jumpcloud™

Build The Ideal MSP:

Addressing Key Challenges and Opportunities

Introduction

In the past few years, managed service providers (MSPs) have struck gold handling IT for small-to-medium sized enterprises (SMEs). Initially a convenient cost-reducing option, they have come a long way helping organizations navigate a rapidly evolving tech environment. But one can only strive toward perfection; MSPs still have a lot to work on when it comes to addressing major concerns, especially around AI and security.

So what does it take to become (and most importantly stay) number one? Collating data from JumpCloud's previous SME IT Trends reports that surveyed thousands IT professionals working at SMEs, there are many critical factors that contribute to building a successful and thriving MSP business.

These stats also focus on areas where MSPs have seen a downfall, raising several crucial questions such as:

- How can MSPs enhance security measures for their clients?
- How can MSPs help organizations become compliant to the required industry standards?
- How can MSPs be more AI-oriented?

Whether you are an established player looking to scale, or simply want to enhance your current service offerings, this 2025 MSP special edition eBook provides valuable insights and actionable advice to help you build an ideal MSP and explore the challenges and opportunities that lie ahead.

Key Findings

MSPs have taken center stage

Be it through cost savings or increased productivity, MSPs have become strategic lifelines for many organizations, helping them navigate a complex IT environment with ease.

From sidekicks to superheroes

MSPs deliver value in many ways: they deliver increased IT effectiveness, a better user experience, strong customer support, and more.

Great powers, greater responsibility

Despite numerous benefits, nearly half of the organizations worry about MSPs' ability to manage security effectively.

Compliance: Your MSP's USP?

More than a quarter of organizations struggle with completing a compliance audit successfully, providing MSPs an opportunity to lend a helping hand.

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 9 in 10 (93%) of organizations surveyed use or are considering using an MSP. 35% use an MSP to completely manage their IT program, up from 29% who said the same 6 months ago (**Chart 1**).

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

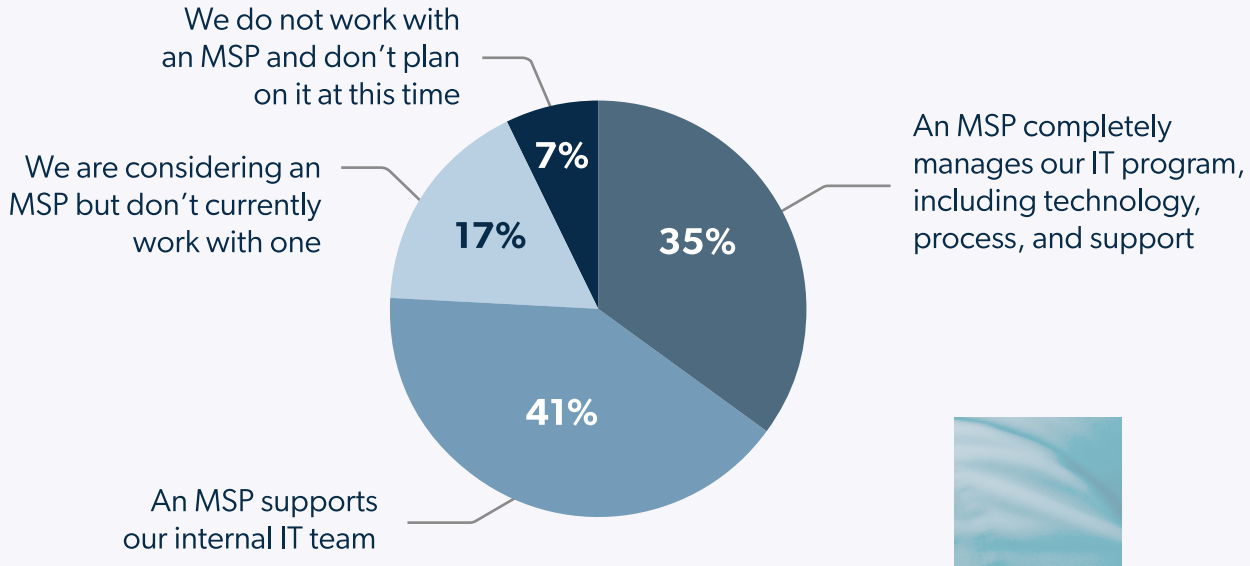


Chart 1

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 2**).

We use MSPs because:

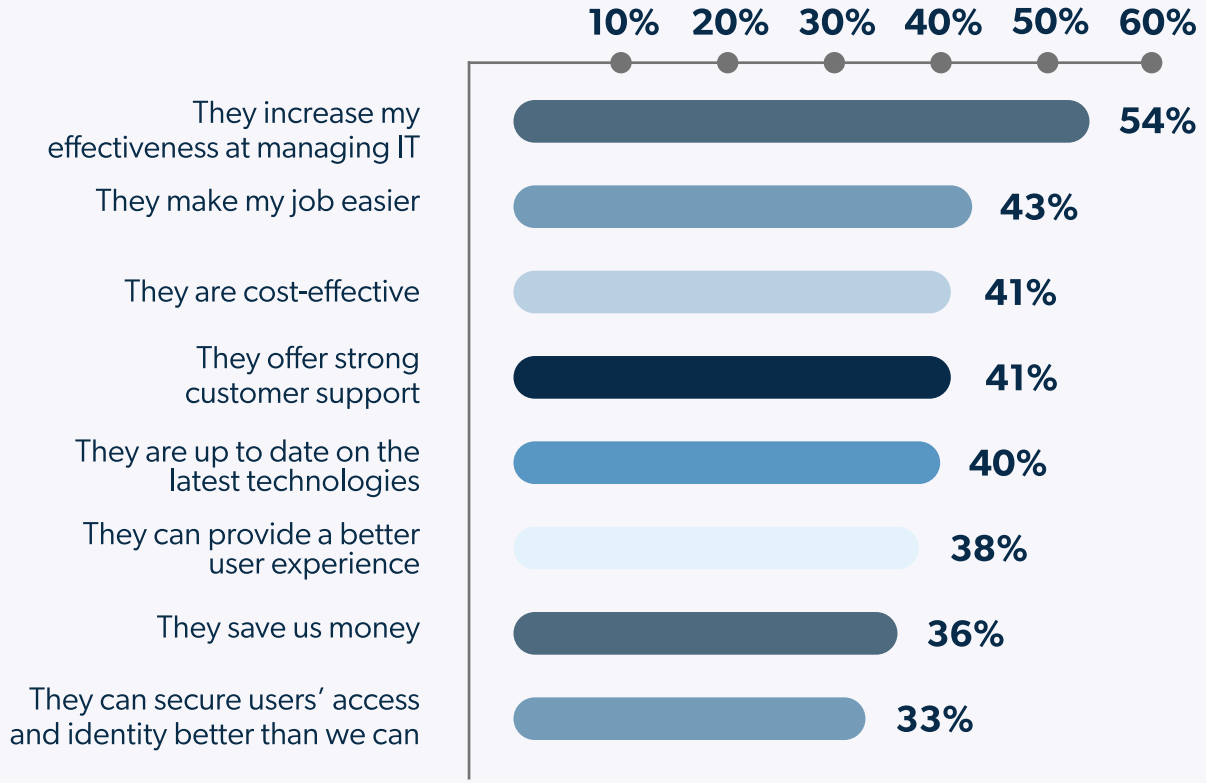


Chart 2

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 3**).

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

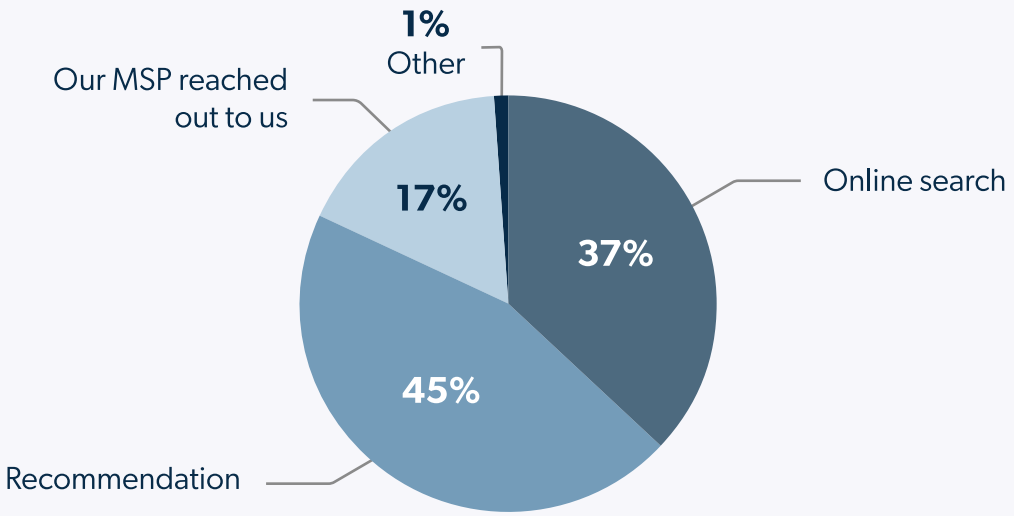


Chart 3

So What's The Holdup With MSPs Saving The Day?

When it comes to security, SMEs have raised concerns about MSPs handling it time and again, with the percentage significantly going up to 44% from 39% six months ago. 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 4**).

Are you concerned about shadow IT?

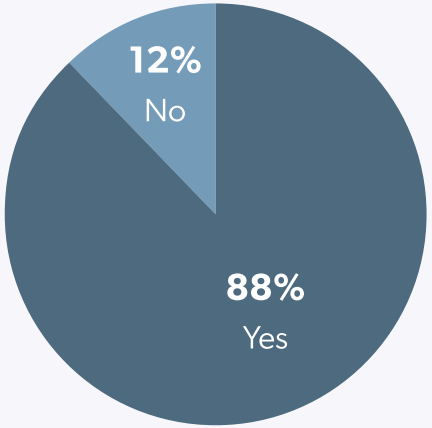


Chart 4

44%

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

MSP Security Check: A Look Into The Past

While MSPs have made progress on many fronts in the IT industry till date, their security scenario still remains quite vulnerable. In 2023, 46.2% of SMEs had concerns about how MSPs manage security, rising to 50% almost immediately in the first quarter of 2024. Even though the percentage fell drastically (39%) in Q3 2024, 44% SMEs have once again raised their guards as they doubt the MSPs capability of protecting their organizations against a horde of new cyberthreats, especially shadow IT (**Chart 5**).

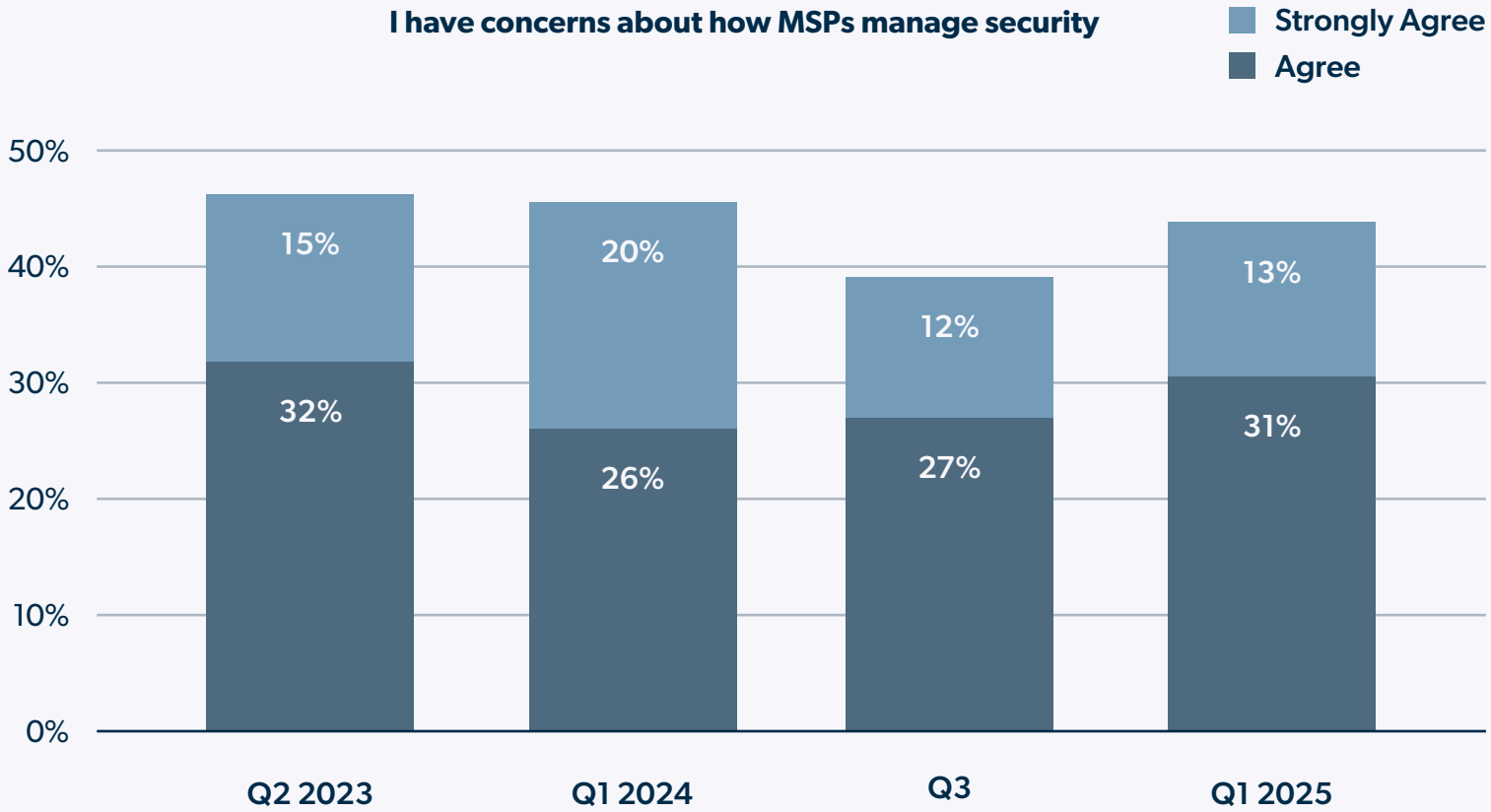


Chart 5

Reasons Why SMEs Don't Want MSPs To Handle Security

One of the primary reasons SMEs are forgoing help from MSPs in the security department is their inability to stay updated with the latest technologies. Another reason is that 38% of SMEs think their security measures are interfering with the overall user experience, while 35% state high cost as a reason (**Chart 6**).

Some other reasons SMEs cite for not hiring MSPs to handle security is the number of service offerings made by the latter (17%), being too small an organization to be a proper client (13%), incompatibility of the security services with their current devices, productivity suite, or IT systems (21%), or having a bad MSP experience (17%).

We don't use MSPs because:

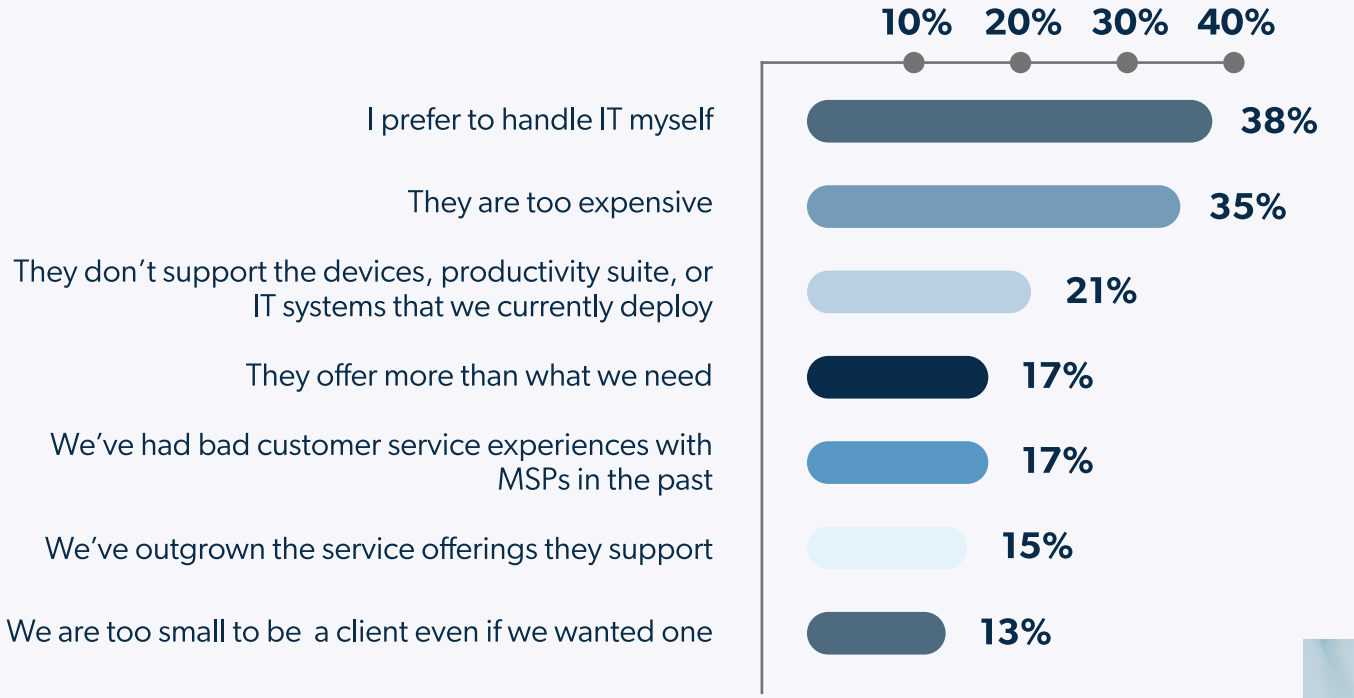


Chart 6

From Sidekick to Superhero

Opportunity #1

~~Double~~ Triple Down on Security

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%).

However, while concerns around their MSPs' ability to handle security are still high, admins report that the top areas for IT spending are cybersecurity tools and services (48%) and IT service providers or MSPs (37%).

What can you do?

Security is arguably the most important area that you can lean into to deepen your relationships with and service offerings for your clients. You'll have to work hard to showcase your willingness, strategic vision, and technical mastery of security processes. This may include:

- Highlighting potential vulnerabilities, recommend solutions, and prioritize remediation efforts in an ongoing or periodic (monthly/quarterly) fashion.
- Utilizing threat intelligence feeds to proactively identify and mitigate emerging threats.
- Conducting regular, in-depth security assessments and providing clients with clear, easy-to-understand reports.
- Automating routine security tasks like patching, vulnerability scanning, to improve efficiency and reduce the risk of human error.
- Establishing clear communication channels such as regular meetings, newsletters, online portals to keep clients informed about security updates, incident response plans, and the overall security posture.

You could look at these options as ways to enhance your offerings or develop new ones:

- Offer flexible and scalable security packages to cater to different budgets and needs of SMEs.
- Clearly demonstrate the return on investment (ROI) of security services by quantifying the value of reduced risk, improved productivity, and avoided downtime.
- Include value-added services such as security awareness training, phishing simulations, and incident response planning in service packages.

From Sidekick to Superhero

Opportunity #1

~~Double~~ Triple Down on Security

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.

What can you do?

Your clients may be wary of adding unnecessary friction to the user experience, as admins report the biggest roadblock to implementing stronger security controls is the perception that additional security measures usually mean a poorer user experience (46%). Combat these perceptions by:

- Assigning a dedicated security specialist to each client or a small group of clients to build strong relationships and foster trust.
- Offering specialized training for SMEs on cybersecurity awareness and best practices.
- Ensuring your technicians have advanced certifications (e.g. CISSP, CISA, Security+) and ongoing training on the latest threats, vulnerabilities, and best practices.
- Prioritizing user experience when implementing security measures.
- Enhancing training efforts around new security protocols to help your clients internalize new motions.
- Minimizing disruptions to end-users while maintaining a strong security posture.
- Regularly gathering client feedback through surveys and feedback mechanisms to identify areas for improvement.

From Sidekick to Superhero

Opportunity #2

Shadow IT: Fighting The Boogeyman of The Virtual World

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.

What can you do?

This is a relatively new area for all organizations, so the path is wide open to explore offerings and additions to your program that hit on SaaS management as a whole. You could consider:

- Implementing proactive discovery tools and techniques to identify all devices, applications, and software used within the SME, including cloud services, mobile devices, and IoT devices.
- Conducting regular surveys to understand employee needs and the applications they are using. When asked what the most common reasons IT thinks employees use shadow IT, they reported:
  - To make their jobs easier (54%)
  - To be more productive (51%)
  - To test out new technology (45%)
  - To gain functionality that authorized tools don't offer (43%)
  - Because the procurement process for new apps takes too long (36%)
  - Existing processes for adding authorized applications are onerous (32%)
- Implementing a robust SaaS management platform to gain visibility into all cloud subscriptions, monitor usage, and control access.
- Conducting regular security awareness training for employees to educate them about the risks of shadow IT and the importance of using approved applications.
- Establishing and communicating clear IT policies that outline acceptable use of technology, including guidelines for using cloud services and personal devices for work purposes.
- Making it easy for employees to request and access IT resources through self-service portals and automated workflows, reducing the need for employees to seek workarounds outside of approved channels.
- Offering regular consultations with SMEs to review their security posture and identify potential shadow IT risks.

From Sidekick to Superhero

Opportunity #3
Compliance: A Window of Opportunity

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.

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 can you do?

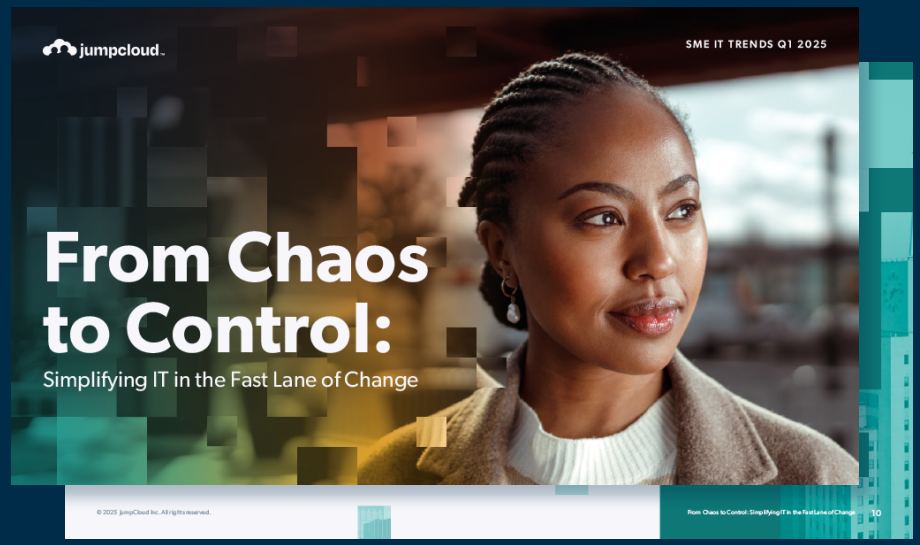
This opportunity will be more specialized than the others, and highly dependent upon your clientele and their specific needs. If you haven't already it's recommended you take some time to learn about where your clients are (and may want to go) and how compliance measures may facilitate (or hinder) that progression.

- Offer your clients specialized Compliance-as-a-Service packages tailored to specific industry standards and client needs. This includes proactive compliance monitoring through regular risk assessments, continuous monitoring, and audits.
- To optimize costs, you can provide Software Asset Management (SAM) services, assist with cloud cost optimization, and manage software subscriptions.
- MSPs can contribute to compliance by providing employee training, conducting awareness programs, and leveraging technology solutions like SIEM, EDR, and CASB.
- Building strong client relationships through regular communication, proactive support, and demonstrating value is crucial for successful compliance partnerships.

Final Thoughts

The more you understand about your audience, the better you can tailor your services to optimize their experience and increase your revenue. This data represents just one section of JumpCloud's 2024 SME IT Trends report. In the full survey, we asked IT professionals about their takes on other pressing issues, including security, AI, how their companies are investing in IT, and more.

To learn more about what SME IT professionals see for their careers, their organizations, and the future of the industry, download the full free report.



Download the full survey findings from JumpCloud's twice annual SME IT Trends report

Download Report

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 | | | |