jumpcloud™

IT Trends Q3 2025

Why a Unified Platform Is the Only Path to Controlling Complexity

Modern IT Is a Minefield.
Here’s How IT Professionals Are Navigating It.

Any IT professional knows that IT management and complexity tend to go hand in hand. You fight everyday to keep it under control, in search of any opportunity to streamline your day before the next wave of change emerges.

The findings from this report will show you that this current wave of change has crashed onto us like a tsunami: rapid advancements in AI, increasingly mobile environments, and a near explosion of SaaS solutions have made your world more diverse than ever.

The diversity is challenging enough without macroeconomic and geopolitical uncertainties strengthening these headwinds. The reaction to uncertainty usually calls for careful spending, while you have expressed a strong preference for resource optimization, automation, and unification to combat these near-term concerns.

AI and security stand out as primary challenges. The number of organizations adopting AI has skyrocketed to nearly 100%. Its rapid rise calls for important conversations to be had: How do we use it responsibly? How do we defend ourselves against its malicious potential?

There aren’t many clear answers yet, but that is not stopping you from seeking them out.

Tackling these complexities will be nearly impossible without strategic partnerships. Collaboration with other departments, security leaders, and Managed Service Providers (MSPs) is crucial for building robust security programs and ensuring overall IT success.

And while AI is what makes all the headlines, it isn’t the only thing that needs your attention.

Your users have an insatiable need for new operating systems and SaaS tools. The data shows that a "monolithic" approach to tooling stifles user productivity and hinders IT teams' ability to manage effectively. The right IT foundation — one that’s unified, automated, and user-friendly — is key to everyone’s success.

In this edition of JumpCloud’s biannual IT Trends Report, IT professionals shared that amidst this uncertainty, they're finding paths to simplify. Resource optimization, automation, tool consolidation, and strategic partnerships are the key strategies they are using to control these complexities.

Table of Contents

Methodology

JumpCloud surveyed 828 IT leaders in the U.S. and U.K. at a 50/50 split. Respondents were IT administrators, IT team leads, IT managers, IT/technology directors, IT/technology vice presidents, chief information officers, and chief technology officers.

Each survey respondent represented an organization with 200-2,500 employees across a variety of industries. The online survey was conducted by Redpoint from May 9, 2025 to June 4, 2025.

IT Architecture

Key Takeaways

IT professionals agree that managing core infrastructure with too many tools leads to complicated systems, inefficiencies, and security vulnerabilities.

And yet, most architectures remain sprawled. It’s a frustrating contradiction.

However, IT professionals state they see the path to reducing sprawl: **IT unification**. Unifying your environment brings your resources under one roof. This simplifies the experience of IT management, optimizing costs, and reducing security gaps along the way.

Another clear trend we see is the move away from single, "monolithic" IT systems. IT professionals are actively seeking alternatives for these more traditional software and device management platforms. The aim is to modernize, gain agility, and improve automation.

While these initiatives may seem at odds with each other, they actually go hand-in-hand when executed strategically. IT unification brings oversight and centralized control so you can offer your organization the heterogeneous environment they need to make work happen *without* scattering them amongst different tools that don’t work well together.

Most IT environments are sprawled.

It takes IT teams an average of 9.3 tools to manage core functions.

IT unification leads the way.

IT teams with fully unified IT play a more significant role in organizational planning and strategy.

The unification journey is ongoing.

Most organizations have started unifying, but only 19% have achieved full IT unification.

Modern IT demands flexible, diverse solutions.

Only 2% of organizations haven’t explored an alternative to Microsoft 365.

Variety Is the Spice of IT Life

IT environments today are diverse. From software to operating system (OS), companies rarely operate with a one-size-fits-all solution.

The average company has about three (2.9) OSes in their ecosystem, and more than half of organizations support mobile devices, with iOS coming in first at 54% and Android hot on its heels at 50% **(Chart 1)**. Organizations with unified IT architecture are more likely to support mobile devices than those with disconnected architectures.

What's more, almost two-thirds (64%) of organizations are using both Microsoft and Google Workspace.

It seems the majority of IT professionals value diversity over homogeneity in their architecture. In today's environment, where SaaS solutions and mobile work reign supreme, a monolithic environment can limit growth opportunities and adaptability.

Committing to a monolith, whether for devices or software, puts you in the minority.

My organization supports:

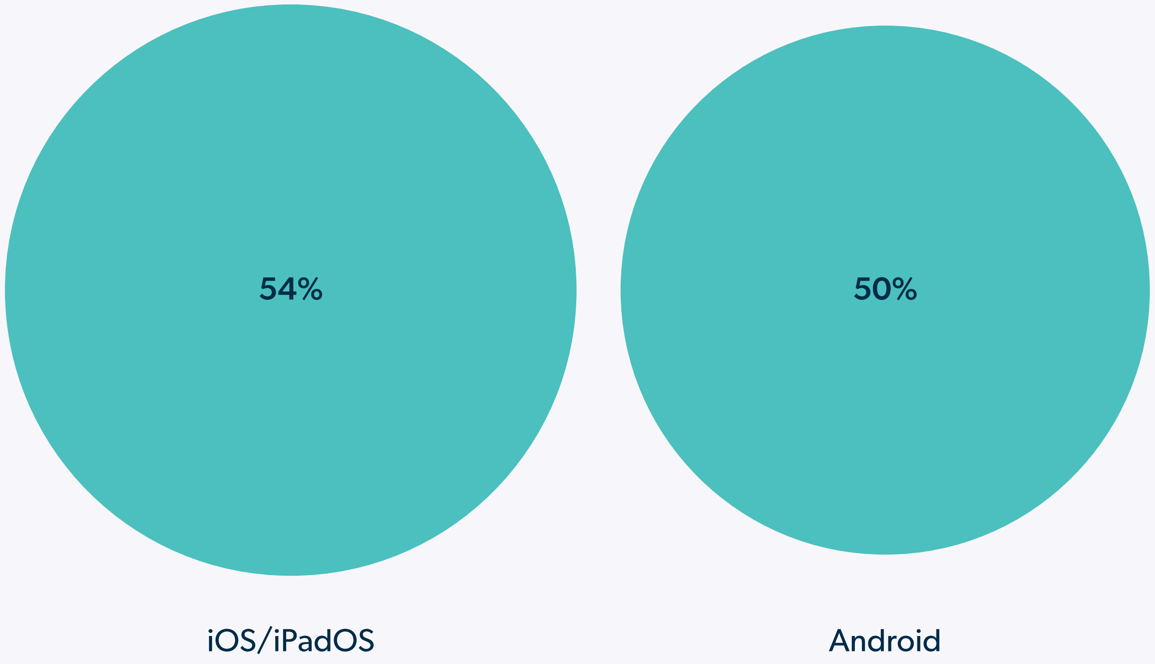

Chart 1

The Benefits of Branching Out

Traditional approaches continue to fade as more viable options emerge that drive value. The challenges associated with ecosystems like Microsoft's have spurred many organizations to explore alternatives. Of the 67% of respondents who stated they use Microsoft 365 as their productivity platform, nearly two thirds of them indicated that they support Google Workspace as well.

These alternatives deliver significant benefits. IT professionals said the top three benefits they associate with using an alternative to Microsoft 365 were improved end-user experience (64%), increased agility (57%), and easier automation (52%) **(Chart 2)**.

Microsoft 365 presents many challenges, and the majority of organizations see benefits to supporting alternatives.

What benefits do you associate with supporting alternative platforms like Google Workspace or open cloud-native solutions?

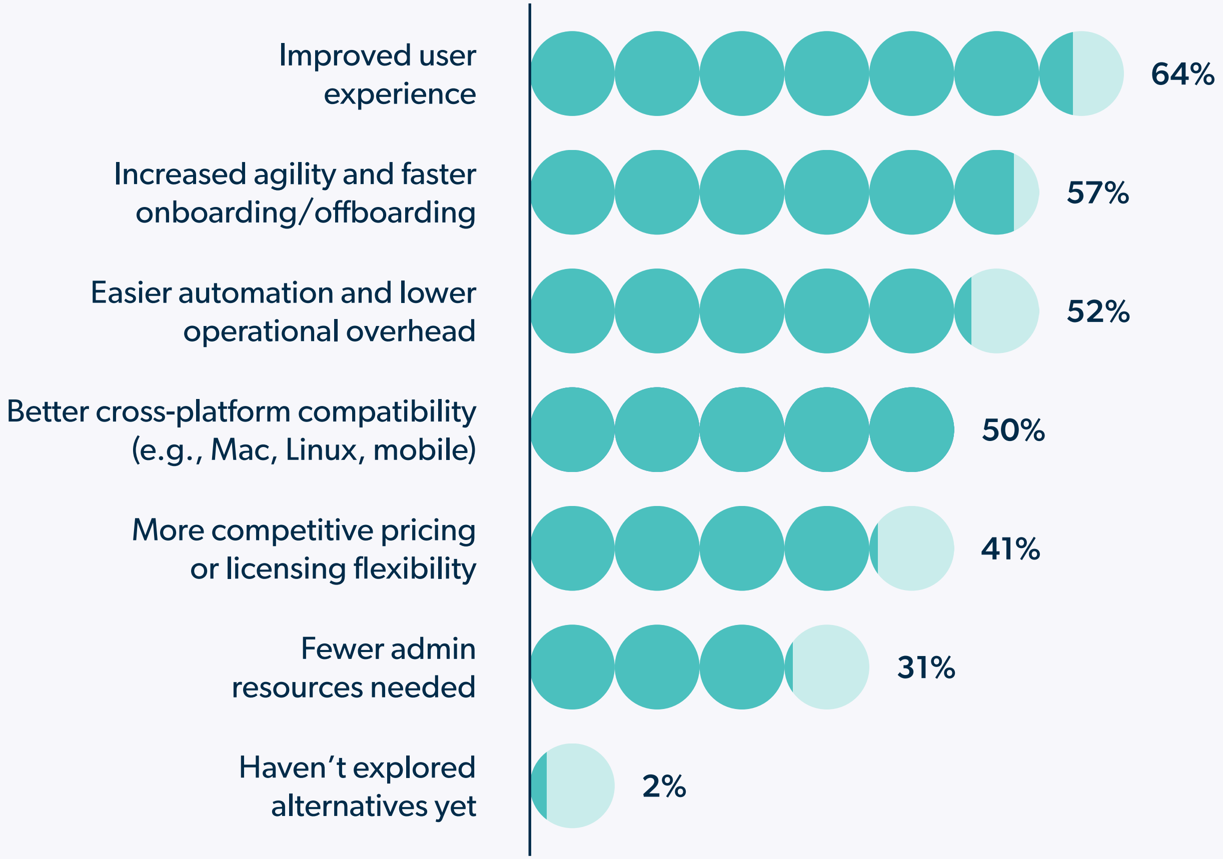

Chart 2

Moving Beyond Microsoft

Only 2% of IT professionals have not explored alternatives to Microsoft. While Microsoft used to be the business standard, organizations cite many challenges with Microsoft 365. That says a lot about the willingness and ability for IT professionals to seek change when faced with ongoing issues despite their long term investments.

Organizations' top three challenges with Microsoft 365 were high overhead (45%), security configuration complexity (44%), and complex licensing and pricing (40%) **(Chart 3)**.

Top Challenges with Microsoft 365

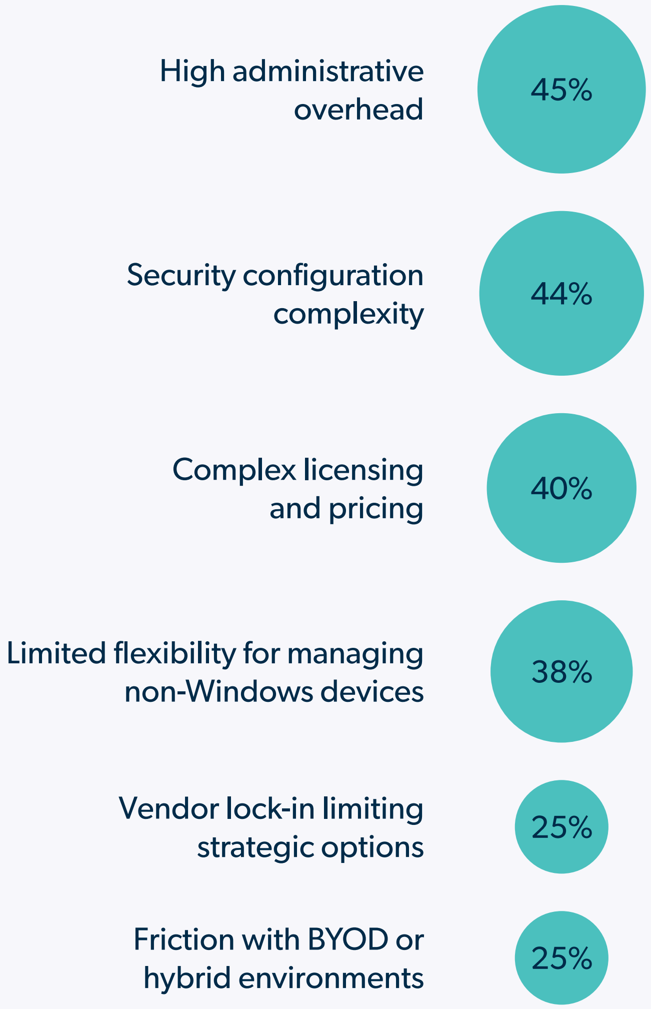

Chart 3

Modernizing Active Directory

Microsoft 365 presents many challenges, and the data shows that the majority of organizations see benefits to supporting alternatives.

Microsoft Active Directory is another common monolith in many environments, and it presents many of the same challenges.

This guide explores the possibilities of moving beyond Microsoft Active Directory, either by augmenting AD or replacing it. Download the guide to explore your options and start charting your path beyond AD.

Get the guide

Tool Sprawl Is a Challenge

While diverse environments are beneficial (and necessary) for many organizations, they are prone to sprawl without intentional management. And sprawl tends to add complexity: 74% of IT professionals said managing all their IT tools and platforms is complex.

The average organization uses 9.3 tools to manage core functions, and only 5% of companies use fewer than four tools to manage core functions **(Chart 4)**.

It takes many tools for organizations to manage IT, which can create complexity.

How many tools does your IT team use to manage core functions?

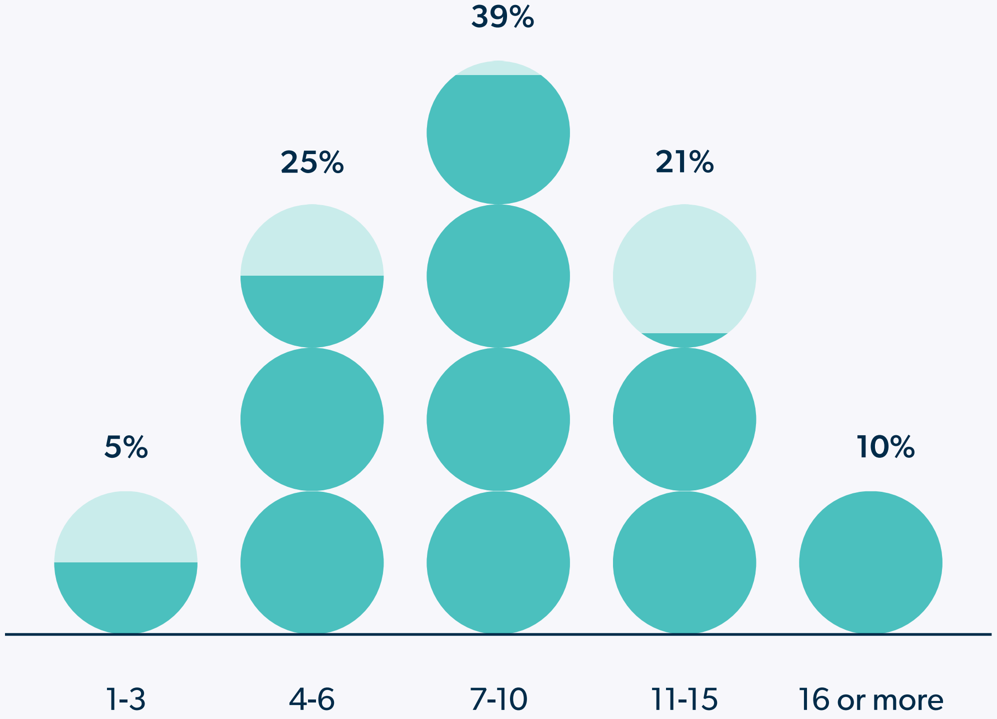

Chart 4

9.3

The average number of tools to manage core functions is 9.3

What Makes Tool Sprawl So Problematic?

IT complexity increases with sprawl. IT professionals with more fragmented environments found IT management to be more complex, and vice versa: companies with unified platforms found IT management less complex.

The number one challenge associated with tool sprawl is security gaps (56%), followed by cost inefficiencies (44%), compliance risk (44%), time-consuming administrative tasks (41%), and lack of visibility across systems (41%) **(Chart 5)**.

Security gaps are by far the biggest challenge associated with tool sprawl.

What are the biggest challenges of managing a fragmented IT environment?

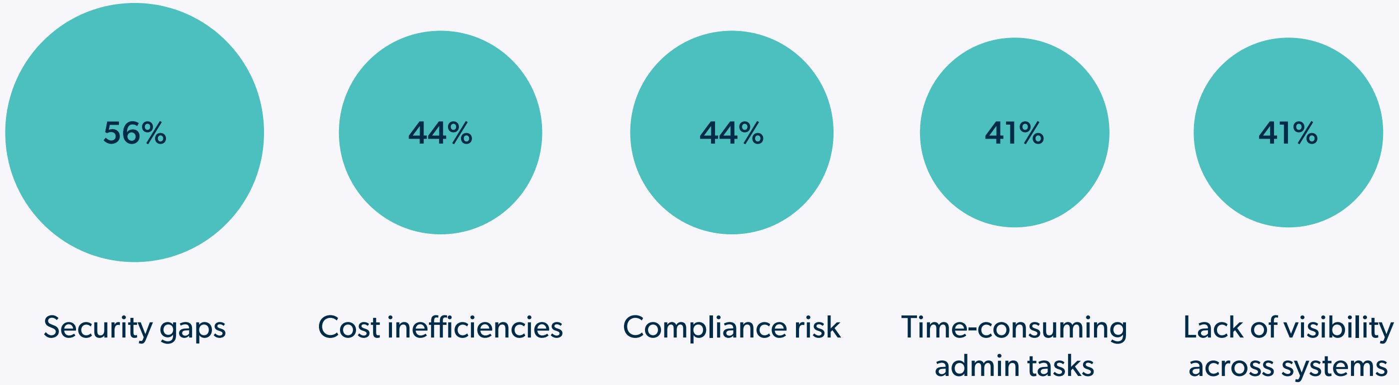

Chart 5

Combatting Tool Sprawl with IT Consolidation

IT consolidation combats sprawl by unifying and simplifying IT management. It earned the #3 spot on organization's list of top priorities this year, and simplifying complex environments was listed as a top missed opportunity for organizations (Chart 25).

IT professionals said the top three benefits of IT consolidation were an improved user experience (55%), increased job satisfaction among IT staff (54%), and a better focus on strategic work (51%) (Chart 6).

In addition, the survey data shows that organizations with unified environments are more likely to support mobile devices, more likely to be actively implementing AI, and more likely to support Google Workspace and hybrid productivity platforms.

Consolidating your IT infrastructure helps combat tool sprawl while improving IT management.

How has IT tool unification impacted your team's productivity or performance?

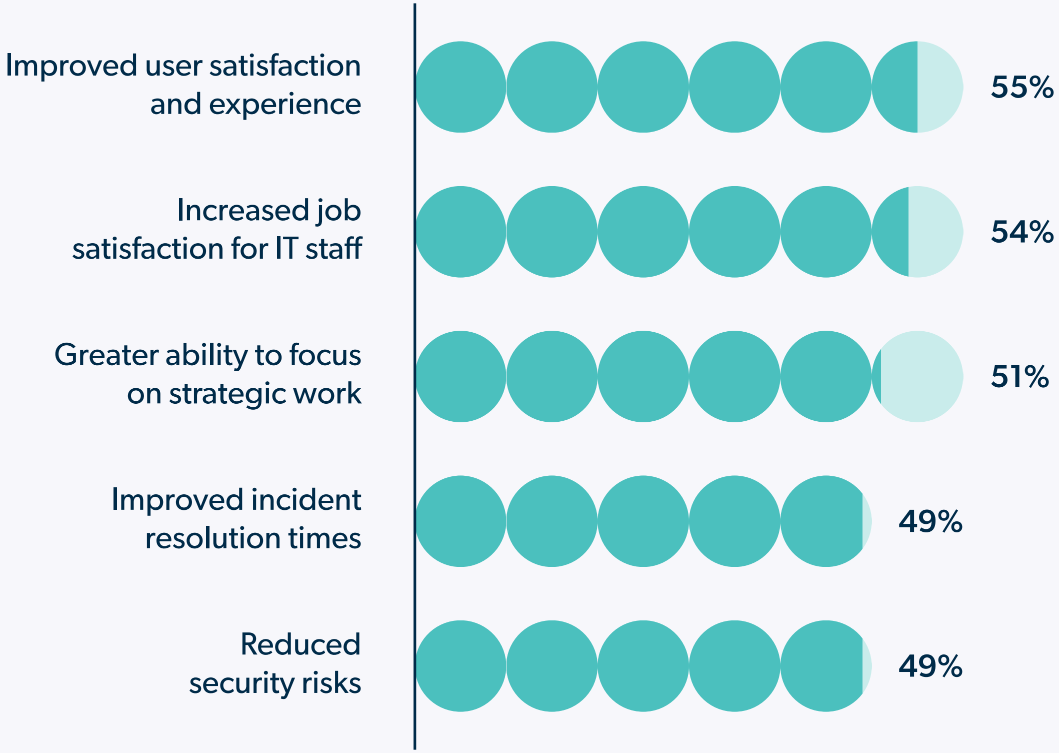

Chart 6

Securing a Seat at the Table

IT consolidation also correlates with IT playing a stronger strategic role in the organization. IT professionals with unified architecture reported better alignment between technology and business goals, improved strategic reporting abilities, higher participation in company planning, and more time for strategic initiatives, compared with the average responses **(Chart 7)**.

This trend may be due to unified architecture offering organizations a more powerful foundation upon which they can make connections and collaborate cross-functionally.

> **"There are various platforms out there that support one or maybe two [operating systems], but finding one that can support all three was huge."**
>
> Read the Case Study →

How has unifying IT tools changed the strategic role of your IT team?

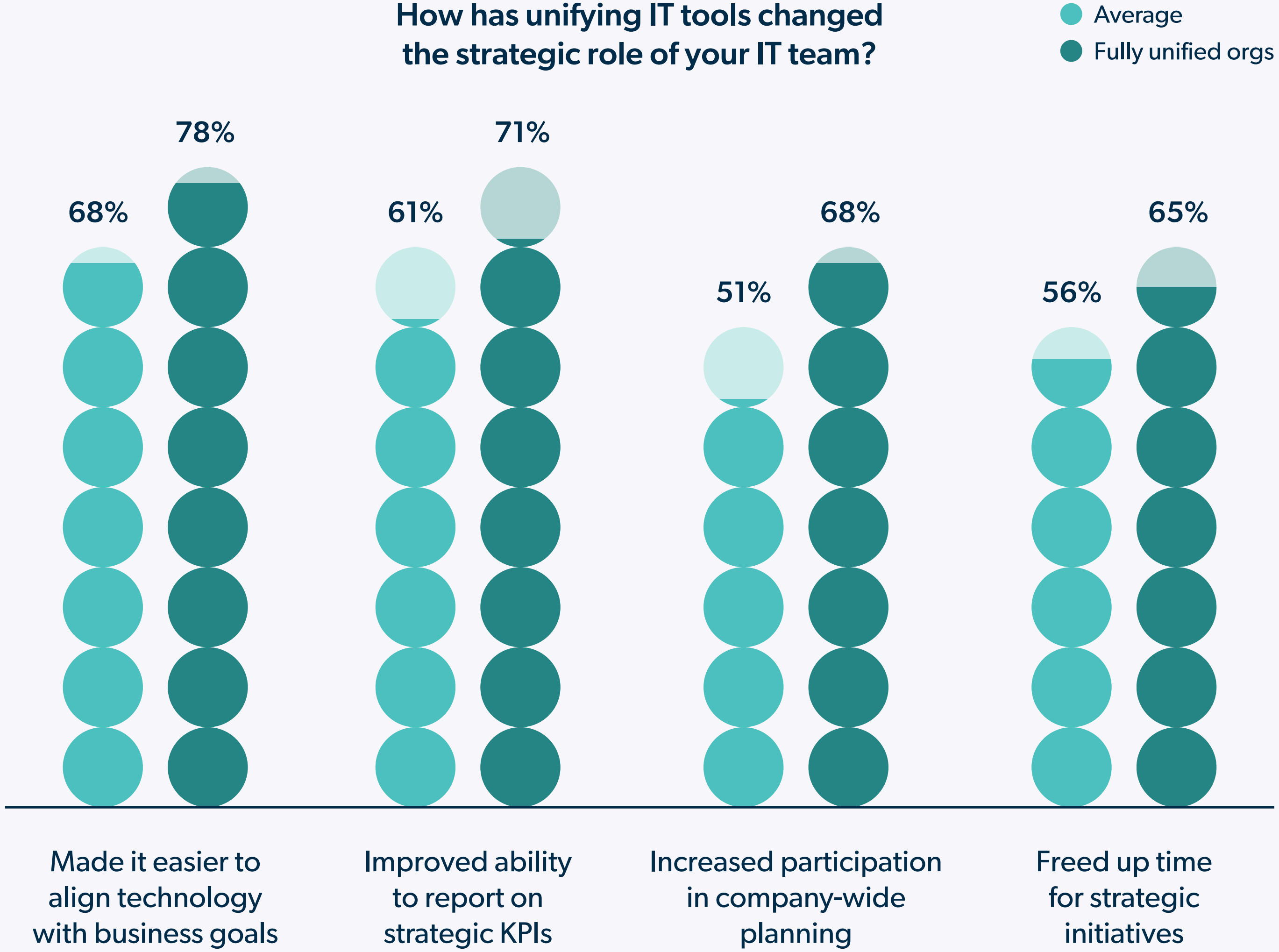

Chart 7

And Yet… Most Organizations Aren’t Unified

IT professionals said simplifying complex environments was one of their top missed opportunities (Chart 25).

Despite many IT professionals wanting to unify their IT environments, most organizations don’t yet have a fully unified architecture. Only 19% of organizations have achieved full IT unification, and 10% are not unified at all. The majority (71%) sit somewhere in the middle, having consolidated some or most of their tools (Chart 8).

Most IT professionals have started their IT consolidation journey, but haven’t fully unified yet.

How would you describe your organization's current level of IT tool unification?

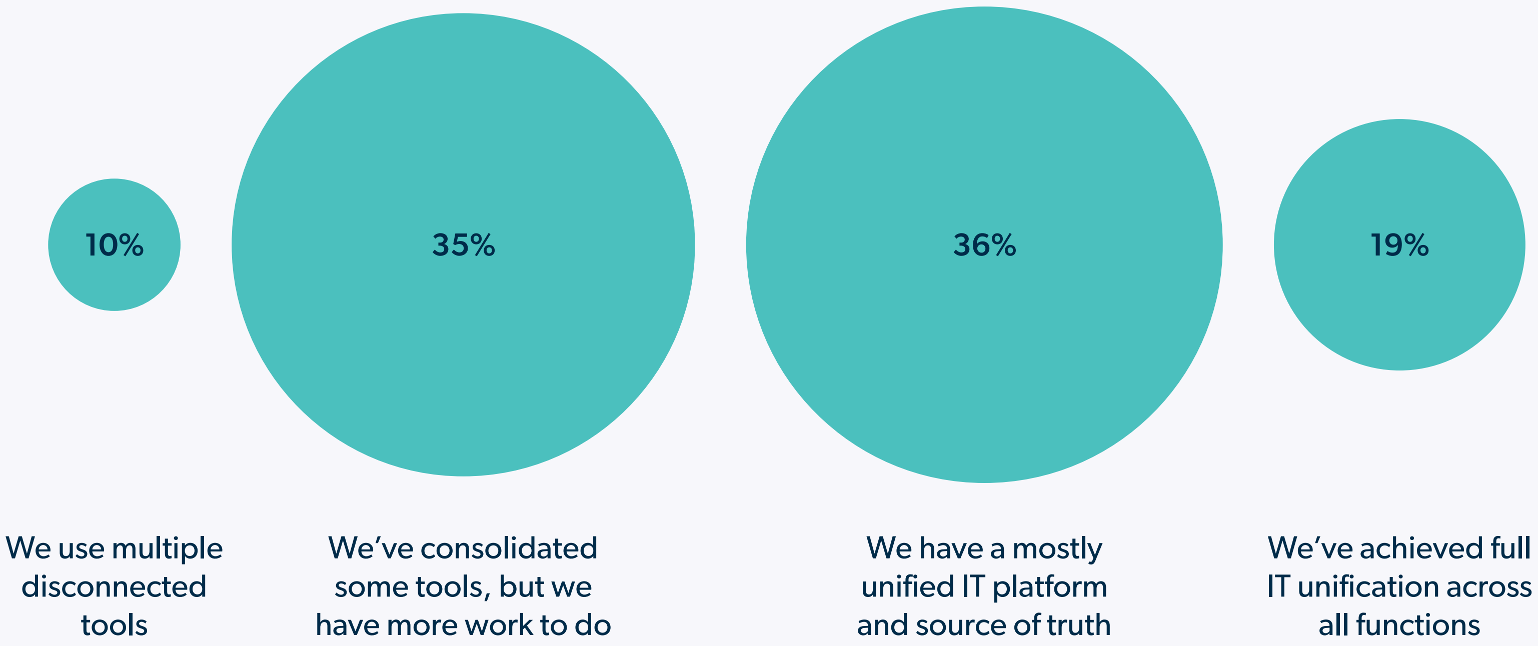

Chart 8

Security

Key Takeaways

IT professionals' key security concerns illustrate an environment where identity is the main threat vector. The best way to protect such environments is with Zero Trust security.

While most organizations have abandoned the more outdated, perimeter-based security model and begun pursuing Zero Trust, most have not yet achieved full Zero Trust implementation. Once again, a gap appears between the reigning problem of today and the ability to address it effectively.

However, the high prevalence of hybrid approaches (which incorporate identity, device, and perimeter-centric tactics) show that the right kind of progress is happening in the ongoing evolution of security best practices.

Change like this is slow and requires more than just new technology and processes. Stakeholder buy-in is essential, from the granters of budget to the recipients of these new security controls. So it's a positive sign that the end-user experience is a major consideration in most security strategies. This aligns with the shift toward identity-centric security, the core pillar of Zero Trust. Single sign-on (SSO) and passwordless authentication are key factors in striking this balance.

Feeling stuck in your Zero Trust journey?

Learn why Zero Trust initiatives often get side-tracked and how to overcome common challenges in the eBook, Where Zero Trust Falls Short.

Top security concerns call for Zero Trust.

AI-driven threats, identity-based attacks, and device security are the top 3 concerns.

Zero Trust adoption is progressing, but not fully realized.

Only 11% of organizations state they have achieved full Zero Trust.

UX cannot be ignored.

Nearly two-thirds (61%) of organizations prioritize the user experience in their security programs.

Today's Top Threats

There's no doubt that AI adoption is surging. But with AI's rise in popularity comes a darker side: new threats and concerns. **This year, AI is IT professionals' number one security concern.**

Identity-based attacks and device security came in second and third place on IT professionals' list of top concerns, underscoring the need for a modern, Zero Trust approach to security. These concerns were followed by ransomware (29%), compliance violations (29%), shadow IT (24%), and insider threats (23%) **(Chart 9)**.

IT professionals' top three security concerns are AI-driven threats, identity-based attacks, and device security.

What have your top security concerns been in 2025?

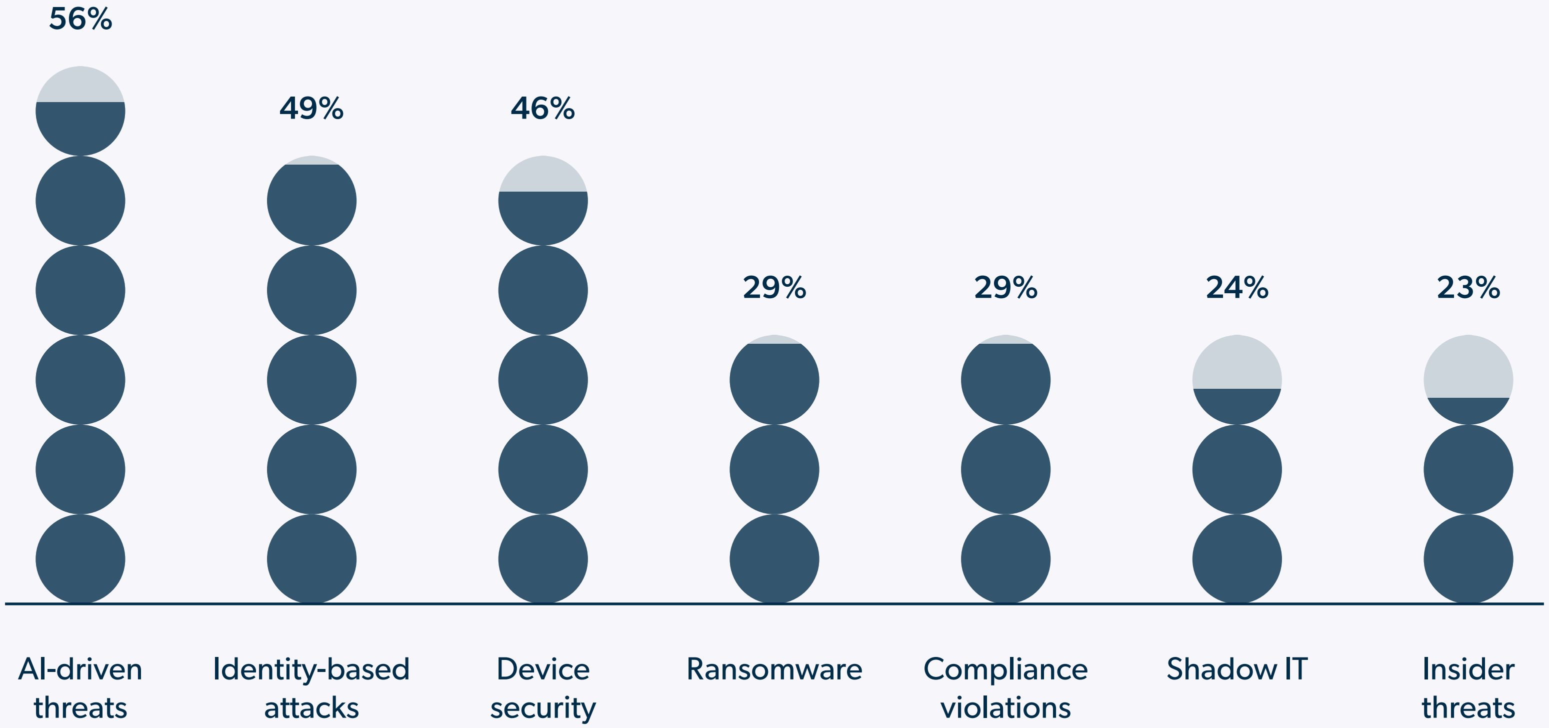

Chart 9

How Are Organizations Securing Their Environments?

While identity-based and device-based attacks are among IT professionals' top security concerns, only 11% have achieved full Zero Trust, with another 22% using identity-centric authentication and access control as their security foundation.

As far as approach type, a focused approach was more popular than a hybrid one: 48% said they use either an identity-centric, perimeter-based, or device-centric model, while 40% said they use a mix of both.

While Zero Trust adoption rates may be less than optimal, there's a bright side: only 15% of organizations are using a perimeter-based model. This model is largely outdated and not well-suited to modern, dynamic, and mobile environments **(Chart 10)**.

While many companies are on their way to achieving Zero Trust, not many have fully achieved it yet.

What have your top security concerns been in 2025?

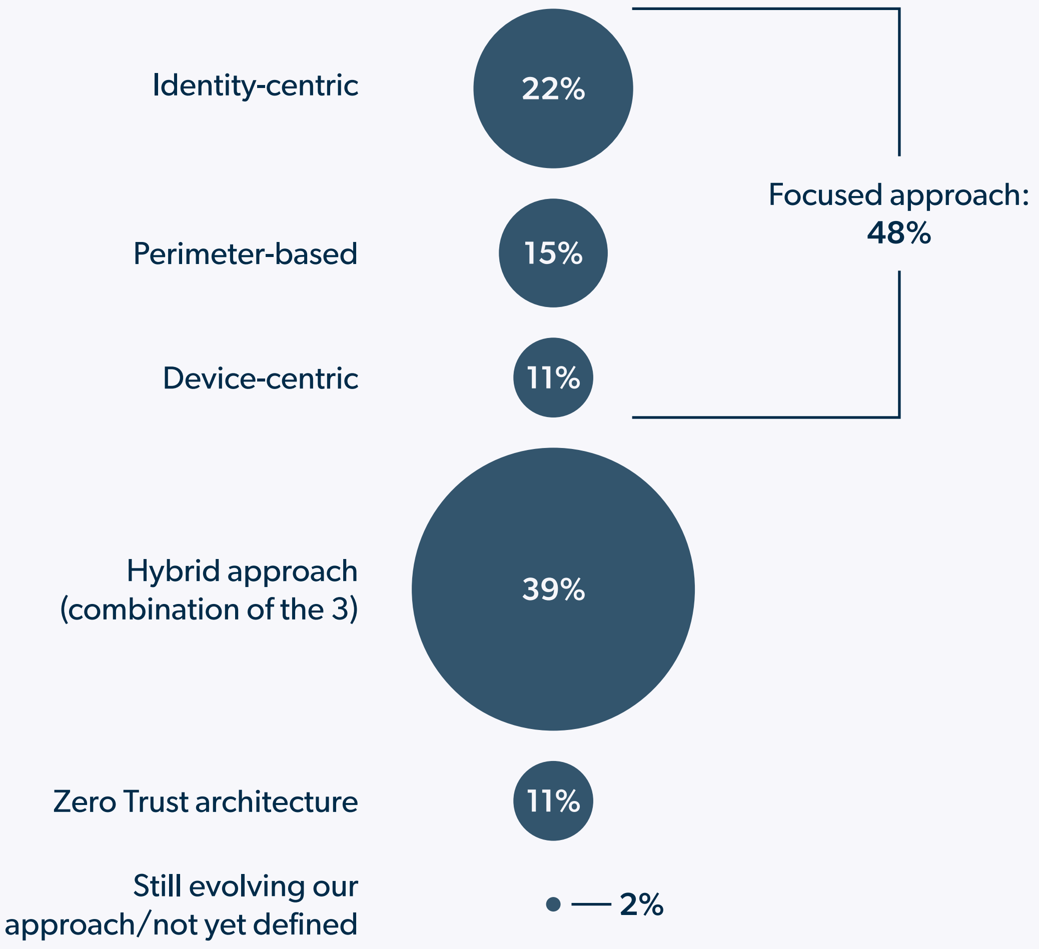

Chart 10

UX + Security = A Balancing Act

IT and security professionals are no strangers to the balancing act between security measures and the friction they impose on the user. Despite these challenges, IT professionals place high importance on the user experience. They ranked improving the end-user experience as their #2 priority for the coming year, and only 2% of organizations said the user experience is not a major consideration in their security strategy (Chart 20).

Over 60% of IT professionals claim to strongly focus on finding the right balance between security and user experience. Over half (56%) actively measure their user satisfaction with security tools and processes, and 25% have adjusted their security program based on user complaints. Nearly half (46%) have implemented single sign-on (SSO) or passwordless access to improve the user experience.

Despite these successes, 29% of IT professionals struggle to align security and the user experience **(Chart 11)**.

IT professionals place high importance on user satisfaction in their security program.

#2

Improving the end user experience ranked second on IT professionals' list of priorities.

How does the user experience influence your security strategy?

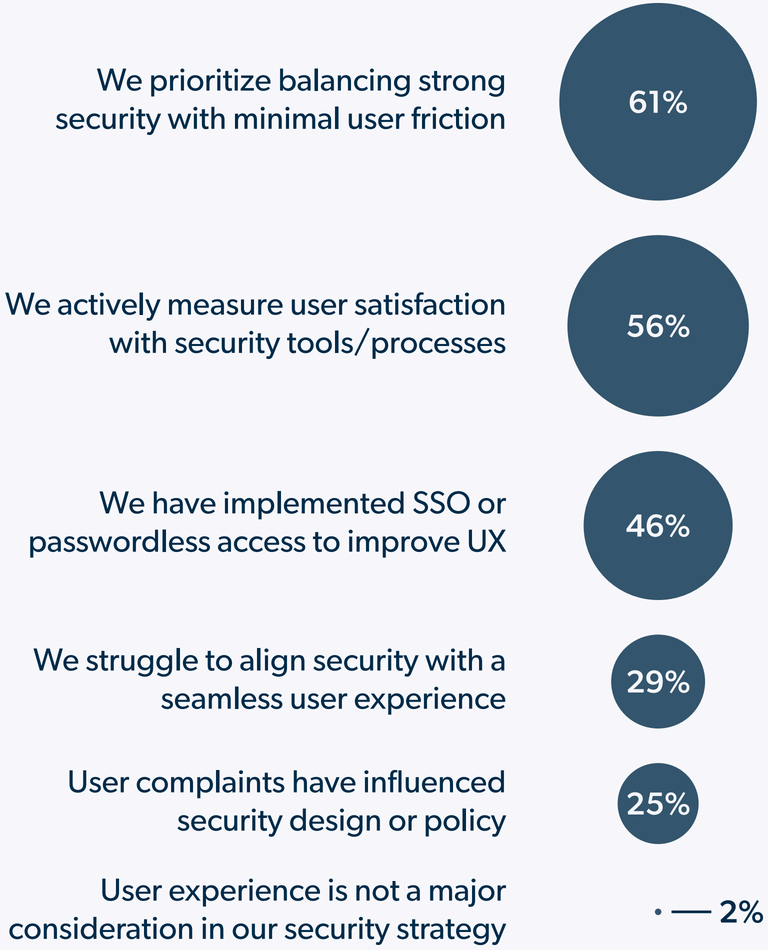

Chart 11

What Does It Take to Secure AI?

As AI popularity rises, so do concerns around its security. For instance, IT professionals are worried about non-human identities, AI connecting with sensitive systems, and the misuse of AI tools (Chart 17).

So, what does it take to secure AI?

For IT professionals, centralized visibility and enhanced audit trails tie for first place at 51%. Automated deprovisioning/key rotations for AI integrations (48%), role-specific access templates for AI agents (46%), privileged access controls for AI tools (45%), and dynamic policy enforcement (44%) follow closely behind **(Chart 12)**.

In the next section, we will explore how quickly AI is being adopted, the challenges it presents, and how IT professionals are addressing these issues.

Visibility and telemetry are ranked as the top necessities for securing AI.

What capabilities would most help your organization securely manage AI-driven tools or agentic systems?

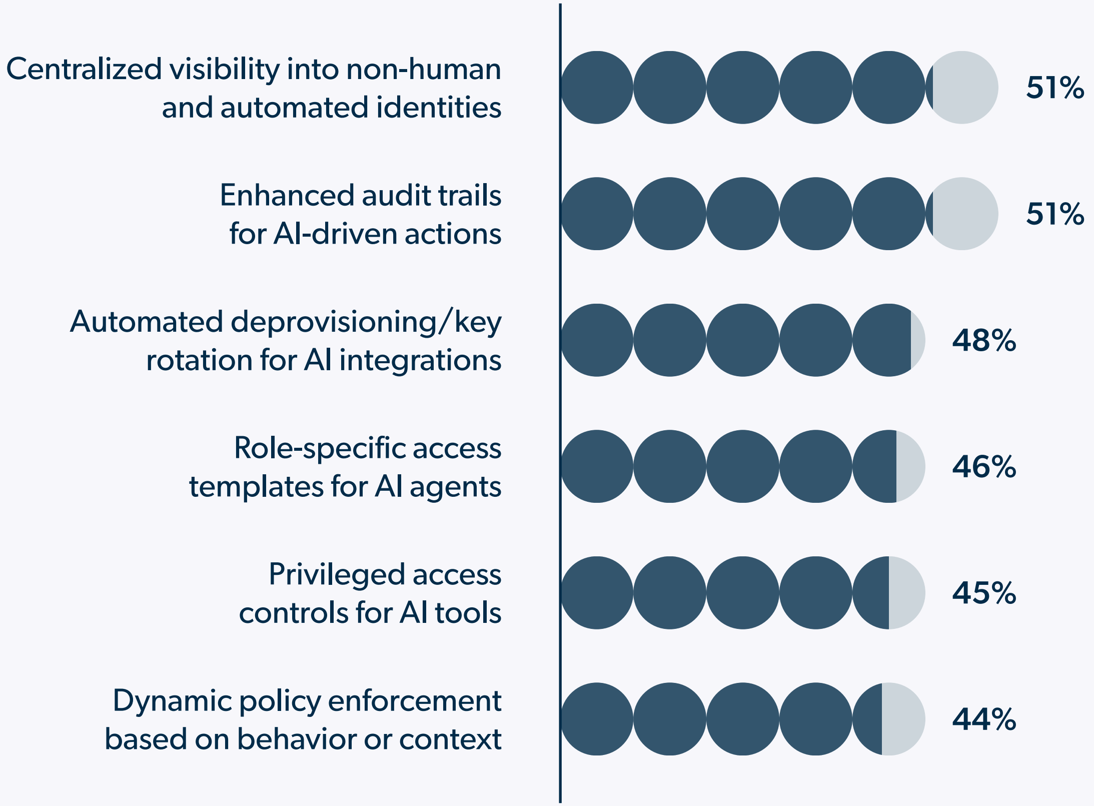

Chart 12

AI

Key Takeaways

AI adoption has skyrocketed over the last few years to become nearly universal: only 0.4% of organizations have no plans to adopt AI. AI is also what IT professionals claim as their number one strategic priority. **Organizations with no plans to adopt AI are in the extreme minority and should seriously consider the implications of falling behind.**

Despite the excitement (or perhaps because of it), AI adoption necessitates careful steps forward. Its rapid rise has yielded new challenges and threats — many of which IT professionals aren't yet sure how to mitigate.

Improper AI scoping, AI misuse, and limited visibility and compliance capabilities with AI tools are causes for concern. Non-human identities only complicate the issue, with fewer than a quarter of organizations actively working to secure them.

IT teams looking to adopt AI securely and intentionally should aim to keep their IT architecture unified, prioritize AI governance, and partner with an AI-savvy MSP. Unification prevents blind spots and tool misuse by keeping everything above board, while smart governance helps proactively establish appropriate scope and permissions for your AI tools. In the next section we'll cover the importance of MSPs and how organizations are looking to them for AI enablement.

AI scope, governance, and telemetry are paramount concerns.

Data quality and security and compliance tie for IT professionals' #1 AI implementation concern.

AI is a top priority — and a top risk.

While AI is organizations' top priority, 94% of IT professionals see big risks associated with AI.

AI use cases are diverse.

Organizations are discovering a wide range of uses for AI, with the average organization is pursuing over 3 use cases for AI.

AI Adoption Is Exponential

The number of companies with no plans to invest in AI is shrinking rapidly.

Since the beginning of 2024, the percentage of companies that have already adopted AI or are planning to has jumped from 86.8% to nearly 100% (99.6%). That leaves a mere 0.4% of companies that don't plan to adopt AI **(Chart 13)**.

The stages and use cases of AI adoption in organizations vary widely. The majority of organizations (63%) are actively implementing AI and/or piloting AI features within existing tools (53%). Experimentation with generative AI or large language models (LLMs) is also popular at 45%, and over a third of organizations (34%) are exploring AI in security-specific use cases. Nearly half are in the researching or planning phase (46%) **(Chart 14)**.

The percentage of companies that don't plan on adopting AI is now close to zero.

Companies with no plans to adopt AI

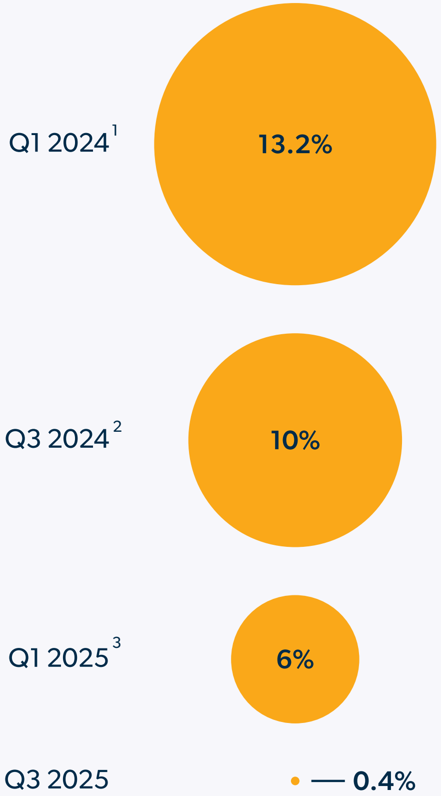

Chart 13

How is your organization currently implementing or exploring AI in IT operations?

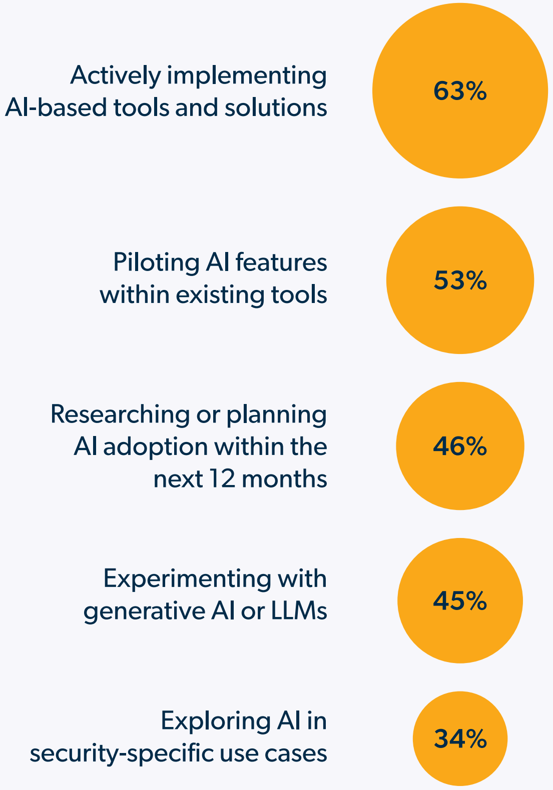

Chart 14

[1] Q1 2024 IT Trends Report

[2] Q3 2024 IT Trends Report

[3] Q1 2025 IT Trends Report

AI Is THE Top Priority

With AI adoption at a breakneck pace, it may come as little surprise that AI was ranked the top priority for IT professionals for the coming 12 months.

Nearly half (46%) of IT professionals said enhancing AI readiness was a top strategic priority this year, making it IT organizations' number one priority.

#1

Enhancing AI readiness is IT organization's top strategic priority.

AI Governance Simplified

AI governance is critical to ensuring proper AI use. Learn how to establish effective governance as you explore and adopt AI.

Download the eBook

How Are Organizations Using AI?

Organizations seem eager to capitalize on the benefits of AI, and its emerging use cases are diverse. On average, IT professionals anticipate using AI in more than three ways in their organization. Those use cases are fairly split between strategic and supportive functions.

The most popular use cases illustrate this diversity well: AI's #1 use case is for helpdesk or chatbots (68%). Behind by only one percentage point is security threat detection (67%), followed by predictive maintenance (48%), user behavior analytics (47%), forecasting or capacity planning (46%), and automated ticketing/workflows (45%) **(Chart 15)**.

IT professionals are pursuing a diverse set of AI use cases spanning automation, security, and strategic support functions.

Which AI use cases are you pursuing or planning to pursue?

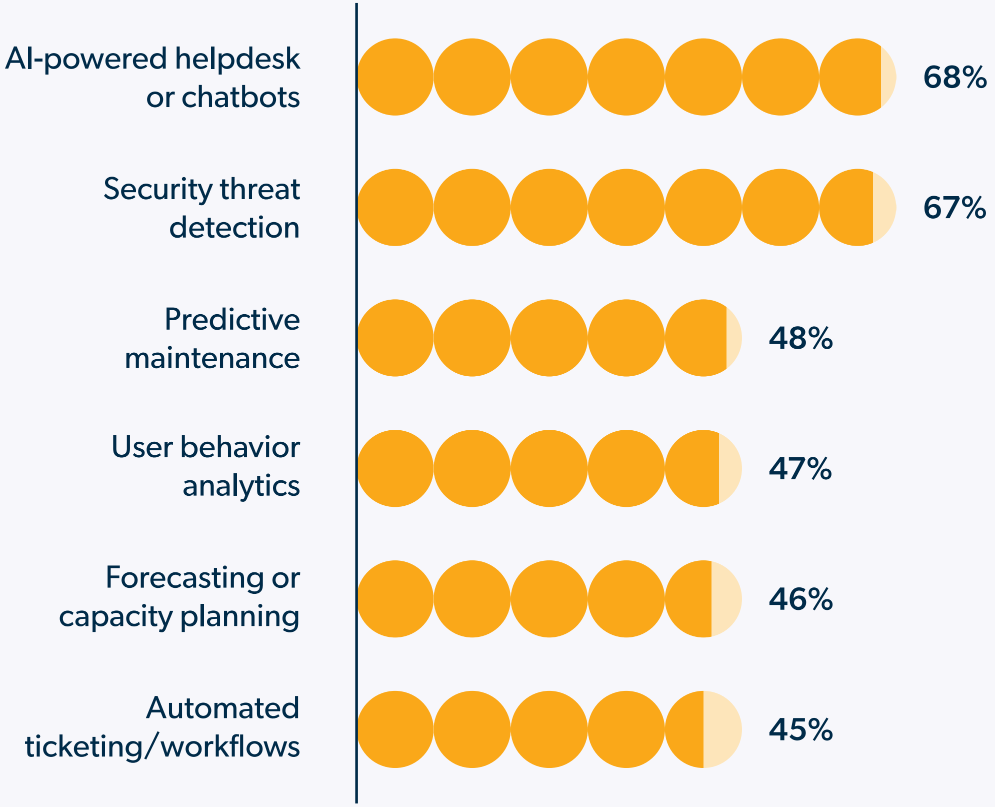

Chart 15

3.2

Is the average number of AI use cases pursued in an organization

AI Implementation Is a Bumpy Road

AI is still relatively new, and it brings its fair share of challenges.

When it comes to AI implementation, data quality and security and compliance tie for the top implementation concern (47%). This is followed by lack of integration across IT systems (44%), budget or resource limitation (39%), lack of internal expertise or training (37%), uncertainty around use cases or ROI (33%), and lack of executive support (23%) **(Chart 16)**.

Executive support coming in last, with less than one-quarter of IT professionals listing it, suggests that leadership is often bought into (if not a main driver for) AI adoption.

Top implementation challenges revolve around data quality, security, and compliance.

What are your biggest challenges with AI implementation?

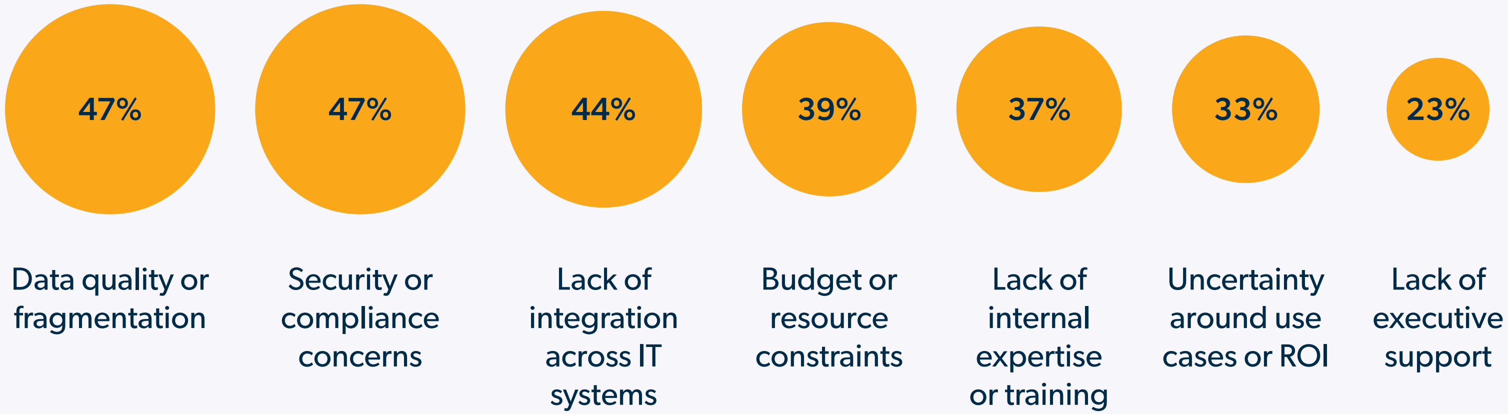

Chart 16

AI Risks Abound

The vast majority (94%) of IT professionals see risks associated with AI in their organization. The top risk plaguing IT professionals is AI tools integrating with sensitive systems without proper review (51%).

Following closely behind is the risk of AI misuse by staff with elevated permissions (45%), lack of identity governance for AI identities (42%), insecure default permissions or API keys for AI tools (38%), unauthorized access or privilege escalation by AI agents (37%), and the inability to track or audit AI-initiated actions (35%) **(Chart 17)**.

AI is almost universally perceived as risky, with the top risks revolving around uncontrolled AI access to sensitive systems and insufficient telemetry.

Which of the following risks do you associate with AI tools and applications in your organization?

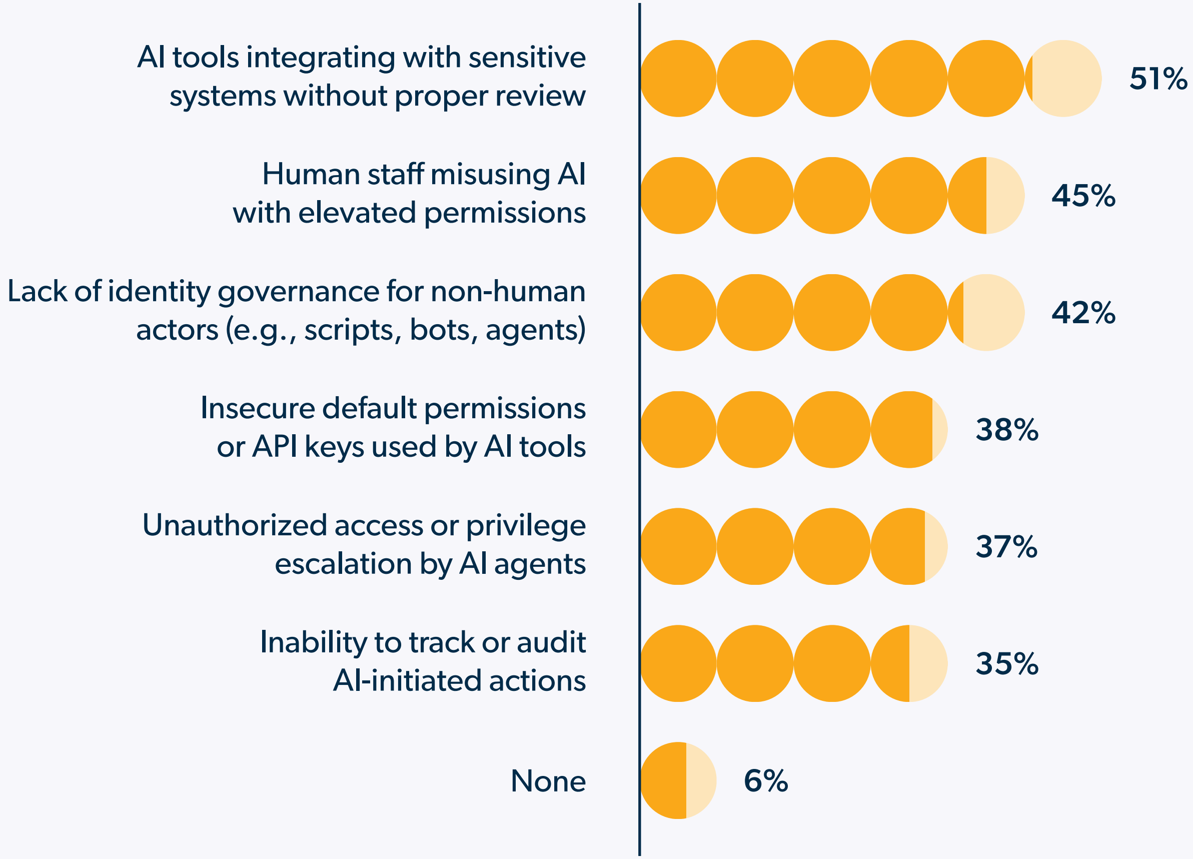

Chart 17

Non-Human Identities Pose New Questions

Many of the top risks that IT professionals anticipate involve non-human or agentic AI. As this technology emerges and gains ground, it poses new questions around security and identity management.

Many IT professionals are considering the new needs non-human identities will bring: only 2% haven't yet addressed the issue.

However, less than a quarter (23%) of IT professionals are currently taking actions to secure or manage them (Chart 18).

While the majority of IT professionals are considering the risks of non-human identities, only 23% are taking action to manage or secure them.

To what extent are non-human identities a security concern for your organization?

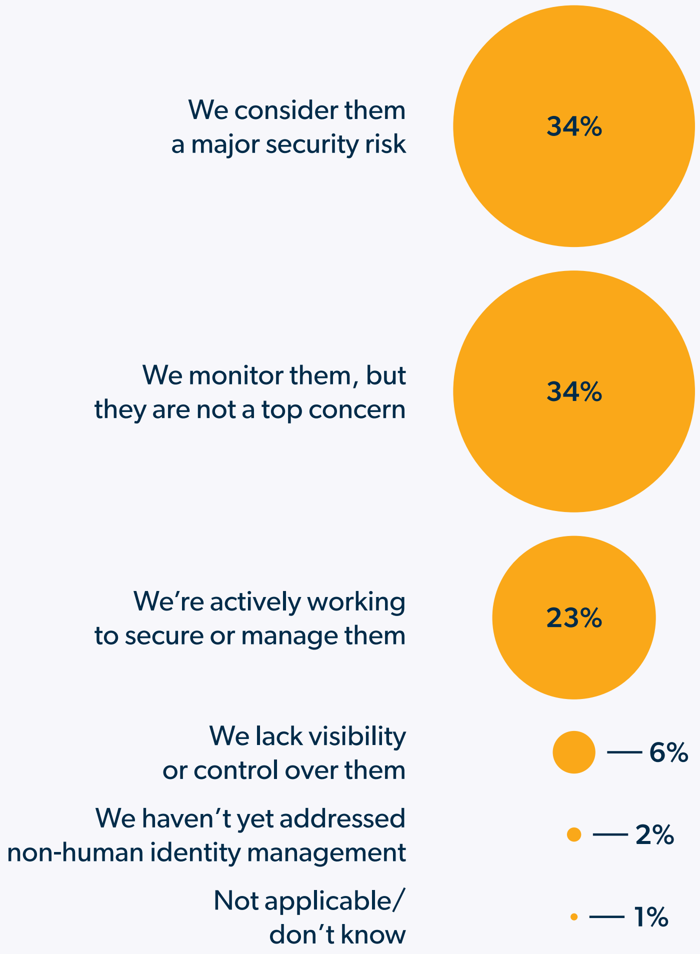

Chart 18

What’s Your Role in All This?

What’s the role of the IT team in driving AI strategy?

IT teams play varying roles when it comes to driving strategic, organization-wide initiatives. The most common comes in the form of support by providing a foundation of unified data systems (63%). Playing a leadership role is also common, with 55% of IT teams leading tool evaluation for productivity and 54% driving automation initiatives with AI.

Finally, advising and partnerships are common as well, with 50% of IT professionals advising leadership on AI governance and risk, and 49% partnering cross-functionally to deploy AI operationally **(Chart 19)**.

IT teams are crucial in both driving and supporting AI strategy.

How is your IT team helping drive strategic AI initiatives across the organization?

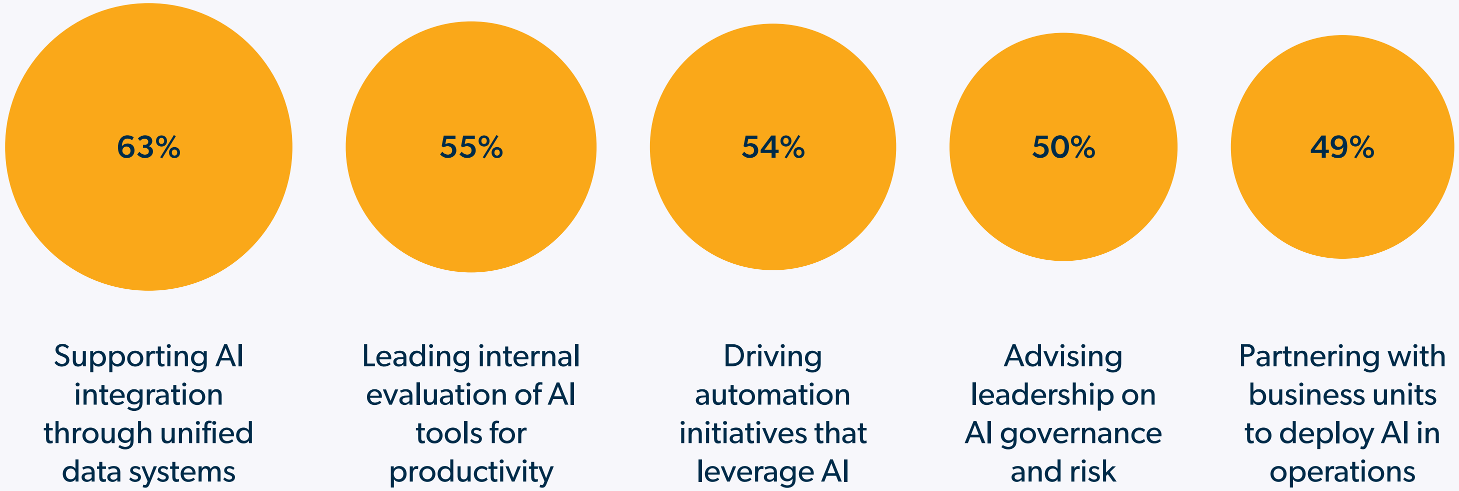

Chart 19

Looking Ahead: Investments & Priorities

Key Takeaways

The security challenges that IT professionals face, combined with global macroeconomic and geopolitical uncertainties, are driving deliberate spending patterns. Budget plans are focusing on automation and resource optimization, and IT unification is the prevailing route to doing so.

As they consolidate, organizations are placing high priority on AI readiness and the user experience. Striking the right balance between these initiatives and security now will be paramount to long-term sustainability and growth.

In addition, MSPs are being seen as a vital strategic player in the IT programs they manage for their organizations, and their influence is only projected to grow. Organizations expect their MSP engagements to bring more to the table than just break-fix support and technical oversight; they need to expand into more strategic planning and advisory roles.

For the MSPs reading this report: this means organizations will look to you for expertise, advisory services, and a means to adopt leading technologies. Prepare your teams by investing in training and exploring options for new offerings around AI, compliance, and advisory services.

The four most important letters: AI and UX.

AI readiness and the end user experience are IT professionals' top 2 priorities.

MSPs play a growing strategic role.

Over 80% of organizations use an MSP, and more than half of them expect their contracts to grow.

Balance optimization with investment.

Cost optimization, and investing in automation and unification, are organizations' top 2 budgeting priorities.

Macroeconomic uncertainty impacts us all.

US and UK IT professionals are equally concerned about macroeconomic and geopolitical headwinds, with tariffs the #1 concern for both.

What Are Your Top Priorities?

We asked IT professionals to list their organization's top three strategic priorities over the next 12 months. AI readiness took the top spot, with 46% of IT professionals including it in their top priorities.

The next most popular initiatives were improving the end-user experience (38%), IT tool consolidation (36%), cloud migration (34%), strengthening compliance and audit controls (30%), SaaS management (29%), shadow IT mitigation (23%), asset management (22%), and privileged access management (20%) **(Chart 20)**.

Organizations' top three priorities are AI readiness, the end-user experience, and IT consolidation.

Strategic priorities over the next 12 months:

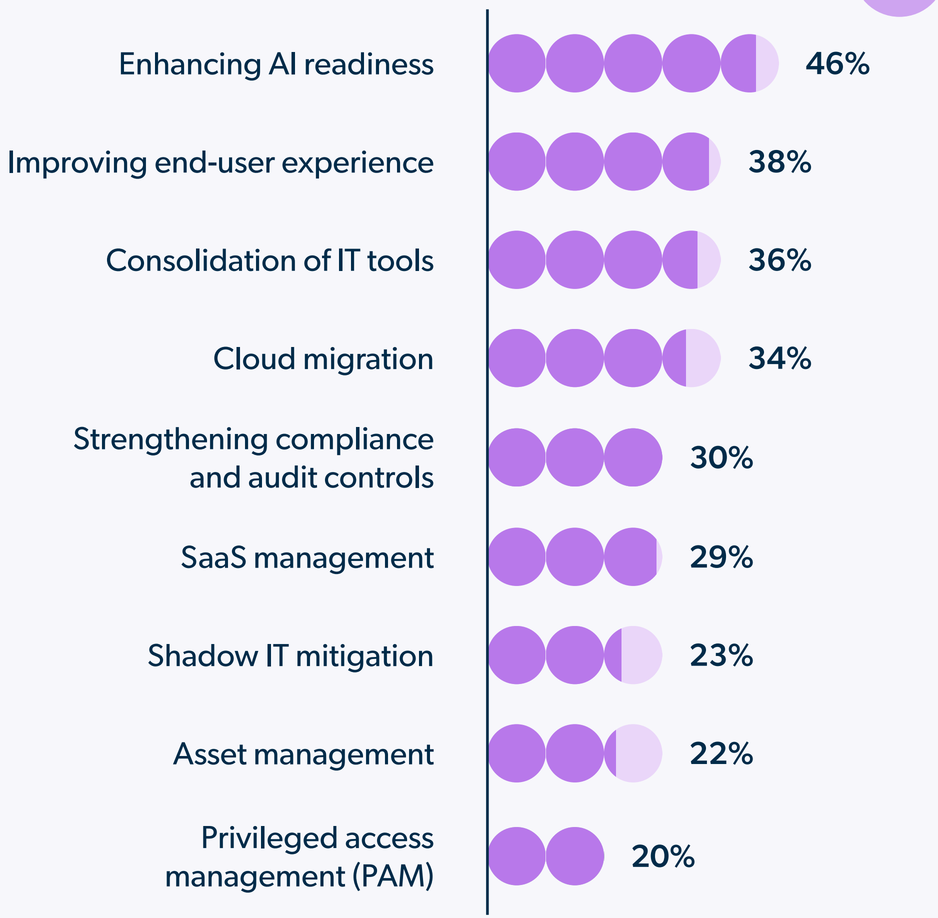

Chart 20

MSP Partnerships Are Paramount

Managed service providers (MSPs) are a major component of organizations' IT programs. Over 80% of organizations collaborate with MSPs. The majority partner with MSPs for specific services (50%), another 21% rely heavily on MSPs for their daily operations, and 10% work with more than one MSP for different functions.

Less than 20% of organizations don't use an MSP, and the majority of those organizations (90%) are exploring working with one in the future. Only 2% of organizations don't use an MSP and aren't considering working with one (Chart 21).

MSPs are a major part of most organizations' IT programs, offering a range of support, from specific services to day-to-day operations.

In what ways does your organization currently work with an MSP?

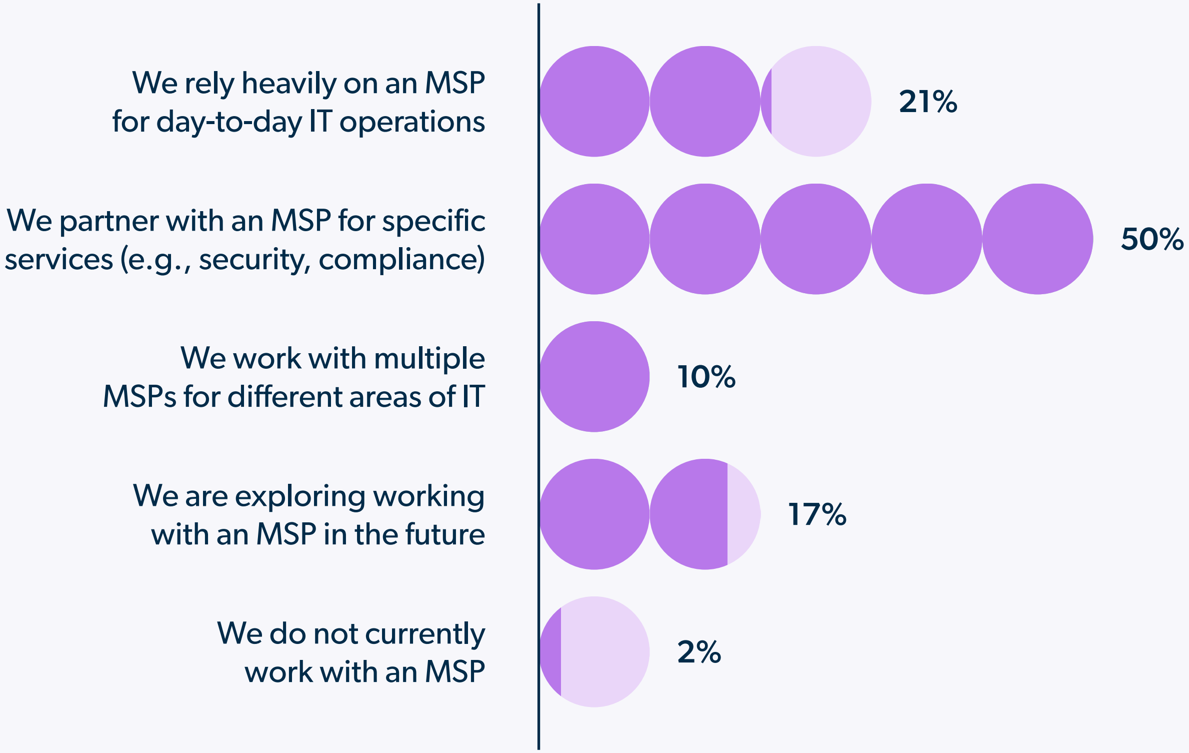

Chart 21

Expect Expansion of MSP Contracts

MSP engagements are expected to grow and diversify, especially in the realm of strategic IT planning and advisory.

The majority of IT professionals expect their engagements to dive more into strategic IT planning (58%) and expand into new service areas (53%). More than one-third (34%) also expect their MSP partnership to shift from technical support to more advisory or consulting roles.

While the majority of IT professionals expect their MSP engagements to grow, one-third expect to reduce their engagements as they bring IT in house **(Chart 22)**.

Most organizations expect their MSP engagements to expand, with strategic IT planning services projected to see the most growth.

How do you expect the role of your MSP to evolve over the next 12–18 months?

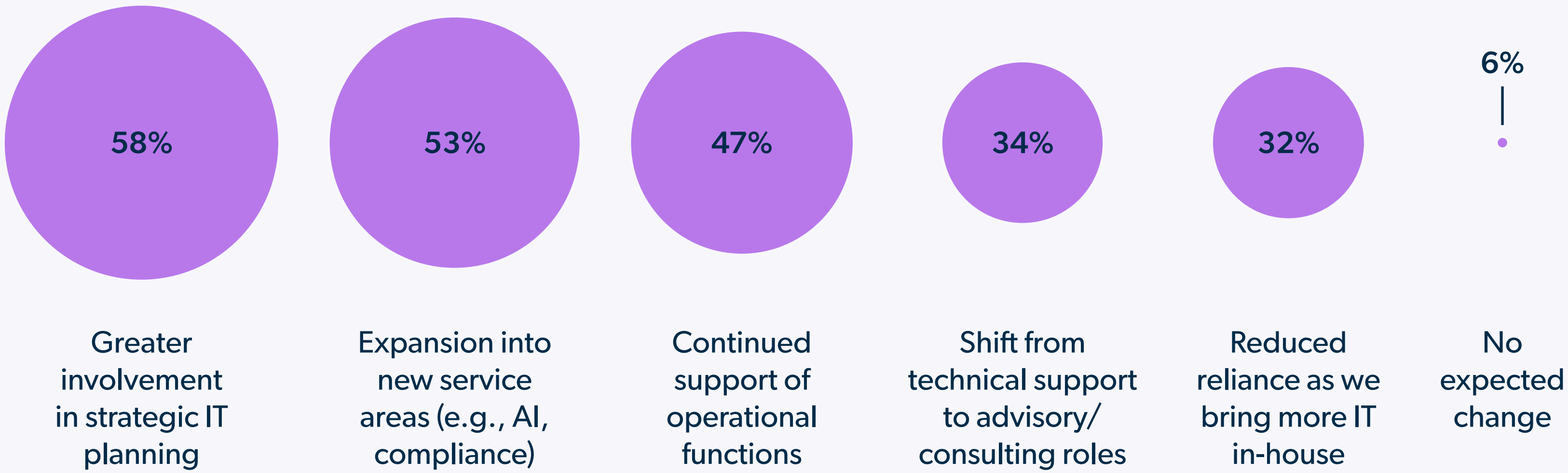

Chart 22

Spend Smarter, Not Harder.

From MSP expansion to investing in initiatives like AI and IT consolidation, organizations have big plans for the coming year. However, organizations are also focusing more closely on budgets and tightening the pursestrings.

When we asked IT professionals how their budgets changed over the last year, the top answer was tied: 54% focused on cost optimization, and 54% increased their investments in automation and unification. The overlap in percentage reminds us that these are not mutually exclusive: it's possible to optimize costs while still investing in new technologies. In fact, these two initiatives go hand-in-hand: investing in automation and unification are part of a cost optimization initiative for many.

In addition, nearly half of organizations also placed greater scrutiny on software procurement (46%), 25% delayed or cancelled IT projects, and another 25% shifted to lower-cost or bundled solutions **(Chart 23)**.

Organizations place heavy emphasis on smart spending and cost optimization.

How has your IT budget changed in the last 12 months due to economic conditions?

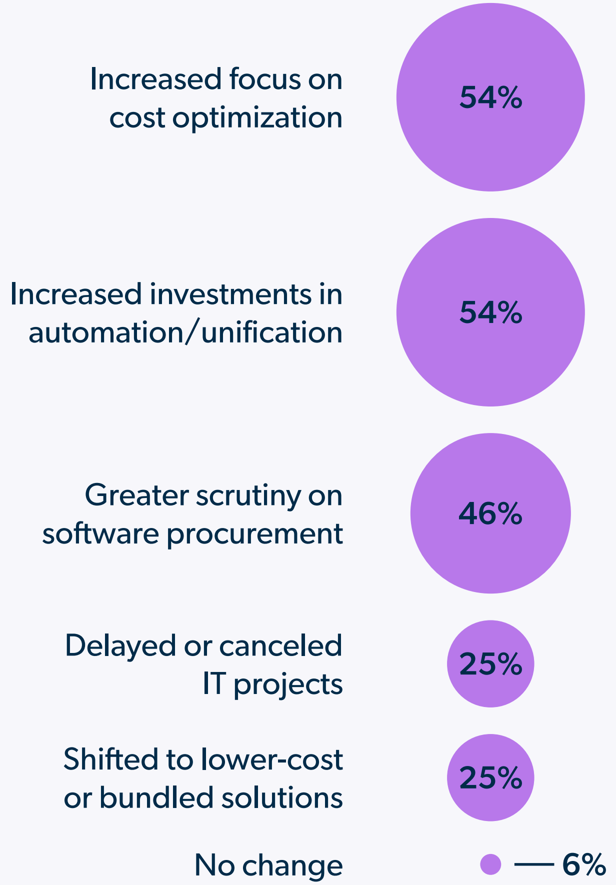

Chart 23

Macro Factors Create Headwinds

There are several macroeconomic factors currently impacting IT purchasing decisions. The top factor on IT professionals' minds is tariffs on imported hardware/software (51%), followed by regulatory and compliance uncertainty (46%), supply chain disruptions (42%), currency fluctuations and regional pricing differences (42%), and political instability (32%) **(Chart 24)**.

Despite the regional and geopolitical factors at play, responses from the US and UK were nearly identical, with no response differing by more than than 4 percentage points **(Chart 24)**. This suggests that these issues are globally impactful.

IT professionals in the US and UK share the same concerns, with tariffs the primary factor influencing purchasing decisions.

What economic or geopolitical factors are currently impacting your IT procurement decisions?

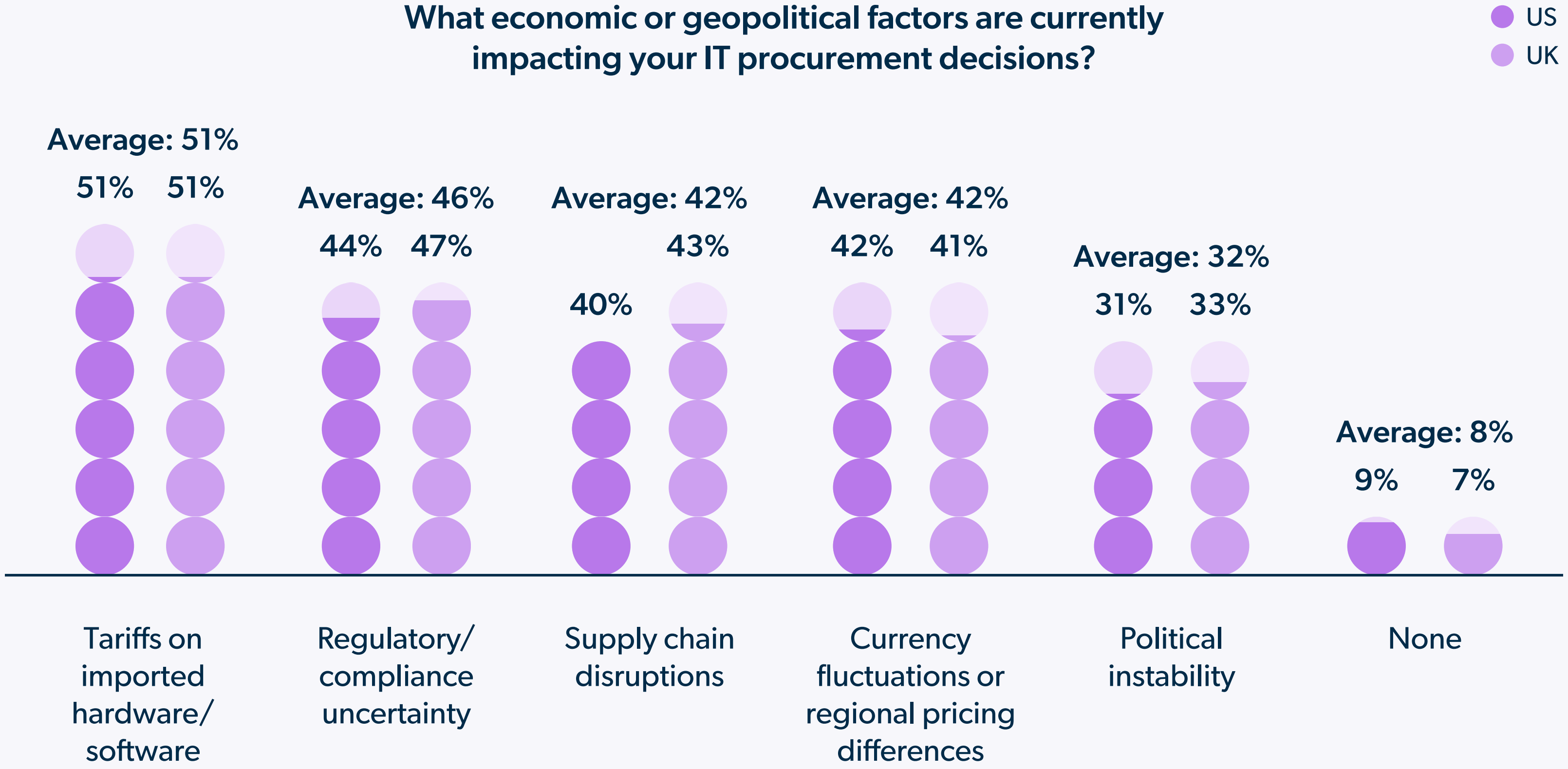

Chart 24

Missed the Boat?

When we asked IT professionals about opportunities they're currently missing out on in IT management, responses were rather evenly spread across the board.

There was a three-way tie for first place between simplifying complex IT environments, automating repetitive IT tasks, and improving collaboration between IT and other departments (42%).

The next most common answers were adopting a unified IT platform (39%), demonstrating IT's impact on business outcomes (36%), leveraging data and analytics for strategic planning (36%), and enabling self-service for end users (29%) **(Chart 25)**.

Missed opportunities revolve around resource optimization and IT securing a more strategic seat at the table.

What do you believe is the biggest missed opportunity in IT management today?

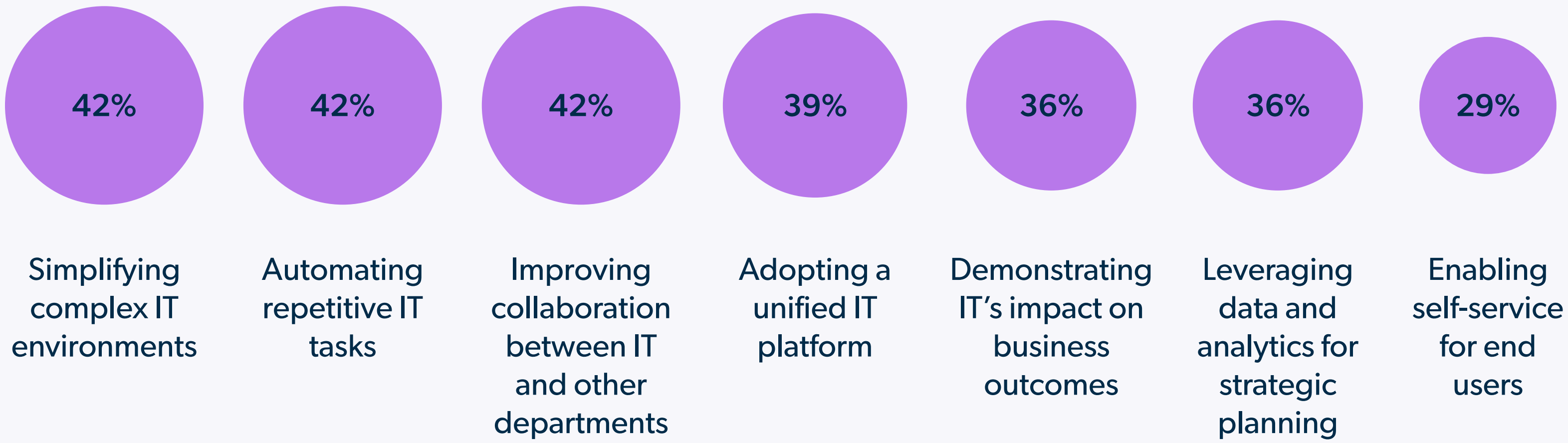

Chart 25

A Playbook for the Strategic IT Leader

No matter which way you look at it, the findings from this report make it clear that IT leaders have a major opportunity in front of them to become the strategic force of their organization. We're not talking about just getting a seat at the table; we mean sitting at its head, leading with intention and an understanding of what it's going to take to stimulate real growth for your organization.

It will ask you to be proactive. To forge strategic partnerships with other departments, leadership, and MSPs. And you will have to keep up with the breakneck developments happening with AI.

But above all else, you will have to answer the unavoidable call to unify. IT unification will help you optimize your resources and spend while maintaining security, enabling users, and building the architecture you need to make work happen.

Unifying your architecture is no longer optional for success. It's what ensures your IT and security programs get organization-wide alignment and keeps you on the leading edge of tooling, processes, and expertise. Cost savings, automation, and IT unification are now the top factors influencing purchasing decisions. Your organization needs you to spend with measured care and demonstrate your ability to keep everyone secure, efficient, and equipped with the right tools.

It isn't easy, but that's not why you do it. While this report sheds light on the key areas that your peers are focused on, you must decide what direction you take. These principles are your guide to understanding what matters most and what you can do to affect positive, strategic change.

Consolidate to Control Complexity

Unified IT is the surest way to manage your environment effectively, deliver the best end user experience, and make the most of your limited resources.

Secure Identities, Not Perimeters

Zero Trust is the key to protecting your organization from modern threats. It centers around identity and extends beyond pure security tooling.

Embrace AI (with Care and Intention)

With AI adoption at nearly 100%, it's no longer optional. But with the new challenges it presents, governance, security, and scoping are paramount to its success.

Invest in Diverse Partnerships

There are too many factors at play to manage everything alone. Invest in your relationships with other departments, leaders, and your MSP to ensure success.

Next Steps

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

Related Reports

MSP Performance and Growth

Get data and insights specific to MSPs: how are they approaching today's challenges, and what do growth and success look like?

Download eBook

IT-Security Collaboration

Get survey data on how IT and Security work together and why their smooth collaboration is essential to success.

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 | Resources | X | in | ▶