



SME IT TRENDS Q3 2024

How Are SMEs Navigating Security?



This edition of SME IT Trends focuses on only the security data from the original report. To see the data on the [SME IT Landscape](#), [SMEs and Devices](#), [MSPs and SMEs](#), and [AI and SMEs](#) sections, download the full report for free.

[Download the Full Report](#)

If you're an IT professional, odds are you're worried about security.

In fact, if you're an IT professional working at a small- to medium-sized enterprise (SME), **there's a 60% chance that security is your number one challenge.**

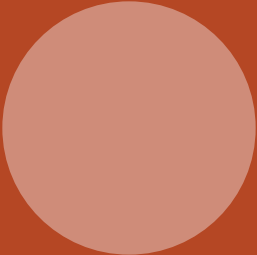
In a recent data report, JumpCloud surveyed more than 600 IT professionals at SMEs on the topic of security. Their answers offer key insights into the cybersecurity landscape and how your peers think about, approach, and experience security.

This data will help answer important questions, including:

- What are the primary security challenges facing IT teams in SMEs?
- Why is shadow IT such a stubborn problem?
- What are SMEs doing to address top security concerns?



Security and SMEs



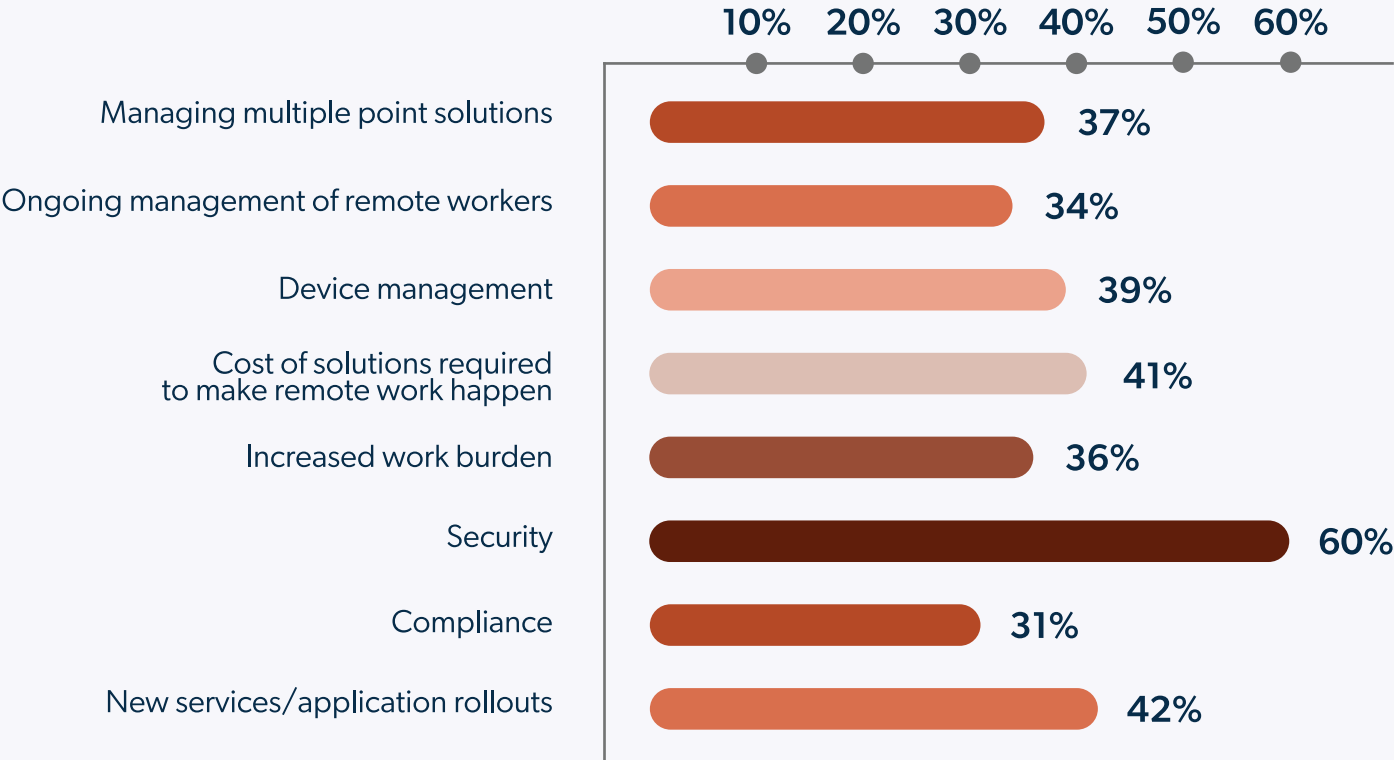


Security is SMEs' Top Challenge



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?



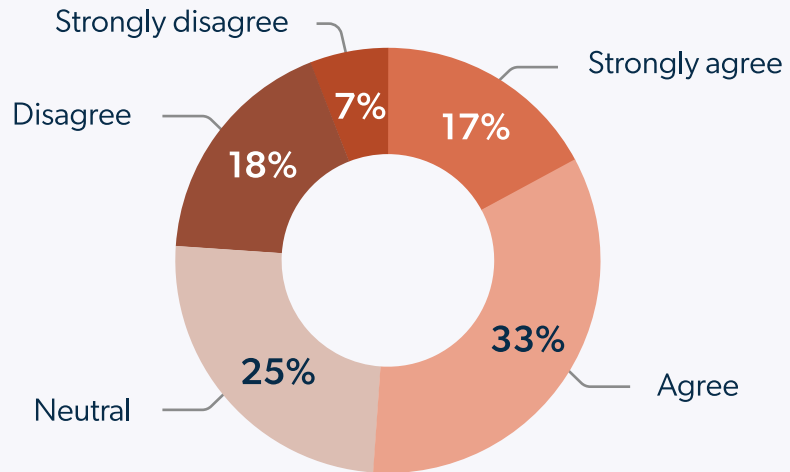


Security is SMEs' Top Challenge



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.



50%

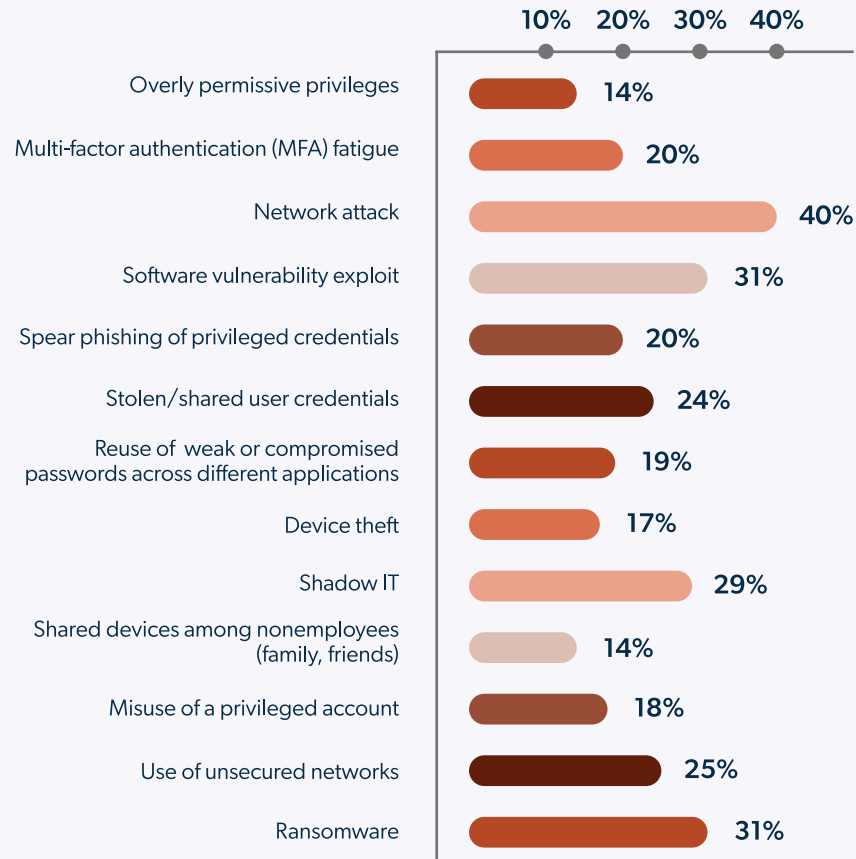
report being more concerned about their organization's security posture than they were six months ago.

What Makes Security So Challenging?



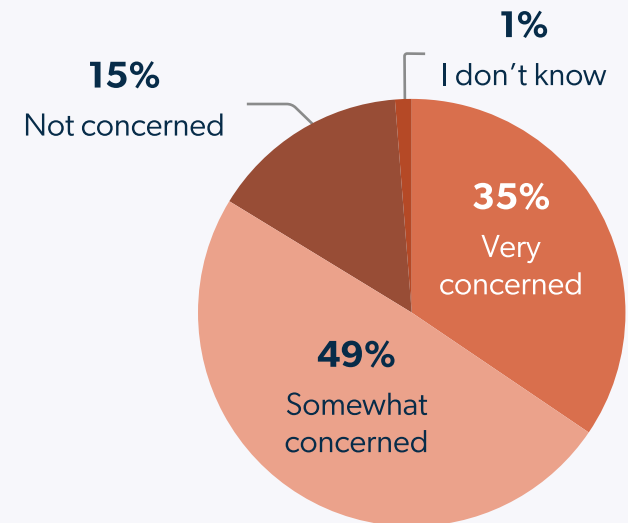
When we asked IT professionals about their biggest security concerns, there was no shortage of answers. The four most common answers were network attacks, software vulnerability exploits, ransomware, and shadow IT.

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



Shadow IT is on the majority of SME IT pros' minds: 84% are either somewhat or very concerned about shadow IT.

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





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?



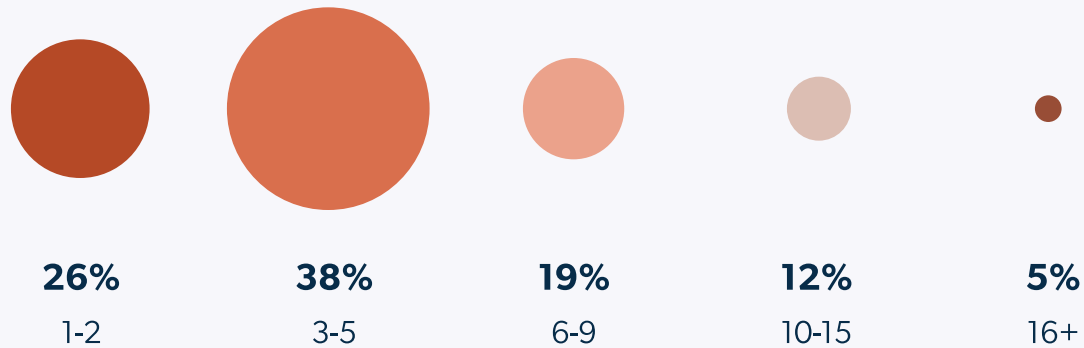
S

Decentralized IT Complicates Things

SME IT teams are working in decentralized environments, which makes shadow IT hard to control. And they're protecting those resources with passwords, which are widely recognized as vulnerable.

Barely one quarter of employees (26%) can access all of their IT resources with just one or two passwords. 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)



95%

of respondents use passwords to secure at least some IT resources, despite SMEs adopting tools like MFA, biometrics, and single sign-on (SSO).

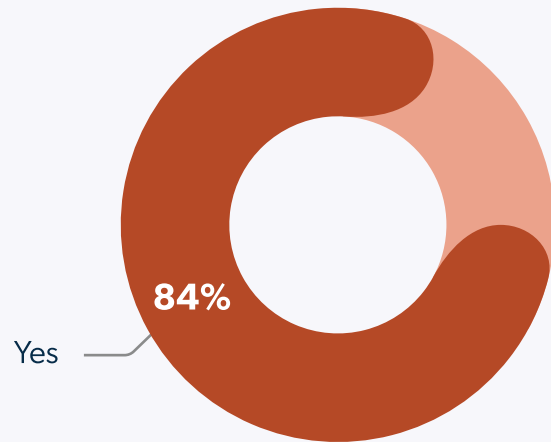


The Bright Side: SMEs Heed the Call

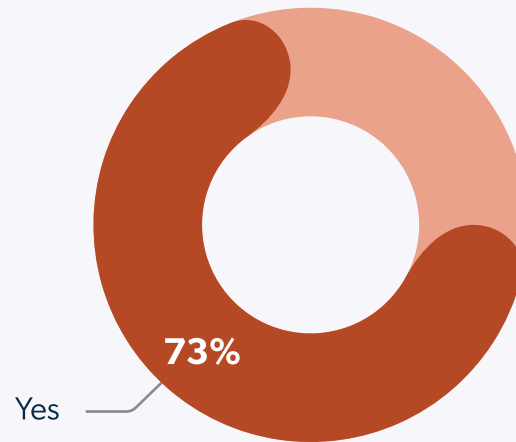


In the face of growing threats, there's a silver lining: SMEs seem to be taking them seriously. SMEs continue to invest in security and support their IT staff. Over eight in 10 SMEs (84%) have an IT security expert on staff, 73% say their organization is financially prepared to recover from a cyberattack, and 82% say that management respects their

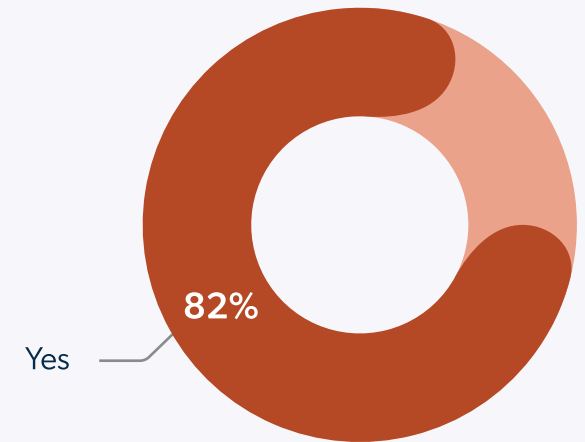
Do you have an IT security expert on staff?



My organization is financially prepared to recover from a cyberattack.



Management respects my counsel and recommendations around IT operations.





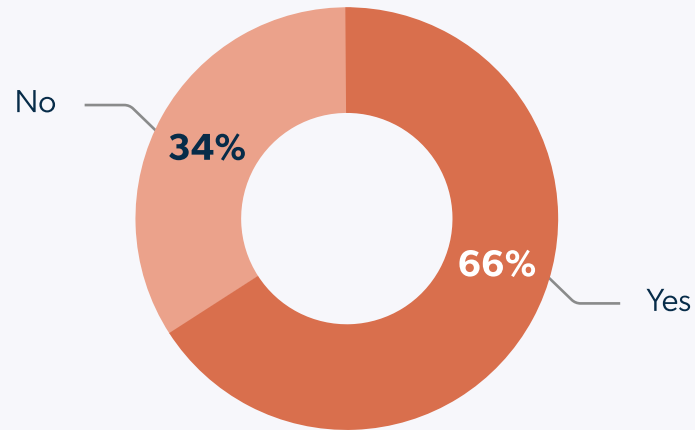
Biometrics May Balance Security



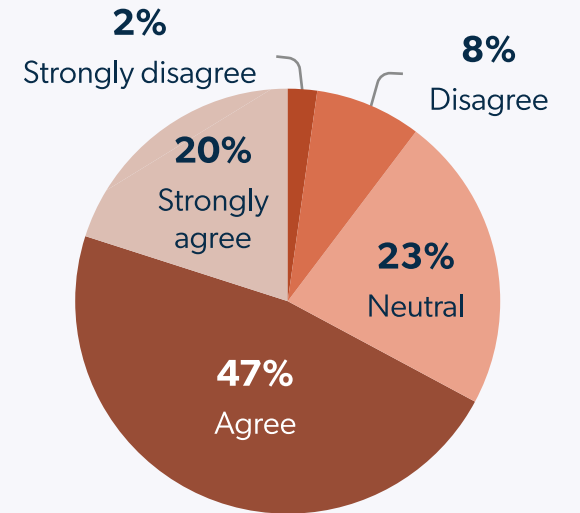
Despite the stubborn resilience of passwords, IT teams seem to be investing in more secure authentication measures. Chiefly, more than half of SMEs have adopted biometric authentication. Biometrics offer the dual benefit of added security without dragging on productivity.

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?



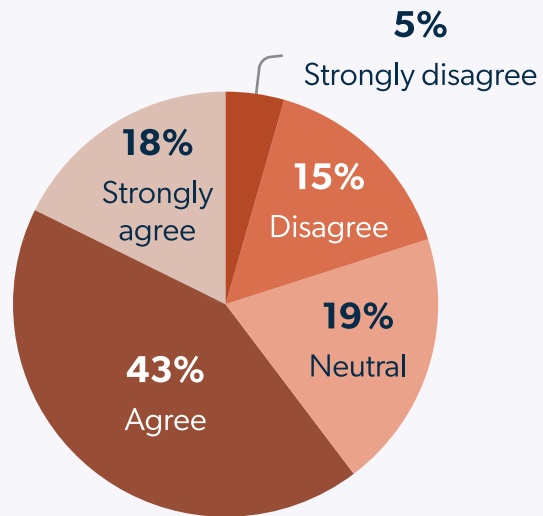
My organization's security posture would be stronger if they required biometrics.



Biometrics May Balance Security

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.



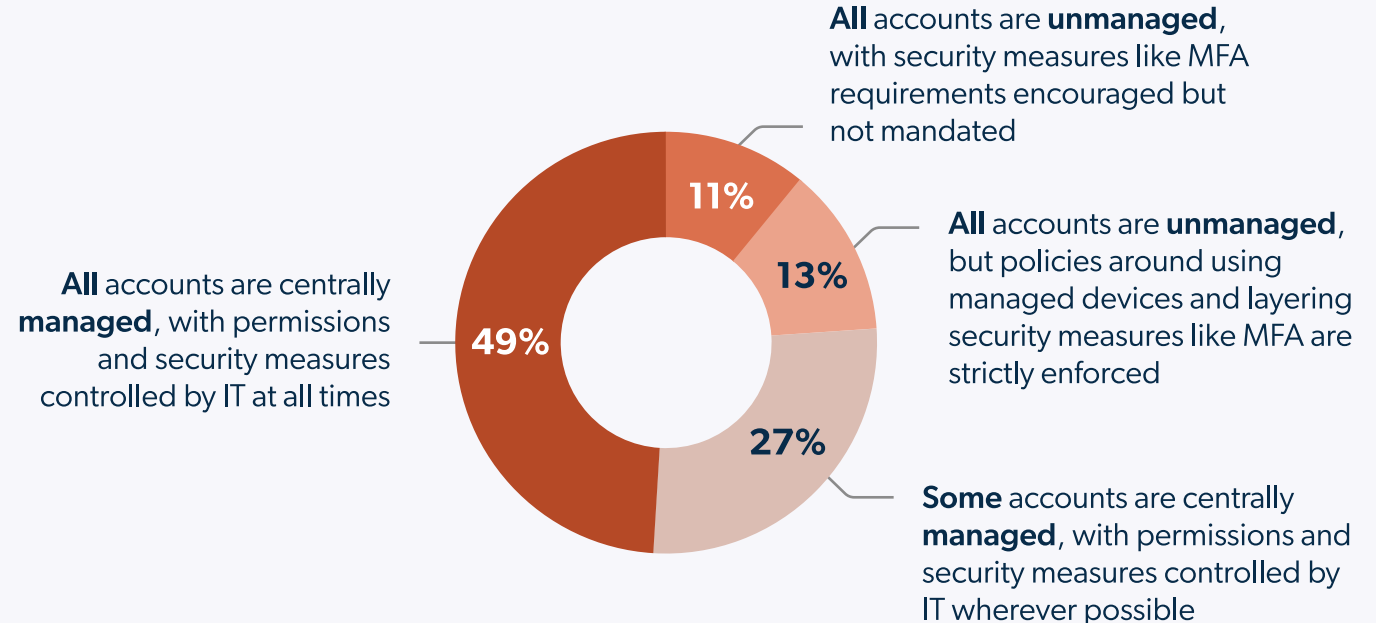
61%

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

SMEs Look to IT Personnel for Guidance

In addition to secure authentication practices, IT teams are leaning toward centralized IT management as a strong opportunity to secure their environments. 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?



Fortifying a Secure Future

There's no doubt that security is a challenge — and will likely remain so for SMEs. However, SMEs seem to be demonstrating intentions to continue investing in security and trusting their IT teams for guidance. That's good news.

But in order to guide your company to a secure future, it's important to understand the market and what other SMEs are doing to combat threats, respond to economic changes, and drive growth. JumpCloud's full SME IT Trends Report dives into all these topics and more. Download the free report, *Detours Ahead: How IT Navigates an Evolving World*.

[Download the Free Report](#)

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.



About JumpCloud®

JumpCloud® delivers a unified open directory 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 is IT Simplified.

About JumpCloud for MSPs™

JumpCloud for MSPs™ provides managed service providers (MSPs) an open directory platform for delivering modern IT services that are identity-centric, cloud-native, and vendor-agnostic. Using JumpCloud, MSPs can centralize identity, access, and device management capabilities under a single Multi-Tenant Portal. To learn more please visit jumpcloud.com/msp.

[Jumpcloud.com](https://jumpcloud.com) | [Blog](#) | [Community](#) | [Resources](#) |  | [in](#) | 

