jumpcloud™

SME IT TRENDS Q3 2024

Detours Ahead

How IT Navigates an Evolving World

SME IT Landscape — I

Security and SMEs — S

SMEs and Devices — D

MSPs and SMEs — M

AI and SMEs — A

Destination: Modern IT

The rules are changing faster than ever for modern IT teams, and those at small to medium-sized enterprises (SMEs) are no exception. Cyberthreats are evolving at breakneck speed and AI is reshaping the digital landscape in real time. External factors like upcoming elections and economic conditions introduce uncertainty.

While the overall economic outlook for 2024 is positive, more than half of IT teams expect layoffs in the months ahead. Nearly three-fourths say future IT budget cuts would put their company at higher risk. And half of IT professionals are more concerned about their organization's security posture than they were six months ago.

As always, IT teams are having to skillfully navigate a complex IT environment, often creating their own map as they go. JumpCloud's newest edition of the SME IT Trends Report reveals how IT teams are forging the best path between uncertainty and opportunity, getting the clarity and control they need to keep every employee secure, connected, and content.

Key Findings

- **Shadow IT lurks:** The digital underbelly of organizations is growing, with unauthorized apps and services creating a sprawling attack surface. IT teams are scrambling to establish visibility and control.

- **Device sprawl:** The variety of computers, phones, tablets, and other devices that organizations need to support is only growing. It's causing IT teams to hunt for the holy grail: a way to manage them that's as flexible as it is secure.

- **Security insecurity:** Threats are multiplying and SMEs are fighting back. C-suites are opening the war chest, but IT admins are wary about whether it's enough to fend off the attacks.

- **Patchworked IT leaves too many holes:** Cobbling together point solutions is creating frustration and giant security holes. IT pros want a better, unified way to manage identity, devices, and access.

- **MSPs are SMEs' unsung heroes:** With mounting complexity, managed service providers (MSPs) are delivering the goods. Though, SMEs are raising the bar with their expectations.

- **The AI hype dims:** The AI fever has broken, leaving behind clear-eyed optimism and IT teams cautiously exploring what's promising versus what's just fluff.

All the trends paint a picture of an IT landscape in flux. The old playbook is obsolete, and SMEs know they must adapt or risk falling behind.

Within the chaos, IT teams are optimistic. They're creating opportunities amid the uncertainty. As budgets tighten and threats loom, the track is clear: **streamline, secure, and simplify**.
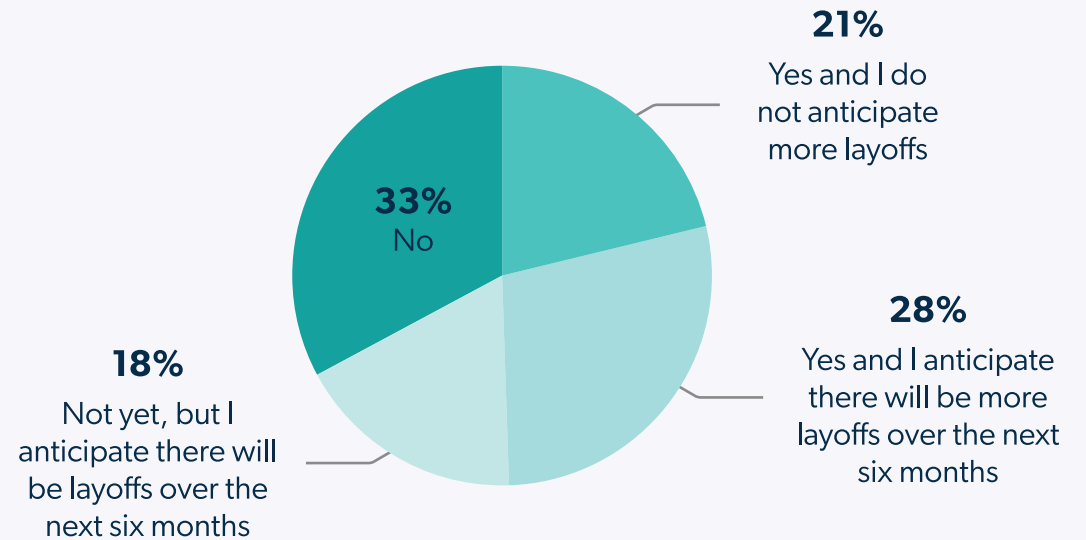
SME IT Landscape

Uncertainty Abounds

Across the globe, IT teams continue to adapt to turbulent economic times. Almost half (49%) of organizations have experienced layoffs in the last six months, down from 57% in Q1 2024. Over a quarter (28%) have gone through layoffs and anticipate more within six months. Meanwhile, 18% have not experienced layoffs but expect them in the next six months and 21% have experienced them and expect no more. Only 33% haven't experienced layoffs and expect none over the next six months.

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

21%
Yes and I do not anticipate more layoffs

33%
No

28%
Yes and I anticipate there will be more layoffs over the next six months

18%
Not yet, but I anticipate there will be layoffs over the next six months
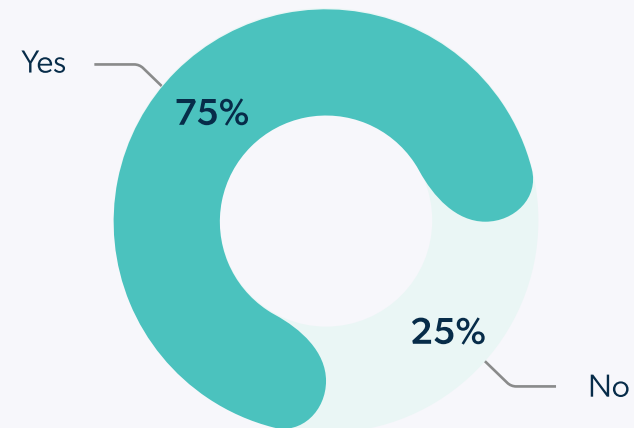
Uncertainty Abounds

Beyond economics, socio-political issues threaten to throw a wrench in the works. When asked about the impact of upcoming elections, nearly half (49%) of IT pros agreed that upcoming elections are adding uncertainty to their organization's future.

Respondents also report inflationary pressures from vendors, though it's ticking down. Three-fourths (75%) report that vendors are increasing their licensing or subscription costs, down from 88% who reported the same in Q1 2024.

Upcoming elections are adding uncertainty to my organization's future success.

Strongly disagree
9%

Strongly agree
20%

Disagree
18%

Agree
29%

Neutral
24%
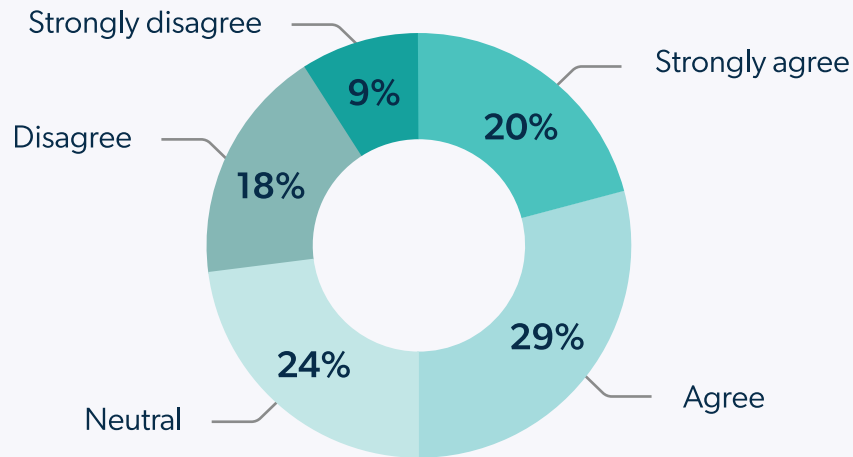
Have you seen vendors increasing their licensing/subscription prices?
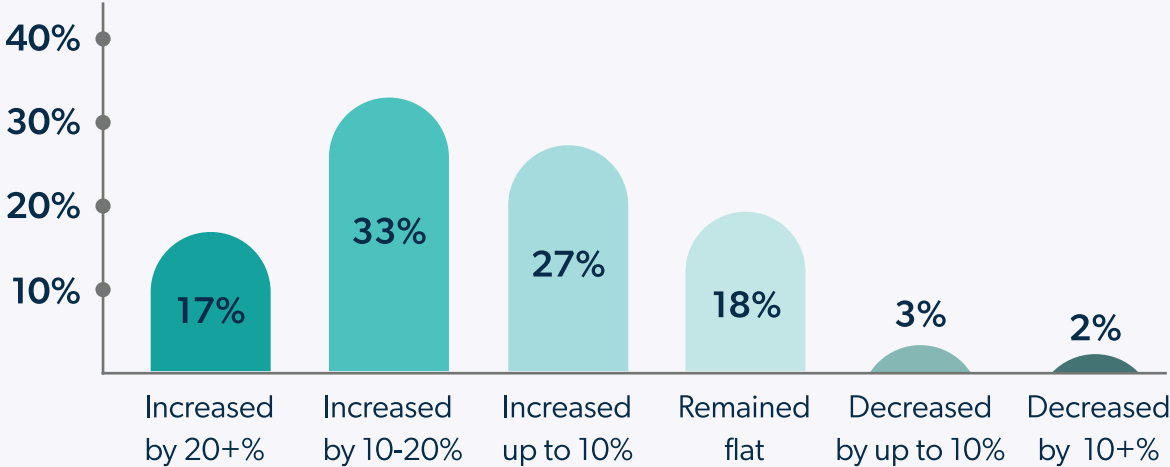
Yes
75%

No
25%

Three Out of Four Will Spend More in 2024

Despite the upward pressure on vendor pricing, IT budgets continue their upward trend. Over three-fourths report an increase in their IT budgets (77%), and 17% report an increase of more than 20% over the last year. Only 5% of SMEs report a decrease in their budget, down from the 6% who reported the same in Q1 2024.

Over the past year, my IT budget:

40%	
30%	
20%	
10%	

- Increased by 20+%: 17%
- Increased by 10-20%: 33%
- Increased up to 10%: 27%
- Remained flat: 18%
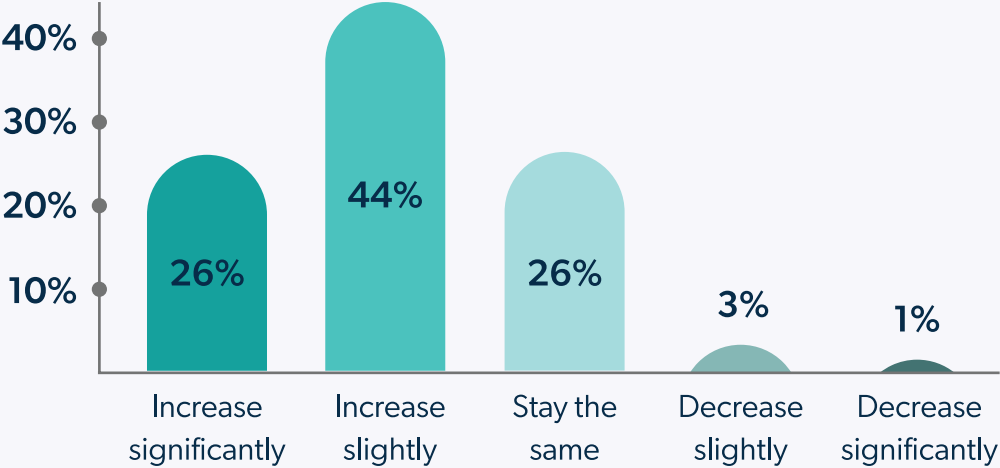- Decreased by up to 10%: 3%
- Decreased by 10+%: 2%

Three Out of Four Will Spend More in 2024

When asked about the second half of 2024, optimism continues as 70% expect their IT budget to increase (compared to 80% who expected the same in Q1 2024). Twenty-six percent expect it to increase significantly (down from 35% in Q1 2024).

In the second half of 2024, I expect our IT budget to:

As a small company, we're always mindful of our budget. It's important for the vendors we work with to have a transparent pricing model that allows us to access enterprise-grade IT management tools without breaking the bank.

— **Ross Derewianko**
Senior Staff Systems Engineer, Voltron Data

Tool Sprawl Is Too Much

The perfect balance between security and user experience continues to be a challenge for IT pros in 2024 and the demand for a unified platform is on the rise. Over eight in 10 (84%) of IT pros would prefer a single platform to manage user identity, access, and security over a mix of best-in-class point solutions, an increase from the 75% who expressed the same in Q1 2024.

I would prefer to use a single platform that consolidates multiple solutions into one interface for identity, access, and security over managing a number of different, best in class point solutions.

35%
Strongly agree

49%
Agree

10%
Neutral

2%
Disagree

4%
Strongly disagree
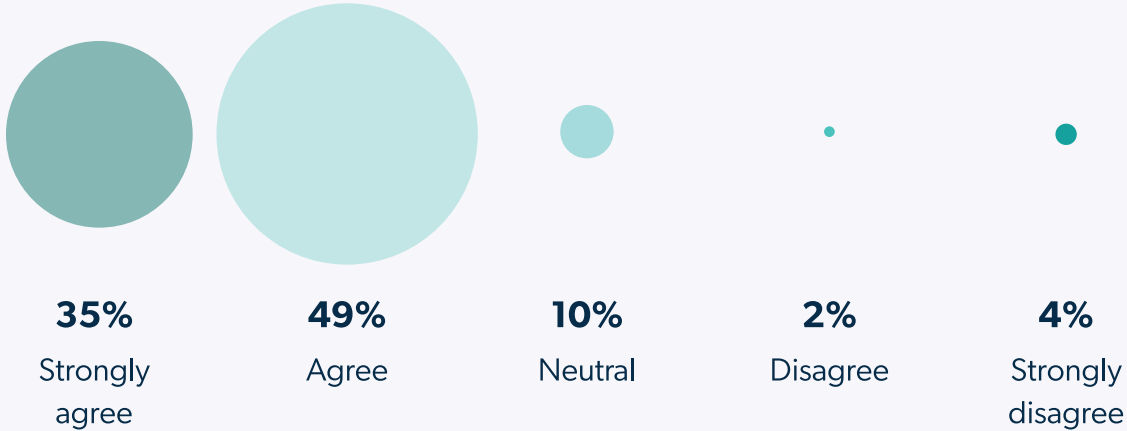
Tool Sprawl Is Too Much

Despite their rising interest in centralized IT management, IT pros currently juggle a number of point solutions. Nearly half of IT pros (45%) require five to 10 tools to manage worker lifecycle; over a quarter (28%) require 11 applications or more; and 10% require more than 15.

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.)

| **2%**	**25%**	**45%**	**18%**	**10%**
1	2-4	5-10	11-15	16+
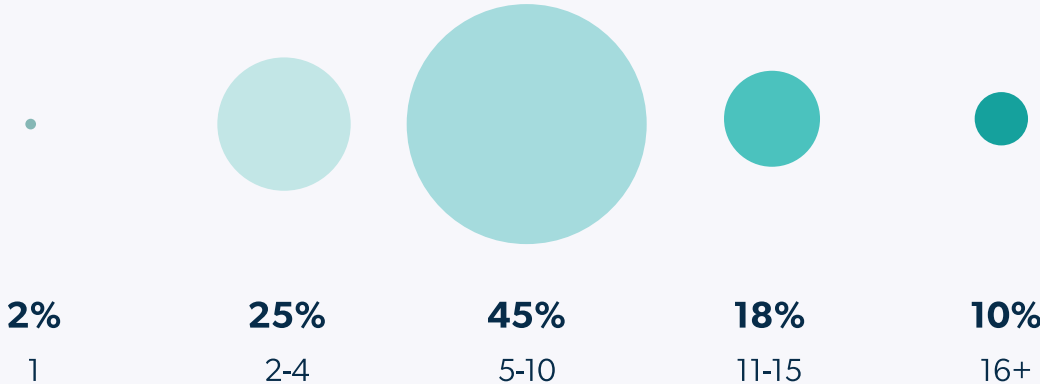
> *Simplifying our IT stack, as well as consolidating everything from onboarding, reporting, and machine management is immensely important to us. Not to mention ease of access for our end users. Flexibility and having everything in one spot for our team, plus reliability, is key for us.*
>
> — **Benjamin Gradidge**
>   Sr. IT Infrastructure Manager, Rethink
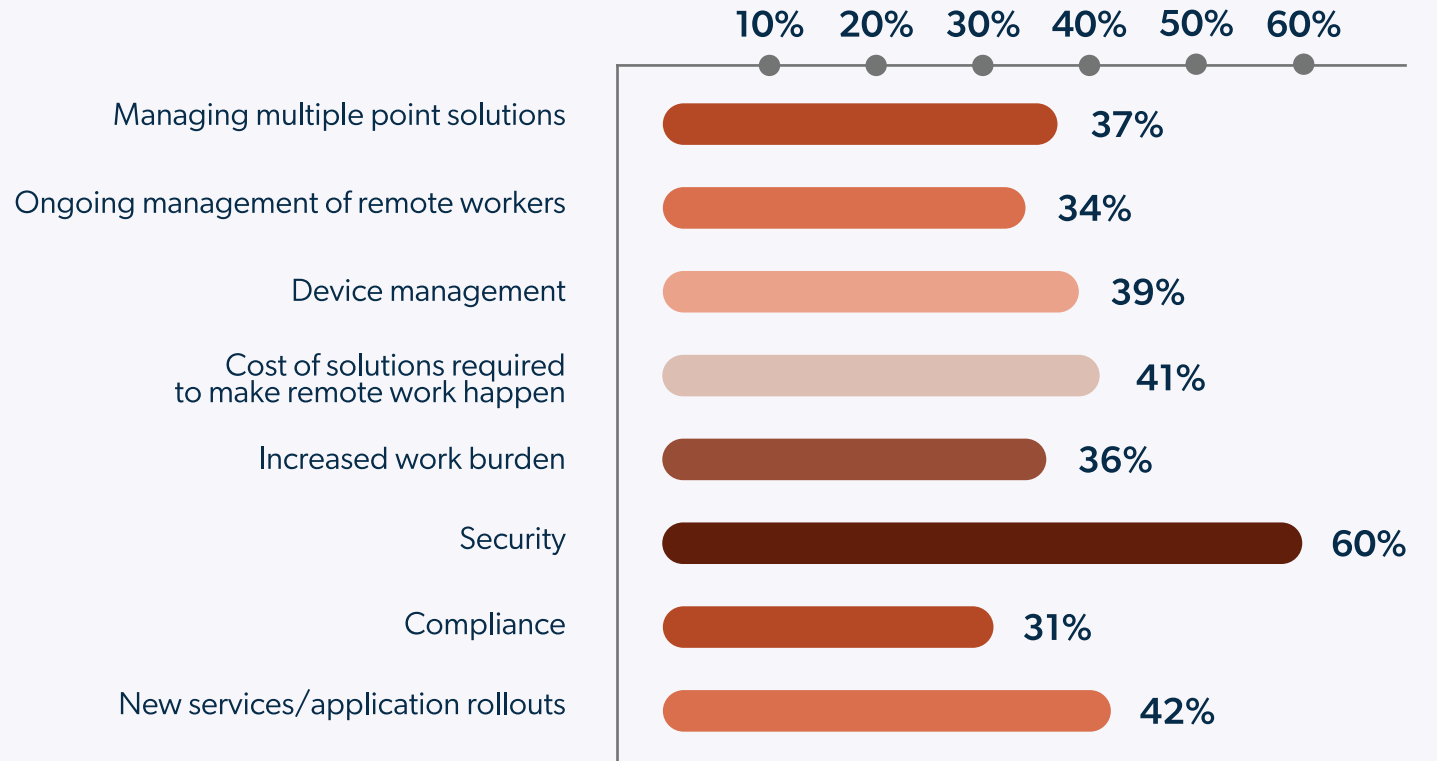
Security and SMEs
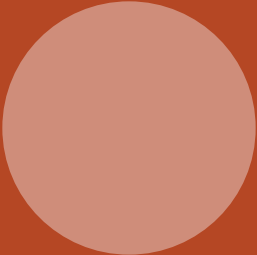
Security Woes are Keeping IT Awake at Night

Security continues to be the biggest challenge for IT teams. When asked about their biggest challenges, 60% of SMEs say it's security, followed distantly by new service and application rollouts (42%), the cost of solutions necessary to enable remote work (41%), and device management (39%).

What have been the biggest challenges to your IT team in Q1 2024?

| Challenge	Percentage
Managing multiple point solutions	37%
Ongoing management of remote workers	34%
Device management	39%
Cost of solutions required to make remote work happen	41%
Increased work burden	36%
Security	60%
Compliance	31%
New services/application rollouts	42%

Security Woes are Keeping IT Awake at Night

Half of IT teams (50%) report being more concerned about their organization's security posture than they were six months ago, down slightly from the 56% who said the same in Q1 2024.

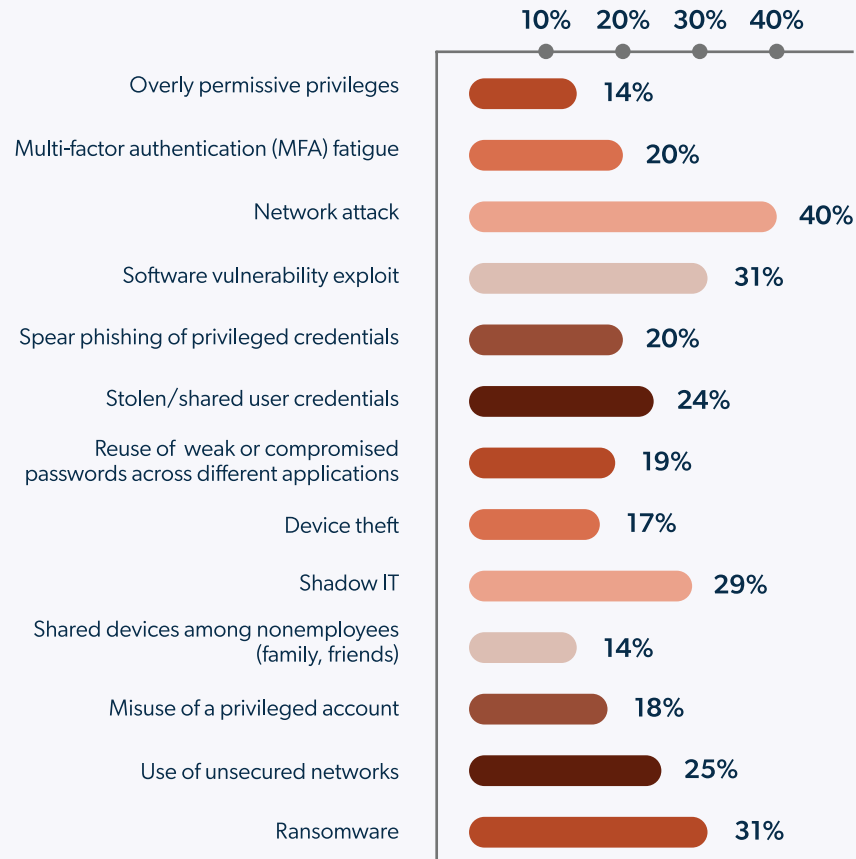**I am more concerned about my organization's security posture than I was 6 months ago.**
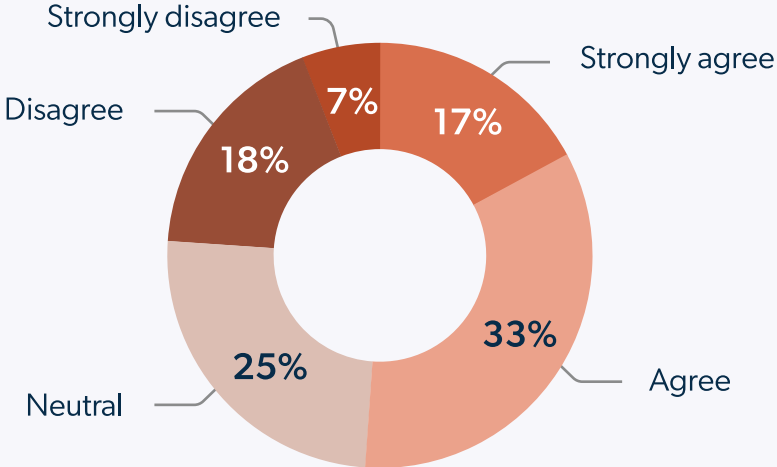
Strongly disagree — 7%
Strongly agree — 17%
Disagree — 18%
Agree — 33%
Neutral — 25%

50%

report being more concerned about their organization's security posture than they were six months ago.

Lurking Fears Around Shadow IT

Shadow IT is growing and has SME IT pros concerned, joining the list of the top security concerns. The four biggest security concerns are network attacks (40%), followed by software vulnerability exploits (31%), ransomware (31%), and shadow IT (29%).

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

Concern	Value
Overly permissive privileges	14%
Multi-factor authentication (MFA) fatigue	20%
Network attack	40%
Software vulnerability exploit	31%
Spear phishing of privileged credentials	20%
Stolen/shared user credentials	24%
Reuse of weak or compromised passwords across different applications	19%
Device theft	17%
Shadow IT	29%
Shared devices among nonemployees (family, friends)	14%
Misuse of a privileged account	18%
Use of unsecured networks	25%
Ransomware	31%

When asked how concerned they are about shadow IT (applications or resources managed outside of IT), 84% of respondents replied they're very (35%) or somewhat (49%) concerned.

How concerned are you about applications or resources managed outside of IT (i.e., shadow IT)?

1% I don't know

15% Not concerned
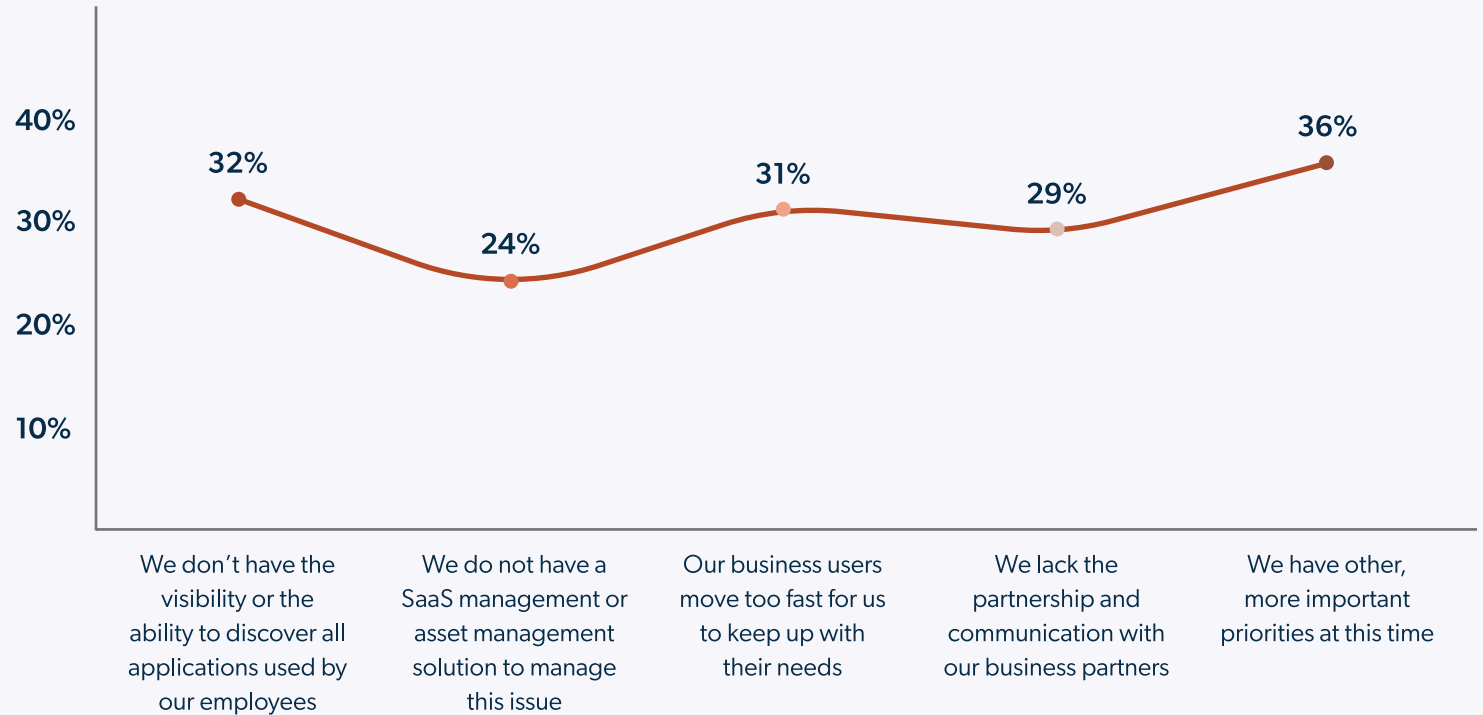
35% Very concerned

49% Somewhat concerned
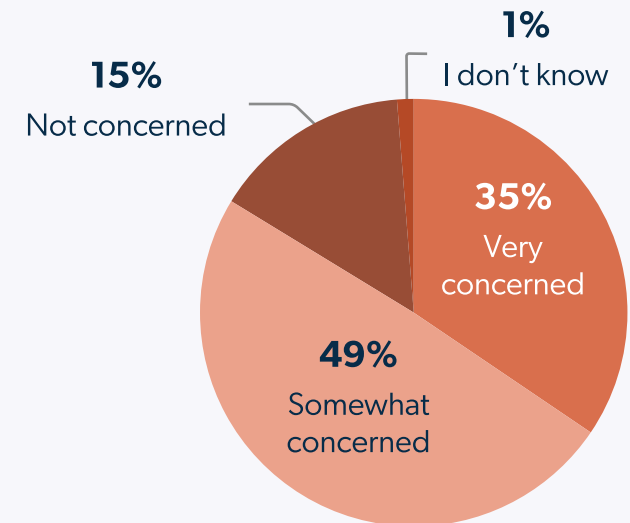
Despite Risks, Shadow IT Not So Simple To Solve

IT pros report a number of reasons for why shadow IT looms so large. When asked what has prevented them from addressing shadow IT, 36% say there are other, more important priorities. Thirty-two percent say they don't have the ability to discover all the applications used by employees. Thirty-one percent say their business users move too fast to keep up with their needs. Twenty-nine percent say they lack partnership and communication with business partners, and 24% say they don't have a SaaS management or asset management solution to manage shadow IT.

Why are you not able to address the issue of shadow IT?

|				
32%	24%	31%	29%	36%
We don't have the visibility or the ability to discover all applications used by our employees	We do not have a SaaS management or asset management solution to manage this issue	Our business users move too fast for us to keep up with their needs	We lack the partnership and communication with our business partners	We have other, more important priorities at this time

Spending and Staffing Steady

In the face of growing threats, SMEs continue to invest in security and support their IT staff. Over eight in 10 SMEs (84%) have an IT security expert on staff, 73% say their organization is financially prepared to recover from a cyberattack, and 82% say that management respects their counsel and recommendations around IT operations.
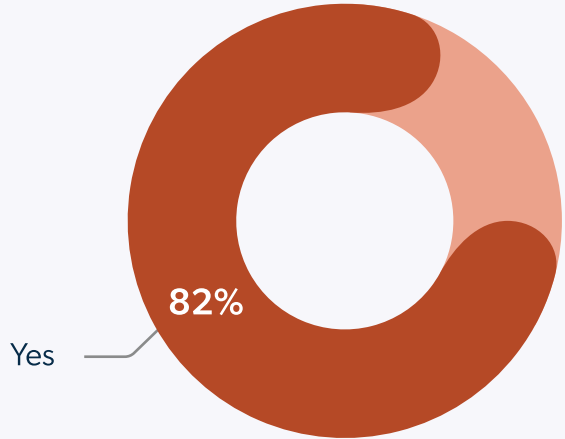
Do you have an IT security expert on staff?

84%
Yes
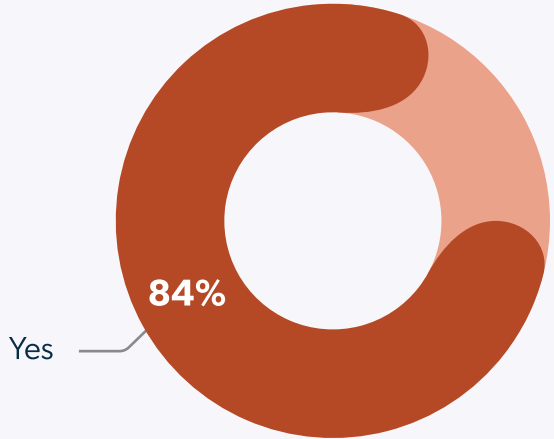
My organization is financially prepared to recover from a cyberattack.

73%
Yes
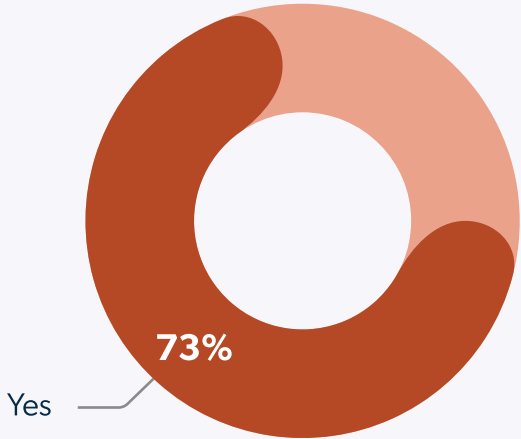
Management respects my counsel and recommendations around IT operations.
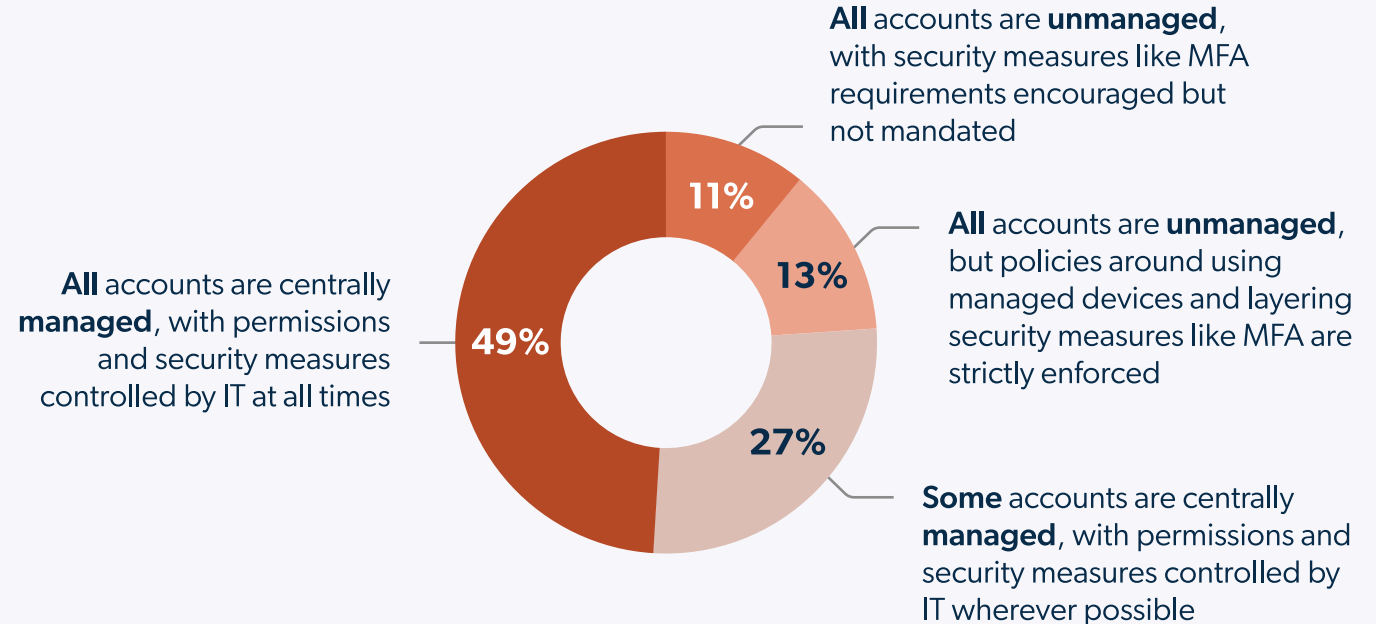
82%
Yes

IT Is the Captain Now

SMEs seeking to fortify their security posture see centralized IT management as a strong opportunity. When it comes to employees accessing IT resources, nearly half (49%) say all employee accounts are managed centrally with permissions and security measures controlled by IT. Only 11% leave accounts entirely unmanaged and encourage — but don't mandate — steps like multi-factor authentication (MFA).

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

All accounts are **unmanaged**, with security measures like MFA requirements encouraged but not mandated

All accounts are **unmanaged**, but policies around using managed devices and layering security measures like MFA are strictly enforced

All accounts are centrally **managed**, with permissions and security measures controlled by IT at all times

Some accounts are centrally **managed**, with permissions and security measures controlled by IT wherever possible

11%

13%

49%

27%

Biometrics May Balance Security

With advances in device hardware, it's not surprising that the number of organizations adopting biometrics is on the rise. IT pros look to add extra security layers without dragging on productivity.

Biometrics adoption is steady with 66% of SMEs requiring it (the same as in Q1 2024), and 67% of IT pros agree their organization's security posture would be stronger if biometrics were required.

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

No — 34%

Yes — 66%
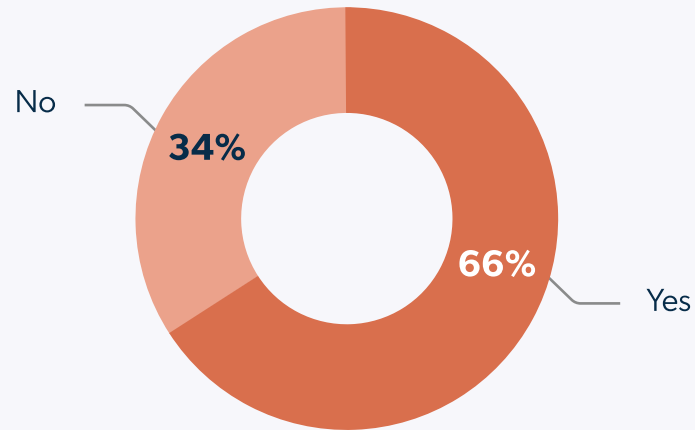
My organization's security posture would be stronger if they required biometrics.

- 2% Strongly disagree
- 8% Disagree
- 23% Neutral
- 47% Agree
- 20% Strongly agree

Biometrics May Balance Security

S
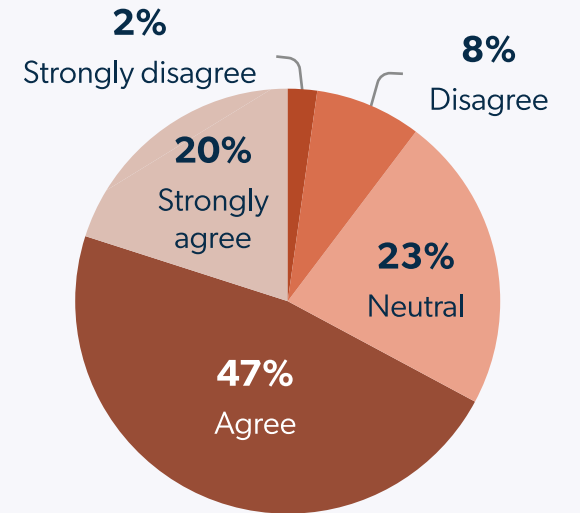
Fewer IT pros are wary about adding friction when adding security measures. Though 61% of respondents agree that additional security measures generally mean a more cumbersome experience, that's down from the 67% who said the same in Q1 2024.

Additional security measures generally mean a more cumbersome user experience.
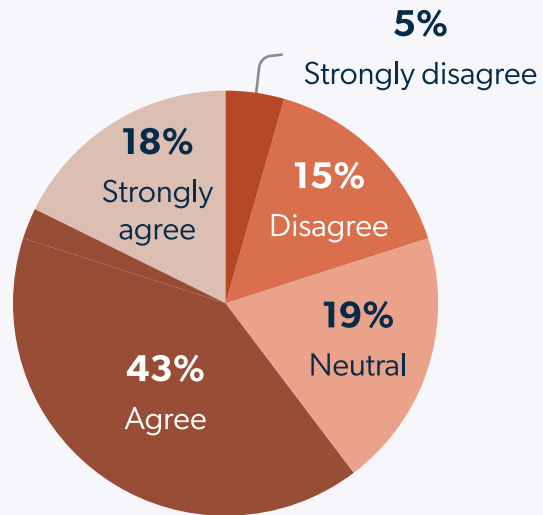
- **5%** Strongly disagree
- **15%** Disagree
- **19%** Neutral
- **43%** Agree
- **18%** Strongly agree

61%

**of respondents agree that additional security measures generally mean a more cumbersome experience.**

Passwords: The Stubborn Survivor

Whether it's legacy systems, complicated integrations, or other reasons, barely one quarter of employees (26%) can access all of their IT resources with just one to two passwords and nearly one-fifth (17%) have to manage 10 passwords or more.
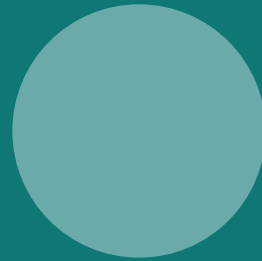
On average, how many different passwords do your employees have to log into their IT resources?
(devices, apps, networks, files, servers, etc., either on-premises or in the cloud)

26%	**38%**	**19%**	**12%**	**5%**
1-2	3-5	6-9	10-15	16+
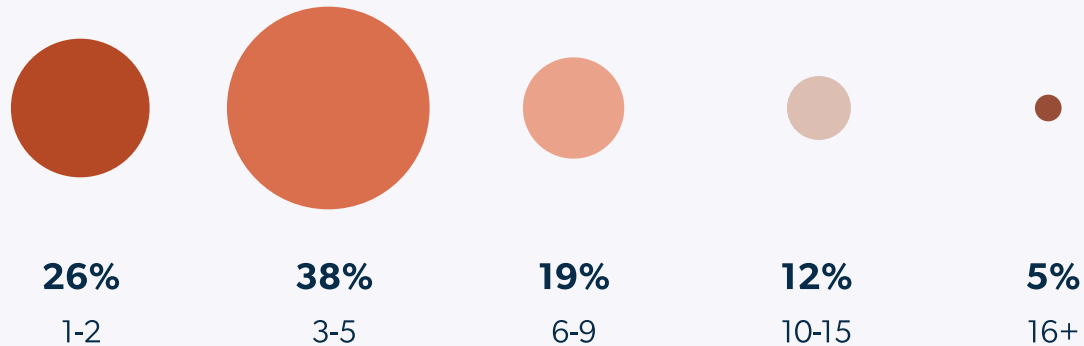
95%
of respondents use passwords to secure at least some IT resources, despite SMEs adopting tools like MFA, biometrics, and single sign-on (SSO).

SMEs and Devices

Device Diversity: Supporting a Full Palette of Platforms

D

With workers logging in from around the world and on a variety of devices, SMEs continue to embrace a variety of devices.

The average SME is made up of 24% macOS devices (up from 22% in Q1 2024), 18% Linux devices (down from 22%), and 63% Windows devices (up from 60%).

For modern organizations, and especially for SMEs, supporting a diverse device environment adds challenges. Securing devices properly, maintaining updates and patches, being able to troubleshoot across different operating systems, and more. As IT teams look to minimize complexity and eliminate unnecessary tools and solutions, establishing a centralized device management system for visibility and control is critical.

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

63%
18%
24%
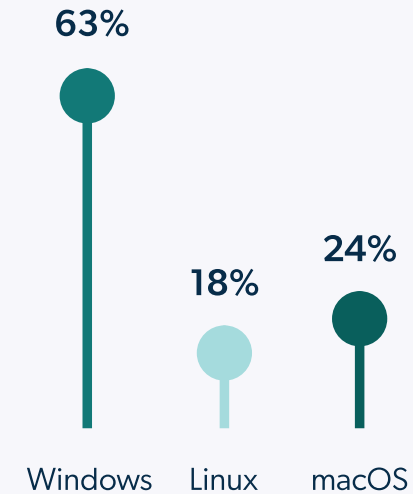
Windows   Linux   macOS

The Future Is Flexible: A Multi-OS Mandate

When looking down the road, IT teams expect they'll need to continue to support a broad range of devices. IT pros expect their use of Windows, Linux, and macOS devices to increase substantially, underscoring their need for identity and device systems that cover multiple device types, from enrollment to security patching to permissions management.

Over the next year, I expect our:

— To increase
— To remain the same
— To decrease
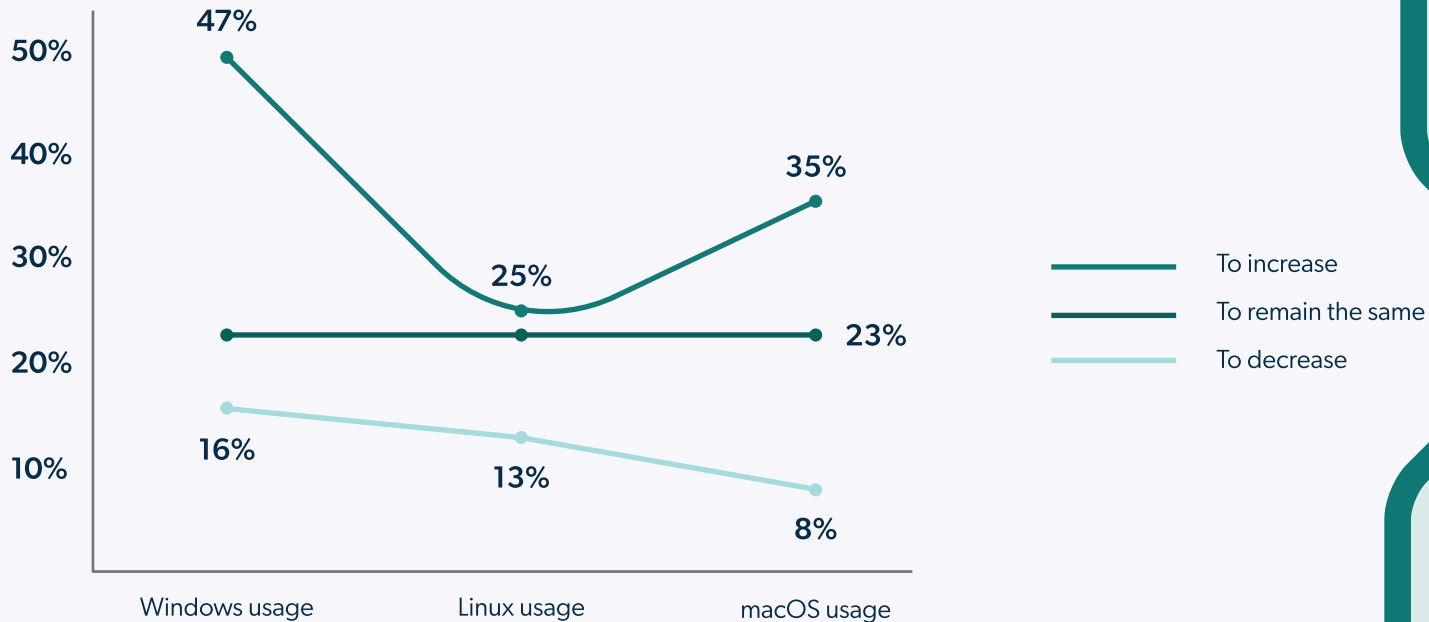
The more our company grows, the more diverse our device mix becomes. Some employees only request macOS, some require Windows, and others are die-hard Linux users. It's only going to grow more complex. The key is finding a solution that can manage them all.
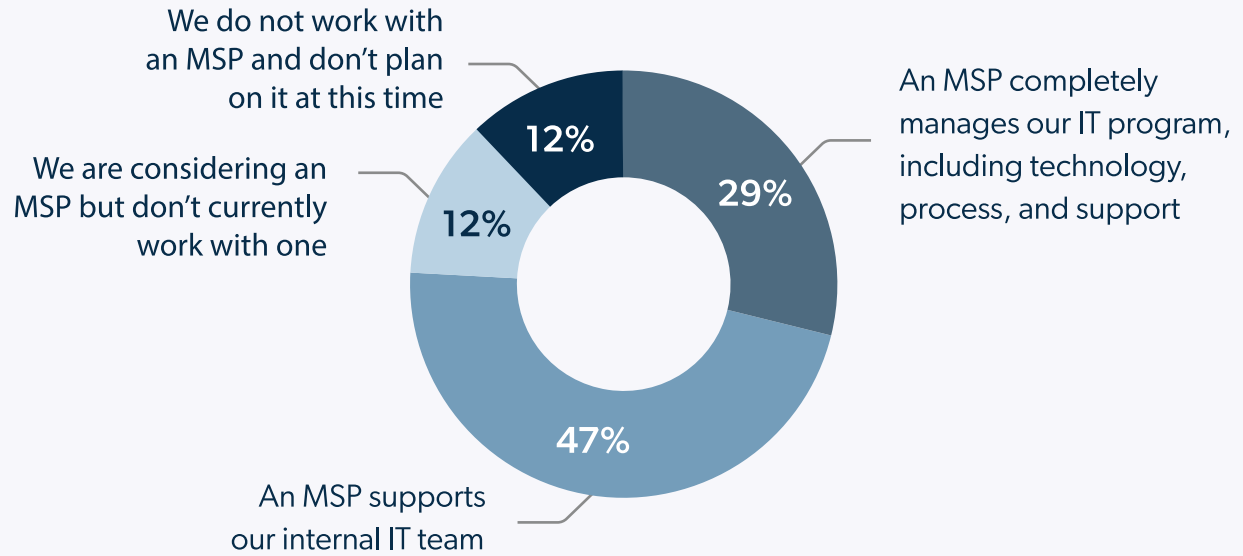
— Frank G.
   IT Director

MSPs and SMEs
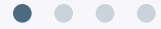
MSP Magic: SMEs' Secret Sauce

SMEs continue to rely on managed service providers (MSPs) to help with identity, user, and device management. Over three-quarters (76%) of SMEs rely on an MSP for at least some functions, the same as the 76% who reported the same in Q1 2024, and another 12% are considering working with one.

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

We do not work with an MSP and don't plan on it at this time
12%

We are considering an MSP but don't currently work with one
12%

An MSP completely manages our IT program, including technology, process, and support
29%

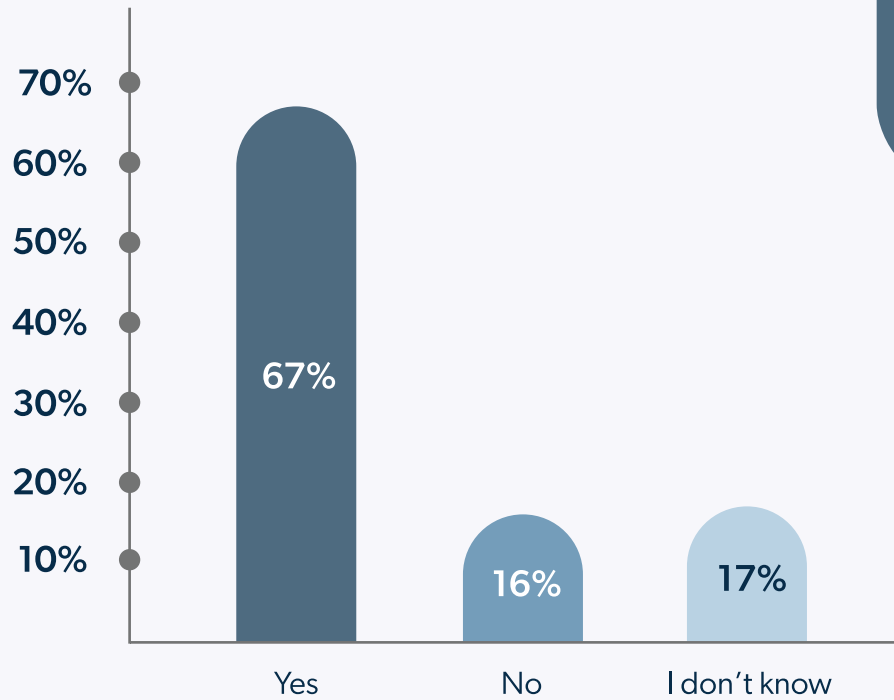An MSP supports our internal IT team
47%

MSP Magic: SMEs' Secret Sauce

The partnership with MSPs is seen as an integral part of IT operations for a majority of SMEs, as 67% of SMEs say they'll increase their MSP investment over the next 12 months.

We plan to increase our MSP investment over the next 12 months.

|		
70%		
60%		
50%		
40%		
30%	67%	
20%		16%	17%
10%		
	Yes	No	I don't know

Leveling Up with MSPs

Generally, MSPs are seen as a critical partner for SMEs, offering a broad range of benefits and functions. The most common reasons SMEs use MSPs are because they are cost-effective (58%), up to date on the latest technologies (55%), provide a better user experience (50%), and they can secure users' access and identity better than the internal team (40%).

We use MSPs because:

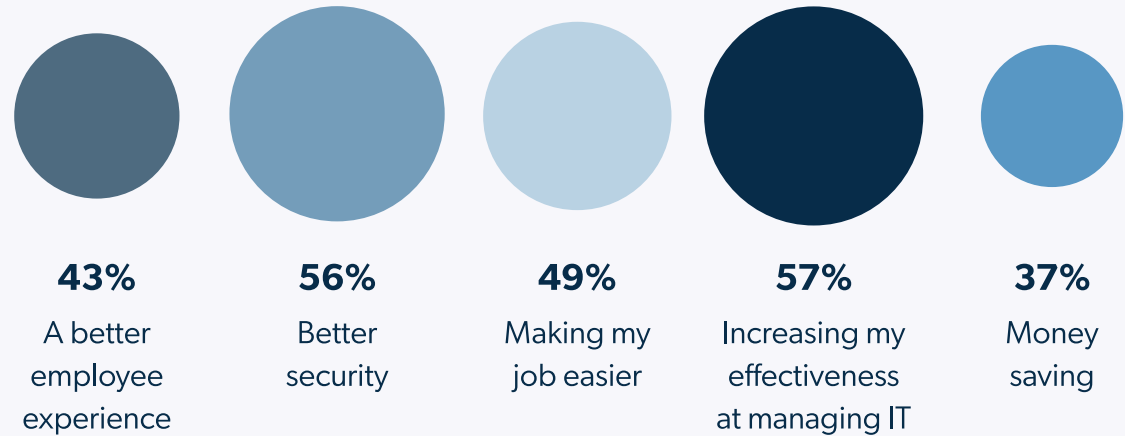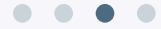|	
They are cost-effective	58%
They are up to date on the latest technologies	55%
They can provide a better user experience	50%
They can secure users' access and identity better than we can	40%
They offer strong customer support	29%
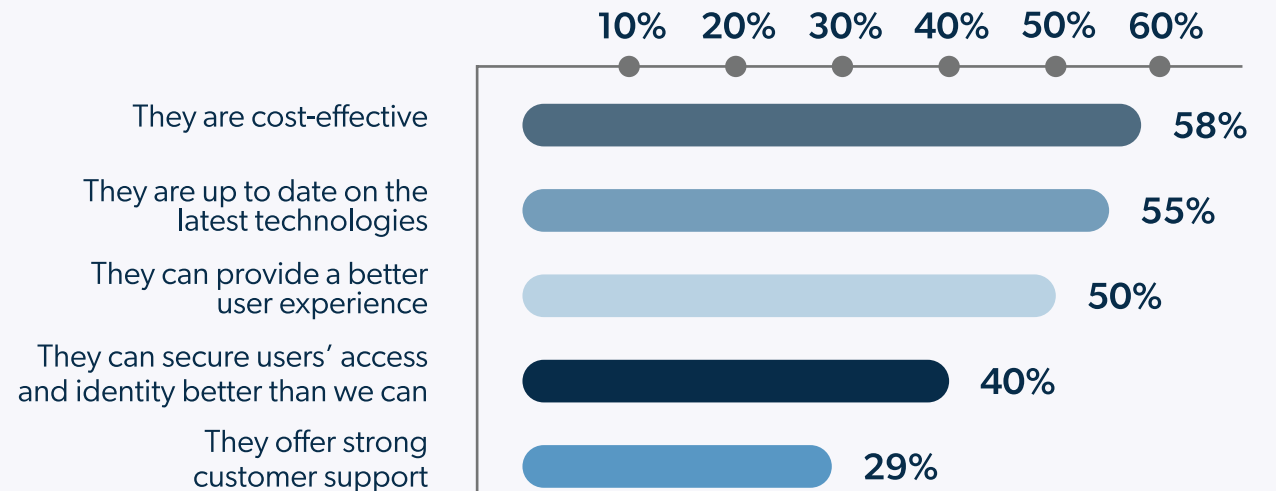
Leveling Up with MSPs

MSPs are seen to deliver cost-savings. But security and improving IT effectiveness are the top drivers of MSP use. Over half of IT teams said MSPs had resulted in better security (56%) and increased their effectiveness at managing IT (57%), and just a little over one-third (37%) said it had saved money for their organization.

Using an MSP has resulted in:

43%
A better employee experience

56%
Better security

49%
Making my job easier

57%
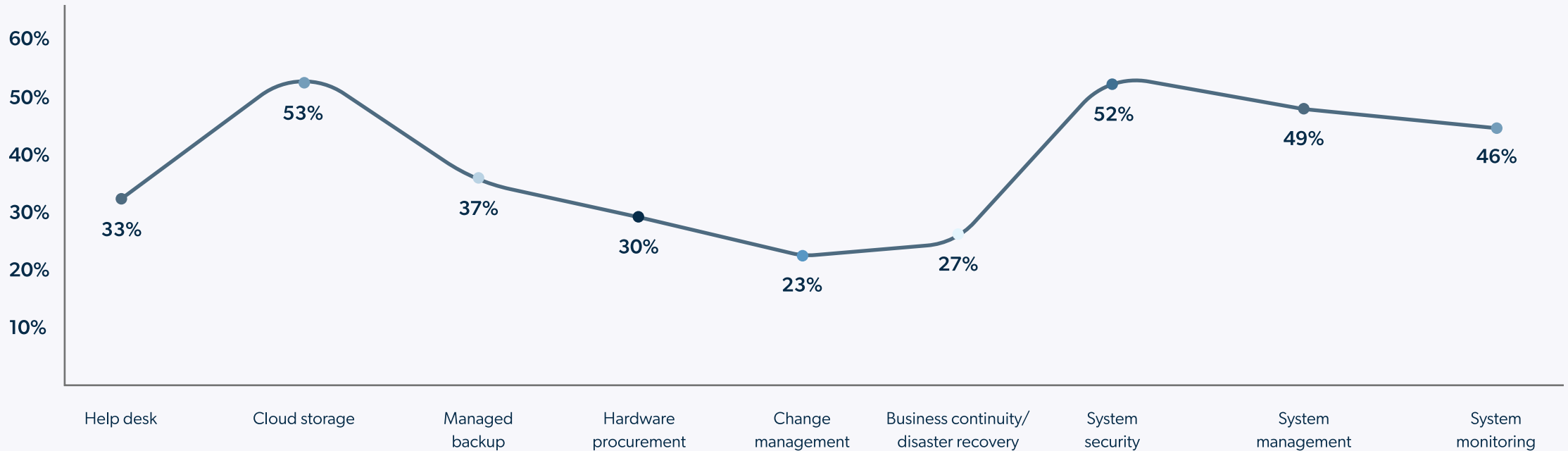Increasing my effectiveness at managing IT

37%
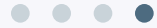Money saving

MSPs Wear Many Hats

The most common IT programs managed by MSPs are cloud storage (53%, up from 52% in Q1 2024), system security (52%, down from 57% in Q1 2024), system management (49% vs. 47% in Q1 2024), system monitoring (46% vs. 51% in Q1 2024), and managed backup (37% vs. 40% in Q1 2024).

What areas of your IT program are managed by MSPs?

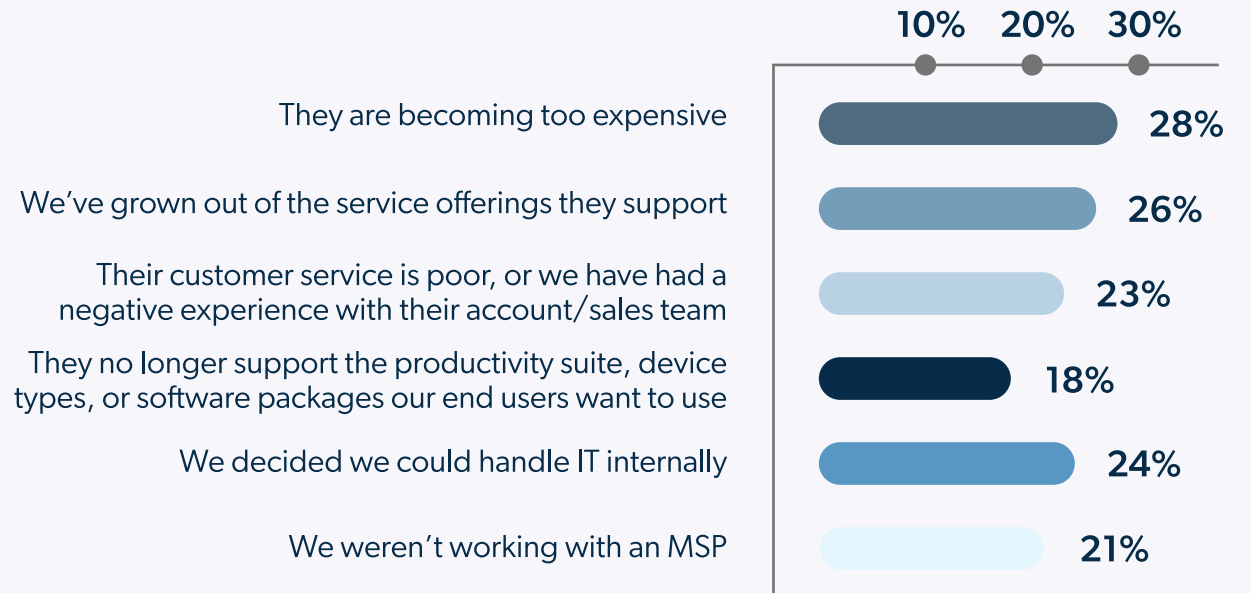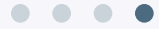| Help desk	Cloud storage	Managed backup	Hardware procurement	Change management	Business continuity/ disaster recovery	System security	System management	System monitoring
33%	53%	37%	30%	23%	27%	52%	49%	46%

MSPs in the Hot Seat: SMEs Demand More

While MSPs and SMEs are deeply integrated, the survey revealed a few areas of concern for MSPs. The percentage of SMEs outsourcing their entire IT program to MSPs has decreased to 29%, down from 42% who said the same in Q1 2024. The most common reason SMEs stop working with an MSP is because they became too expensive (28%), followed by growing out of the service offerings the MSP supports (26%), taking IT internal (24%), and a negative customer service or sales team experience (23%).

Have you recently stopped working with an MSP, and if so, why?

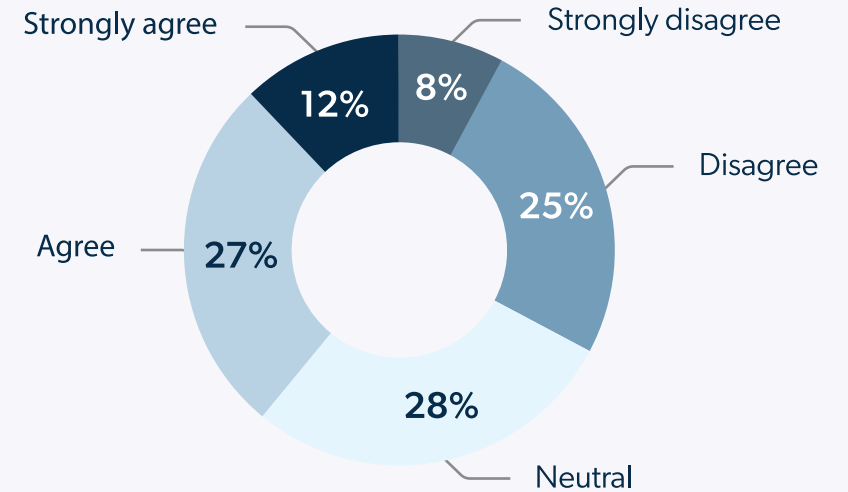|	
They are becoming too expensive	28%
We've grown out of the service offerings they support	26%
Their customer service is poor, or we have had a negative experience with their account/sales team	23%
They no longer support the productivity suite, device types, or software packages our end users want to use	18%
We decided we could handle IT internally	24%
We weren't working with an MSP	21%

MSPs in the Hot Seat: SMEs Demand More

For those who don't use an MSP, nearly half (47%) say it's because they prefer to handle IT themselves and 39% say it's because MSPs are too expensive.
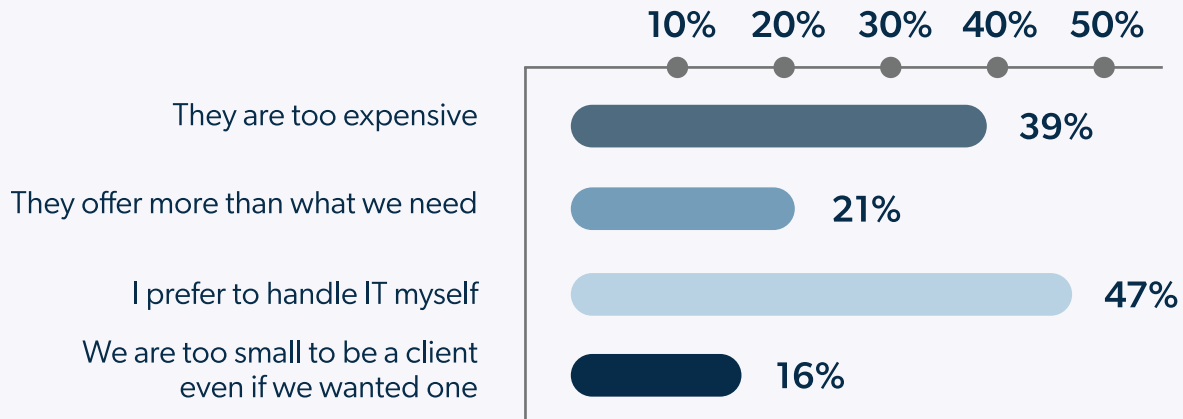
And for all respondents, including those that use MSPs, nearly four in 10 (39%) have concerns about how MSPs manage security, even though security is the number one driver for SMEs to use MSPs overall.

We don't use MSPs because:

- They are too expensive — **39%**
- They offer more than what we need — **21%**
- I prefer to handle IT myself — **47%**
- We are too small to be a client even if we wanted one — **16%**

(scale: 10% 20% 30% 40% 50%)

I have concerns about how MSPs manage security:

- Strongly agree: **12%**
- Strongly disagree: **8%**
- Disagree: **25%**
- Neutral: **28%**
- Agree: **27%**

AI and SMEs

AI Planning Accelerates

A ● ● ● ● ●
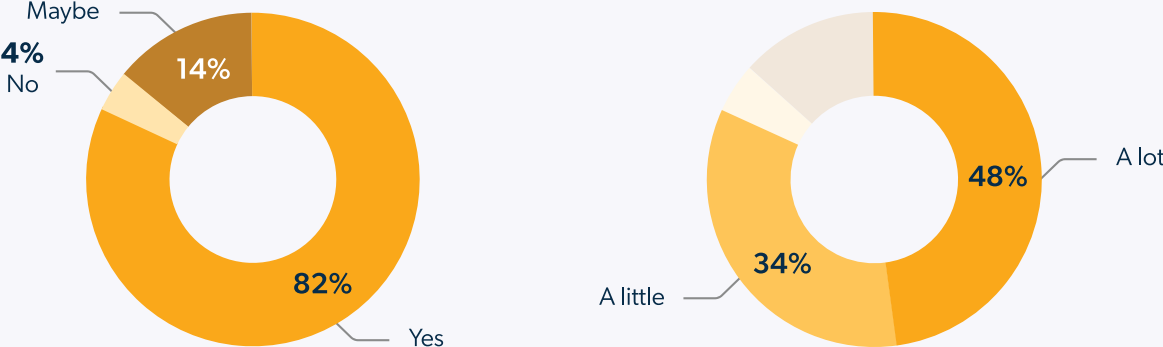
As AI continues to evolve and is used in new applications and use cases, SMEs are pursuing a measured approach while retaining fears around its potential impact. Organizations picked up their planning for AI. Only 10% have no plans to implement AI, down from 13% six months ago. Those planning AI initiatives within the next six months increased to 35% from 27% in Q1 2024. Eighty-two percent say their organizations should be investing in AI (48% say a lot), versus 76% in Q1 2024.

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

6 months	35%
7 - 12 months	32%
13 - 18 months	18%
19 - 24 months	5%
No current plans	10%
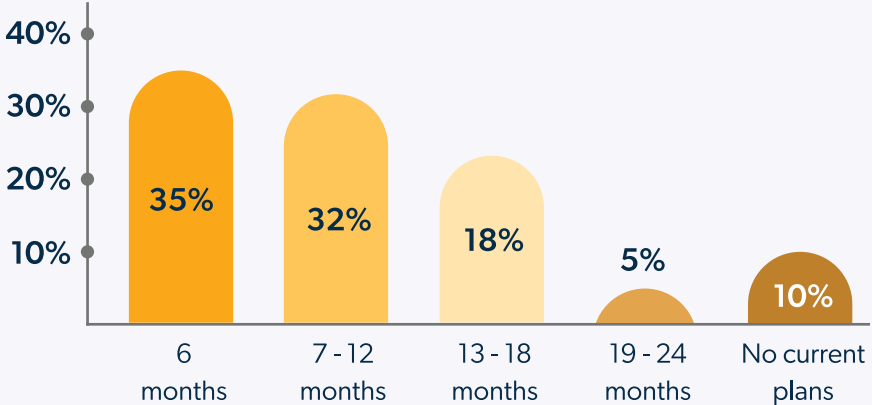
Our organization should be investing in AI initiatives for IT.
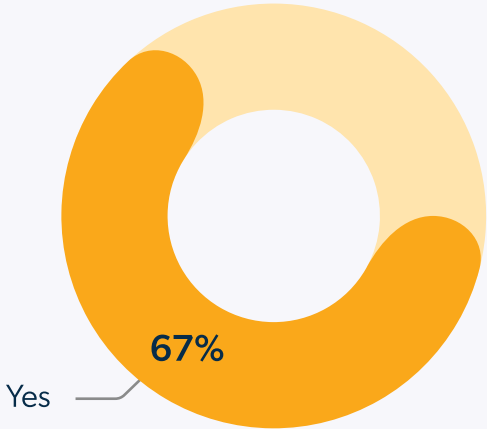

Maybe 14%
No 4%
Yes 82%

A lot 48%
A little 34%

AI Appetite: A Measured Approach

SMEs are being intentional about AI. Over two-thirds of SMEs have a policy around AI (67%, up from 63% in Q1 2024), and 60% say their organization is moving at exactly the right speed with respect to AI, up from 55% in Q1 2024. Seventy-seven percent see AI as a net positive for their organization, down slightly from 79% in Q1 2024.
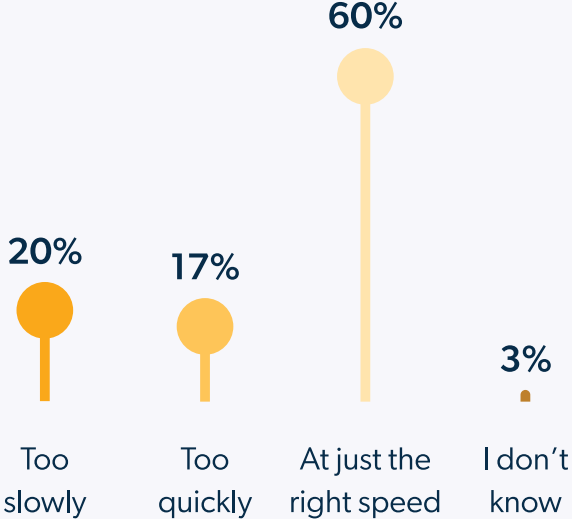
Does your company have a policy around AI?

Yes 67%

AI will be a net _____ for my organization.

Negative 5%
Neutral 18%
Positive 77%
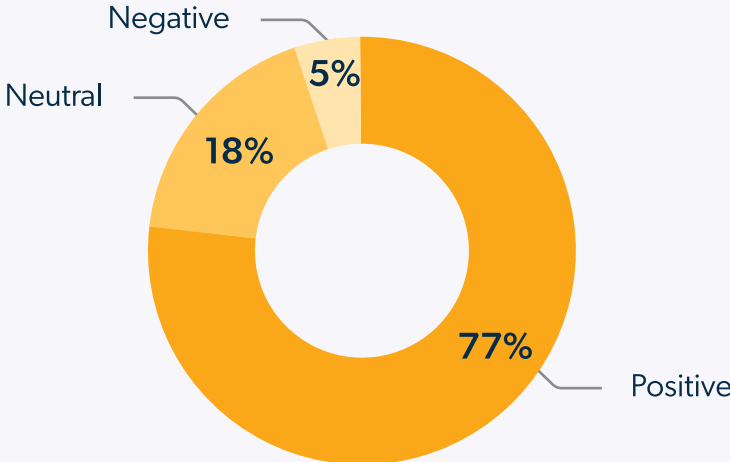
My organization is moving _____ around AI.

60% At just the right speed
20% Too slowly
17% Too quickly
3% I don't know

Conflicting Opinions Rise Around AI

When asked how their general opinion changed over the last six months about how AI will impact their day-to-day job, 22% say the impact of AI is much lower than they thought it would be. Thirty-four percent say the potential impact of AI is the same but it is moving slower than they thought it would. Twenty-one percent say their opinion hasn't changed, and 23% say they feel the impact of AI is even greater than they thought it would be.

How has your general opinion changed over the last 6 months about how AI will impact your day-to-day job (through efficiency enhancements or net-new technologies)?

I feel like the impact of AI is even greater than I thought it would be

I feel like the impact of AI is much lower than I thought it would be

23%

22%

21%

34%

My opinion has not changed at all

I feel like the potential impact of AI is the same, but it is moving slower than I thought it would be
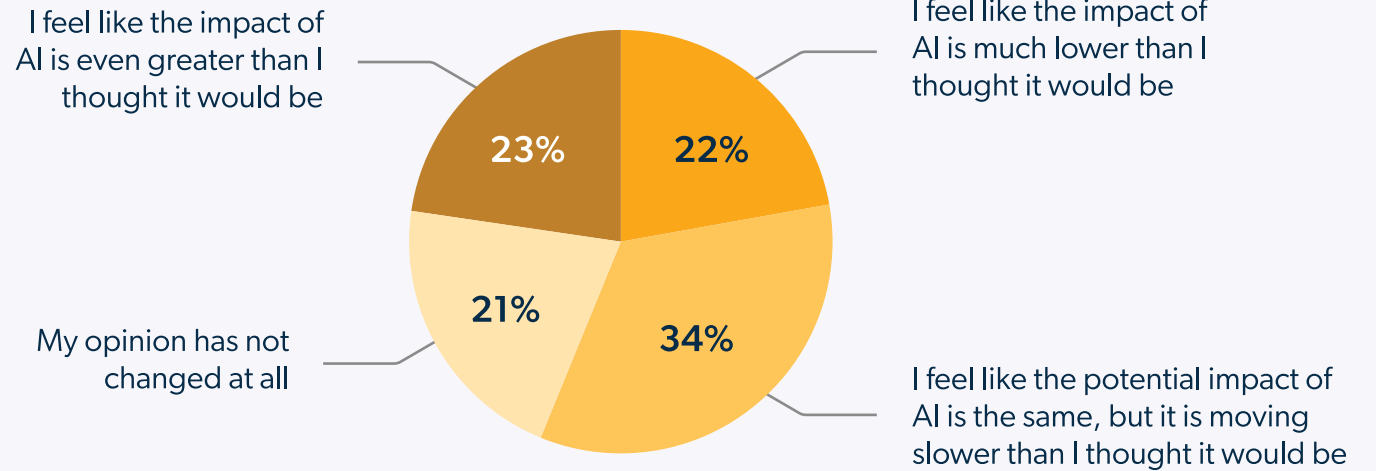
The Queen's Gambit: Strategizing Security Around AI

For all of the contributions of AI to the IT landscape, its impact on security continues to concern IT pros. In 2024, a quarter of organizations (25%) have experienced AI-generated attacks.
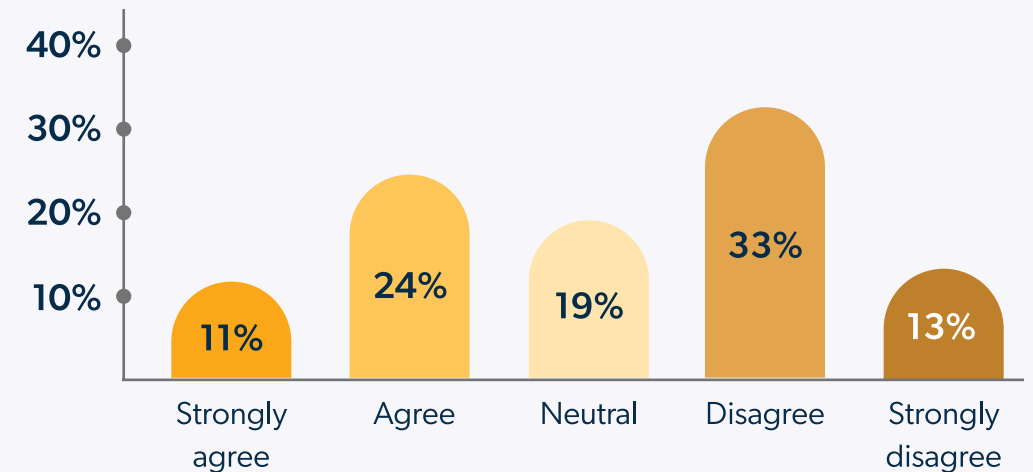
When asked about the speed of AI, fear dominates. Sixty-one percent agreed that AI is outpacing their organization's ability to protect against threats, roughly the same as the 62% who said so in Q1 2024.

Though as familiarity with AI grows, it's possible that fears around it are lessening. The number of IT pros who strongly agreed about AI outpacing their organization's security dropped to 22%, down from 29% in Q1 2024. Just over one-third of IT pros (35%) say they're worried about AI's impact on their job, down significantly from the 45% who said the same in Q1 2024.

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

- 3% Strongly disagree
- Disagree 15%
- Strongly agree 22%
- Neutral 21%
- Agree 39%
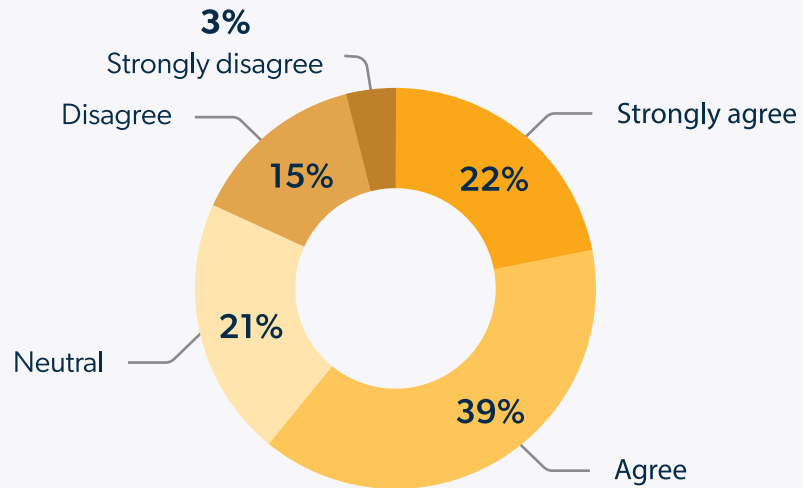
I am worried about AI's impact on my job.

Strongly agree	Agree	Neutral	Disagree	Strongly disagree
11%	24%	19%	33%	13%

Final Stop: Thriving in Modern IT

The seventh edition of JumpCloud's SME IT Trends Report reveals that in 2024's complex IT landscape, success hinges on flexibility, foresight, and a dash of digital daring. "Detours Ahead: How IT Navigates an Evolving World" can serve as a map for your IT journey, equipping you with the information you need to chart the best path forward for IT success.

A few considerations as you plot your route:

- **Shine a light on shadow IT**: Deploy tools that can help you spot a rogue app faster than you can say "unauthorized download" or "device not recognized."

- **Embrace diversity**: Diverse device landscapes aren't going anywhere, but a system that can handle Windows, macOS, Linux, and more can make managing them easy.

- **Maximizing your MSP**: Evaluate costs, features, and results, and be prepared to make a change if your MSP is no longer serving you.

- **Unify (or die trying)**: Admins have been telling us for years that they want a single tool to manage identity and access management (IAM). Now's the year to make it happen.

- **Make security your superpower**: Whether biometrics, AI, or centralizing IT, supplement your security efforts while keeping your digital guard up.

By focusing on flexibility, visibility, and control, SME IT pros can turn potential pitfalls into stepping stones. It's not just about surviving today's digital wilderness, it's about thriving in it.

Final Stop: Thriving in Modern IT

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 612 IT decision-makers in the U.K. and U.S., 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 June 4, 2024 to June 7, 2024.

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, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including General Atlantic, Sapphire Ventures, Sands Capital, Atlassian, and CrowdStrike.

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