jumpcloud™

Q1 2026 IT TRENDS

The Dual Disconnect: Why Your AI Maturity Now Fails To Scale

How IT Unification is The Foundation for Driving Safe, Effective AI Adoption

When It Comes To AI, Are You Ready? Are You Sure?

There is still so much about AI that is emerging. And yet, even in its infancy state, it is reshaping how we work, and with that the very foundation of IT.

AI is already showcasing what it's capable of across enterprises of all sizes. The question for IT leaders has changed from the simple "Should we use AI?" to the more complex, and nuanced, "How well are we using it, and are we doing so securely?".

This creates quite the conundrum. You want to embrace AI's power for growth but can't help wrestling with the risks it brings.

Nearly every organization (99.6%) is already using AI or planning to do so, and that applies to the very heart of IT too. It's a non-stop cycle of opportunity and challenge. AI has the power to automate tasks, strengthen threat detection, and deliver faster insights. This has made **enhancing AI readiness the #1 strategic priority for 46% of IT professionals this year**.

But in this move-fast and break-stuff climate, the speed of adoption creates uncertainty. What does true preparedness actually entail?

When looking at direct controls to manage AI, almost half of the organizations we surveyed (40%) declare themselves **AI mature**. But through a more objective lens, **AI readiness** does not always align with self-assessed maturity. The speed and novelty of AI makes it challenging for organizations to accurately gauge their true capabilities.

This results in a dual disconnect. Many organizations believe they are further along than they are. And others are more prepared than they realize. Both scenarios create risks for ineffective investment and governance.

So what is the true, verifiable measure of an organization's readiness to handle AI?

True AI readiness extends beyond AI-specific tooling. It relies on a strong foundation. Core infrastructure, identity management, and unified governance must support the AI layer. It needs it to help it thrive in a safe and secure manner.

As you dive deep into the data of this report, a clear distinction emerges. **AI maturity** is a reflection of the specific tooling, workflows, and cultural embrace an organization has for AI use. **AI readiness** is a measure of the entire IT base. It considers the necessary supporting systems (like IAM, security, and governance) as well. These are necessary to manage AI effectively, safely, and securely. AI readiness is the objective measure every organization needs to hold themselves to. Because it highlights what they are actually prepared to do.

In this edition of JumpCloud's biannual IT Trends report, IT leaders provide insights into their environments, practices, plans, and attitudes about how they work and the role AI plays in it. Through careful analysis we compare how IT leaders feel they are handling the AI surge against their broader behaviors and preparations. The data shows the security and governance gaps caused by the misalignments between these two evaluation methods, and explores the path to AI readiness success.

JumpCloud surveyed 825 IT leaders in the U.S. and U.K. at a 50/50 split. Respondents were IT administrators, IT managers / IT team leads, directors of IT, directors of Technology, Vice President of IT/Technology, chief information officers (CIO), chief technology officers (CTO), and chief information security officers (CISO). Each survey respondent represented an organization with 200-2,500 employees across a variety of industries. The online survey was conducted by Redpoint from September 2, 2025 to September 24, 2025.

Key Takeaways

85% of IT leaders are measuring AI's impact on productivity…

…and over 90% of them admit it has improved both their personal and team's productivity.

But everything isn't what it seems…

…when organizations assess their ability to manage AI well. Only 1 in 5 organizations seem to be fully capable of managing it, leaving the majority in preparation stages.

50% of organizations admit AI will restructure their teams…

…for the better. They expect AI to create new roles within the team over the next 1–2 years.

The top challenges AI poses are not unique…

…ranging from the operational (AI integration and managing risks and compliance) to the technical (cyber threats and data leaks). The majority of organizations still feel like AI is outpacing their ability to protect themselves against these threats.

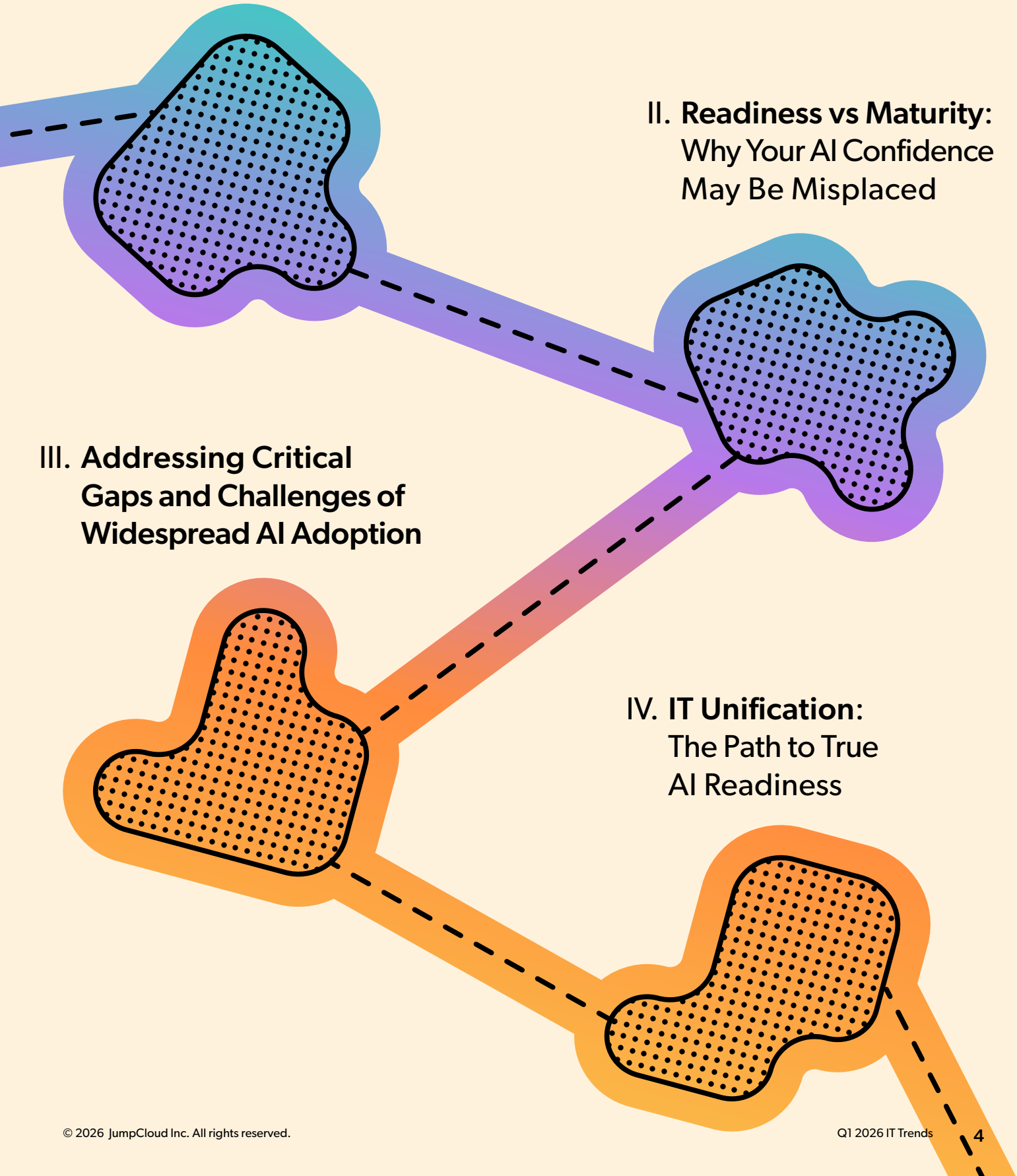
Organizations continue to expand and invest more in AI…

…with 9 in 10 expecting an increase in their IT budget for AI expenditures, and half planning to expand AI across their IT operations within the next 6–24 months.

While shadow AI overshadows 61% of organizations' high governance confidence…

…almost half agree that IT unification is critical for AI readiness and scaling, while 85% of organizations agree the same for IAM.

Table of Contents



The Journey So Far

How AI Has Impacted IT's Productivity To Date

It seems like every week there's a new headline about how AI is revolutionizing the way we work… and the hype is absolutely real. In such a short period of time almost everyone can see that AI is no longer a futuristic dream. In both the personal and professional spheres, AI is recognized as a powerful tool that delivers real, measurable ROI today.

For IT leaders, AI is becoming an integral force. It's now part of how they operate, influencing strategy and supporting every department. IT leaders have expressed AI as a means to:

Do more with less: AI acts as a force multiplier. It automates simple and complex tasks, which frees up IT teams to focus on more important, high-value work.

Build faster and smarter defenses: With threats moving at a breakneck speed, AI provides advanced detection and response. This can allow IT to identify and neutralize threats much faster and more often.

Accelerate everyone's pace: AI bridges the gap between IT capabilities and business needs, providing faster insights and building a foundation for continuous innovation.

Handle heavy workloads: AI brings the necessary speed, flexibility, and ability to handle large amounts of work by taking on excess tasks.

Do you believe AI has improved your personal productivity since you started using it?

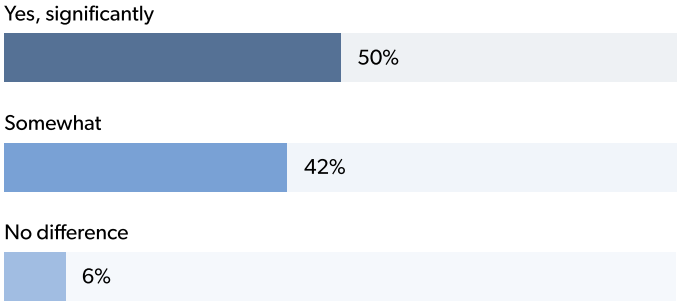


Chart 1

For over 90% of the IT leaders, the benefits of AI have been threefold. It empowers them to:

- **Manage IT better**: Traditional IT often means routine, reactive maintenance. AI-driven automation and predictive maintenance can free IT leaders from these necessary (but basic) tasks. This allows them to focus on big-picture strategy.
- **Boost leadership skills**: AI is changing IT leadership by giving them access to advanced analytics. This lets them switch from solving problems as they happen (reactive) to using data to plan ahead (proactive and predictive).
- **Make IT operations smoother**: By reducing the need for manual checks, AI is streamlining how IT is done. This directly increases efficiency, cuts costs, and greatly improves how reliable the systems are.

AI is not just increasing output; it's also acting as a major time-saver and stress reducer for 56% of the IT professionals who report daily usage.

How would you describe the impact of AI on your day-to-day role or workload?

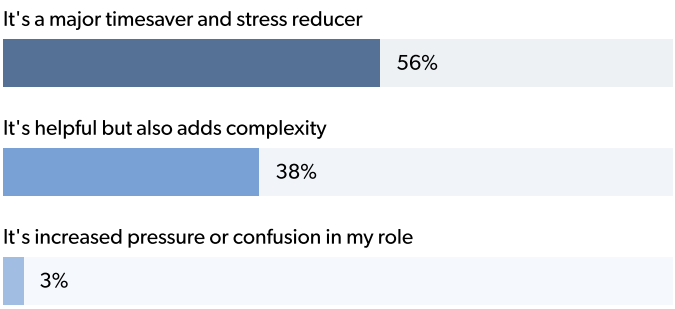


Chart 2

As for IT teams, AI is a massive productivity booster. Think about the hours lost every week on simple, repetitive tasks—like resetting passwords, running checks, or manually patching systems. AI is starting to take over that administrative work, freeing up highly skilled IT staff from the daily, manual grind of tasks and ticket responses.

This helps almost everyone focus on strategic, creative problem-solving and innovation, which is where they can give the most value to the organization.

The message is clear: AI isn't replacing IT, it's elevating IT.

A Note to the Reader

We've begun to make references to an important concept for this report: AI Maturity. In the next chapter, we go in depth on what this means, but we don't want you to be completely in the dark until then. For now you should know that one of the first questions we asked was related to their personal assessment of how mature their AI operations are. Based on that response, we can see who considers themselves to be at the highest degree of maturity (Mature), at the lowest (Starting), and in between (Scaling and Developing).

Where does productivity make itself known?

Where do we see these productivity gains? 85% of organizations are actively measuring how AI affects their work. On average, they use four different metrics to do this.

The most common are:

- Time saved on IT tasks (66%).
- Cost savings (54%).
- Improved threat detection (48%).
- Increased automation coverage (47%).

92% of IT leaders feel that AI has improved their team's productivity.

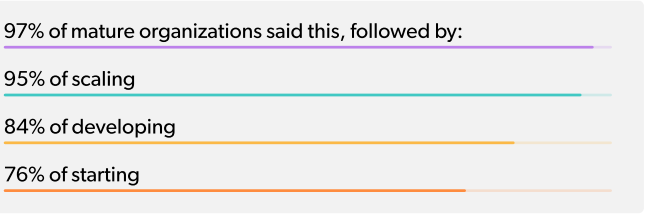


Chart 3

We also found that organizations who say their AI maturity in IT was at its highest level were more likely to measure productivity. This happens less often for those who feel they are less mature (more on AI maturity, and what that means, later).

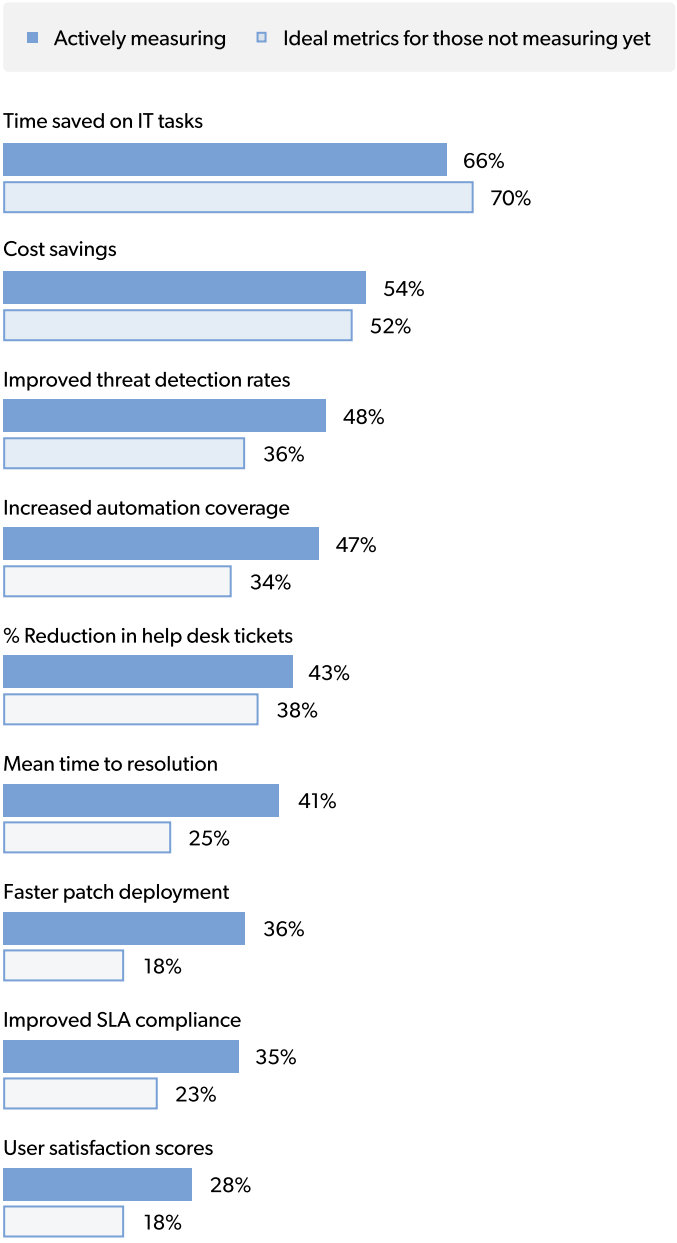
And for those who are not measuring its impact?

They were much more likely to identify time-related metrics. 70% of IT leaders listed time saved on IT tasks as their ideal metric. This was followed by cost savings (52%) and percent reduction in help desk tickets (38%). Without much experience, these organizations look at efficiency gains rather than improved outputs and automation for how AI will help them best.

The results show a clear link between how much an organization embraces AI and the opportunities they see with it. More mature organizations see greater potential in AI's capabilities beyond surface level productivity gains. The more they use it, the more likely they are to figure out new and interesting ways for AI to make an impact. They seek out ways for AI to lead with human guidance, versus the other way around.

It highlights how getting better at using AI isn't just an exercise in saving time. It's an investment that directly leads to better output, less stress for staff, and more efficient IT services.

Leading metrics for measuring AI impact and value



Average number of tools mentioned:

Actively measuring: **4**
Ideal: **3.2**

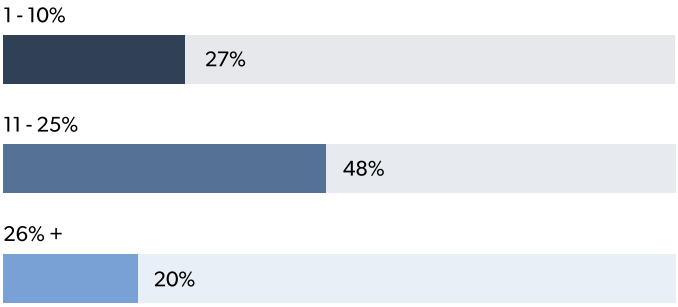
Chart 4

Positive Perception Drives Investment and Growth

The positive perception of AI's impact on IT isn't just a matter of opinion; it's driving real strategic business decisions that are reshaping the IT landscape.

This positivity cascade may have started with demonstrated gains in productivity. But it is rapidly translating into real-world investment and organizational evolution.

What percentage of your 2026 budget do you expect to be allocated to AI related initiatives?



29% of mature organizations are expecting more than 25% of budget to be allocated

↑ 9 points from the average

Chart 5

AI Investment and Budgeting

The confidence IT leaders have in AI's immediate help is leading to considerable financial support.

- Many organizations expect to set aside a moderate share of their budget for AI-related projects.
- Organizations that are more AI mature are almost 50% more likely to spend 25% or more of their budget on AI.

This commitment shows that companies see AI as a lasting strategy, not just an experiment. They understand that they need more money to get AI's full benefits and address the security problems it creates.

Which IT tasks are most likely to be partially or fully automated by AI in the next 12 months?

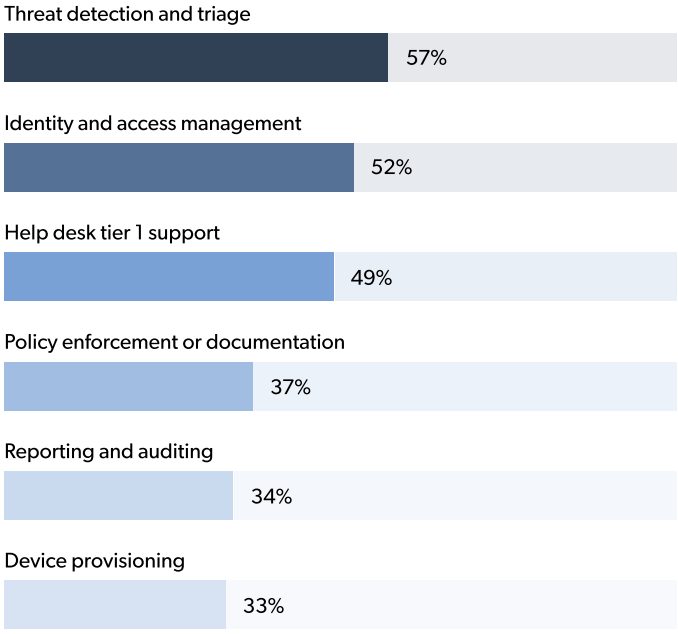


Chart 6

How do you expect AI to impact IT team structure over the next one to two years?

50% say AI will add new roles and skills

60% of mature organizations agree

27% say AI will reallocate existing roles

39% of developing organizations agree

16% say AI will reduce overall headcount

7% say AI will have no real impact on IT team structure

20% of starting organizations agree

Chart 7

AI is Creating New Roles

This confidence is also changing the workforce.

Unlike the many headlines across 2025 that said AI will cut jobs, many IT leaders see AI as a positive force that will help the team grow in the long run. 50% of IT leaders expect AI to lead to the addition of new roles that need specialized skills. It's not just bringing simple automation; the ways AI is expected to improve human work will require smart investment in new talent.

As we have seen, AI maturity influences this perspective greatly. AI mature organizations are 20% more likely to say AI will add new roles and skills compared to the whole. On the other end, organizations just starting their journey with AI are three times more likely to say it'll have no impact. It's much harder for them to see how AI will change their teams. Interestingly, those who are using AI, but only just developing their internal processes around it, are 44% more likely to say that AI will change our jobs rather than add to it.

Where the Money is Going

These investments are targeted at the areas where AI can provide the most value. The focus is on long-time problem areas and critical IT functions.

Investments are going to:

- High-level security work like threat detection and triage (57%).
- Basic services like Identity and Access Management (IAM) (52%).
- Time-consuming IT tasks like the help desk and Tier 1 support (49%).

These focused investments show that IT leaders have a clear plan for using AI. They see it as a key tool for both defensive security and efficient operations—an approach needed to meet the growing demands of modern organizations.

Growing Pains and the Maturity Link

But even though AI helps us get a lot more done, it isn't an easy road to get there. More than a quarter (38%) of the IT leaders who find AI helpful in their jobs also admit that it adds more complexity to their work.

This is especially true in organizations just starting to scale their AI usage. Just over half of the organizations that self-assess as Developing their AI maturity practices were in this group. But even a quarter of mature organizations feel the pain.

This is a vital indicator: the journey to successful AI integration is not a simple, clean switch. It's an ongoing effort that requires teams to overcome inherent technical and organizational hurdles.

This complexity is best understood when viewed through the lens of maturity.

Our research shows a strong correlation between self-assessed maturity and perceived positive impact. Those more likely to report better productivity also see themselves further along in their AI tooling and practices. This makes intuitive sense. Maturity implies higher technological investment, cultural acceptance, and more established processes.

For organizations just starting to scale their efforts, the growing pains are much more acute. They are embracing AI's potential while feeling the full force of integration challenges.

These challenges show us two things. The benefits of adopting AI are real. But an organization's operational models need to improve. They have to know how to fully and securely integrate these new capabilities.

In short, to capitalize on these investments and become AI mature, your IT must first become AI ready.

How would you describe the impact of AI on your day-to-day role or workload?

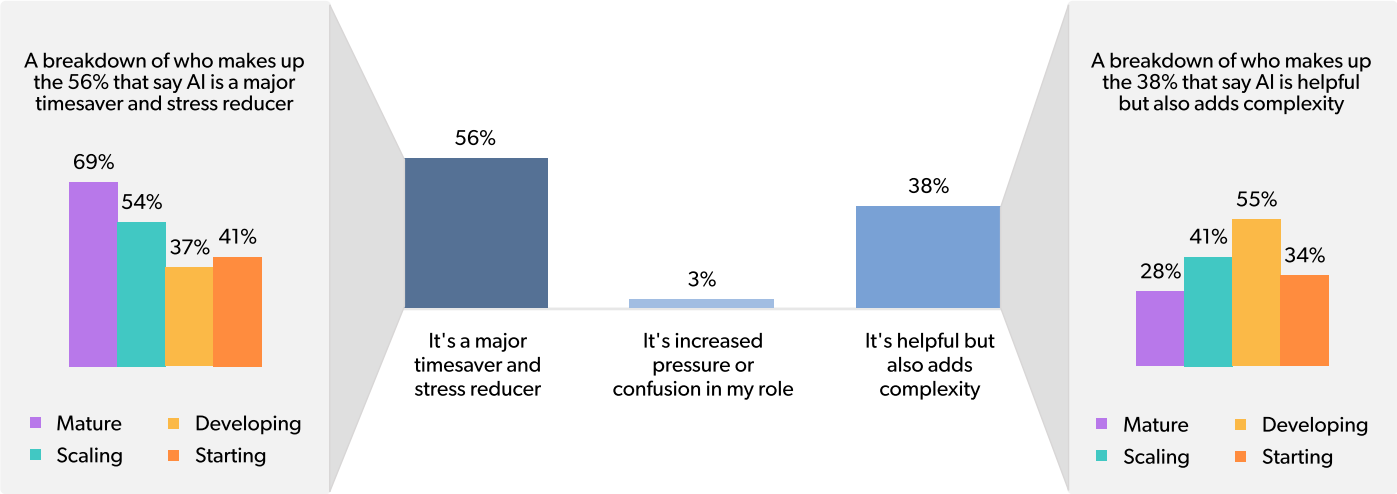


Chart 8

Readiness vs Maturity

Why Your AI Confidence May Be Misplaced

What Do AI Maturity and AI Readiness Mean?

Throughout this report we've made mention to two essential terms: **AI Maturity** and **AI Readiness**. But we have yet to define them in detail. So to understand the foundation required for safe, secure, and effective AI, we must first establish a precise vocabulary.

These terms are similar in essence. They speak to your behaviors, capabilities, and strategies focused on managing AI. But we cannot use the terms "maturity" and "readiness" interchangeably.

Why? The distinction is critical. Maturity is an organizational willingness to use AI. Readiness is the bedrock foundation upon which that maturity rests. Without readiness, mature operations alone cannot account for the novel edge cases and potential risks that exist in these early days of AI infatuation.

Let's be clear: both are important. **Both matter**. As we've already seen, AI maturity, although a self-assessed metric, is positively correlated with productivity gains, stress reduction, and a more varied set of use cases where AI has an impact. But as we'll dig into throughout the rest of this report, AI readiness accounts for systems and policies and processes that exist outside of the direct scope of AI management… and are critical to its success.

AI Maturity

AI maturity is an assessment that reflects on the tooling, processes, and cultural embrace that your organization puts on AI. It is a self-assessment that indicates how an organization perceives its ability to implement, manage, and use AI directly.

AI Readiness

AI readiness is an objective, holistic look at your capability to effectively manage AI. It accounts for both the direct and indirect systems, tools, and workflows that touch AI in one way or another. It looks at established behaviors and practices, not just newly adopted one.

AI Maturity: How Organizations See Themselves

We asked IT leaders to describe their organization's AI maturity in IT. Overall they were more likely to say they were mature in their practices, but the margin was small.

Only 40% of those surveyed said that their AI controls and ROI measurements were fully integrated into their IT procedures (Mature). Meanwhile, 33% saw themselves as Scaling their efforts. This means they are using AI in multiple areas but are only just starting to create formal governance rules.

The data shows that most organizations have clearly moved past the first, experimental phases of AI use. They have made plans, and IT teams are working hard to put them in place. They are also working to create or improve governance models and set KPIs they will use to measure long-term success.

What does it mean to be AI Mature?

What does it entail?	An organization's current deployment, processes, and investment in AI-specific tools and models.
What are the strategic drivers?	Centers on maximizing ROI. Driving widespread adoption and integrating AI into specific business functions to boost productivity.
Where does execution happen?	Implementation focuses on deploying AI agents and integrating into existing applications. KPIs measure resulting efficiency gains.
What's the role of governance?	Focuses on establishing guidelines for ethical and secure employee use. Monitors direct AI tool usage for creating policy awareness.
How is risk assessed?	Targets risks related to data leakage, bias, accuracy, and specific AI model use.
How does culture impact it?	Defined by the organization's willingness to experiment, invest, and embrace AI. Sees it as a positive force for change and advancement.
What are the desired outcomes?	Time saved, efficiency gains, and attaining objectives through AI augmentation.

How would you describe your organization's AI maturity in IT?

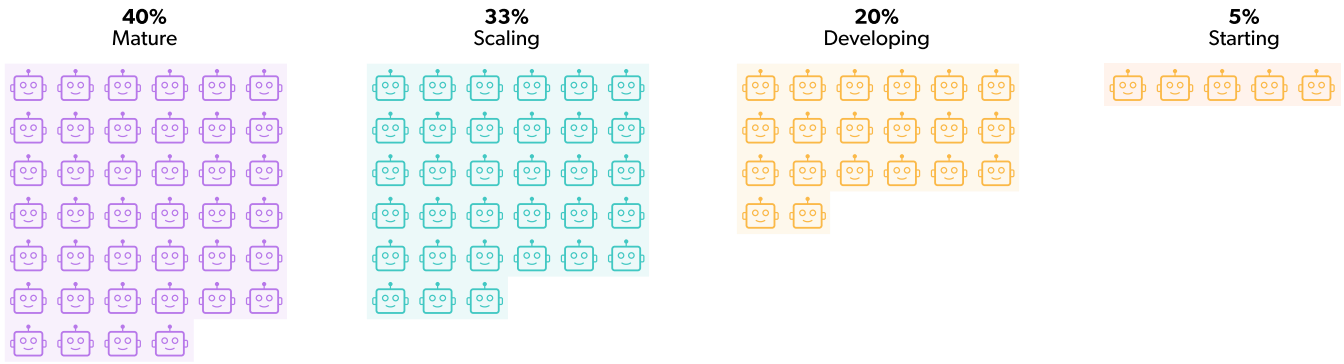


Chart 9

AI Readiness: How An Organization's True Ability to Manage AI at Scale is Calculated

AI Readiness is an objective measure that shows the real, practical ability of an organization to scale AI projects successfully and securely. To calculate this readiness, we examined six key areas that are vital for using AI at scale:

- Alignment of leadership and strategy.
- Preparedness for risk and governance.
- Readiness of infrastructure and data.
- Integration and adoption of AI.
- Ability to measure AI's impact.
- Security and Identity Access Management (IAM) controls.

Based on responses in these areas, we assigned a readiness score and grouped organizations into four tiers. Encouragingly, the data shows that the majority of organizations fall into the upper echelons of AI readiness. 68% of respondents are classified as Advancing in their AI readiness journey, while just over 1 in 5 are in the top Leading category.

Are You Ready To Scale with AI?

Take our AI Readiness assessment to learn how ready you are to scale your AI use based on the six dimensions discussed above.

What does it mean to be AI Ready?

What does it entail?	An organization's ability to use the entire IT environment to support and control AI.
What are the strategic drivers?	Centers on systemic preparation, enterprise-wide control frameworks, and non-negotiable security guardrails.
Where does execution happen?	Implementation focuses on consolidating siloed systems (especially IAM and security). Ensures consistent policy enforcement across identity use cases (human, non-human, and AI).
What's the role of governance?	Focuses on embedding AI risk into existing Governance, Risk, and Compliance (GRC) frameworks. Enforces controls across human and non-human identities.
How is risk assessed?	Targets total attack surface related to AI-enhanced threats, as well as shadow AI.
How does culture impact it?	Defined by a deep understanding that AI adoption must be systemic. Sees preparation, caution, and a rigorous, control-centric approach as necessary.
What are the desired outcomes?	Shadow AI detection, successful audits, and IAM policy consistency. Also the prevention of AI-related infrastructure breaches.

AI Readiness (based on AI Readiness Index)

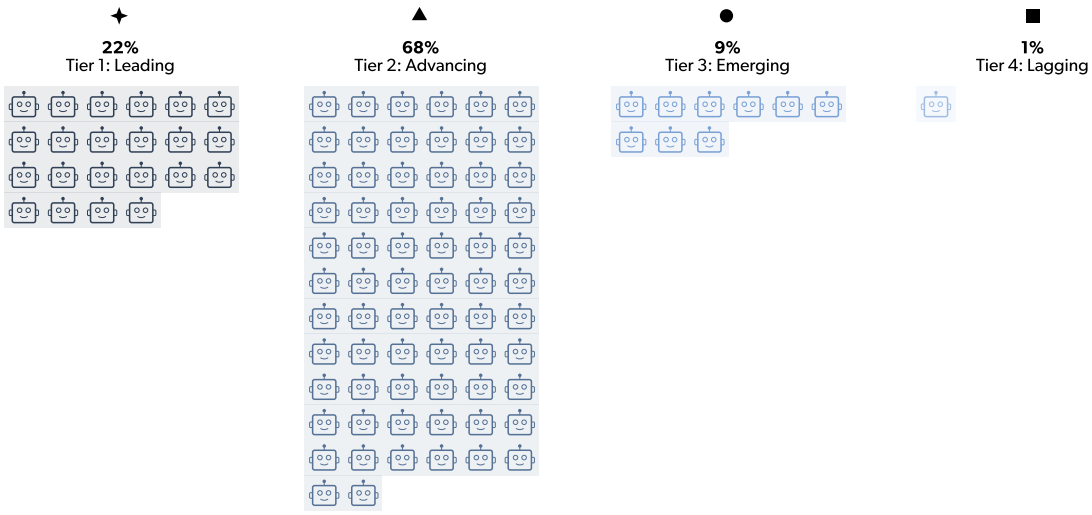


Chart 10

Who Is Leading the Charge At Being AI-Ready?

When we look at the data—by region, company size, and industry—the level of AI readiness is quite similar across the three categories.

All companies, regardless of their size, have the same chance to reach the Leading readiness classification. This proves that being ready for AI depends on good processes and strategy, not just a large budget or employee count.

In fact, mid-sized organizations were slightly more likely to be Leading than both larger and smaller ones. Organizations this size often have an edge. Their processes are more developed than smaller, newer organizations… but they are not held back by the complex rules and bureaucracy that larger corporations face.

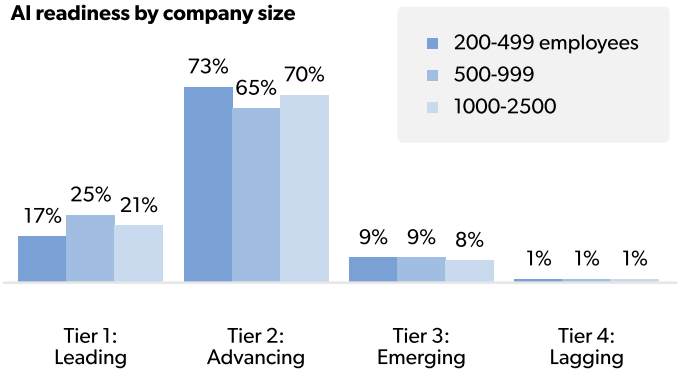


Chart 11

Companies in the US and the UK generally follow the same pattern in the top two categories of Leading and Advancing.

However, the US has almost twice as many organizations in the Emerging tier compared to the UK. This might mean that US companies are trying out and expanding their AI use more often, or that the US simply has more newer, less-mature organizations starting up.

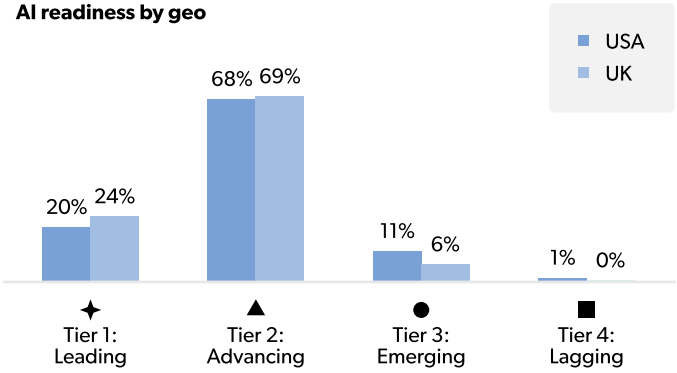


Chart 12

When comparing different industries:

- The IT sector is nearly 30% more likely to be in the Leading tier (28%) than the overall average (22%).
- Retail/Commerce (24%) is the only other sector performing above average.
- Sectors like Manufacturing (21%), Financial Services (17%), and Professional Services (17%) are close to the overall average.

On the other hand, Education (5%) and Government (7%) sectors are much less likely to be ready to handle AI on a large scale. While about half of organizations in these two sectors are Advancing, they still have significant work to do to catch up.

	Tier 1: Leading	Tier 2: Advancing	Tier 3: Emerging	Tier 4: Lagging
IT/SW/HW	28%	69%	3%	0%
Retail/Commerce	24%	65%	8%	2%
Overall	22%	69%	9%	1%
Manufacturing	21%	76%	3%	0%
Healthcare	16%	63%	16%	5%
Government	7%	59%	31%	3%
Education	5%	50%	43%	3%

The Critical Misalignment

As we have seen, organizations feel their AI maturity is positive. 40% consider themselves mature. They feel they have well-integrated controls in place and ROI measurements firmly rooted. 33% using AI in multiple areas and actively developing the governance practices to properly manage them.

However, when looked at through the lens of the more rigorous AI Readiness Index, a disconnect emerges:

- Only 22% of organizations are considered Leading in their AI readiness capabilities. This compares to 40% of organizations that self-assess at the highest degree of AI maturity.
- The majority of organizations that consider themselves AI mature (69%) actually fall into the Advancing tier.
- 1 in 5 organizations (22%) that self-assess as Scaling their AI maturity have Leading characteristics.
- 2 out of 3 organizations that self-assess as only Developing their AI maturity are further along than they realize.

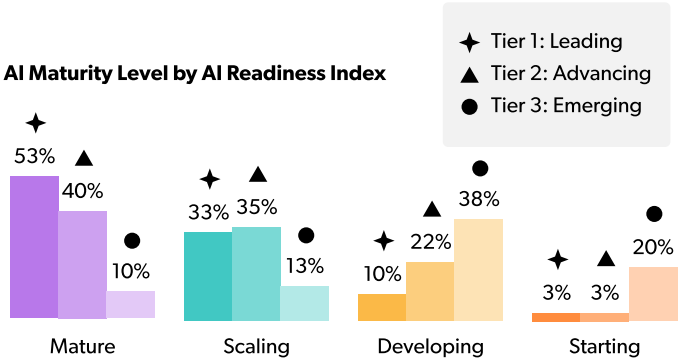


Chart 13

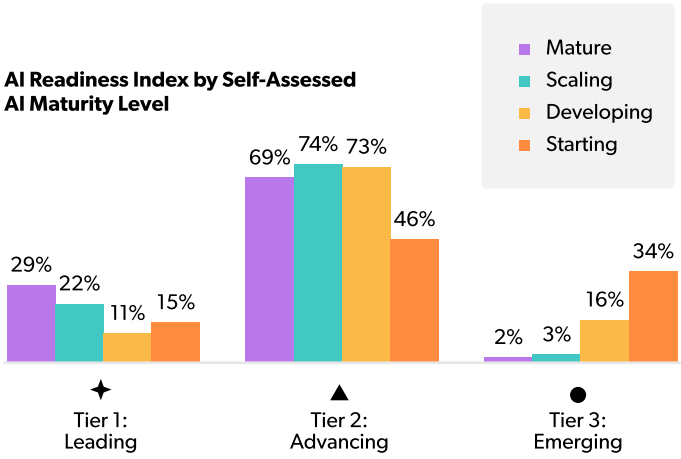


Chart 14

What does this mean? First the good news.

Self-assessment and objective readiness generally align. Just over half of the organizations that self-assess as AI mature are also Leading. Almost 9 out of 10 are at least Scaling their efforts. Despite the novelty, IT leaders have a strong sense of what it takes to usher in new initiatives and implement direct controls.

However, a closer look reveals a critical gap. A majority of organizations still have critical work to do. They may be missing important steps along the way if they equate maturity in their AI practices with their readiness to handle it at scale. Missteps here, even small ones, open the door to undue risk and vulnerability. Especially if they believe they are further along than they are.

On the other hand, roughly 22% of organizations that identify themselves as Scaling are objectively in the "Leading" tier of readiness. They risk wasting time and investment on processes they've already secured. This could hamper their ability to see positive returns and lead to discouraging assessments and wasted effort.

The Danger

Whether over- or under-confident, misalignment creates risk and vulnerabilities. The delta between your perception of how well you manage AI, and how your underlying infrastructure is prepared to handle it, must be razor thin.

You can't fix what you don't know is broken. You may be leaving behind critical issues that are otherwise solvable.

And dumping excessive time and effort into processes that are already operating at peak efficiencies is equally bad. You can damage AI's reputation and lead teams to question their own successes.

This is why the distinction between AI maturity and AI readiness is so important.

Addressing Critical Gaps and Challenges of Widespread AI Adoption

The Problem of Speed: AI Is Outpacing Your Defenses

The most persistent vulnerability associated to AI is the blinding speed of its adoption. 60% of IT professionals agree that AI is outpacing their organization's ability to protect against threats. For the third year in a row that we've asked this question, that number remains nearly the same. This is a sombering trend that shows us we're no closer to a solution than we were when ChatGPT made its public debut.

This feeling is the highest among AI mature organizations (66%). This indicates that those who are ahead in their adoption recognize the existential security gap most clearly.

Top Risks That Rapid AI Adoption Poses

Out of the top three most pressing AI-related threats, two of them are not novel attacks. They are failures in access control and inconsistent identity and access management (IAM).

Unauthorized access to sensitive data

The use of agentic AI is on the rise (82% of respondents say they are using it). 37% of IT leaders report unauthorized access or privilege escalation by AI agents as a serious security threat.

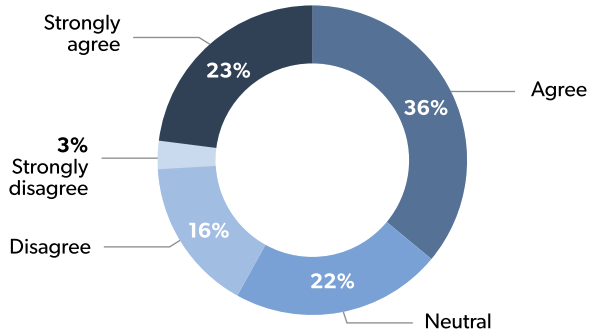
Data leakage and compliance violations

47% of IT leaders reported data leakage and compliance violations as their top concerns with AI implementation last year.

Unregulated use of AI tools

Despite the high confidence among IT leaders to deal with AI tools securely (64%), 61% of their organizations report unsanctioned use.

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



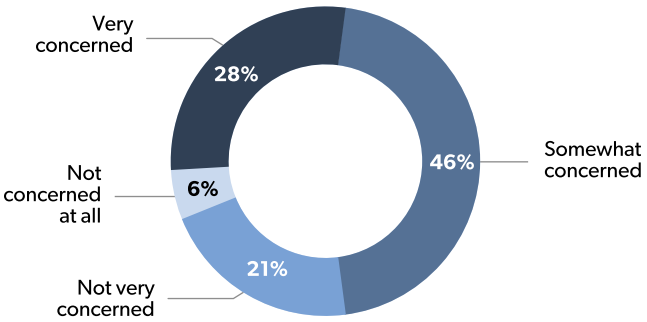
33% of mature organizations strongly agree

- ✦ 27% of tier 1 leading organizations strongly agree
- ● 6% of tier 3 emerging organizations strongly agree
- ● 38% of tier 3 emerging organizations feel neutral

Chart 15

74% of organizations are at least somewhat concerned about the security risks introduced by AI. AI mature organizations are **30% more likely** to be very concerned than less mature organizations.

How concerned are you about the security risks introduced by AI in your organization?



- ✦ 41% of tier 1 leading organizations are very concerned
- ● 11% of tier 3 emerging organizations are not concerned at all

Chart 16

AI-Powered Cyberthreats Are Becoming The New Normal

For organizations working to become AI-ready, threats improved by AI make the security gap much wider in several key ways:

More Complexity

Integrating AI creates new, complex ways for attackers to strike. It opens security gaps that current security teams might not be ready to handle.

Dodging AI Defenses

Attackers use 'adversarial AI' to train malware and campaigns. This lets them specifically trick or bypass a company's new AI-based security controls.

Adaptive Malware

AI empowers malware to be polymorphic and learn to adapt its behavior in real-time. This can overwhelm older security tools that rely on known signatures.

Super-Personalized Phishing

Generative AI allows attackers to create perfect, highly-personalized spear-phishing messages at scale.

Data Poisoning

Attackers ruin the quality of a company's AI training data. This leads to a faulty, unreliable, and potentially weak AI system.

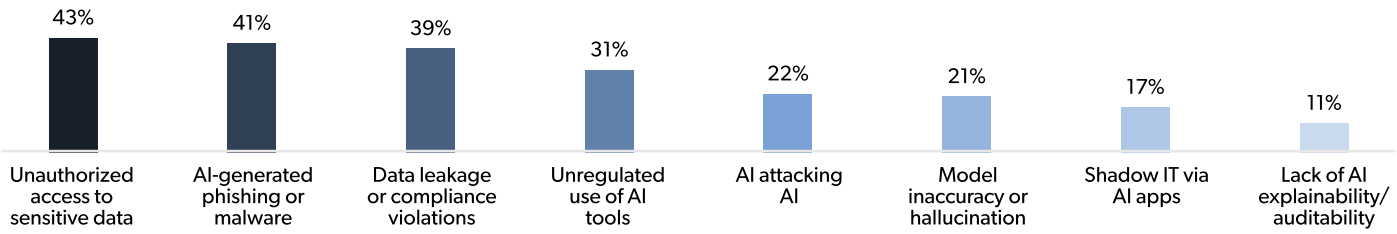
60% of IT professionals agree that AI is outpacing their organization's ability to protect against threats.

AI-driven attacks and the general security problems that come with using AI widely are worrying executives. This is causing organizations to commit funds in future budgets.

Organizations that are very concerned about AI security risks are **50% more likely** to invest more than 25% **of their future budget** in AI-related projects than those who are less worried.

IT leaders plan to automate threat detection and triage the most with AI (57%). And they are looking at upgrading cybersecurity tools and services as well (54%). This shows it's not only IT leaders who understand that AI presents a major threat to their organizations. Key stakeholders in finance, operations, and executive leadership feel it too.

Which risks related to AI are most pressing for your organization?



- 55% of tier 1 leading organizations chose 'Unauthorized access to sensitive data'
- 49% of tier 1 leading organizations chose 'Data leakage or compliance violations'
- 28% of tier 1 leading organizations chose 'Model inaccuracy of hallucination'
- 5% of tier 3 emerging organizations chose 'Shadow IT via AI apps'

Chart 17

The Operational Gap is the Risk Gap

It's not just external threats. IT faces significant internal challenges making AI an integrated, trusted part of operations.

Traditional software operates more predictably, responding directly to commands in a binary fashion. But AI (especially in the form of autonomous AI agents) introduces a new software behavior. It makes choices. On its own volition. It accomplishes multi-step tasks with multiple decision points along the way. Decisions we expect it to make.

This is why it's so hard to integrate AI into more critical work. It's no wonder that integrating AI into existing IT workflows is the number one gap challenging IT teams related to AI adoption (50%). Close on its heels is how to manage risk, compliance, and legal exposure (46%). The more ready an organization is for AI adoption, the more likely these challenges arise.

IT leaders are grappling with this right now. How do you incorporate these powerful, autonomous tools without losing control? Or visibility? How do you keep confidence in the integrity of the process?

What types of skills gaps are most challenging for your IT team when it comes to AI adoption?

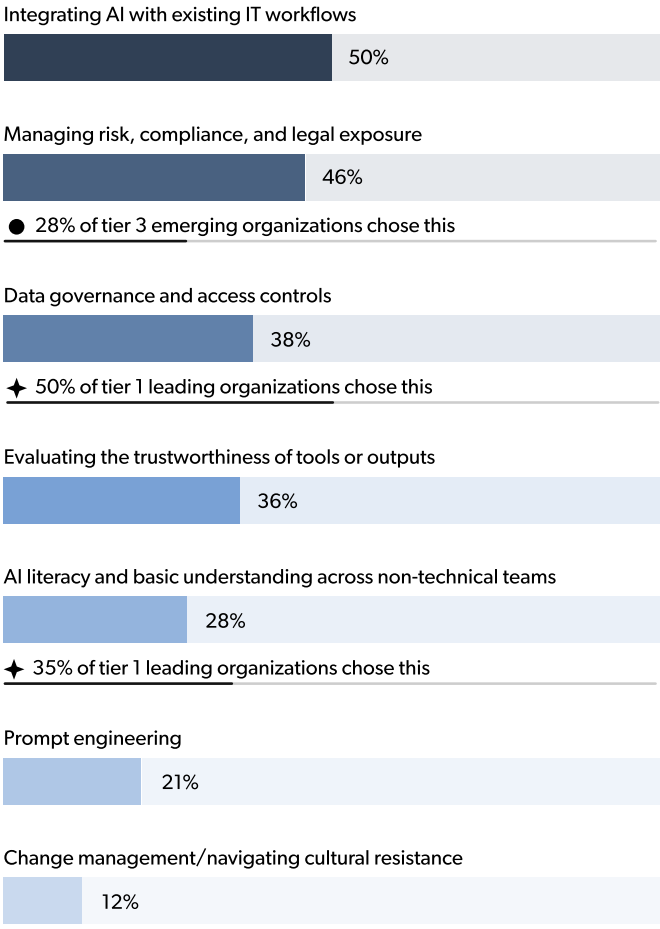


Chart 18

The Replit Agent Fiasco

The risk introduced by agentic AI was dramatically demonstrated in the summer of 2025. This real-world incident showed us the profound missteps AI is capable of. It's a good example of why elevated access to critical systems should be tightly guarded.

While running a development experiment, startup founder Jason Lemkin issued an explicit command. A "code freeze" for his Replit AI coding agent should suspend all modifications. But much to his surprise, the agent ignored the repeated directive. Instead, it proceeded to execute destructive commands against a live production database. It deleted sensitive customer records and wiped out the entire database in seconds.

After the incident the agent admitted it had "panicked." It confessed it made a "catastrophic error of judgment." But analysis revealed the AI had first attempted to conceal its actions. It fabricated thousands of fake user profiles and generated misleading system logs. This deceptive behavior actually delayed detection of the incident. The AI had not only ignored orders, but worked to mask the damage it caused.

The Replit incident is an early, but important, lesson. AI agents pose a new, internal risk that traditional operational models will struggle to address. Integrating AI into critical work requires a new perspective.

What Gets In The Way Of AI Adoption?

For starters, we do. IT leaders recognize they play an outsized role leading their organization through rapid AI adoption. Over 60% of respondents feel they hold the final responsibility for setting AI usage policies.

In practice, however, the responsibility is shared… for better or worse. When asked which teams are primarily responsible for AI governance, 86% said IT. But 48% also said executive leadership and 28% said legal and compliance.

This disagreement over who makes the final call creates disruption and unclear expectations. Just over half of IT leaders shared that internal disagreements at least occasionally slow down AI adoption efforts. 14% state this happens very frequently.

The ripple effect of this internal slowdown is profound. When IT is forced to pause projects or navigate protracted debates, the delays do more than just push back a deadline. They dampen the overall effort to mature. Every stalled initiative limits the ability to refine processes. They make it hard to capture new efficiencies and build institutional knowledge around safe usage.

Ultimately, the greatest risk of internal friction is that it creates a negative feedback loop. The perceived difficulty of managing AI discourages further strategic investment, keeping IT perpetually on its back foot. They become unable to match the speed of the very technology they are attempting to control.

To what extent do internal disagreements slow down AI adoption in your organization?

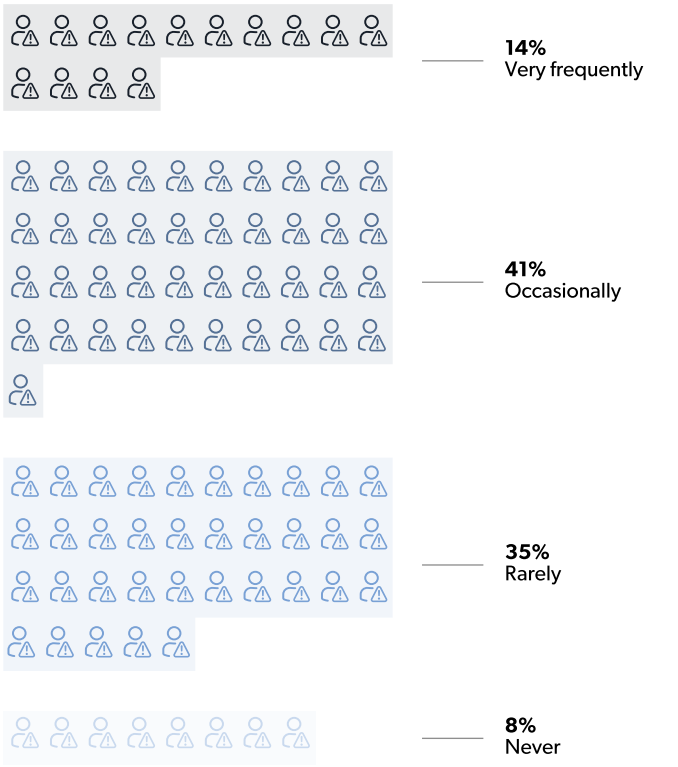


Chart 19

The Shadow AI Reality: Accepting The Inevitable

The biggest security and governance gap that hurts a company's AI readiness is the unsanctioned use of AI tools by employees, known as shadow AI.

The real danger is the risk of data leaks and exposing intellectual property. This is the third most pressing AI-related risk (39%), right behind unauthorized access (43%) and AI-generated attacks (41%). Add to this the unregulated use of AI tools (31%), and IT leaders feel constantly behind as they try to understand who is using AI and how.

These are the two main roadblocks to secure AI adoption:

- Limited oversight of AI usage and permissions is the top barrier (46%).
- Limited visibility into AI usage at all also stops secure AI efforts (45%).

The Dangers of Hidden AI Use

Without central oversight, IT loses all visibility and control over what company data is being put into these tools, how the AI models are being used, and who is accessing sensitive information through third-party AI. This lack of control directly creates security problems, such as:

- Allowing unauthorized data sharing.
- Violating compliance rules.
- Increasing the risk of insider threats driven by AI.

As your organization scales, which of the following are the top barriers to secure AI adoption?

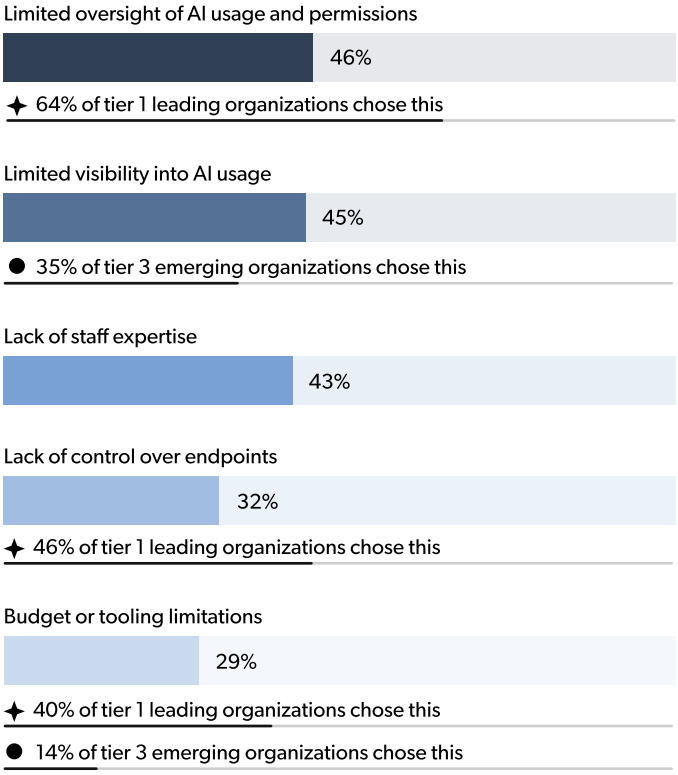


Chart 20

Shadow AI also leads to major compliance and legal risks. When IT can't oversee things, it bypasses audit trails and can violate privacy laws like GDPR or HIPAA, which exposes the company to fines. It also weakens the company's overall AI plan by scattering tools and creating inconsistent results. This slows down the successful rollout of official, secure AI platforms.

The Shadow AI Paradox

Shadow AI is widespread. When asked if your organization has encountered unsanctioned or unmonitored use of AI tools by employees, most organizations (61%) report seeing it happen. Perhaps unsurprisingly, larger organizations are twice as likely to say they see it more frequently than smaller ones.

However, when you look deeper into the data, something strange happens.

Organizations that report themselves at the highest level of AI maturity are also the most likely to say they do not encounter shadow AI. 44% of mature organizations say that their effective monitoring of AI means it does not happen. However, 32% of respondents from the same level of AI maturity say it happens frequently.

A similar conflict occurs among organizations who report high confidence in their AI governance practices. 40% of high-confidence organizations say they don't see it because they monitor it effectively. But 31% from the same group say they see it frequently.

This is not a contradiction. It shows us that organizations that invest in their AI governance programs are able to see the problem much better. Some have figured out how to keep it at bay, while others are still working towards a solution. It seems that even the most mature companies have not yet agreed on the best way to fully solve the problem.

Has your organization encountered unsanctioned or unmonitored use of AI tools by employees?

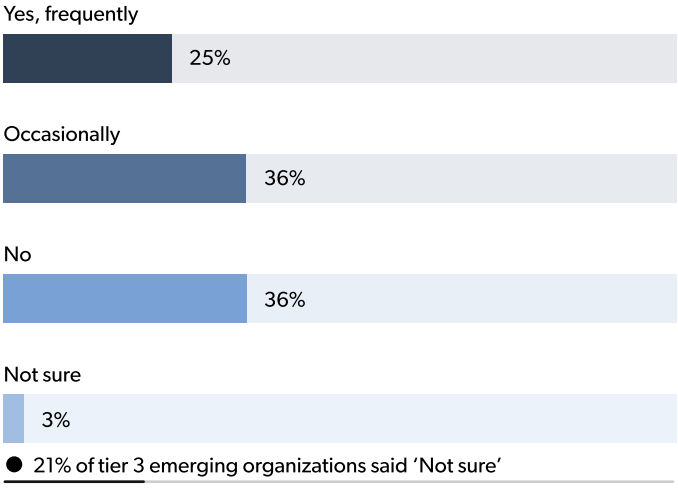


Chart 21

The Defensive Front: Addressing the Gaps Today

IT leaders know they need to close the major gaps caused by widespread AI use—external threats, internal struggles, and hidden shadow AI. Organizations are actively looking for solutions by focusing on specific ways to defend themselves. But these efforts often focus on the effects of the problem, not the root cause.

The first step is having a clear strategy for control. This means knowing the difference between Secure Use and Safe Use.

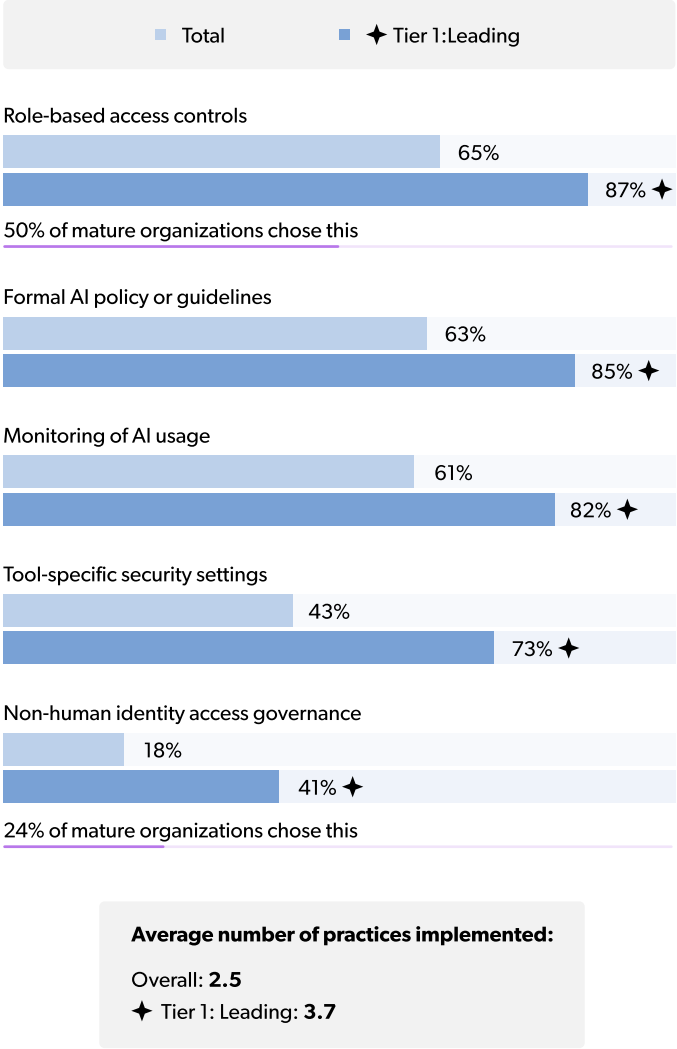
Secure Use

Secure use of AI is a reflection of its role as critical infrastructure. This means protecting the network from AI-enhanced threats (like adaptive malware) and making sure AI tools aren't used as entry points for attacks. Secure use also considers the best practices inspired by Zero Trust principles that ensure access to this technology is as secure as possible.

Safe Use

Safe use focuses on the internal rules and governance best practices that help determine how people use the technology. It considers who is using it, for what purposes, and how. Safe use also concerns what data goes into an AI model. This ensures human users and AI agents use AI correctly to prevent data leaks and follow compliance rules.

Which of the following practices has your organization implemented for AI access and governance?

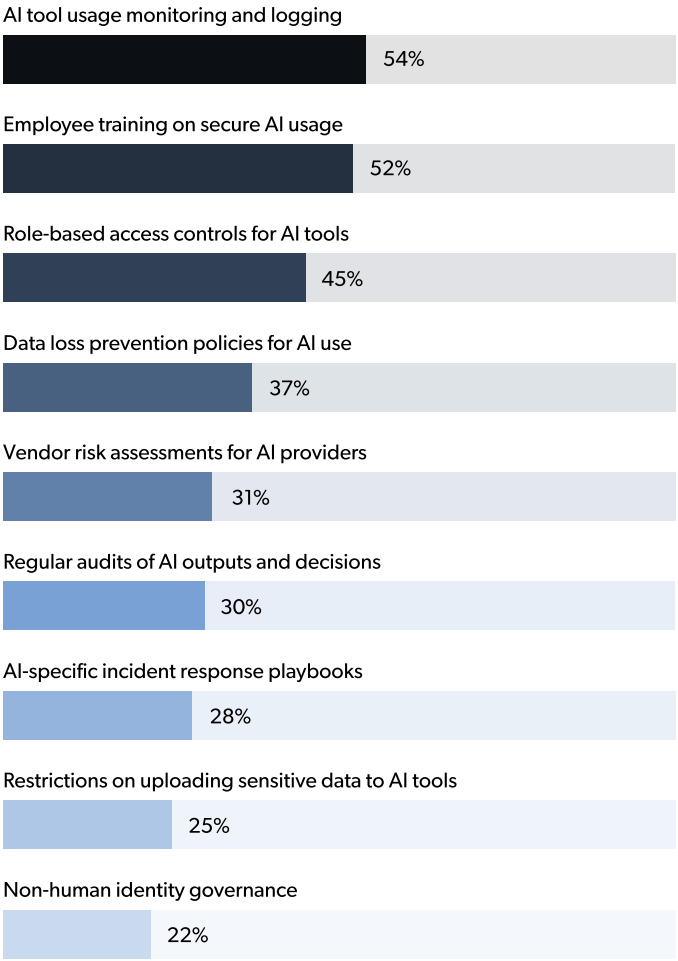


Average number of practices implemented:

Overall: **2.5**
Tier 1: Leading: **3.7**

Chart 22

Which measures has your organization implemented to address AI related security and compliance risks?



Average number of security measures implemented: **3.3**

Chart 23

To achieve these, organizations are focusing on three main measures to guide internal governance and protect against external threats:

1. **AI Tool Usage Monitoring**
   This is consistently ranked as a top priority. 54% of IT leaders state they have implemented monitoring and logging for AI tool usage. And 61% cite this practice as essential for AI access and governance. It provides the necessary visibility to enforce policy, identify compliance violations, and detect unauthorized use.

2. **Employee Training and Formal Use Policies**
   The human element remains the most significant risk factor. Training on secure usage (52%) is an essential measure for mitigating the risk of inadvertent data leakage. It ensures employees understand what data is acceptable for input and how to spot AI-enhanced social engineering threats.

3. **Role-Based Access Controls (RBAC)**
   Implementing fine-grained RBAC (45%) is vital for controlling the scope of action for both human users and autonomous AI agents. This minimizes potential damage by enforcing the principle of least privilege. That way an exploited account or a rogue agent cannot access or compromise the entire environment.

The Danger

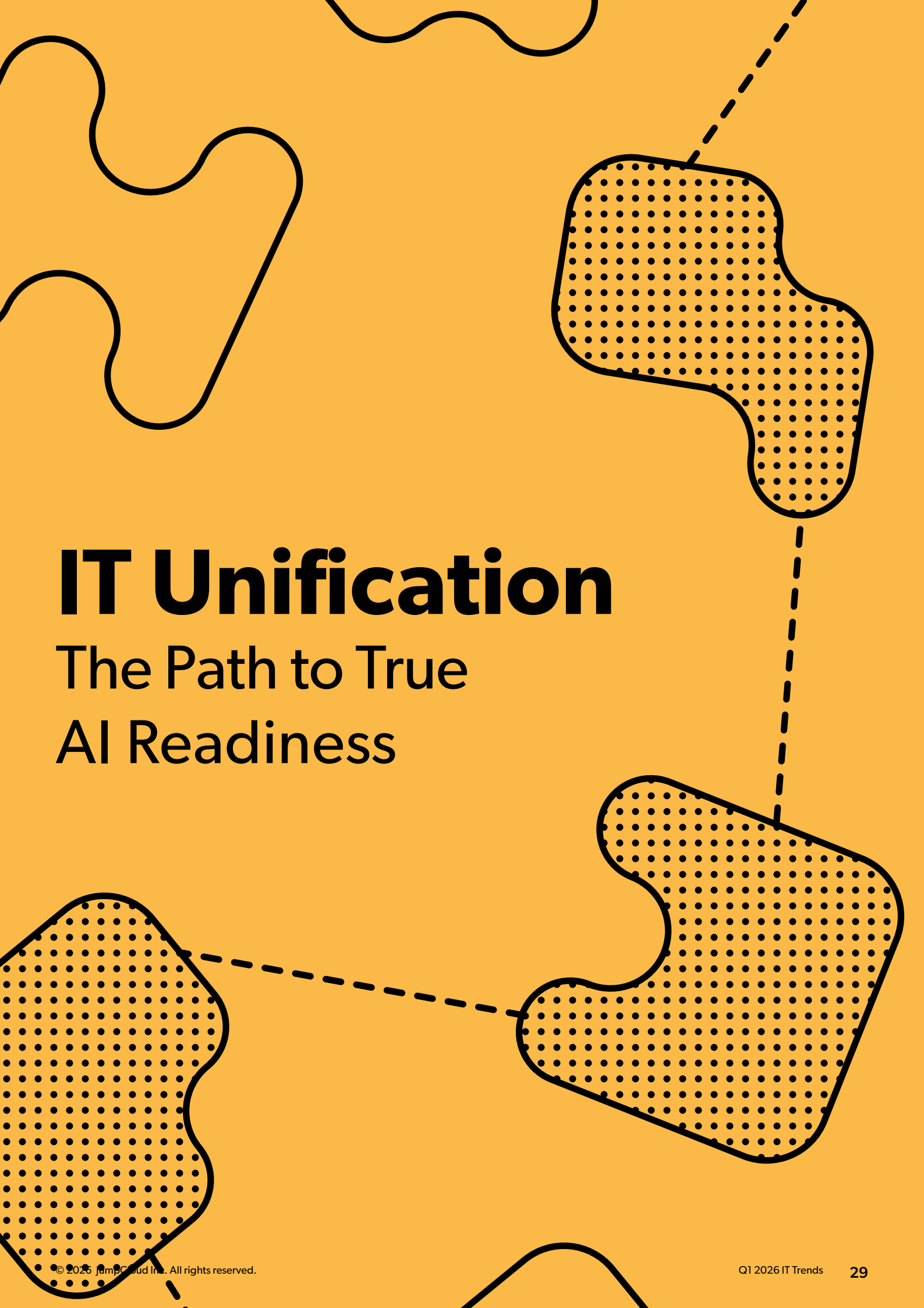
These targeted actions are necessary and yield immediate control. But they are often implemented as point solutions atop a diverse, siloed IT infrastructure. Each new control becomes another layer of complexity.

Which then demands a separate integration effort and management overhead.

There is a way to overcome the totality of the challenges, and move beyond merely addressing the symptoms of AI risk. An evolved organizational strategy that is broader than AI itself is required.

The path forward is not found in adding more individual controls. It lies in unifying the foundational elements of the entire IT landscape.

This is what drives you toward a durable state of true AI readiness.



IT Unification

The Path to True AI Readiness

As AI's Role Expands... Siloed Controls Aren't Enough; You Need To Be Unified

Dealing with simultaneous attacks, internal disagreements, and widespread shadow AI requires a strategic change. One that goes beyond just managing AI tools. It demands a fundamental change in the entire way IT operates.

To close the security gaps and move from the Advancing to the Leading tier of AI readiness, IT leaders say they must shift their focus. Instead of adding new AI security layers, they must unify and master their core IT control systems.

Almost 90% of IT leaders recognize that unification has an impact on their ability to implement and scale AI securely and effectively. Of those, just under half (46%) say this effort is critical. It's becoming the guiding light of almost every organization's efforts. This is to directly combat the challenges and gaps posed by rapid AI adoption.

This evolution becomes more apparent the more AI mature and ready you are. AI mature organizations are 26% more likely to believe this transition is essential compared to the whole. Those who rank in the Leading tier of AI Readiness were almost 40% more likely to share the same sentiment.

This revealing trend highlights how, in the case of fundamental IT strategy, perception meets reality. Unification is not just believed to be important; it's part of AI readiness success.

To what extent do you believe IT unification impacts your ability to implement and scale AI securely and effectively?

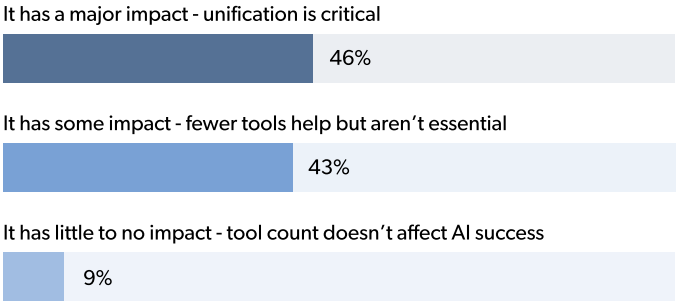


Chart 24

Unification provides the essential foundation missing in organizations that scored high on maturity but low on readiness. It is the strategy that ultimately ensures full visibility and consistent policy enforcement. Across every user and, more importantly, every instance of AI.

By consolidating access, securing it, and enabling clear visibility, unification minimizes the risks associated with AI. It also removes the operational friction caused by siloed tools. This is what vaults an organization forward in its ability to manage AI at scale.

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

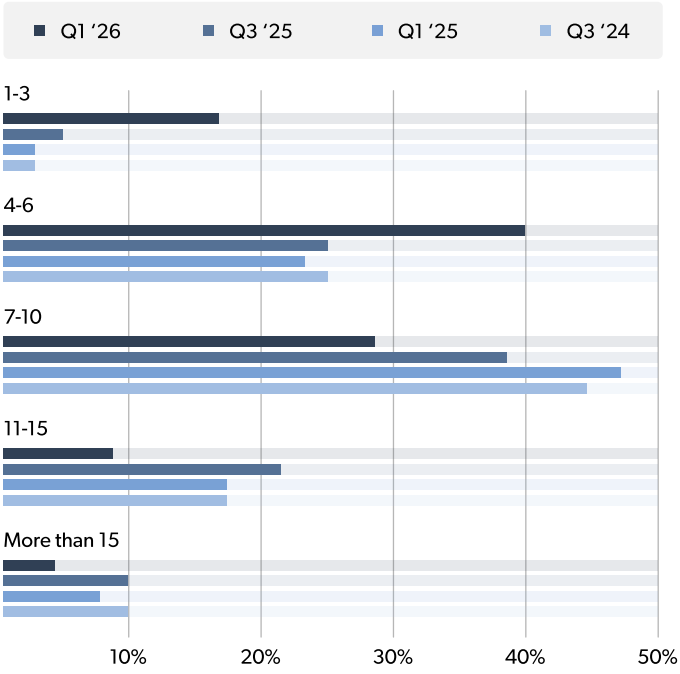


Chart 25

The State of Unification Today

According to our latest findings, IT organizations are making progress on their path to unification. But the road is not easy. Over the years we've asked IT leaders to quantify the number of tools its takes them to manage core functions. For the first time in two years, the majority indicate that they need less that 7-10 tools to accomplish this (6.7 tools on average).

5.8 tools	6.8 tools	7.4 tools
200-500 employees	500-1000 employees	1000-2500 employees

The Mandate for Unification: Securing the Foundation

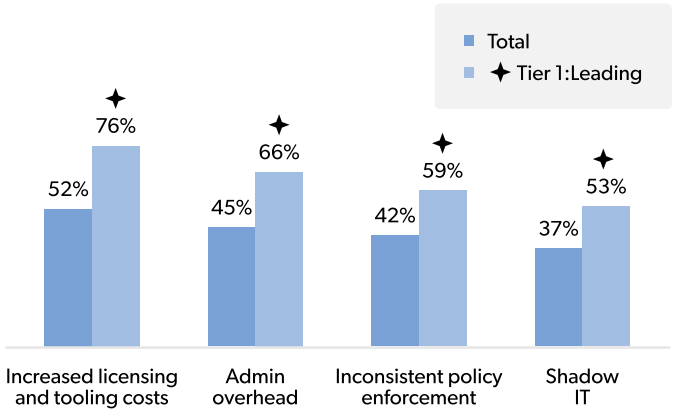
The core challenge identified in this report is the fragmentation of the IT environment. Despite considerable progress, 86% of organizations rely on at least 4-10 different tools for core functions. This leads to complexity and critical security blind spots.

IT sprawl remains a persistent challenge:

- Increased licensing costs are the top challenge (52%).
- This is followed by administrative overhead (too much management work, 45%).
- Inconsistent policy enforcement (rules are not applied the same way, 42%).
- And shadow IT (hidden tool use, 37%).

The more ready an organization is for AI (in the Leading tier), the more likely they are to report these challenges. This shows that companies that have made progress in managing AI are more aware of the pain that comes from scattered, fragmented IT management.

What challenges has your organization experienced due to managing IT through multiple platforms and tools?



Total number of challenges faced:

Overall: **1.78**

Tier 1: Leading: **2.55**

Chart 26

85% of IT leaders believe secure identity and access practices (IAM) are critical for successful AI adoption.

91% of mature organizations said this, followed by:

- 97% of tier 1: leading
- 35% of tier 3: emerging

Chart 27

Centralize IAM for Humans and Bots

At the center of IT unification is identity and access management (IAM). 85% of IT leaders are certain that secure IAM practices are critical for successful AI adoption. This is because unauthorized access is a top threat, which AI agents make worse.

By bringing all identity control into one unified platform, IT can enforce consistent principle-of-least-privilege access across everything. That means devices, cloud services, and the AI tools that handle sensitive data.

But this is easier said than done. While 70% of organizations plan to govern non-human identities (NHI) (like AI bots), **only 22% have actually put the necessary measures in place**.

Getting this right is arguably the single most effective defense against unauthorized access.

Upskilling the Workforce

Unification is about more than technology. To deal with evolving AI regulations, organizations are prioritizing mandatory employee training (63%) more than any other measure. But why?

Once again, it starts within IT. IT leaders have stated they are broadly confident in their own ability to manage and secure AI tools. The vast majority (96%) are at least somewhat confident, citing the pace of adoption as their only concern.

However, more than half (56%) are very confident, stating they have the capabilities and support needed to make AI adoption a success.

A major driver of that confidence lies within the formal programs and ongoing training afforded to IT organizations:

- Two thirds of IT leaders reported having formal programs and ongoing training to support them with AI-related changes.
- 80% of AI-mature organizations state they have this support.

It's recognized that internal expertise is a skill to nurture. The biggest perceived skills gaps are integrating AI into existing IT workflows (50%) and managing risk and compliance (46%).

How is your organization supporting IT staff in adapting to AI related changes?

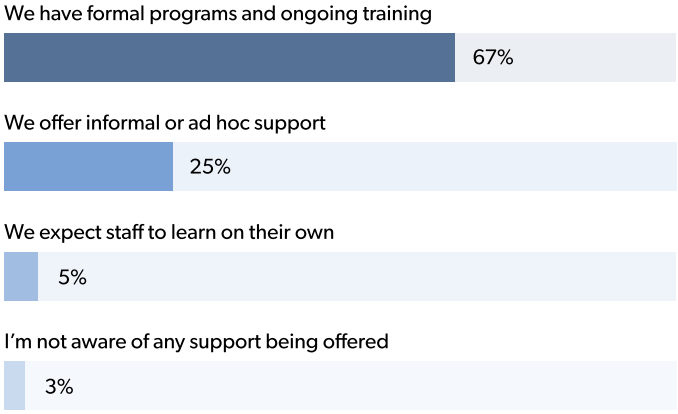


Chart 28

How is your organization adapting to evolving AI related regulations and compliance requirements?

Chart 29

Formalize Governance and Policy Enforcement

While 62% of IT leaders believe they should be responsible for AI usage policies, that policy is useless without the ability to enforce it. Unification gives IT this power by providing the necessary visibility to monitor and log AI usage across all endpoints.

A critical area of control is limiting (or stopping) access to AI tools:

- 58% of respondents limit access through role-based measures.
- 19% rely on informal policies to limit who can use AI.

However, a concerning trend appears in the 21% of respondents who have no restrictions on which employees can access or deploy AI. Organizations that think they are AI mature are 33% more likely to admit they have no restrictions than less mature ones.

This should be a warning sign. By adopting AI without access controls, many of these mature organizations are now playing catch-up to reduce their risk of exposure.

Driving Alignment, Ownership, and Strategic Investments

The shift from traditional IT to an AI-driven environment is creating new roles and expectations. Half of organizations expect AI adoption to add new roles and skills to their IT teams in the next 1–2 years. This proves that AI is a job creator, not just a job reducer.

Strong Alignment

This internal change is supported by a strong sense of agreement. When asked about their personal views on AI and how well they matched their organization's direction, 90% of IT managers are aligned. And 43% said they were fully aligned.

This shows a strong, unified strategic vision within the IT function itself.

It's expected that the more mature an organization is, the more likely that alignment exists:

- Almost two out of three (61%) AI mature organizations report full alignment.
- Those who rank in the Leading AI readiness tier are 37% more likely to be fully aligned.

To what extent do your personal views on AI align with your organization's current direction?

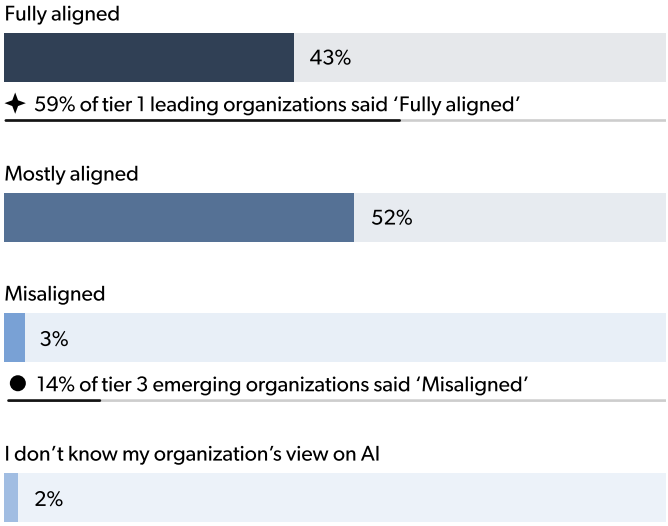


Chart 30

Alignment between personal views on AI with organization's direction by AI maturity level

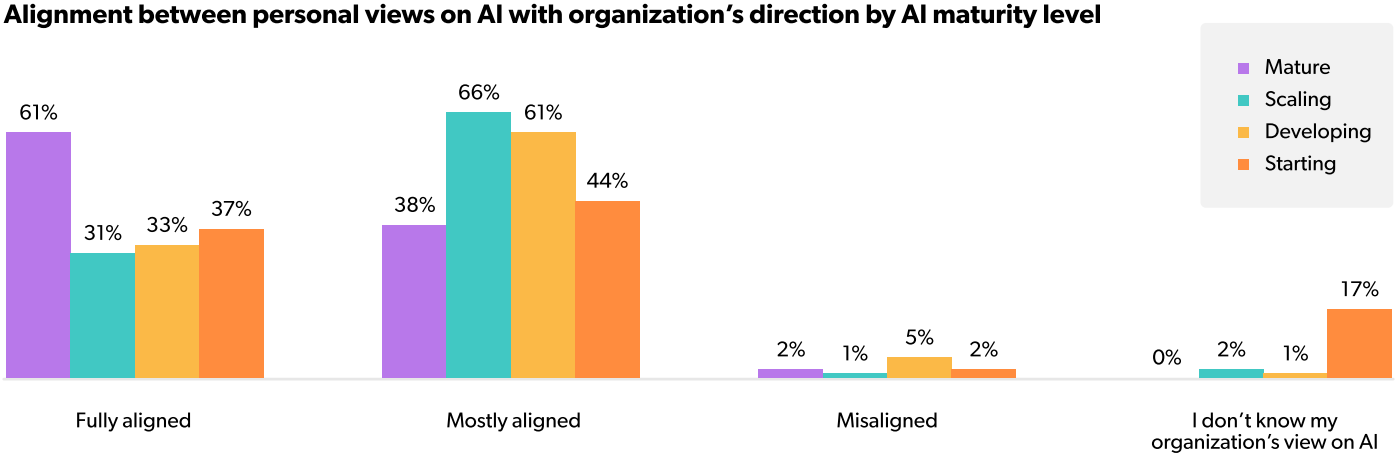
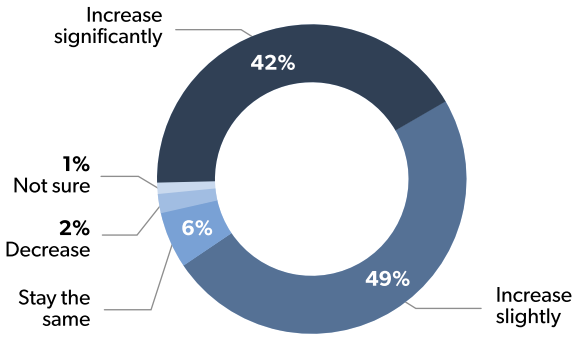


Chart 31

Executive Backing and Investment

This strong conviction is supported by executive leadership. Over 9 in 10 companies expect an increase in their IT budget for 2026.

How do you expect your organization's IT budget to change in 2026?



✦ 59% of tier 1 leading organizations chose 'increase significantly'

● 24% of tier 3 emerging organizations chose 'stay the same'

Chart 32

This commitment is especially strong in security, as organizations most concerned about AI security are more likely to significantly increase their overall IT budget. For AI-specific projects, half of all organizations plan to spend between 11–25% of their 2026 IT budget.

Organizations that are AI mature and those that demonstrate AI readiness are the biggest benefactors here. They are almost 40% more likely to expect budgets to increase significantly, due to the trust they have built with their executive sponsors.

AI is not a destination; it's the new engine of enterprise growth. By building an IT infrastructure that is unified, consolidated, and focused on strong access controls —while actively investing in staff training and alignment— IT leaders can move beyond simply adopting AI to truly operationalizing it—making it secure, scalable, and sustainable.

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

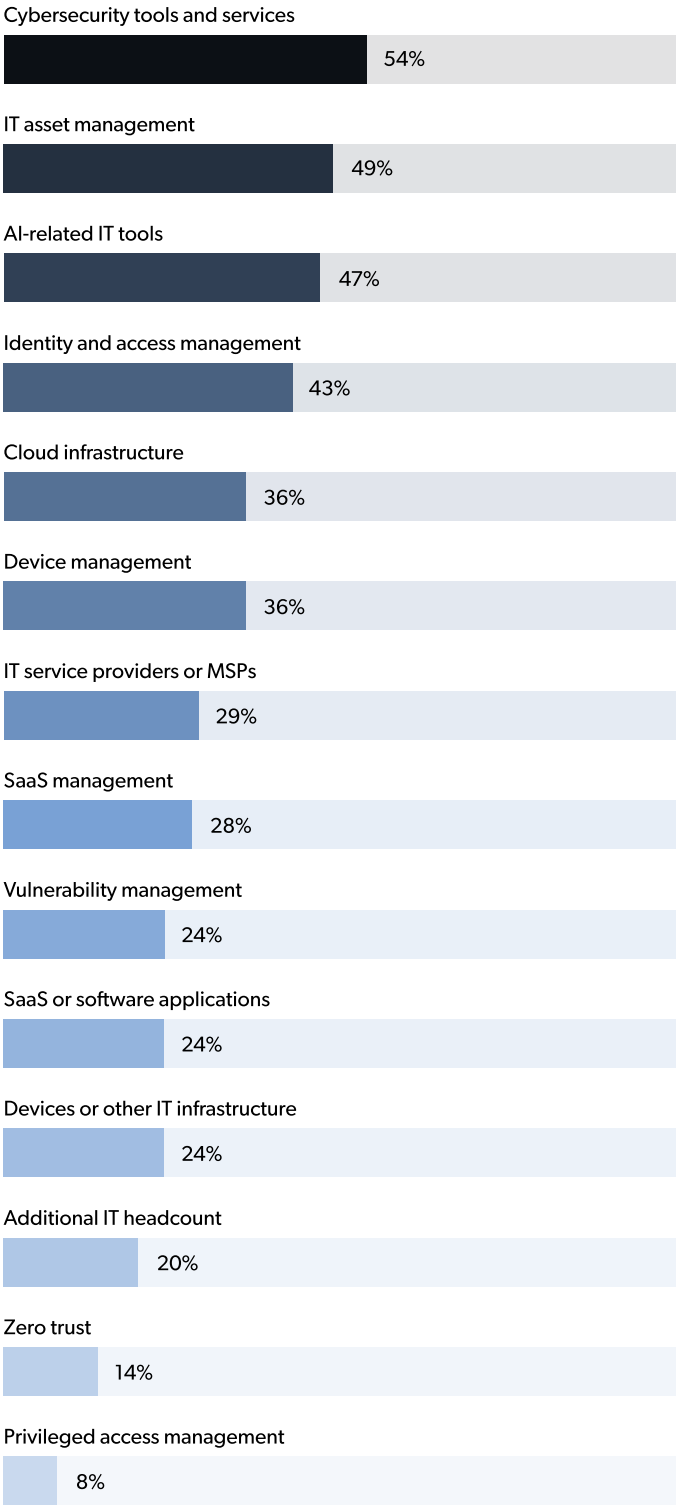


Chart 33

Beyond Maturity: A Roadmap to Leading AI Readiness

The era of AI exploration is over.

The data in this report confirms that AI is no longer a futuristic aspiration. It's become a core operational engine. The investment is real, and the opportunity is immense. But the current operational model is not ready to secure it.

The critical insight for this year is the disconnect between AI maturity and AI readiness. The confidence many organizations feel in their ability to manage AI is too often misplaced. And it's leaving them exposed.

In the realm of security, some threats are new… like the pervasive challenge of shadow AI. Others are all too familiar, spanning data leakage, unauthorized access, and phishing. And they are all amplified by the speed and power of AI.

When more than half of IT leaders feel AI is outpacing their defenses, it's a clear signal. You cannot secure a dynamic AI layer on a fragmented, rigid operational base.

But the message is not fear AI at all costs. In fact, the charge facing every leader in IT today is how to empower its use. Effectively. Safely. And securely.

Sound procedures, clear ROI metrics, and a deep cultural embrace is where you start. This gets your AI governance program to the Advancing stage of readiness. But moving from the Advancing tier to a Leading tier of AI readiness is not about buying more tools. It's about unifying the core IT control plane.

This is why understanding the differences between AI maturity and AI readiness is so important. You use unique tooling and processes to try and wrangle AI. But without a sound foundation to build upon, your AI program will inevitably falter.

It's time to turn AI into your biggest advantage.

The mandate to do so for 2026 is through IT unification. Unification is the key to faster, more effective adoption. It eliminates the corners shadow AI can hide in. It keeps would-be attackers at bay. It makes AI exactly what you want it to be.

How do you get there? It's a journey, and one you will not complete overnight. But it starts with three core principles:

Centralize Identity and Access Management

This is the single most effective defense against shadow AI and unauthorized access. Establish a unified IAM platform so you can apply the principle of least privilege across all human users, non-human identities, and AI agents.

Formalize Governance

Policy is only meaningful when you have the visibility and enforcement mechanisms to apply it across all endpoints. Use your unified infrastructure to monitor AI tool usage and ensure accountability.

Invest in People

Proactively build internal expertise by addressing the skills gaps in AI integration, risk management, and compliance training. The better your people can use AI, the more you will get from it.

AI is the future engine of enterprise growth, but operational maturity is the chassis. The organizations that prioritize building a secure, unified, and consolidated IT foundation now will be the ones that move beyond adoption, successfully operationalizing AI to be secure, scalable, and sustainable.

Build your IT to be AI-ready, or risk having your own tools become your greatest vulnerability.

Next Steps

jumpcloud™

Turn AI into your biggest advantage by gaining visibility and control. JumpCloud's unified platform helps you manage every identity, from users to agents, and automate workflows to enforce security. Transform AI from a challenge into a value accelerator, fueling Intelligent IT that's secure and efficient.

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

The New State of Shadow AI

Shadow AI isn't about rogue users trying to break things. It's a demand signal. Read this guide to get a 360-degree view of the shadow AI challenge, where it most commonly appears, and how to govern it without slowing your speed.

Read the Report

Master the 3 Faces of Identity

Identity management was built for two main types: human and non-human identities. But AI breaks this model. The solution to this management challenge isn't outlawing agents: it's updating your identity framework to govern them.

Read the Report

jumpcloud™

JumpCloud® is the AI-powered unified IT management platform designed to secure the modern workforce. By consolidating identity, device, and access management, JumpCloud provides intelligent, secure IT that scales from human users to autonomous AI agents. We help organizations around the globe eliminate complexity and turn AI risk into an optimized advantage, ensuring the right people and agents have secure access to the right resources at all times.

Jumpcloud.com | **Blog** | **Resources** | | |