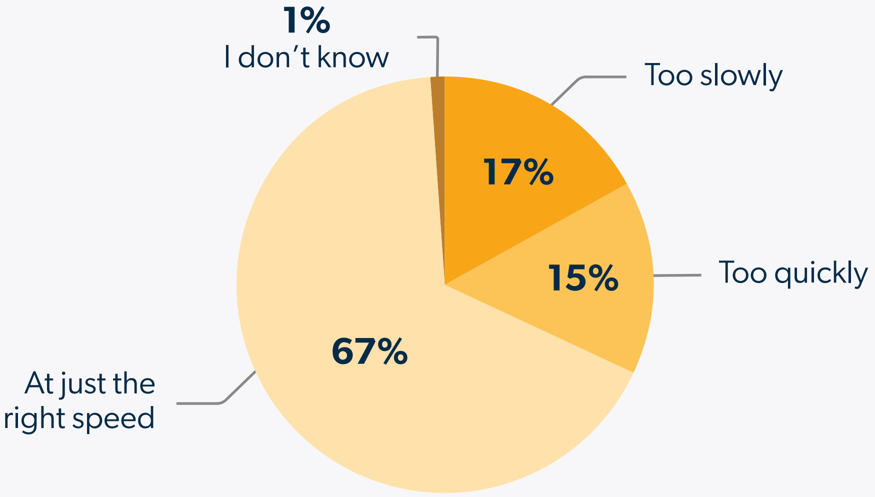


Chart 34

> **"Keeping pace with all the improvements and changes keeps me up at night. AI has brought a new way of doing business and requires major adjustments."**
>
> — Anonymous survey respondent

Alarm and Anxiety

While there's an increase in readiness to adopt AI, there's also an increase in IT teams' worry about the risk AI poses. Now over two-thirds of admins (67%) believe AI is outpacing their organization's ability to protect against threats, up from 61% in Q3 2024 (**Chart 35**).

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

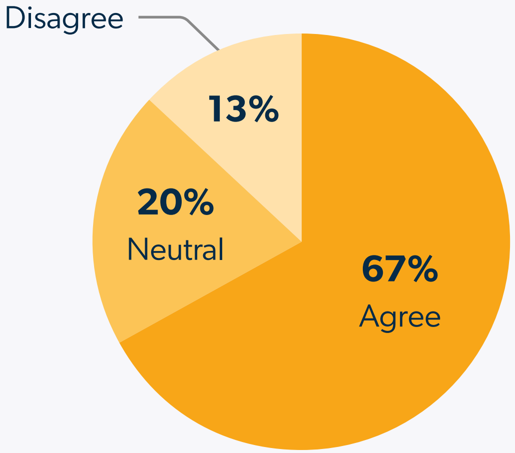


Chart 35

> **"What keeps me up? That the increasing use of AI might take over my job."**
>
> — Anonymous survey respondent

Alarm and Anxiety

Despite admins' excitement around AI potential, more are worried about AI's impact on their job (up to 37% from 34%). Looking at responses across job titles indicates a pervasive worry no matter where respondents sit in the organization (**Chart 36**).

I am worried about AI's impact on my job:

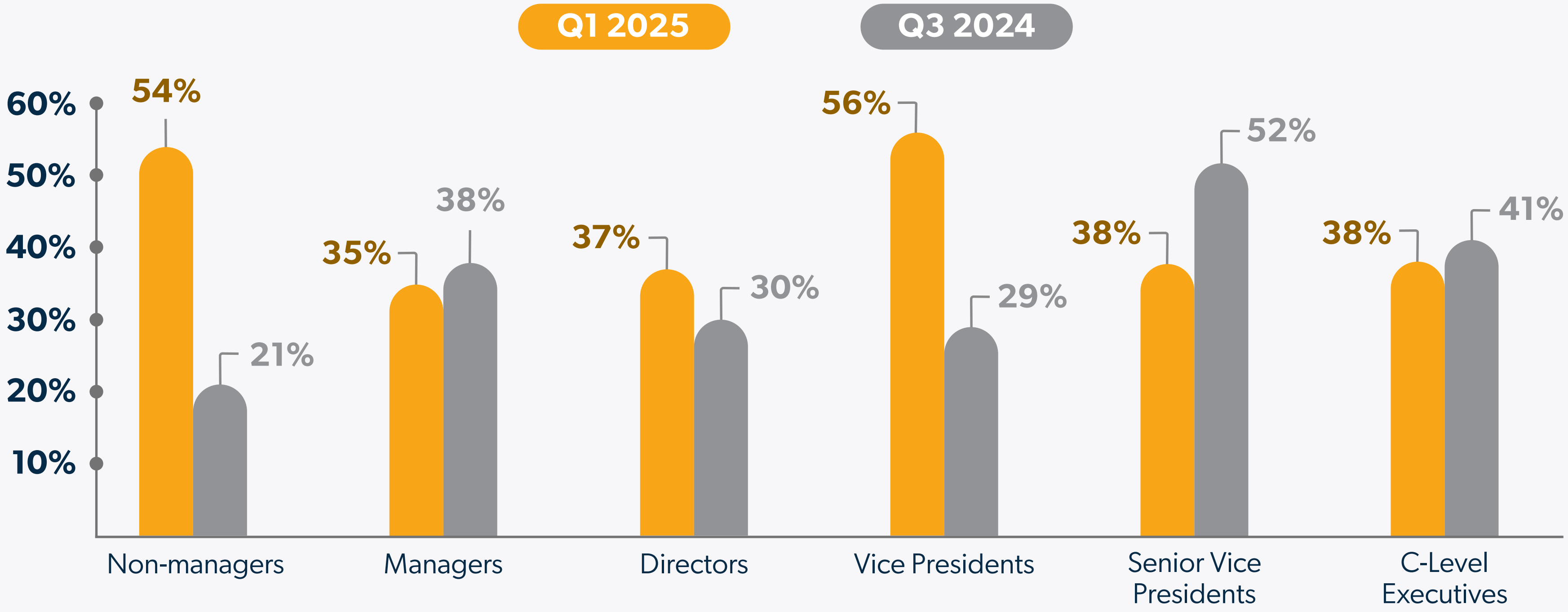


Chart 36

Hype, Hesitation, and Policy Gaps

There's a broad spectrum of expectations around AI. When asked about how their general opinion about the impacts of AI changed over the last six months, a plurality (31%) said they feel like the potential impact of AI is the same, but it is moving slower than they thought it would be; 33% feel the impact of AI is even greater than they thought it would be; 21% say their opinion hasn't changed, and 15% feel that the impact of AI is much lower than they thought it would be (**Chart 37**).

How has your general opinion about the impacts of AI changed over the last 6 months?

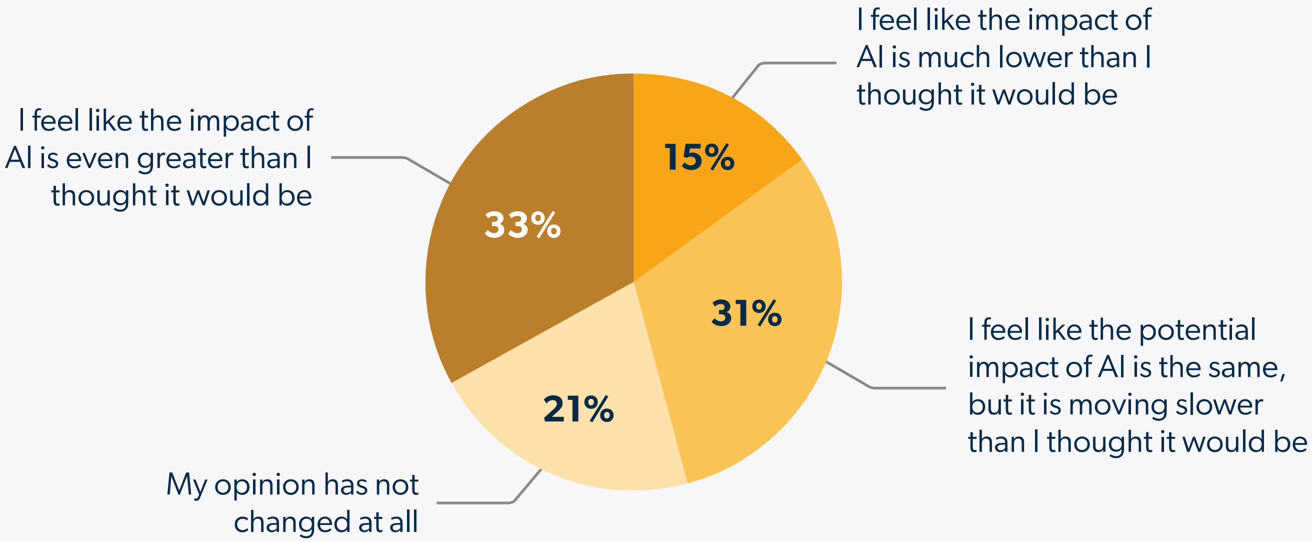


Chart 37

Hype, Hesitation, and Policy Gaps

This broad spectrum also exists across wider organizational approaches to AI. Nearly half encourage the use of AI tools (47%) or have developed policy to help guide employee AI use (49%). 41% allow limited access, 28% have controls that prevent AI access, and 21% have no policies or restrictions (**Chart 38**).

In terms of AI, my organization:

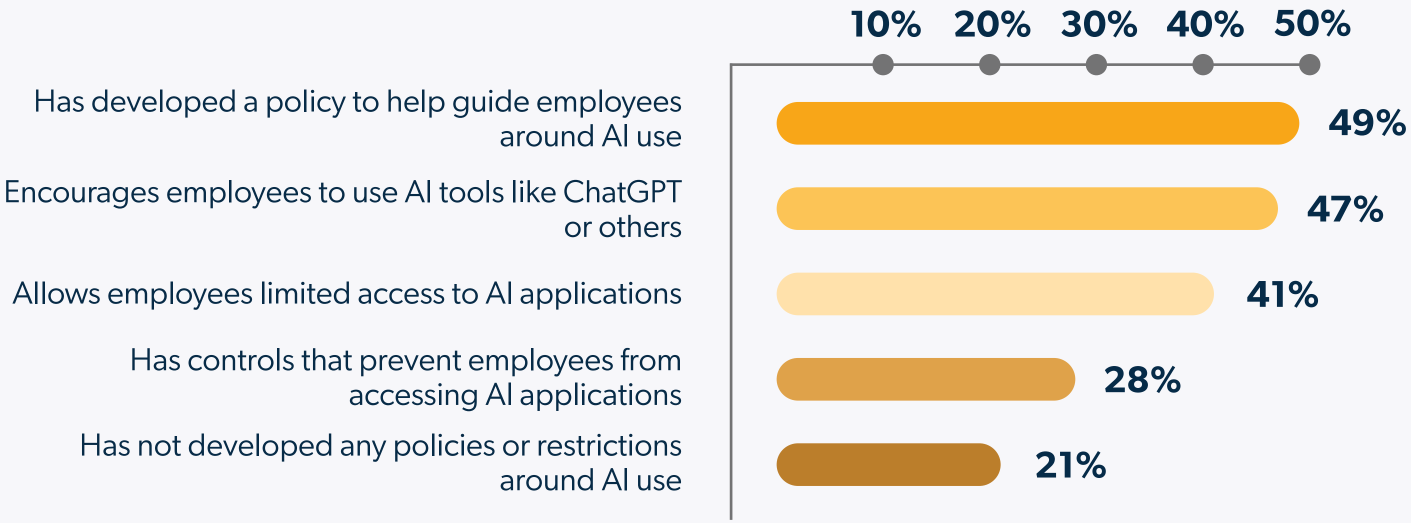


Chart 38

Final Thoughts

The Q1 2025 SME IT Trends Report, "From Chaos to Control: Simplifying IT in the Fast Lane of Change," captures a critical transformation in IT strategy: IT is no longer just a support function—it's a strategic enabler driving organizational success. As organizations face relentless challenges—diverse device ecosystems, shadow IT, and the accelerating impact of AI—IT teams must lead with innovation and adaptability. Security remains paramount, but it's clear that IT is stepping into a new role: not just managing change but actively shaping the future.

Organizations have an opportunity to pivot from reactive problem-solving to proactive innovation. Those that thrive in 2025 and beyond will be those that empower IT to be a catalyst for growth. This means treating IT not as a cost center, but as a strategic partner—integrating technology choices with business objectives, fostering cross-functional collaboration, and seeking regular insights from all stakeholders to stay ahead of disruption. This holds true both for internal teams and for those who rely on external MSPs—-the key to success at scale means centering IT and gaining greater visibility into, and control over, the broad spectrum of user needs.

AI is no longer on the horizon; it's here, reshaping IT plans and business models alike. To harness its power responsibly, organizations must lead with clear governance and innovation frameworks that balance opportunity with risk. Shadow IT, meanwhile, should not be viewed merely as a threat but as a call to align IT strategies with real user needs, turning gaps into opportunities for business-led IT.

IT teams are charting a bold course, from simplifying IT sprawl to driving organization-wide agility. The imperative is clear: embrace the pace of change or risk being left behind. In this environment, organizations can't afford to simply "keep up"—they must set the pace.

Setting the Pace: The Path Forward

Simplify IT to drive agility

Admins have been crystal clear in every edition of JumpCloud's survey that simplified IT is what they want. Investing in a unified platform for managing devices, identities, and access enables IT teams to consolidate tools and processes, and vastly improve the simplicity of managing IT. Automation can be a central part of freeing IT professionals from routine tasks so they can focus on more strategic priorities. Regular audits of workflows and tool usage gives critical visibility for continuous improvement in the user experience, and IT admins' experience in managing those users.

Elevate IT as a strategic partner

IT must transition from being a back-office function to a cornerstone of organizational strategy. By embedding IT into decision-making processes, organizations can align technology initiatives to better support broader business goals. Regular cross-functional reviews can ensure technology investments contribute directly to measurable outcomes, fostering greater collaboration across departments.

Turn shadow IT into a strategic advantage with a business-led IT approach

Rather than viewing shadow IT as merely a risk, organizations can leverage it to identify gaps in existing processes and tools. Mapping unauthorized applications reveals unmet user needs and allows IT to streamline approval and procurement processes without impacting security. Identify and appoint IT advocates across various business teams to further enhance visibility and collaboration—and transform shadow IT from a vulnerability into a driver of innovation.

Lead in AI with governance and vision

AI's rapid growth requires a careful balance between its potential and its potential risks. Governance frameworks will allow organizations to encourage innovation while maintaining robust security and ethical standards. IT teams should adopt flexible processes to evaluate (and purchase) AI tools quickly and to refine strategies regularly based on user feedback. Organizations should also prioritize AI literacy at all levels.

Setting the Pace: The Path Forward

Innovate without compromising security

With the rise in cyberattacks, there's no question that today's threats must be countered with stronger protections without affecting end users' experience. Organizations should settle on a process for adopting organization-wide biometric authentication and MFA at minimum, while also evaluating tools and processes to address risks like AI-driven attacks and shadow IT, before a cyberattack forces the issue. For smaller teams, an MSP can often offer a critical security boost, serving as the bulwark against increasingly sophisticated cyberattacks.

Focus on leadership and agility

Every organization needs IT leaders who can anticipate trends and drive innovation. Ongoing benchmarking against industry standards can lead to ongoing refinement of best practices. Ongoing investment in training and education gives teams the tools they need to manage future disruptions. By building a resilient IT culture, organizations can develop the IT agility and strategic foresight necessary to thrive in an era of rapid change.

Thousands of organizations worldwide rely on JumpCloud to fulfill their commitments and tackle the most pressing technology challenges, regardless of the uncertainties they face. JumpCloud delivers a unified open directory platform that makes it easy to securely manage identities, devices, and access across your organization.

With JumpCloud, IT admins grant users secure, frictionless access to the resources they need to do their job, and manage their entire fleet of Windows, macOS, Linux, iOS, and Android devices from a single console. JumpCloud is IT Simplified.

If you want to find out how JumpCloud can help you get to the destination that matters most to your organization, start a free trial or get in touch with our global sales team.

Start Free Trial

Get In Touch

Methodology: JumpCloud surveyed 900 IT decision-makers in the U.S., U.K., and Australia 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 4, 2024 to November 11, 2024.

jumpcloud™

JumpCloud® delivers a unified identity, device, and access management platform that makes it easy to securely manage identities, devices, and access across your organization. With JumpCloud, IT teams and MSPs enable users to work securely from anywhere and manage their Windows, Apple, Linux, and Android devices from a single platform.

Jumpcloud.com | Blog | Community | Resources | 𝕏 | in | ▶