

Path to the Autonomous Digital Workplace

How organizations can move from
AI-powered tasks to AI-driven workplaces





How to read this report

This report uses several terms to distinguish between survey findings, workplace groups and different levels of AI-enabled action.

AI assistance: AI supports a task initiated by a person, such as summarizing information, generating ideas or analyzing data. A person reviews the output and decides how to use it.

Autonomous action: AI identifies a need and takes action without requiring direct approval each time. These actions remain subject to defined permissions, guardrails and escalation rules.

Autonomous workplace: a work environment that uses AI agents to sense, decide, act, and continuously learn — driving autonomy across people, technology, and work to accelerate business performance.

Autonomous IT: an application of the autonomous digital workplace in which AI agents detect and resolve current or predicted technology issues with progressively less direct human intervention. People remain responsible for governing the systems, defining guardrails and managing exceptions.

Autonomous systems: AI-enabled technologies capable of making decisions or taking actions with progressively less direct human intervention.

Employees: refers specifically to non-management employees surveyed. When this report compares employees with managers, employees should be understood as this non-management group.

Generative AI: refers to AI systems that create new content, such as text, images, code, summaries, recommendations or ideas, in response to prompts or other inputs. In this report, it is most often associated with AI assistance, where a person initiates the task, reviews the output and decides how to use it.

Guardrails: the permissions, limits and rules that define what an autonomous system may access, decide or change.

Human-approved action: AI recommends or prepares an action, but a person must review and approve it before the action is carried out.

Human in the loop: refers to a model in which a person reviews, approves or intervenes in an AI decision or action.

Human oversight: refers to the broader supervision of an AI system, including setting guardrails, monitoring performance, reviewing significant actions and managing exceptions. It does not necessarily mean approving every action.

IT decision-makers/ITDMs: refers to respondents with responsibility for IT purchases, policies, budgets or strategy.

Managers: refers to respondents with management responsibilities.

Other decision-makers: refers to respondents with decision-making responsibility outside of IT.

Pre-approved actions: routine, lower-risk actions that an autonomous system is allowed to take within defined guardrails, without requiring approval each time.

Predictive IT: when IT processes use AI to identify risks before they affect a person’s workflow, allowing teams to intervene before people are aware of the issue.

Proactive IT: when IT processes detect and resolve recurring issues earlier through automation, reducing repeated disruption and revealing patterns that affect performance.

Reactive IT: when IT processes fix technology issues after disruption occurs. Issues are identified through tickets, alerts or employee complaints, meaning productivity has often already been affected.

Respondents: refers to the people who participated in the survey. This term is used when reporting survey findings.

Trusted autonomy: the conditions that make people more confident in allowing autonomous systems to act. In this report, those conditions include security, decision quality, control, reversibility and accountability.

Workforce: refers collectively to the people within an organization.



Table of contents

(Clickable links)

- 000 · From AI assistance to the autonomous digital workplace 05
- 00 · Research methodology 07
- 01 · AI is already part of everyday work 09
- 02 · Comfort declines as AI gains authority 15
- 03 · The AI Confidence Gap is not evenly distributed 25
- 04 · IT is the operational core of the autonomous digital workplace 30
- 05 · Ambition is moving faster than readiness 40
- 06 · The path to the autonomous workplace 46
- 07 · Conclusion 51



Introduction

From AI assistance to the autonomous digital workplace



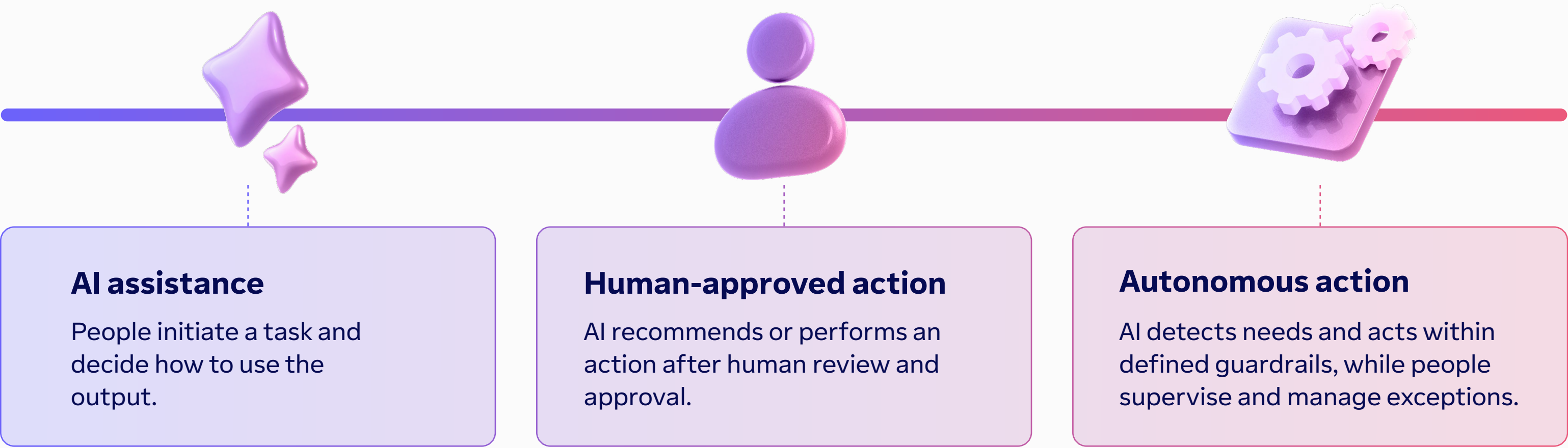


From AI assistance to the autonomous digital workplace

AI has quickly become part of everyday work. People use it to summarize information, develop ideas, analyze data, create content and complete repetitive tasks.

The widespread adoption of generative AI has introduced millions of people to a more direct, user-driven form of AI. But prompting a tool to perform a task represents only one stage in the workplace’s broader evolution.

The next stage will be defined by systems that can identify needs, evaluate conditions and take action — not just wait for instructions.



This is the autonomous digital workplace: an environment that uses AI agents to sense, decide, act, and continuously learn — driving autonomy across people, technology, and work to accelerate business performance.

The autonomous digital workplace reduces repetitive work, prevents disruptions and allows workers to focus on activities that require judgment, creativity and human connection.

IT is both an early application of the autonomous digital workplace and a critical foundation for scaling it. AI-enabled IT systems can detect recurring issues, identify risks and resolve certain problems before they interrupt work. Over time, IT professionals move from manually handling every intervention to supervising autonomous systems, creating new automations and managing exceptions. In this way, autonomous IT provides a practical starting point

for broader workplace autonomy while strengthening the digital systems work depends on.

As such, using AI for assistance is not the same as trusting it to act independently. The path to the autonomous digital workplace will depend on whether organizations can give AI greater authority while maintaining the security, transparency, accountability and human oversight the workforce expects.



“The next stage of workplace AI will be defined by trust.

Organizations will not succeed by giving AI unlimited authority. They will succeed by building systems that can act safely, transparently and accountably, while helping people and businesses perform at a higher level.”



Oliver Steil, Chief Executive Officer, TeamViewer



Methodology

Research methodology





Research methodology

The survey was conducted by **Sapio Research** in May 2026 using an email invitation and online survey. In total, 4,200 managers and employees (50:50 split) across the U.S. (1,000), Australia (400), Brazil (400) Canada (400), France (400), Germany (400), Italy (400), Japan (400), Singapore (400) and the U.K. (400) were surveyed.

4,200
managers and employees
(50:50 split) surveyed



U.S.	Australia	Brazil	Canada	France
1,000	400	400	400	400
Germany	Italy	Japan	Singapore	U.K.
400	400	400	400	400



Section one

AI is already part of everyday work



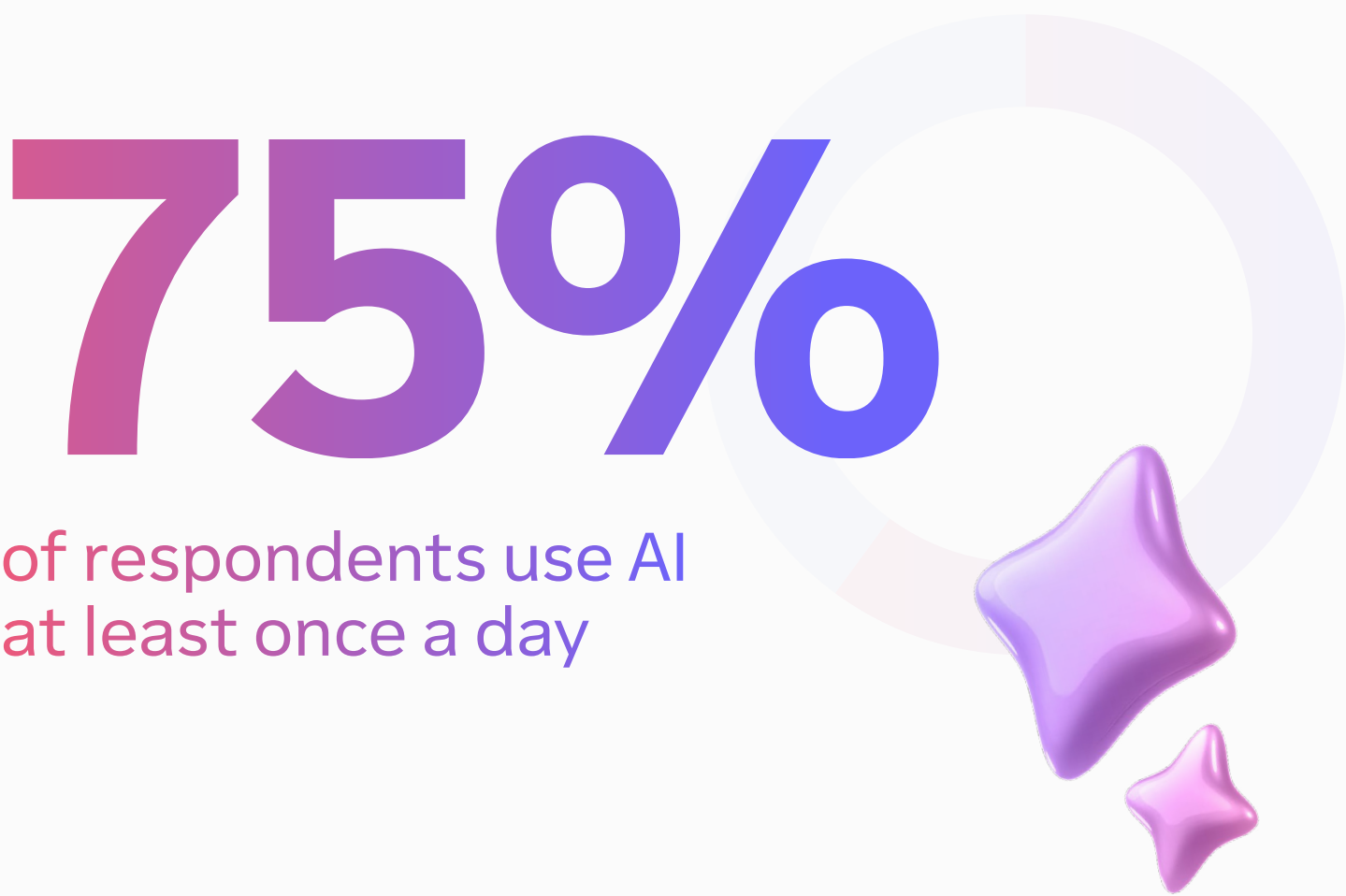


AI is already part of everyday work

AI, especially generative AI, has become an everyday workplace tool.

People are using it for familiar, well-defined tasks and are already seeing meaningful benefits and efficiency gains. But these interactions remain largely user-directed: a person initiates the task, reviews the result and decides what happens next.

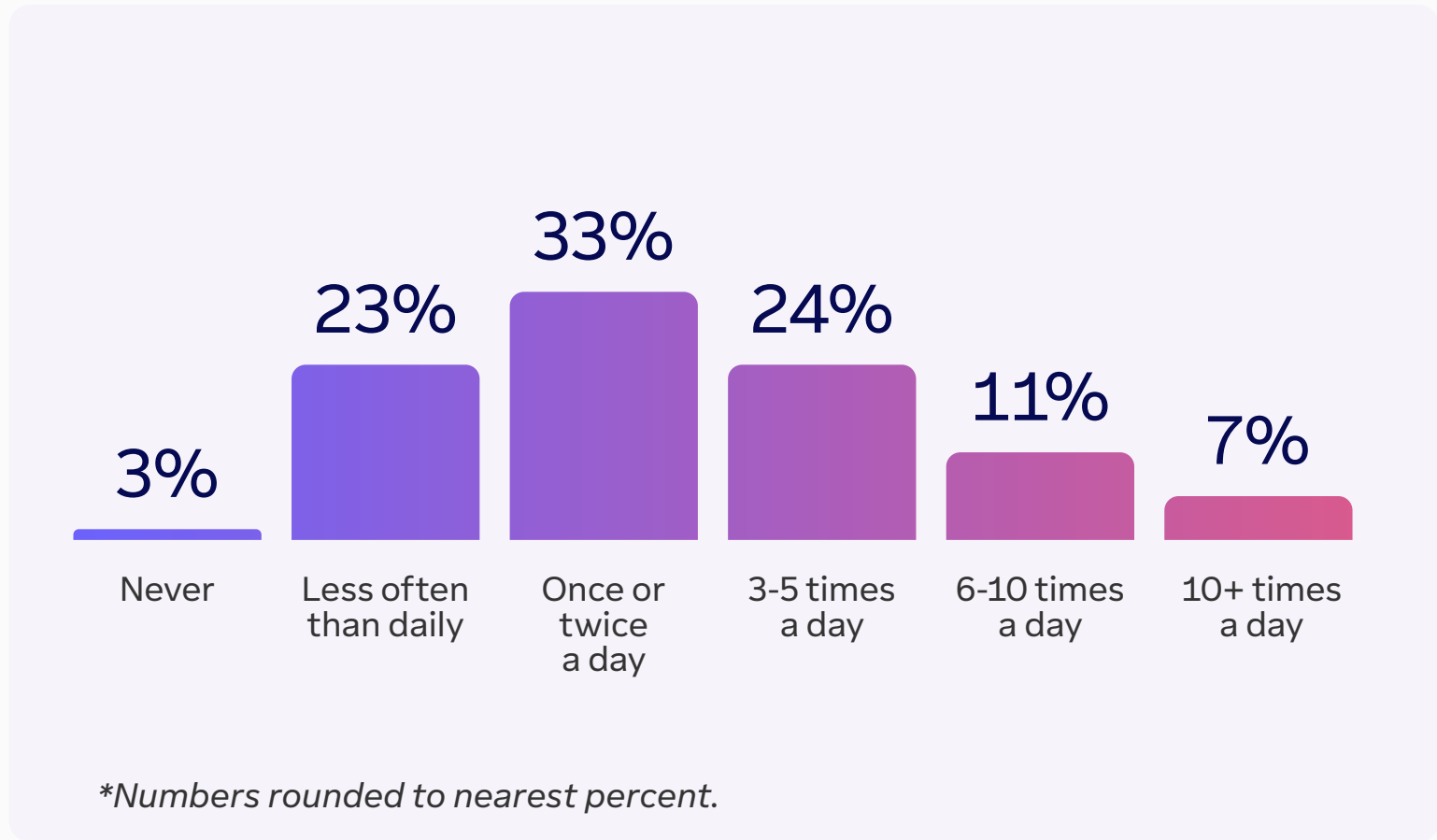
1.1 Prompting is becoming a daily habit



Respondents prompt an average of three times per day.

Rather than using AI continuously, respondents appear to draw on it at specific points in their workflow, such as when they need to understand information, generate a starting point or complete a routine task more efficiently.

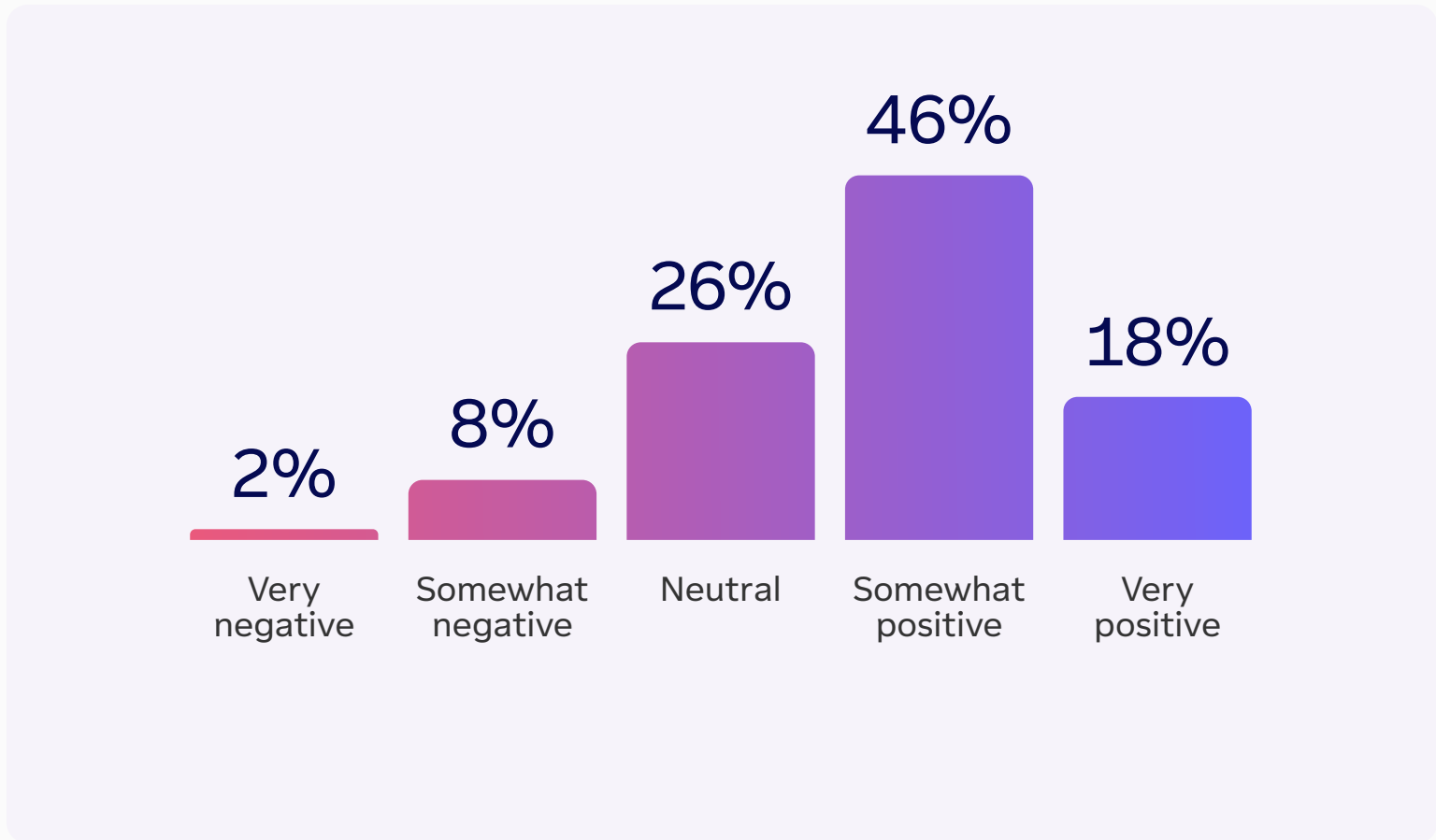
Frequency of AI usage



More use is associated with more positive experiences

The survey finds that people who use AI more regularly are also more likely to describe their experience positively.

Experience of using AI tools in day-to-day work

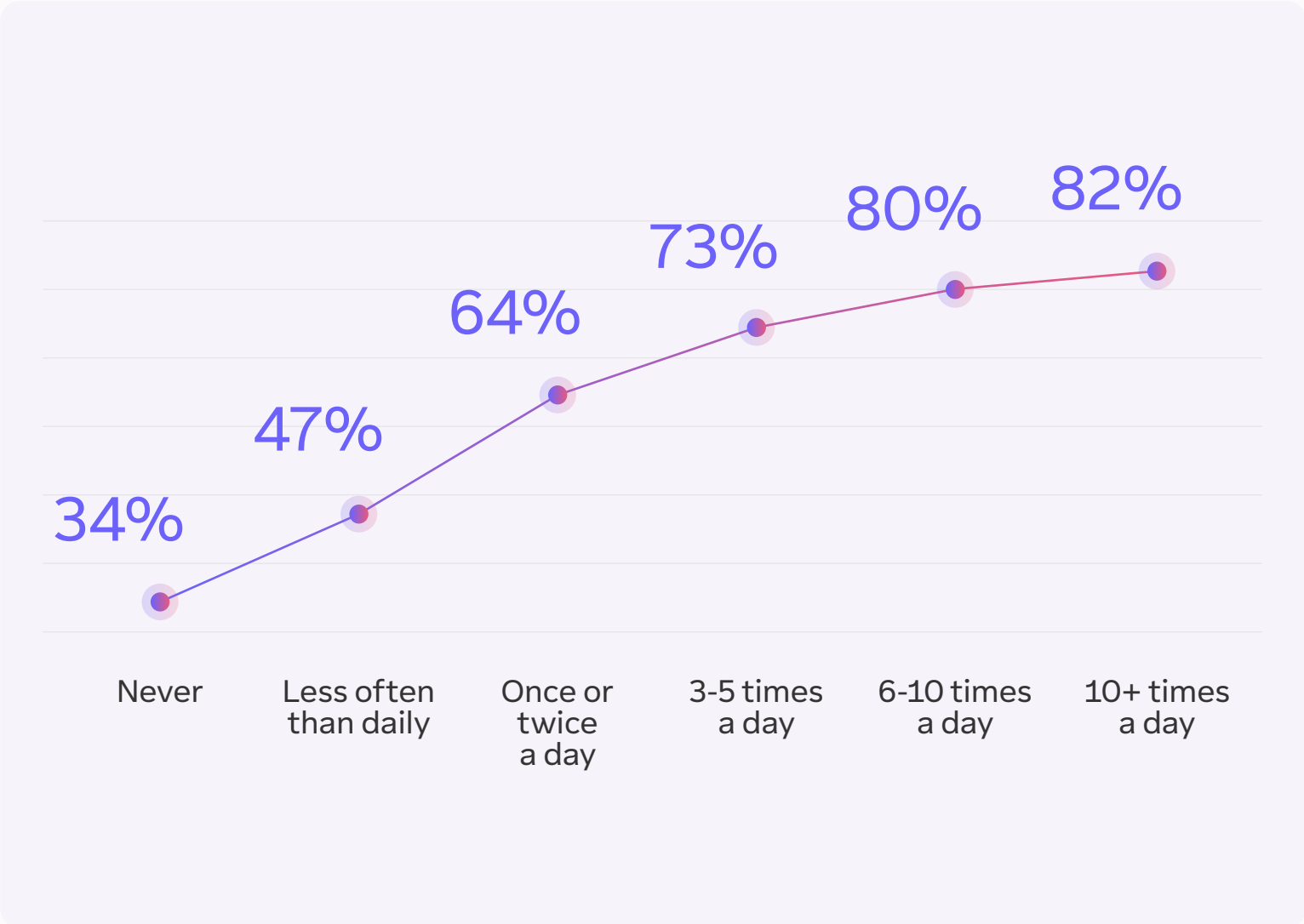


64% = Somewhat/Very positive





% Somewhat/Very positive experience by number of AI prompts per day



This pattern matters because frequent interaction gives people an opportunity to learn where AI is useful, how to ask better questions, and when its output requires additional judgment.

The association should not necessarily be interpreted as proof that frequency alone produces better outcomes. However, findings point to a reinforcing cycle.

Greater familiarity may help users develop stronger prompting skills, set more realistic expectations and recognize which tasks are particularly well suited to AI support.

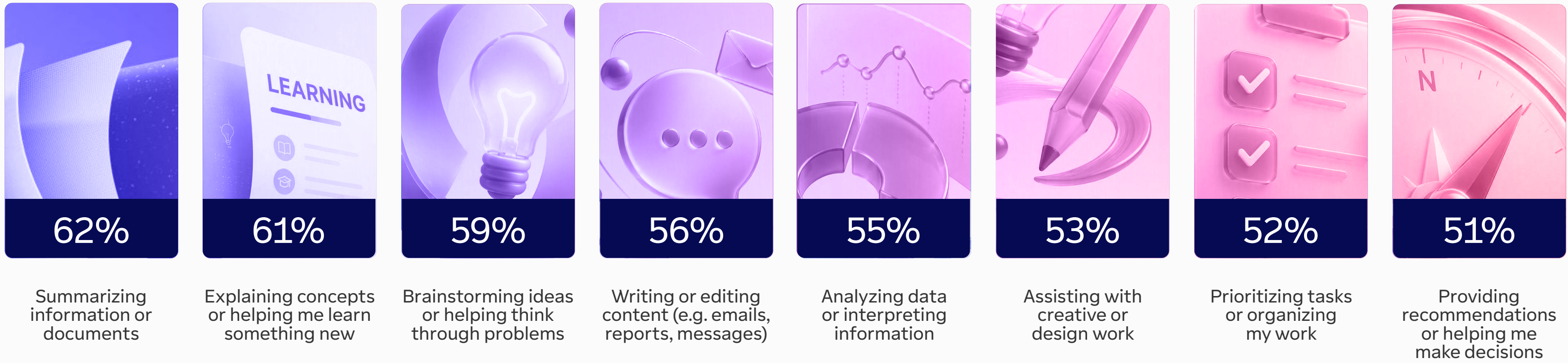
TAKEAWAY

Useful outcomes encourage more frequent use — and familiarity may help people get more from AI.

1.2 Familiar, well-defined tasks are the starting point

Respondents are most comfortable using AI when the task has a clear purpose and the output can be reviewed before it is applied.

Comfort using AI for user-directed tasks



The most accepted use cases position AI as an assistant. It processes information, generates ideas or provides a starting point, while the worker retains control over the final result.



1.3 Workers are realizing tangible benefits

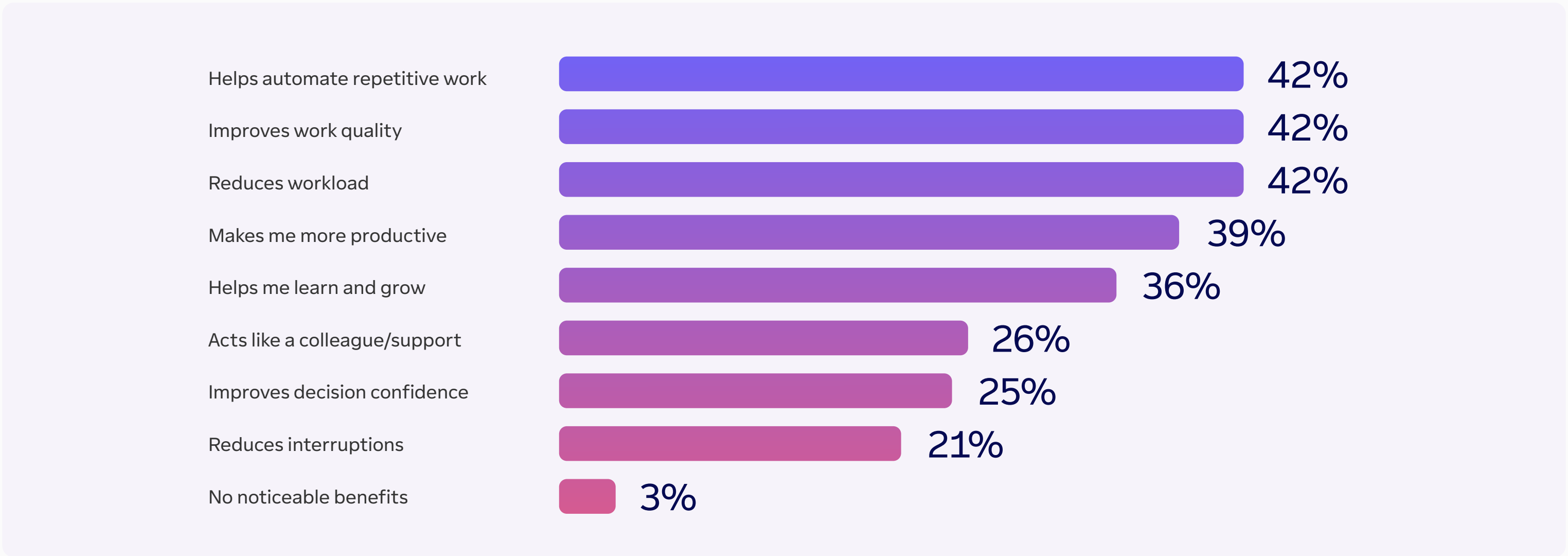
AI adoption is being driven by practical value, not novelty.



Respondents identify an average of three benefits from workplace AI. However, those benefits are not experienced equally: **30%** of employees identify only one benefit, while **30%** of managers identify three.

Especially when it comes to productivity, managers are more likely to say AI will boost productivity (**43%**) than employees (**35%**).

Benefits of AI in the workplace



T A K E A W A Y

AI is already helping people reduce effort, improve quality and accomplish more.





1.4 Verification remains part of the AI workflow

As AI becomes part of everyday work, people are taking an active role in ensuring its outputs are accurate and appropriate.

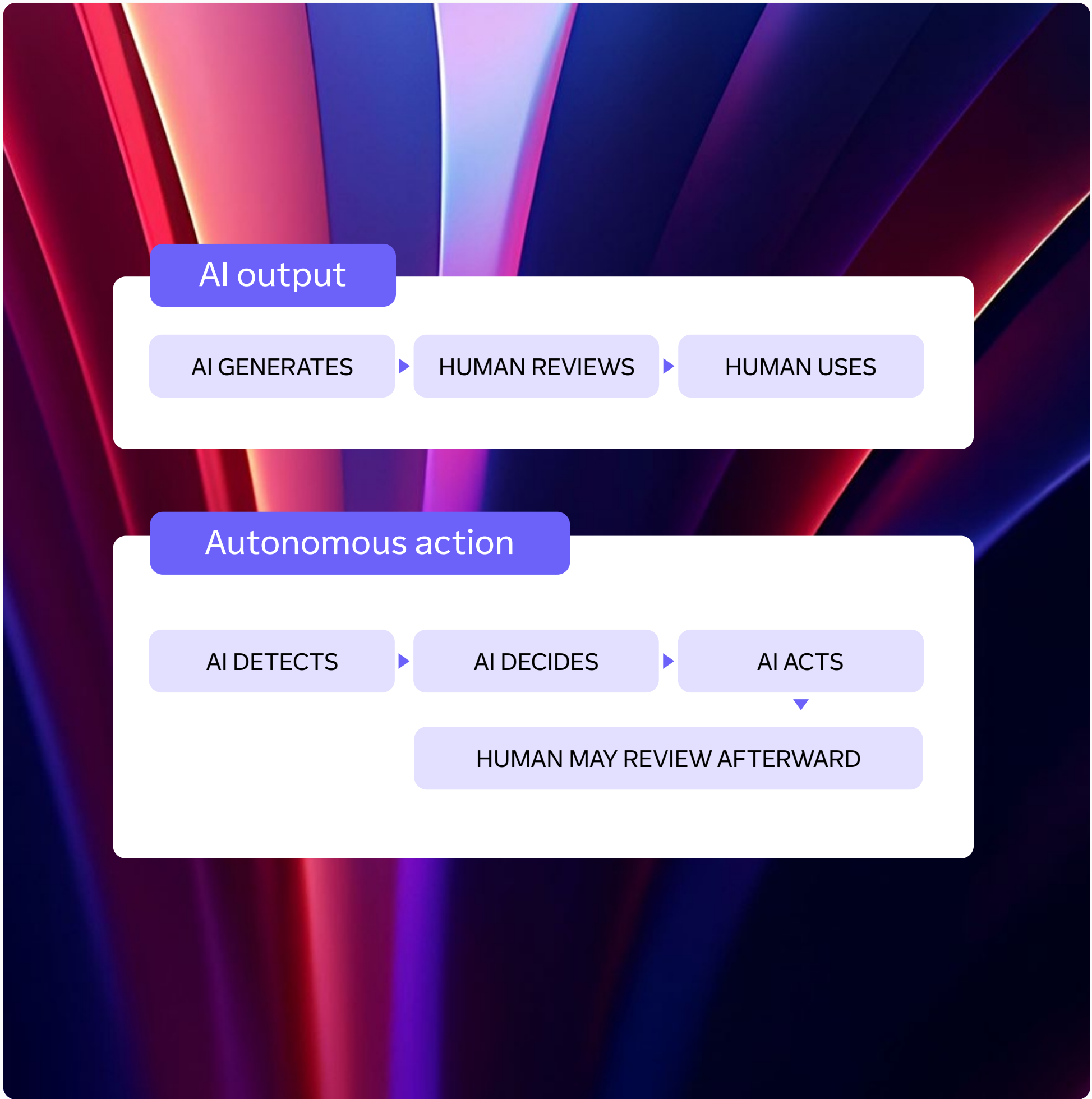


The oversight burden

Although most respondents check outputs at least some of the time, **72%** do not verify every output before using it. This may reflect the practical difficulty of reviewing everything as AI becomes embedded in more daily tasks.

What this means for autonomous action

When AI produces a summary or draft, a worker can check it before use. When AI begins taking autonomous action, an error may have consequences before a person can intervene.





Verification can be a bridge to trusted autonomy

Today, respondents often review AI-generated work before acting on it. As systems become more reliable, transparent and familiar, some of that oversight can shift from checking every output to supervising defined actions within clear guardrails.

This does not mean allowing AI to act without limits. It means establishing which actions are low-risk and pre-approved, which require human review before execution and which should always be escalated. For example, an autonomous system may be trusted to complete a routine, reversible task within predefined boundaries, while pausing for approval before making a change that could affect security, sensitive data or business operations.

Organizations can support this transition by helping people understand when AI can be trusted, making system activity visible and applying stronger safeguards to higher-risk actions.



“The move from AI assistance to autonomous action is not a leap of faith. It is an architecture question. Organizations need to define what a system can access, what actions are pre-approved, when it must pause for human approval and how people can intervene when risk increases. That is how verification evolves from checking every output to supervising systems with confidence.”



Mei Dent, Chief Product and Technology Officer, TeamViewer



T A K E A W A Y

Verification helps build confidence in AI. As AI use grows, organizations will need to make oversight more targeted and manageable by defining pre-approved actions, clear guardrails and escalation points for higher-risk decisions.



Section two

Comfort declines as AI gains authority



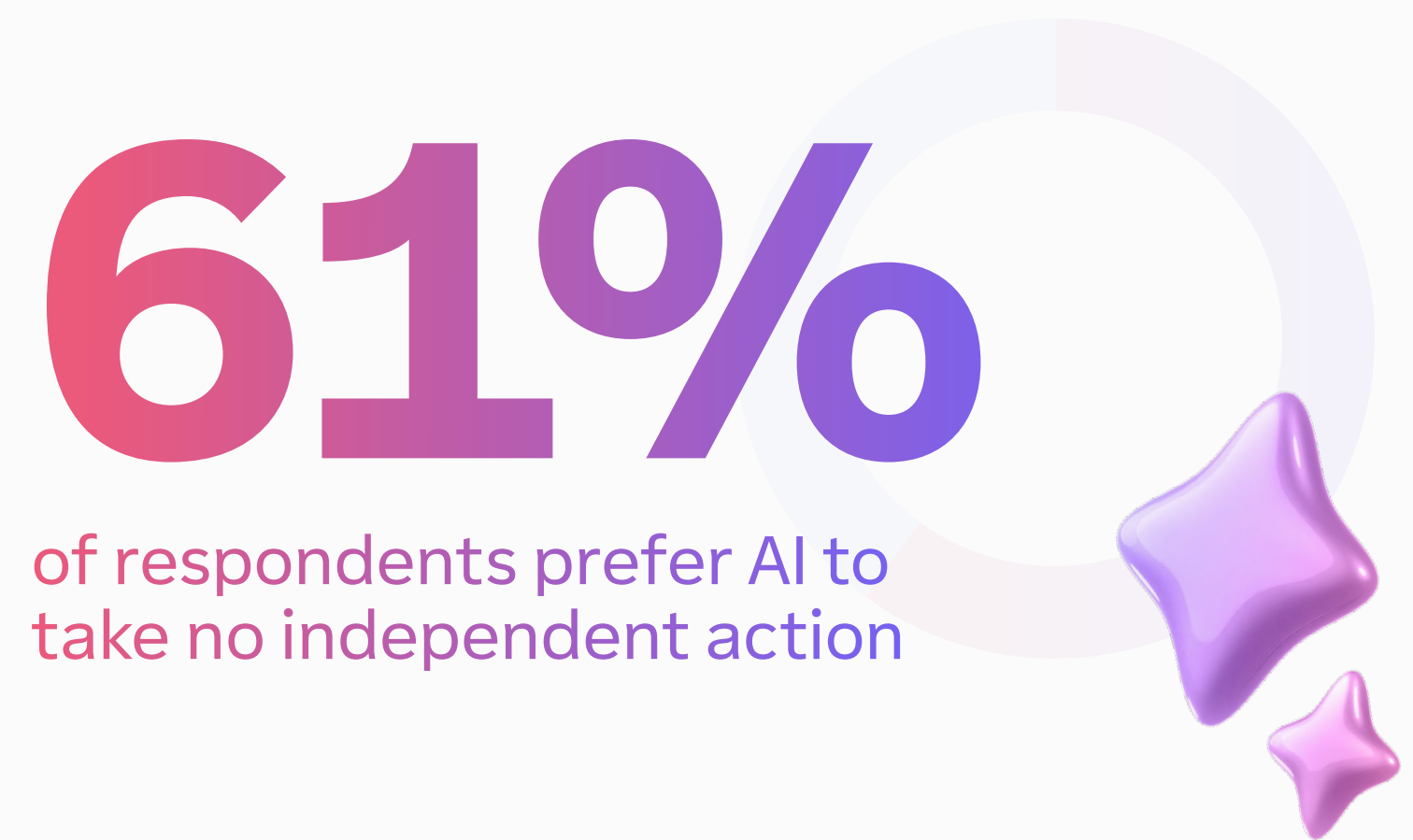
Comfort declines as AI gains authority

Respondents are open to delegating work to AI, but not without limits. Comfort is highest when a person initiates the task and reviews the result. It declines when AI operates in the background, accesses sensitive information or takes action without direct approval.

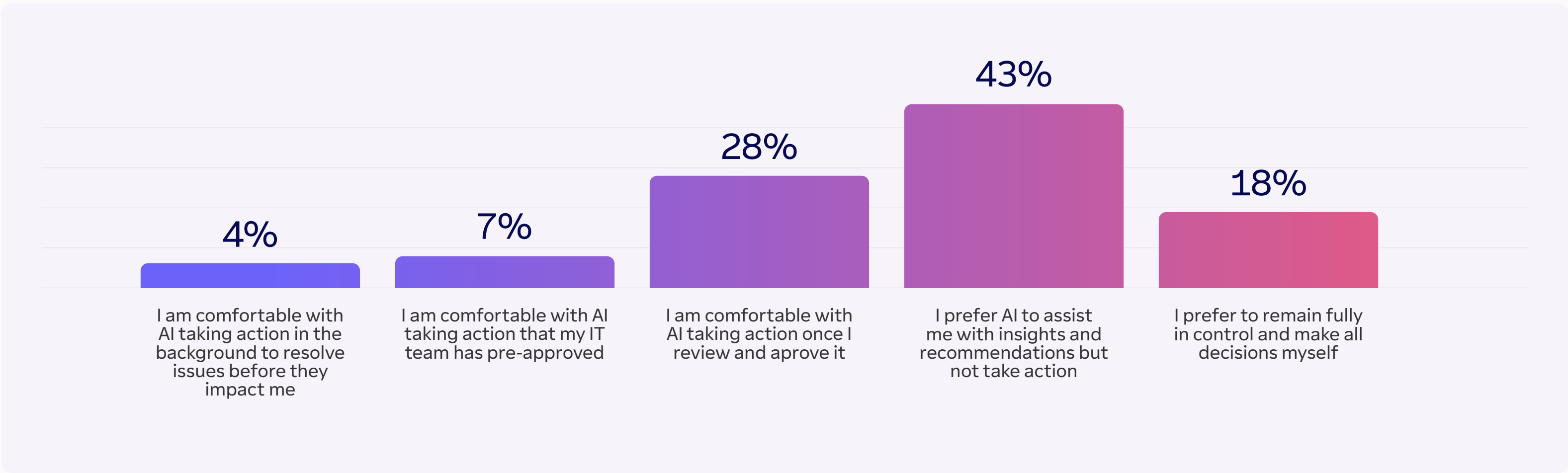
2.1 The AI Confidence Gap

Respondents are increasingly comfortable working with AI, but they are less ready to give it independent authority.

More than three in five respondents prefer AI to take no independent action. This includes **43%** who want AI to provide recommendations while they make the final decision and **18%** who prefer to make decisions without AI recommendations. The remaining **39%** are open to AI taking action, although most still want those actions to require human approval.



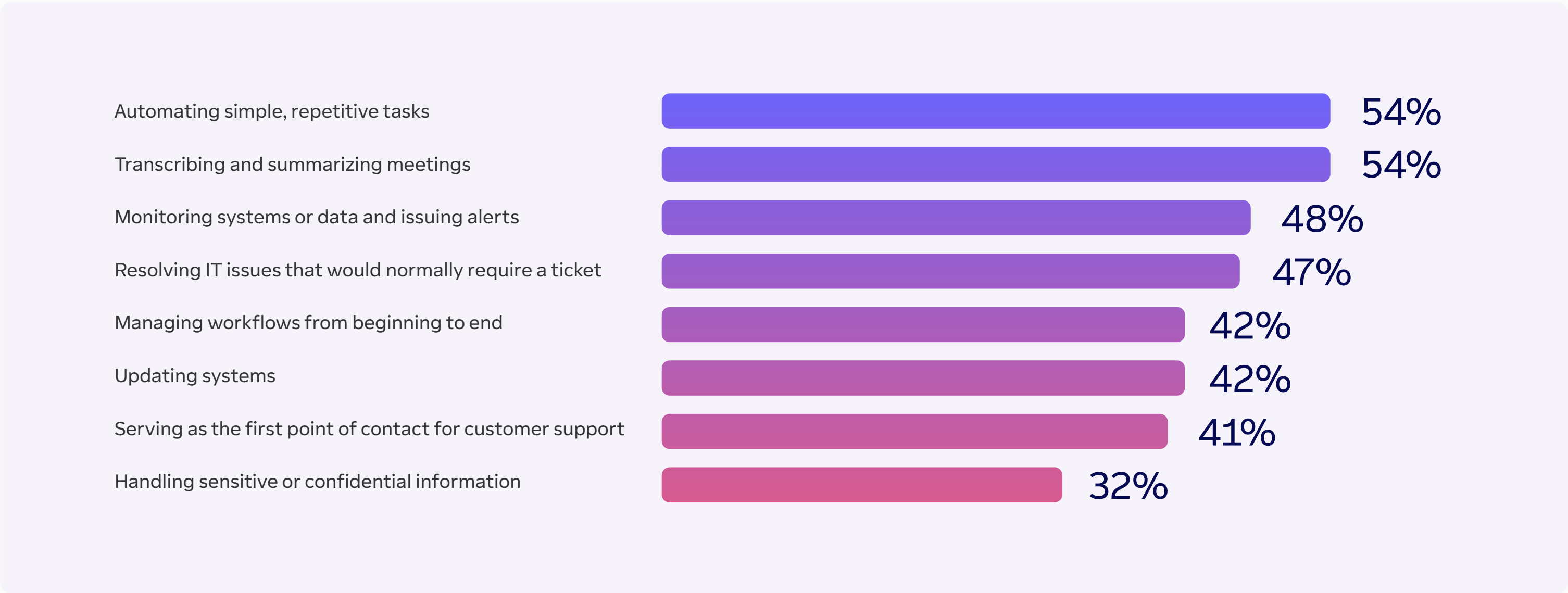
Preference for AI level of control





Comfort also varies considerably by task

% very/completely comfortable with AI handling tasks without human input

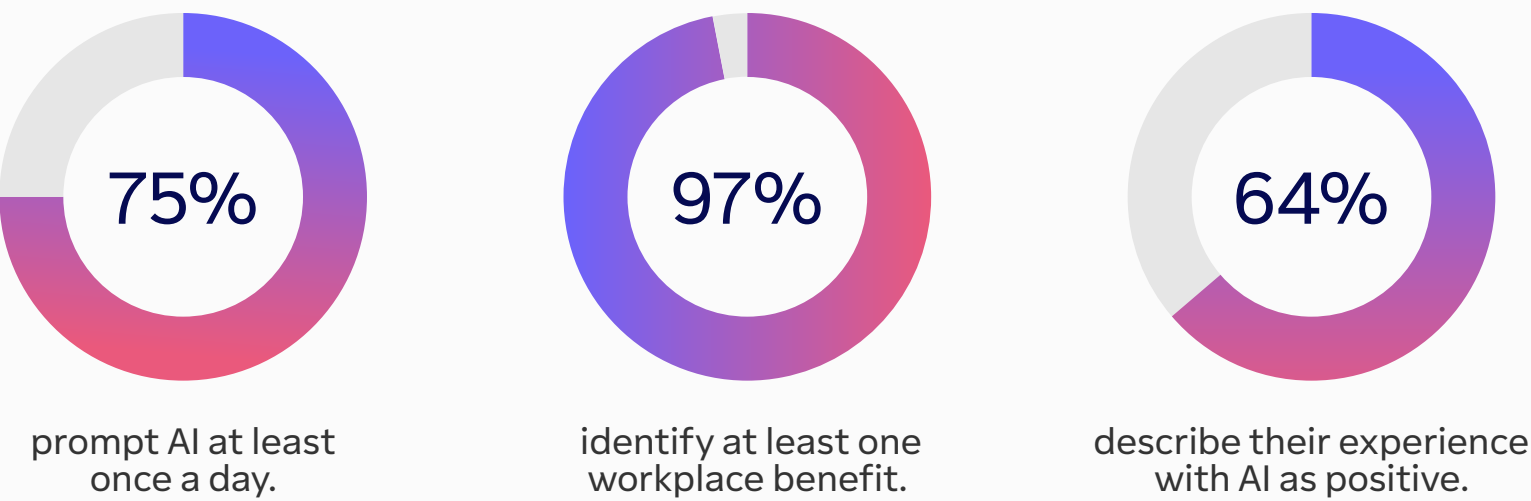


The pattern is clear: respondents are more willing to delegate routine, contained activities than tasks involving sensitive information, broader access, greater judgment or more significant consequences.

However, the findings also reveal broad conditional openness. At least **70%** of respondents are moderately, very or completely comfortable with AI handling seven of the eight tasks presented to respondents in the background. Across every use case, between **25%** and **31%** are moderately comfortable, suggesting a large middle group whose confidence may depend on the safeguards, transparency and experience surrounding deployment.

Handling sensitive or confidential information is a clear exception. While **57%** are at least moderately comfortable with this use case, **22%** are not at all comfortable.

This creates an AI Confidence Gap. The workforce is already using AI regularly and recognizing its value:

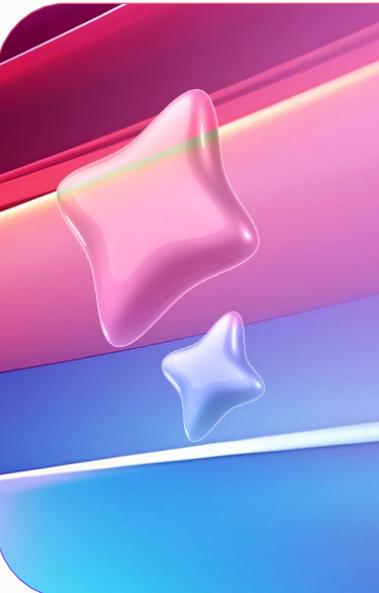


But confidence declines as AI gains greater authority:





The gap does not mean workers are rejecting autonomous systems. It reflects an important distinction between trusting AI to produce an output and trusting it to execute an action. A summary, recommendation or draft can usually be reviewed before it affects someone’s work. An autonomous action may have consequences before a person has the opportunity to intervene.



AI assistance

- High adoption
- Positive experiences
- Recognized benefits
- Worker reviews the result



Autonomous action

- Lower readiness
- Greater perceived risk
- Wider potential consequences
- Stronger demand for safeguard

T A K E A W A Y

Respondents are ready to work with AI, but confidence falls as systems gain greater access and authority. Closing that gap will require safeguards that make autonomous action secure, understandable and appropriately bounded.

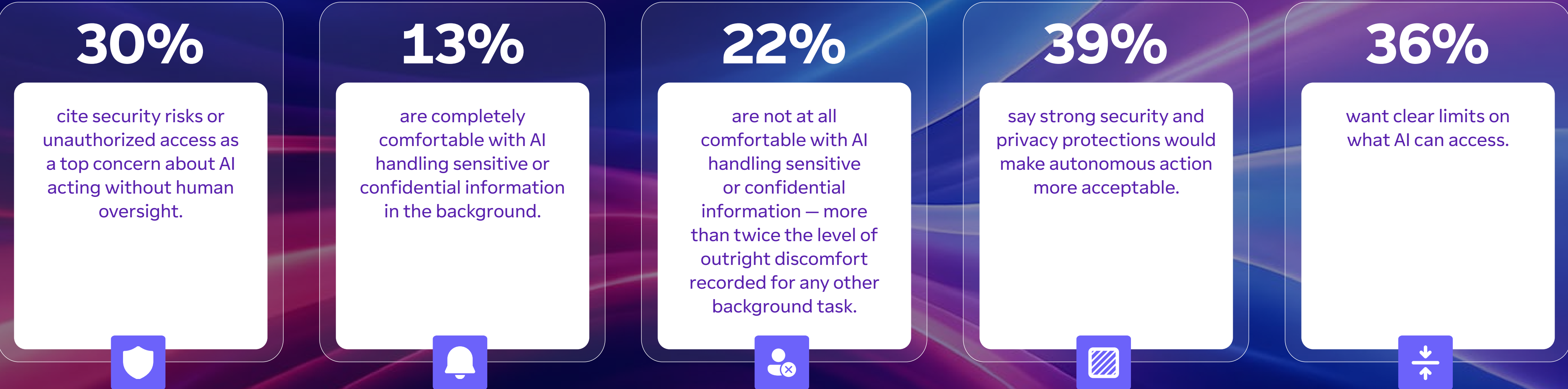


2.2 Requirements for trusted autonomy

Respondents’ concerns about autonomous systems fall into five closely connected pillars: security, decision quality, control, reversibility and accountability. The data also points to the safeguards that could help organizations build confidence in each one.

SECURITY

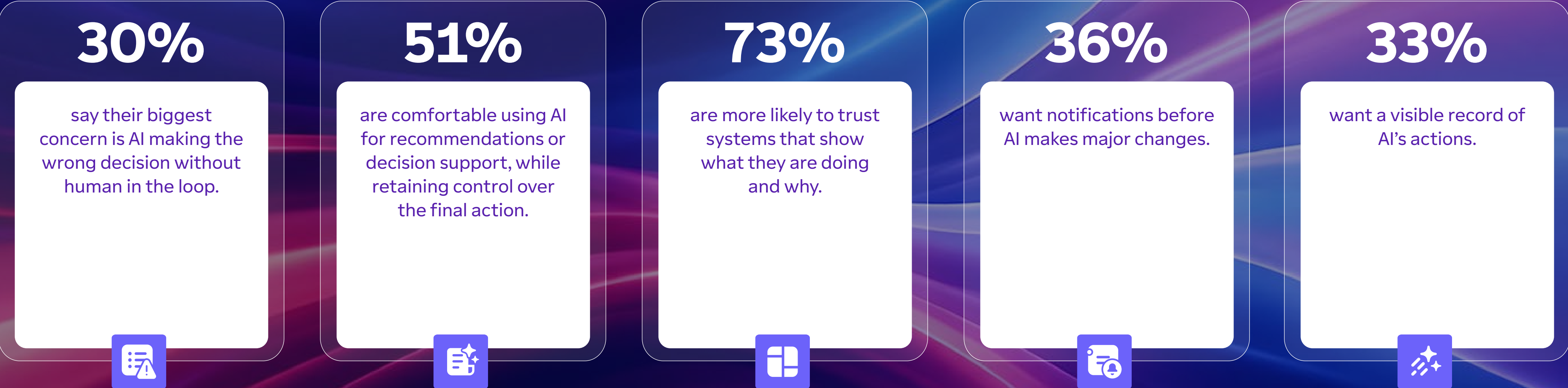
Could the system expose sensitive information, enable unauthorized access or create new vulnerabilities?



Closing the confidence gap: Handling sensitive information represents the clearest boundary for autonomous AI. Strong security protections, clearly defined access limits and greater visibility into how information is used could help build confidence.

DECISION QUALITY

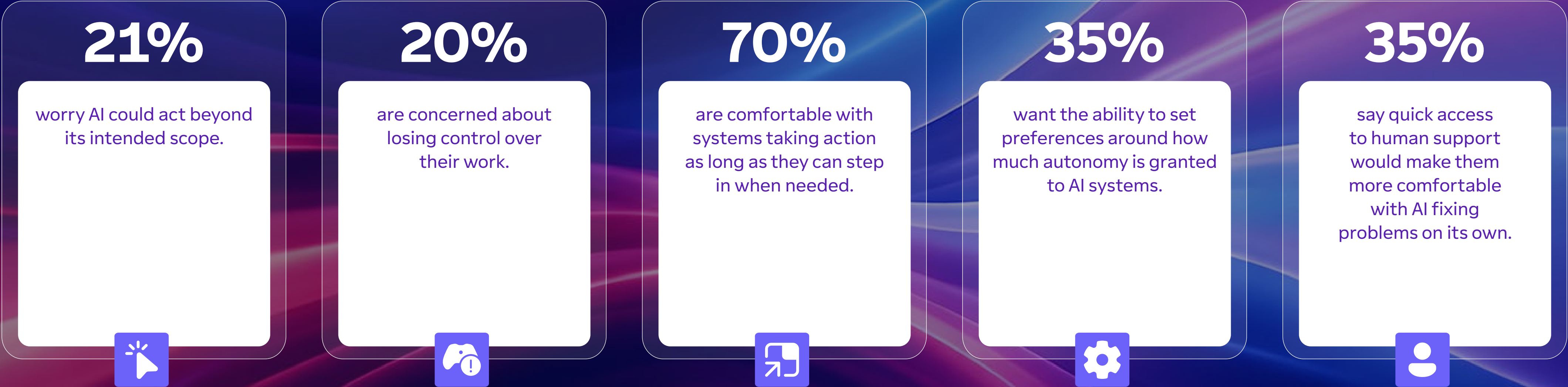
Will AI understand the context well enough to make the right choice?



Closing the confidence gap: Respondents are concerned that AI may make poor or contextually inappropriate decisions, but greater explainability, visibility and advance notice could help them trust how decisions are reached.

CONTROL

Can people limit what the system does and intervene when needed?

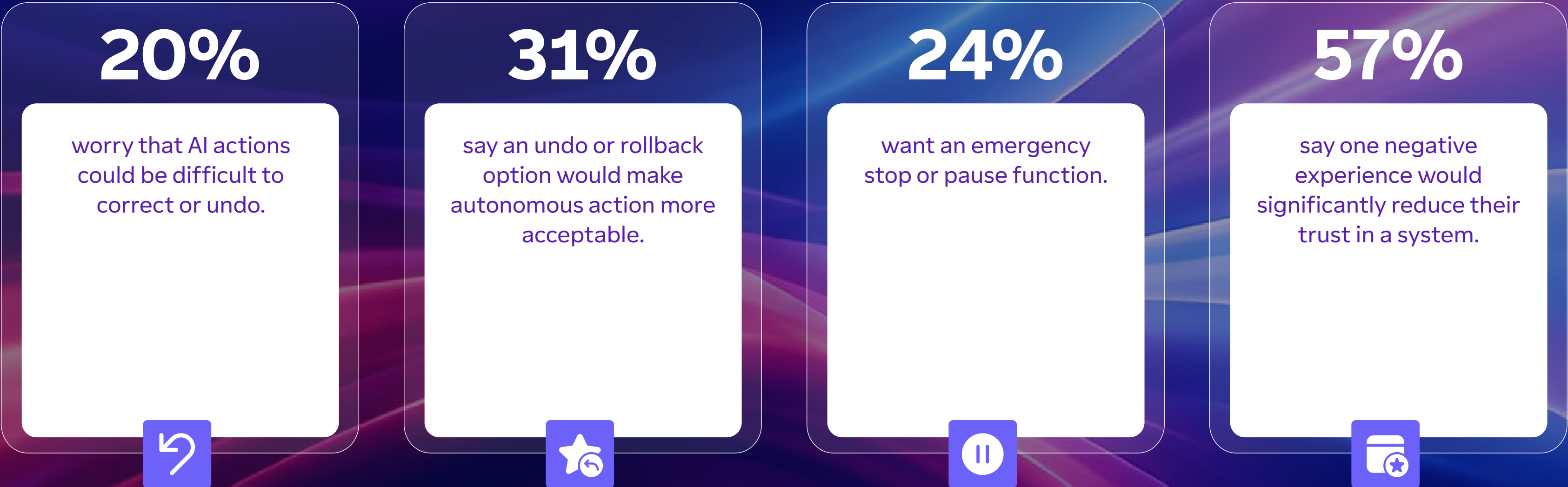


Closing the confidence gap: Respondents are concerned about surrendering too much control, but defined boundaries, user-controlled settings and accessible human intervention could make autonomous action feel more manageable.



REVERSIBILITY

Can an incorrect action be stopped, corrected or rolled back quickly?

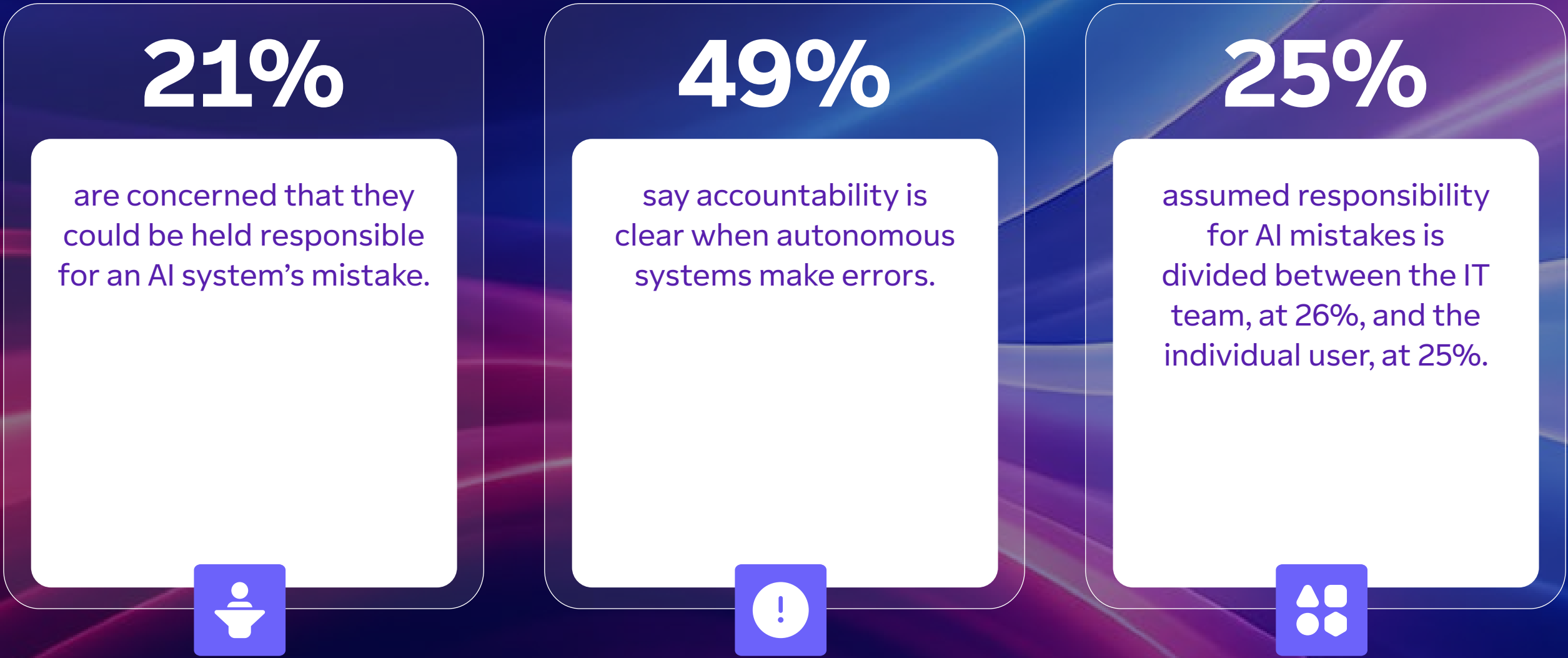


Closing the confidence gap: Respondents are concerned that an AI mistake could be difficult to recover from, but rollback, pause and recovery capabilities could prevent a single error from permanently undermining trust.



ACCOUNTABILITY

Is it clear who owns the outcome when an autonomous system makes a mistake?



Closing the confidence gap: Respondents are concerned about being blamed for decisions they did not fully control, but clear ownership, escalation and remediation processes could make accountability more equitable and transparent.



T A K E A W A Y

Closing the AI Confidence Gap will require more than improving technical performance. Organizations must give their people confidence that autonomous systems are secure, explainable, bounded, reversible and governed by clear human accountability.



Section three

The AI Confidence Gap is not evenly distributed





The AI Confidence Gap is not evenly distributed

Not all types of workers are experiencing AI in the same way. Managers report more benefits and more positive experiences than non-management employees. Employees feel more personally exposed when autonomous systems make mistakes. IT decision-makers, meanwhile, use AI more frequently and are more ready to allow it to act.

These differences matter because the people leading AI adoption may not see its risks and rewards in the same way as the employees affected by it.

3.1 Managers are seeing more value in workplace AI

Managers are more positive about AI and identify more benefits from its use.



Managers are also more comfortable allowing AI to operate in the background. For example, **60%** are very or completely comfortable with AI automating repetitive tasks, compared with **48%** of employees. For monitoring systems and issuing alerts, the figures are **53%** and **43%**, respectively.

T A K E A W A Y

Managers are not only seeing more value from AI; they are also more willing to delegate defined activities to it than employees.



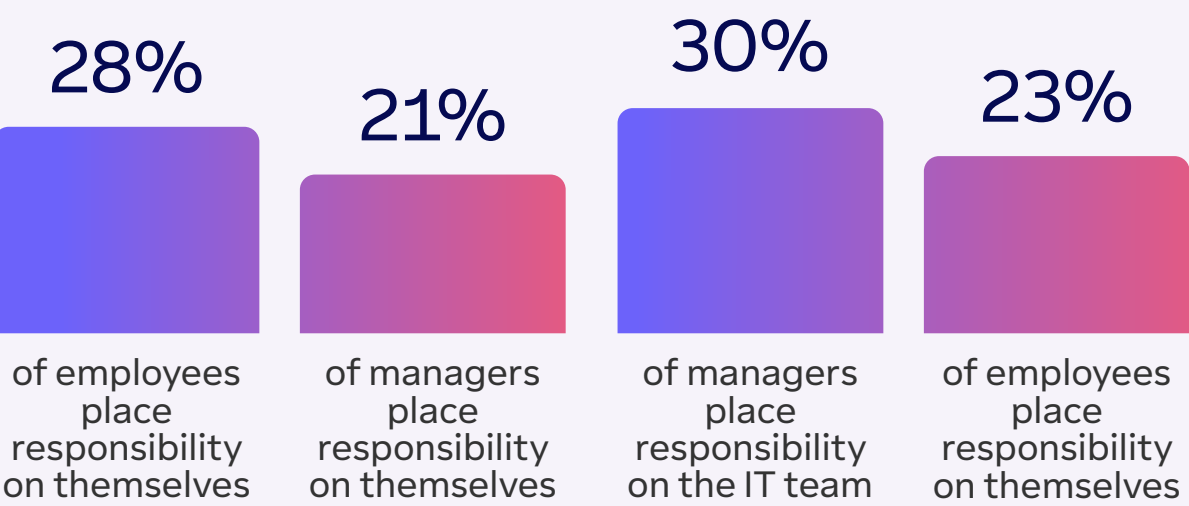
Managers may assess AI through broader outcomes such as productivity, efficiency and team performance. Employees may judge it more directly through its effect on their own workload and day-to-day responsibilities.



3.2 Employees feel more exposed when autonomous systems fail

Managers and employees also differ in where they place responsibility for autonomous action.

When asked who should be held responsible if an autonomous system negatively affects their work:



Employees may therefore feel personally accountable for actions taken by systems they did not select, design or deploy.

This could help explain why employees are less confident in autonomous action. Their caution may reflect concern about being held responsible without having corresponding authority or control.

T A K E A W A Y

Employees may perceive greater personal risk from autonomous systems, even when they have less control over how those systems are deployed.



3.3 IT decision-makers are further along the confidence curve

IT decision-makers (ITDMs) show greater familiarity with AI and greater readiness to allow it to act.

- ITDMs prompt AI an average of **five times per day**, compared with **three times per day** among other decision-makers.
- **48% of ITDMs** say AI has made them feel more in control of their responsibilities, compared with **34% of other decision-makers**.
- **55% of ITDMs** are mostly or completely ready for AI to act on their behalf, compared with **33% of other decision-makers**.

Greater familiarity with workplace technology and its safeguards may give ITDMs more confidence in how autonomous systems can be governed.

However, the two groups also focus on different risks:

- **33% of ITDMs** cite security as their leading concern.
- **33% of other decision-makers** are most concerned about AI making the wrong decision.

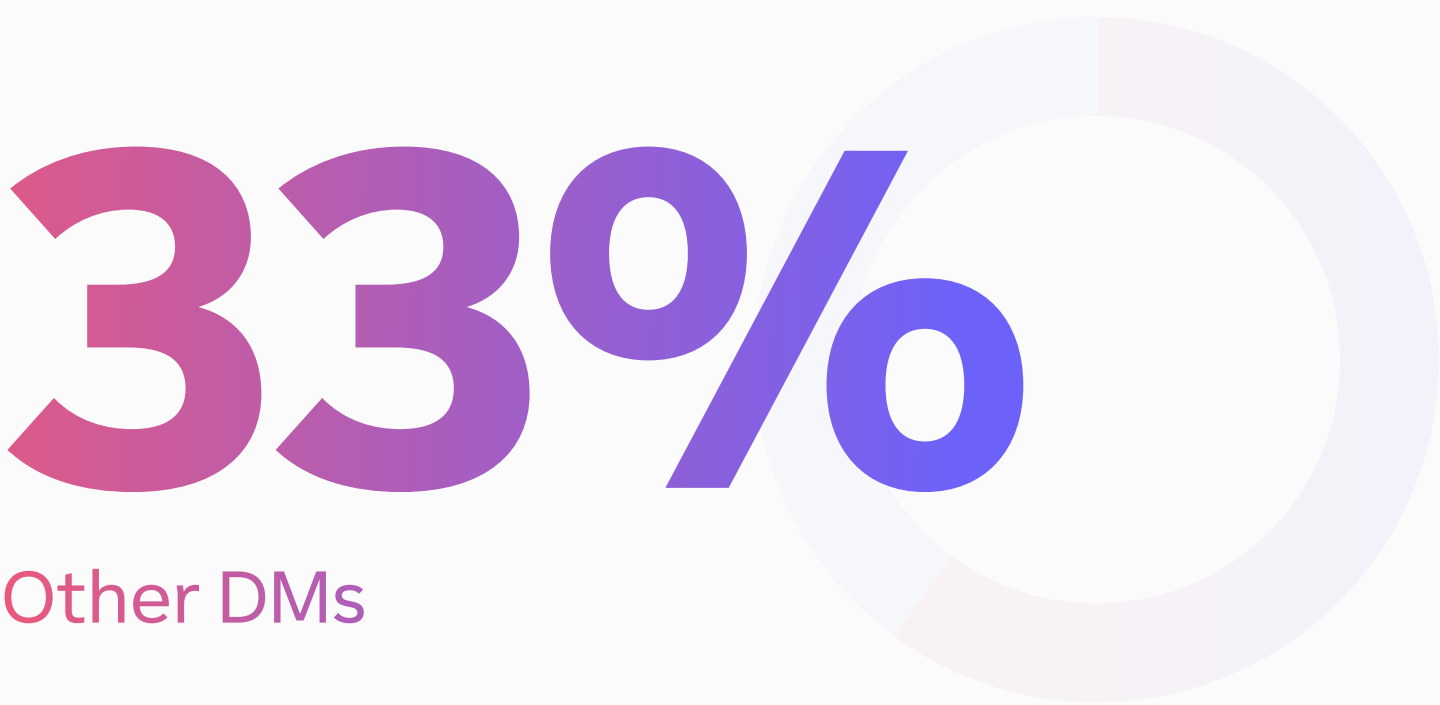
This distinction reflects two pillars of trusted autonomy. ITDMs are especially focused on protecting systems and data, while other decision-makers place greater emphasis on decision quality and business consequences.



Personal readiness for AI decision-making



Mostly/completely ready



TAKEAWAY

Those closest to the technology are more ready to delegate, but they may evaluate autonomous systems through a different risk lens than other workplace groups.

3.4 Closing the organizational confidence gap

The differences between managers, employees and IT decision-makers point to an imbalance between who makes decisions about AI and who may experience the consequences.

Those leading adoption are generally more positive about AI and more willing to delegate work to it. Employees, meanwhile, are more likely to feel personally exposed when autonomous systems make mistakes, despite often having less influence over how those systems are selected, configured or deployed. Closing this gap is ultimately a question of trust: organizations need to show that autonomy will be introduced with clear guardrails, shared accountability and meaningful input from the people affected by it.

Readiness therefore cannot be assessed solely through usage levels or the confidence of those overseeing implementation. Organizations must also consider whether:

- Their people have a meaningful voice in where and how autonomy is introduced, and how its rules, guardrails and approval points are defined.
- The people affected by autonomous decisions understand what authority the system has.
- Responsibility for errors sits with those who control the technology, rather than defaulting to individual users.
- Employees can challenge, escalate or seek review of actions that negatively affect their work.
- The benefits and risks of autonomy are distributed fairly across different workplace groups.

IT offers a practical place to begin closing this gap. Because many IT issues can be identified, measured and resolved through repeatable processes, organizations can use IT to test autonomous action, demonstrate safeguards and build trust before expanding autonomy more broadly across the workplace.



“People will not trust autonomous systems simply because they are told the technology works. Trust grows when employees understand how decisions are made, have a voice in where autonomy is introduced and know they will not be blamed for outcomes they could not control.”



*Kai Werner, Chief Human Resources Officer,
TeamViewer*



T A K E A W A Y

Autonomous systems will earn trust when the people affected by them have a meaningful voice in how they are introduced and governed — and IT can provide an early proving ground for getting that balance right.



Section four

IT is the operational core of the autonomous digital workplace





IT is the operational core of the autonomous digital workplace

The autonomous digital workplace depends on the systems, devices, applications, access points and digital experiences that people use every day. That makes IT one of the most important domains for workplace autonomy.

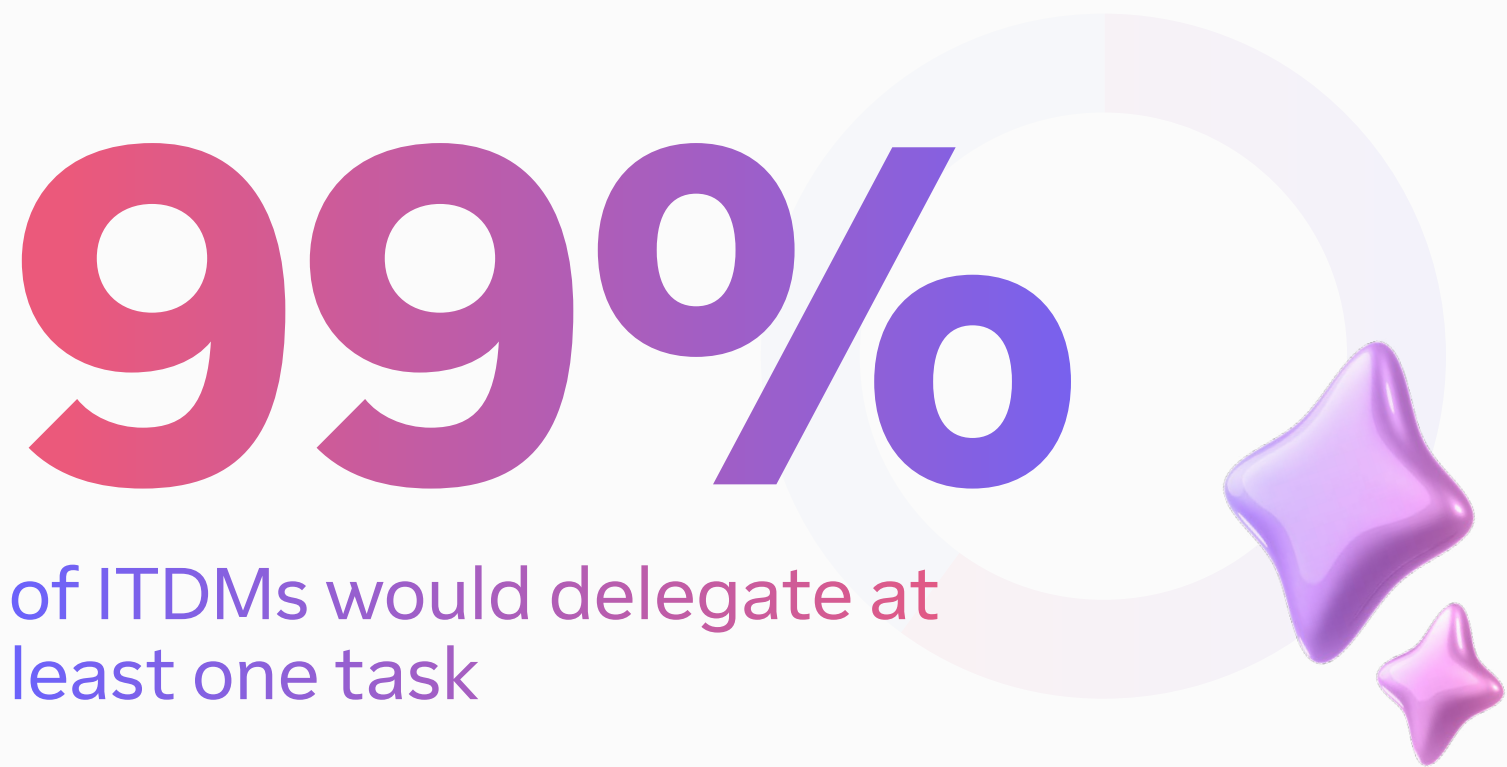
IT, especially IT service, is likely to be one of the first areas where autonomous systems see broad adoption. Many technology issues are repetitive, measurable and governed by established processes. That makes them well suited to earlier detection, automated remediation and autonomous action within defined guardrails.

But IT is more than an early use case. It is the operational foundation that determines whether people can work productively, securely and without disruption. If autonomous systems can prevent technology issues, protect access, optimize performance and resolve common problems before they affect work, they can demonstrate what trusted autonomy looks like in practice.

The opportunity is not simply to resolve issues faster. It is to shift intervention earlier – preventing disruption before it reaches the workforce.

4.1 IT leaders are ready to delegate defined tasks

Almost all IT decision-makers are comfortable delegating at least some IT-related work to an AI agent.



Section four

The tasks ITDMs are most comfortable delegating include:



Comfort is highest for routine, repeatable and clearly defined work. It falls when an action becomes broader in scope, more consequential or harder to reverse.

This mirrors the wider workforce findings: readiness for autonomous action increases when tasks are bound, measurable and supported by clear safeguards.

T A K E A W A Y

IT leaders are more ready to delegate than other groups surveyed — but they are still most comfortable starting with defined, high-confidence tasks.



4.2 The shift from reactive to autonomous IT

The evolution toward autonomous IT can be understood across four stages.

Reactive IT

When IT fixes technology issues after a disruption occurs. Issues are identified through tickets, alerts or employee complaints, meaning productivity has often already been affected.

Proactive IT

Recurring issues are detected and resolved earlier through AI-powered monitoring and automation, reducing repeated disruption and revealing patterns that affect performance.

Predictive IT

AI identifies risks before they affect a person’s workflow, allowing teams to intervene before people are aware of the issue. Successful fixes are then replicated across affected or similar endpoints.

Autonomous IT

AI agents detect and resolve current and predicted issues without requiring direct human intervention each time. They make context-aware decisions, adapt and act within defined guardrails, while people supervise and manage exceptions.

TAKEAWAY

As IT shifts toward autonomy, the goal moves from resolving disruption quickly to preventing it altogether.



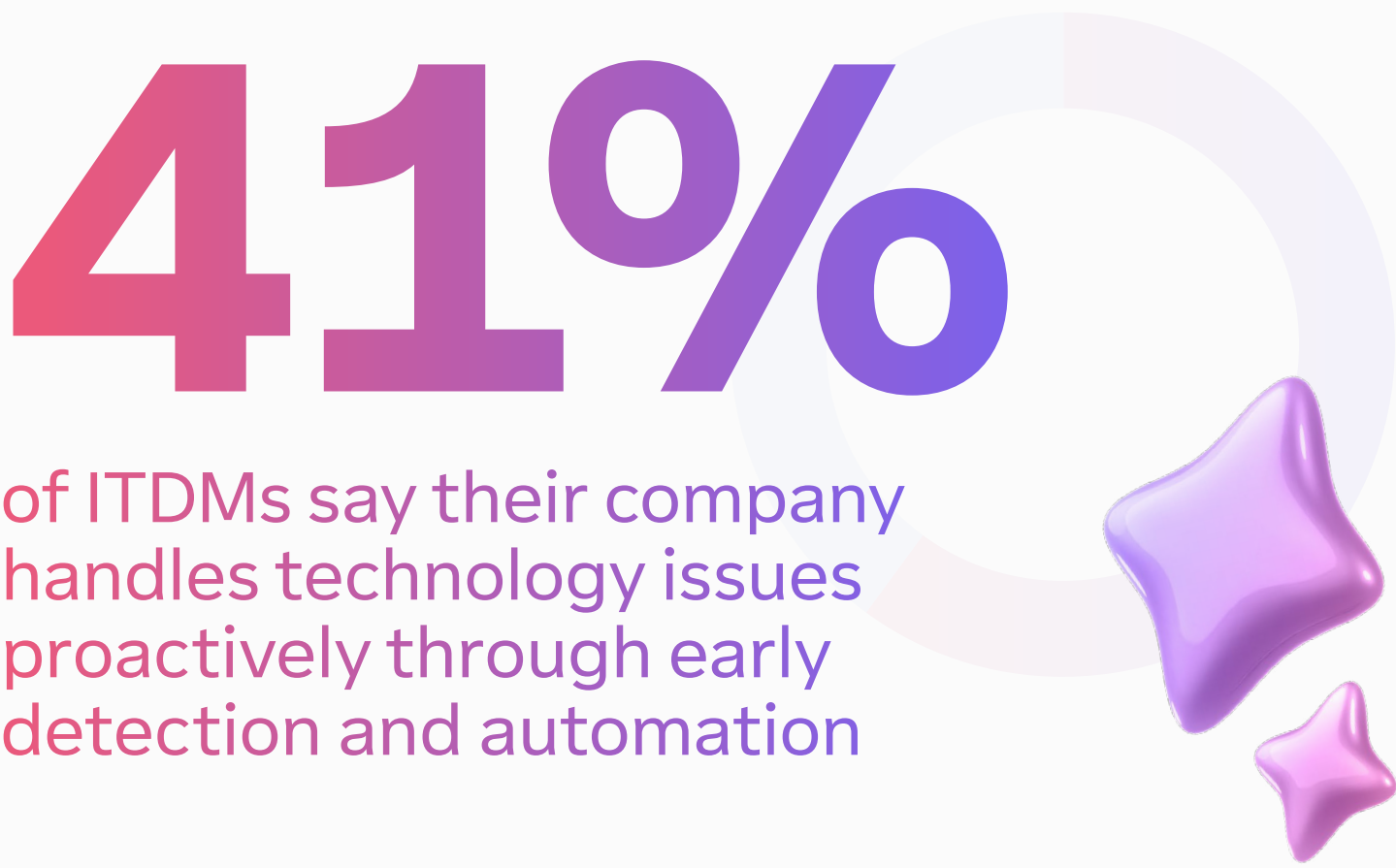


4.3 Most organizations have moved beyond reactive support

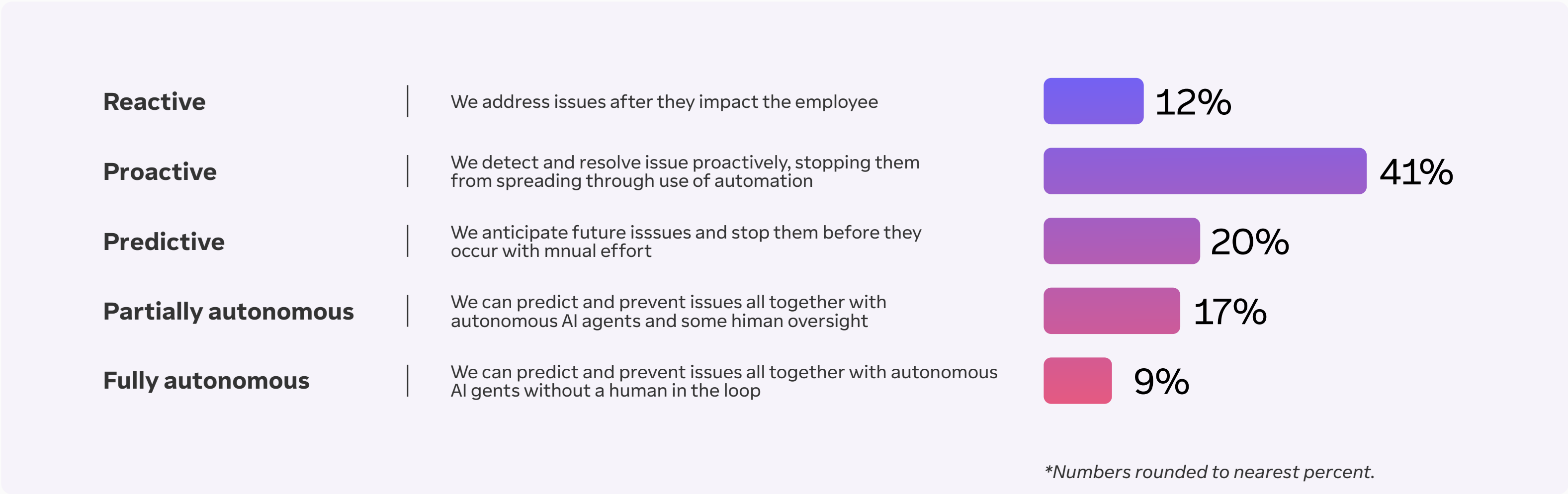
Only **12%** of ITDMs describe their organization’s primary approach to handling technology issues as reactive.

The largest group, **41%**, says technology issues are handled proactively through early detection and automation. This likely does not mean that every IT workflow is proactive today. Rather, it suggests that many organizations have established proactive capabilities for certain recurring issues, systems or use cases.

Combined, **26%** describe their organization as partially or fully autonomous. Here too, the finding should be understood as a signal of progress, not a claim that autonomous IT is fully embedded across the organization. For many IT teams, autonomy is likely concentrated in specific tasks, tools or environments where actions can be clearly defined, monitored and controlled.



Current IT maturity



The findings show meaningful progress. Most organizations no longer rely solely on people reporting issues after disruption occurs. Proactive IT is becoming more common, especially where teams can detect patterns, automate known fixes and reduce repeated incidents.

But the data also shows that fully autonomous IT remains uncommon. For most organizations, predictive capabilities are the next major step, while autonomous IT is still experimental, selective and aspirational.





“Proactive IT has become a much more realistic operating model for many organizations because teams can now detect recurring issues earlier and automate fixes for known problems. The next step is predictive IT: using AI to anticipate friction before it affects the employee experience. Fully autonomous IT is where the market is heading, but for most organizations, it is still emerging. The priority now is to prove autonomy in specific, trusted use cases before expanding it more broadly.”



Andrew Hewitt, VP of Strategic Technology, TeamViewer

T A K E A W A Y

Most organizations have shifted beyond purely reactive support, but autonomous IT is still selective rather than universal. Proactive capabilities are becoming more common, predictive IT is the next step and fully autonomous IT remains an emerging model.



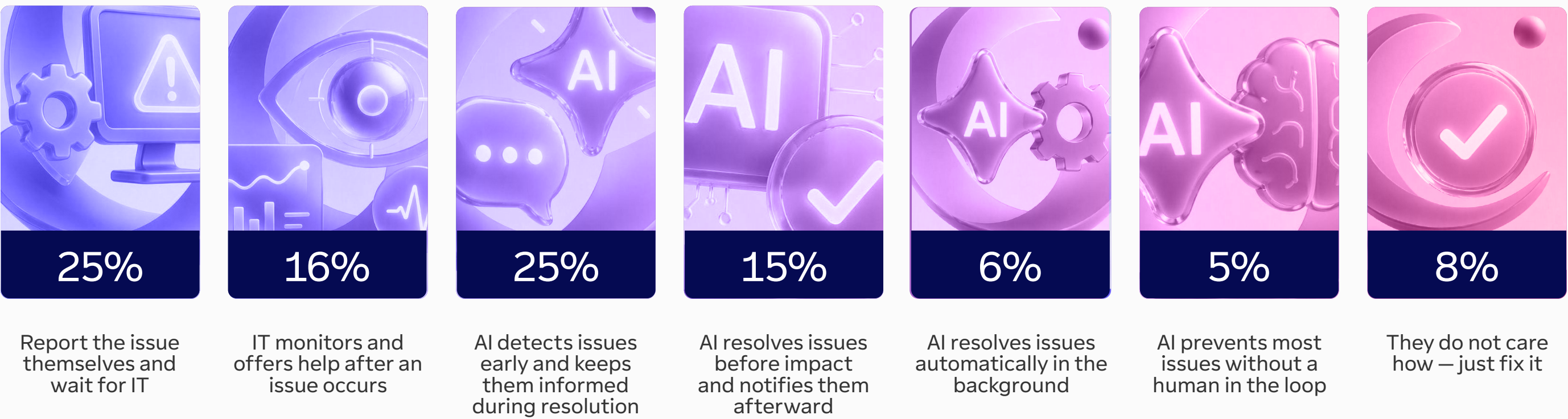


4.4 People want IT issues prevented – but they still want visibility

For most people, the digital workplace is experienced through the tools, devices, applications and systems they rely on to do their jobs. That makes IT support one of the most visible tests of whether autonomous systems can improve work without undermining trust.

Respondents show clear interest in earlier detection and resolution.

How respondents would prefer IT to handle technology issues



Together, **40%** prefer AI to detect or resolve issues before they affect work while keeping them informed during or after the intervention. By comparison, only **11%** prefer AI to operate automatically or prevent issues without human involvement or communication.

A separate finding shows broader openness to AI systems working in the background to handle IT support tasks: **78%** are at least moderately comfortable with AI resolving issues they would normally submit a help-desk ticket for, while only **5%** are not at all comfortable.

Taken together, the results suggest that respondents are receptive to IT becoming more predictive and autonomous, but many are not yet ready for that shift to happen invisibly.

Notifications and clear information about what changed can help preserve trust as intervention moves into the background.





4.5 Human involvement should match the level of risk

Visibility does not necessarily mean that a person must approve every action. The level of human involvement respondents expect depends heavily on the potential consequences.



How much human involvement should AI require when resolving IT issues?

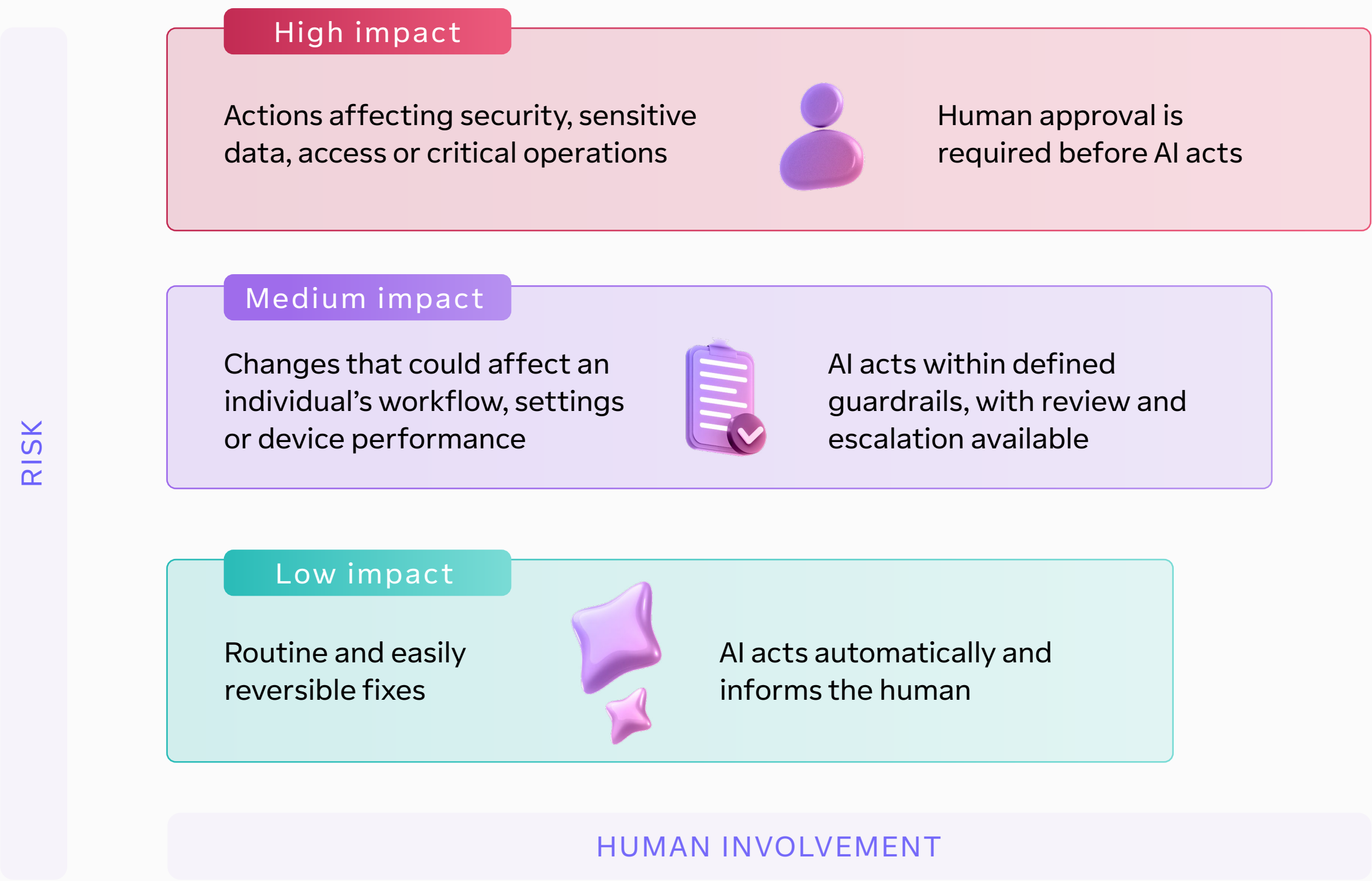




The largest group favors conditional oversight: AI can handle some issues, but a person should become involved when security, data or business operations are at stake. At the same time, nearly one-third still want human involvement before any action, showing that confidence in autonomous resolution is not yet universal.

This approach does not remove people from IT decision-making. It reserves direct human judgment for situations where an incorrect action could have meaningful consequences.

The findings point toward a risk-based model in which oversight increases with the potential impact of an action:



TAKEAWAY

Human oversight should be calibrated to the level of risk rather than applied equally to every IT action.

4.6 Autonomous IT can demonstrate what trusted autonomy looks like

IT provides organizations with an opportunity to test autonomous action in an environment where outcomes can be observed and measured.

Organizations can begin with tasks that are:

 Repetitive

Resolving recurring issues such as clearing application caches, restarting failed services or freeing up disk space.

 High volume

Addressing common problems that affect many people, such as slow device performance, application crashes or connectivity issues.

 Clearly defined

Automating responses when specific conditions are met, such as remediating a known software conflict or restarting an unresponsive application.

 Easy to monitor

Tracking whether an automated fix restored device health, improved application performance or prevented a support ticket.

 Reversible

Rolling back a configuration change or restoring a previous setting if an intervention does not have the intended effect.



Low risk

Handling routine maintenance and performance issues without accessing sensitive data or changing critical business systems.

These use cases allow organizations to establish clear boundaries, measure outcomes and build confidence before extending autonomous action to more complex workplace processes.

That is what makes IT central to the autonomous digital workplace. It is both a proving ground for trusted autonomy and the operational foundation that determines whether digital work runs smoothly, securely and without disruption. The next challenge is determining whether organizations have the leadership, skills, governance and workforce readiness needed to move from isolated use cases to autonomy at scale.



“IT is a natural proving ground for autonomy because the outcomes are visible. You can see whether a fix worked, whether a ticket was avoided, whether performance improved and whether the user experienced less disruption. That measurability is critical for building trust.”



Andrew Hewitt, VP of Strategic Technology, TeamViewer





Section five

Ambition is moving faster than readiness





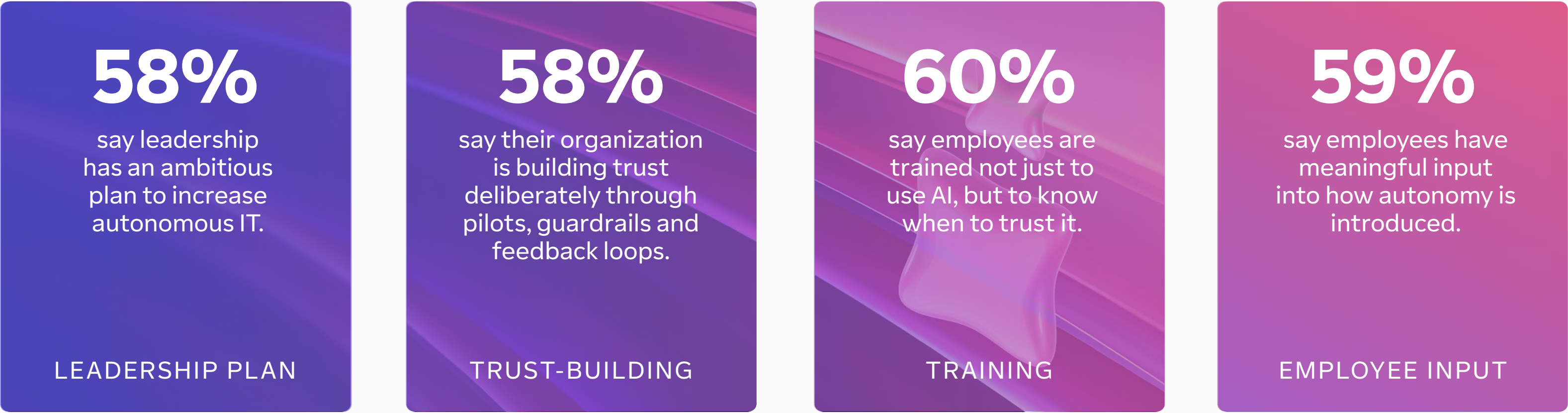
Ambition is moving faster than readiness

Autonomous IT can show what trusted autonomy looks like in practice. But scaling autonomy beyond isolated use cases requires more than technical capability. Organizations need the right foundations: connected systems, clear ownership, defined guardrails, workforce trust and a shared understanding of where autonomous systems can act, where human approval is required and who is accountable when something goes wrong.

The findings suggest that many organizations are moving in this direction, but readiness is still uneven. Leaders may see the opportunity, and IT decision-makers may be more comfortable delegating defined tasks, but confidence across the broader workforce is still developing.

5.1 Organizations are beginning to build the foundations for autonomy

Many respondents say their organizations are already preparing for greater system autonomy.



T A K E A W A Y

Organizations are starting to build the foundations for autonomy, but trust, training and employee involvement are not yet universal.

These findings point to meaningful progress. Many organizations are not approaching autonomy as a purely technical rollout. They are beginning to recognize that trust must be built through pilots, communication, governance and employee involvement.

But the numbers also show that this work is far from complete. In each case, roughly four in ten respondents do not agree that these foundations are already in place. For autonomy to scale, organizations will need to make trust-building a deliberate part of implementation, not something assumed after deployment.



5.2 Personal readiness still trails organizational ambition

While many organizations are preparing for greater autonomy, individual readiness remains more cautious.

Only **35%** of respondents say they are mostly or completely ready to trust AI to act more autonomously in their work. Another **32%** say they are ready only in limited, low-risk situations, while **31%** say they are slightly ready or not ready at all.

This is an important distinction. People may use AI regularly and recognize its benefits, but that does not mean they are ready to give autonomous systems more authority. Readiness depends on whether people understand what the system can do, trust the quality of its decisions and believe they can intervene when needed.

The gap is especially important because organizational confidence can easily be overstated. More than half of respondents say employees in their organization are ready for greater system autonomy, but fewer say they are personally ready to trust AI independently in many areas.

That suggests organizations should not measure readiness only by AI adoption or leadership ambition. They also need to assess whether people feel protected, informed and empowered as autonomous systems take on more responsibility.

Readiness is not the same as usage.



T A K E A W A Y

AI adoption is not the same as readiness for autonomy. People are more likely to trust autonomous systems when they understand their authority, limits and escalation paths.



5.3 Accountability remains a critical trust gap

Autonomy creates a new question for organizations: when a system acts, who owns the outcome?

Only **49%** of respondents agree that accountability is clear when autonomous systems make mistakes.

That uncertainty matters because people are already concerned about being held responsible for actions they did not fully control. Earlier findings show that responsibility is divided across individual users, IT teams, managers and vendors when AI takes an action that negatively affects work.

For autonomous systems to earn trust, accountability cannot default to the person closest to the outcome. Organizations need to define who controls the technology, who approves its use, who monitors performance, who handles escalation and who is responsible for remediation when something goes wrong.

This is especially important for employees, who may have less influence over how autonomous systems are selected, configured or deployed. To build trust, organizations need to show that autonomy will be governed rather than imposed.

That means ensuring:

- People have a meaningful voice in where autonomy is introduced and how its rules, guardrails and approval points are defined.
- The people affected by autonomous decisions understand what authority the system has and where its limits are.
- Responsibility for errors sits with those who control the technology, rather than defaulting to individual users.
- Employees can challenge, escalate or seek review of actions that negatively affect their work.
- The benefits and risks of autonomy are distributed fairly across different workplace groups.



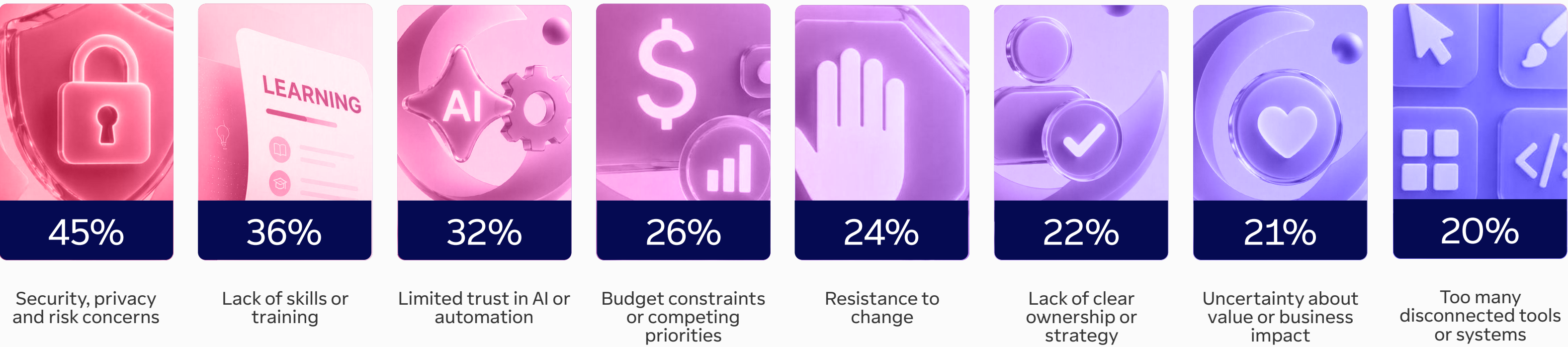
T A K E A W A Y

Trust depends on clear accountability. People are more likely to accept autonomous systems when they know who owns the outcome and how harmful actions can be challenged or corrected.

5.4 Barriers to autonomous IT show what must be solved before autonomy can scale

IT decision-makers also identify significant barriers to greater AI adoption and more autonomous ways of working.

The top barriers include:



These barriers show that the challenge is not only whether AI can perform a task. It is whether organizations have the systems, governance and confidence required to let AI act responsibly.

Security and privacy remain the leading concerns, reinforcing the need for strong access controls, defined permissions and clear limits on what autonomous systems can do. Skills and training are also central, because people need to understand not only how to use AI, but when to trust it, when to verify it and when to escalate.

Disconnected tools create another practical barrier. Autonomous systems rely on context. If workplace data, devices, workflows and support systems are fragmented, it becomes harder for AI to detect issues accurately, act safely and prove impact.



“Customers are not looking for autonomy for its own sake. The business case for autonomy is strongest when it is tied to outcomes people can feel and leaders can measure: time recovered, issues prevented, tickets avoided, risk reduced and employees able to stay focused on their work.”



Mark Banfield, Chief Revenue Officer, TeamViewer

T A K E A W A Y

Scaling trusted autonomy requires secure systems, connected data, clear ownership, workforce readiness and measurable business value.



5.5 Scaling autonomy requires a trusted architecture

The path from isolated autonomous actions to an autonomous digital workplace depends on more than expanding the number of tasks AI can perform. Organizations need a trust architecture that defines how autonomy is introduced, governed and measured.

That architecture should include:

Clear guardrails

What the system can access, decide and change.

Pre-approved actions

Which routine, low-risk tasks AI can complete without individual approval.

Risk-based oversight

When AI can act independently, when it should notify people and when it must pause for human approval.

Visible activity

Logs, explanations and notifications that show what the system did and why.

Escalation and rollback

Clear ways to challenge, pause, reverse or correct AI actions.

Defined accountability

Ownership for system behavior, outcomes and remediation.

Feedback loops

Mechanisms for people to report issues, refine guardrails and improve system performance over time.

This is how organizations can move from experimentation to scale. Autonomy should not be introduced as a blanket transfer of control from people to systems. It should expand gradually, beginning with defined, measurable and reversible use cases before extending to more complex workflows.

Autonomous IT provides an early model for this transition. It shows how organizations can define safe use cases, monitor outcomes, calibrate oversight and build confidence through visible results. The same principles will be needed as autonomy expands across the broader digital workplace.



T A K E A W A Y

Trusted autonomy requires a clear operating model. Organizations need to define where AI can act, where people must approve and how accountability, visibility and control are preserved as autonomy scales.



Section six

The path to the autonomous workplace



The path to the autonomous workplace

The autonomous workplace is not a distant concept. IT decision-makers already expect a significant share of digital workplace services to run autonomously by the end of the decade.

But the findings also show that autonomy will not scale on technical capability alone. People need to trust how autonomous systems act, understand where human oversight remains, and see that accountability, control and transparency are built into the model.

The path forward is not about removing people from every process. It is about moving human effort to where it adds the most value.

6.1 The workplace will become significantly more autonomous

IT decision-makers expect an average of **39%** of digital workplace services to run autonomously by 2030.

Expectations are even higher in larger organizations. Among companies with at least 1,000 employees, ITDMs expect approximately **45% or more** of digital workplace services to run autonomously by 2030.

This signals a meaningful shift in how organizations expect digital work to be supported. Autonomous systems will not remain limited to isolated pilots or narrow experiments. They are expected to become part of the operating model for the digital workplace.

The question is no longer whether workplace autonomy will grow. It is how organizations will govern that growth.

That means defining where autonomous systems can act, how decisions are monitored, when people need to approve or intervene and who owns the outcome when something goes wrong.



T A K E A W A Y

Workplace autonomy is expected to expand significantly by 2030. The challenge now is building the governance, trust and oversight models needed to scale it responsibly.





By 2030

39%

of ITDMs expect digital workplace services to operate autonomously

45%+

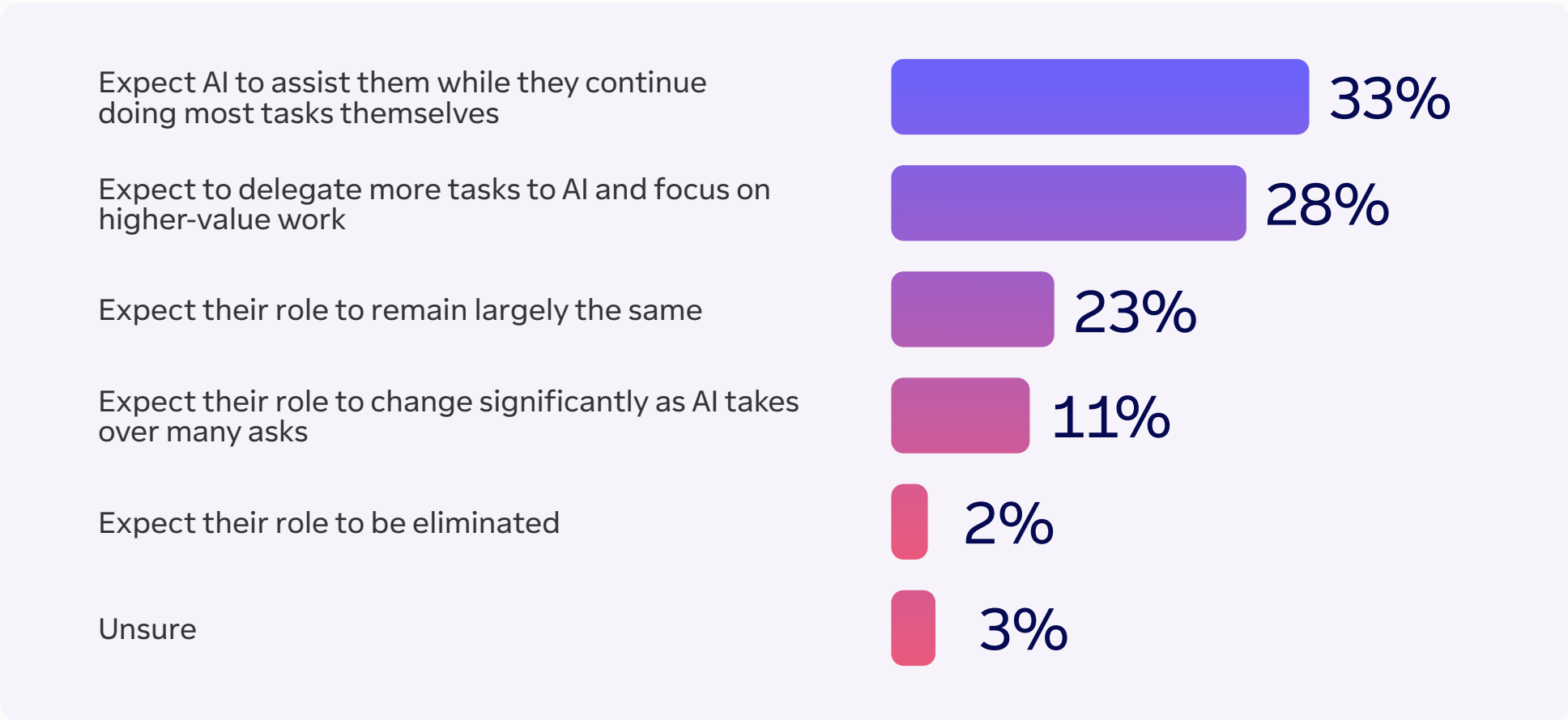
among organizations with 1,000+ employees



6.2 People expect AI to reshape, not eliminate, their roles

Most respondents do not expect AI to replace their role outright. Instead, they anticipate a redistribution of work.

By 2030



These findings suggest that people largely expect AI to change the shape of work rather than remove them from it. The future role of people in the autonomous digital workplace will be less about performing every task manually and more about supervising systems, applying judgment, handling exceptions and focusing on higher-value activities.

This shift will require new skills. People will need to know when to trust AI, when to verify its output, when to intervene and how to escalate decisions that require human judgment.

T A K E A W A Y



Most respondents expect AI to reshape work rather than eliminate it. As autonomy grows, human roles will shift toward supervision, judgment, exception handling and higher-value work.

“AI will change the shape of many roles, but that does not mean the human contribution disappears. It shifts toward judgment, collaboration, creativity and oversight. Organizations need to prepare people for that shift, not treat it as a purely technical rollout.”



Oliver Steil, Chief Executive Officer, TeamViewer

6.3 What organizations must do next

The autonomous digital workplace will not be built by simply adding more automation. It will require a deliberate operating model for trusted autonomy. Organizations should focus on six priorities.

PRIORITY 01

Build the foundation

Autonomous systems depend on context. Before organizations make workflows autonomous, they need connected systems, reliable data, clear ownership and stable processes.

If tools, workflows and data sources remain fragmented, AI will have a limited view of the workplace. That makes it harder to detect issues accurately, act safely and prove impact.

Organizations should begin by improving visibility across devices, applications, workflows and support systems so autonomous systems have the context needed to make reliable decisions.

PRIORITY 02

Start with defined use cases

Autonomy should begin where the risk is manageable and the outcome can be measured.

The best starting points are tasks that are repetitive, high volume, clearly defined, easy to monitor, reversible and low risk. These use cases allow organizations to test autonomous action, measure outcomes and refine guardrails before expanding into more complex workflows.

Autonomous IT provides a practical model. Routine remediation, device optimization and recurring issue resolution can demonstrate how AI acts within boundaries while improving the employee experience.

PRIORITY 03

Match oversight to risk

Not every action requires the same level of human involvement.

Routine, low-risk and reversible actions may be completed automatically within defined guardrails. Medium-risk actions may require notification, review options or escalation paths. High-risk actions affecting security, sensitive data, access or critical operations should require human approval before execution.

This risk-based model preserves human judgment where it matters most without forcing people to review every routine action equally.

6.3 What organizations must do next

The autonomous digital workplace will not be built by simply adding more automation. It will require a deliberate operating model for trusted autonomy. Organizations should focus on six priorities.

PRIORITY 04

Apply the five pillars of trusted autonomy

Autonomous systems will earn trust when people believe they are secure, explainable, bounded, reversible and governed by clear accountability.

Organizations should design around five pillars:

- **Security:** Protect sensitive systems, data and access.
- **Decision quality:** Make system reasoning visible and understandable.
- **Control:** Define what the system can and cannot do.
- **Reversibility:** Make it possible to pause, undo or correct actions.
- **Accountability:** Clarify who owns system outcomes and remediation.

These pillars turn autonomy from a technical capability into a trust model.

PRIORITY 05

Prepare people to supervise AI

As AI takes on more activity, people will need to move from using AI outputs to supervising AI-enabled systems.

Training should go beyond how to use AI. People need to understand when AI can be trusted, when outputs should be verified, when actions require approval and how to intervene or escalate when something does not look right.

This is especially important as human oversight shifts from checking every output before use to supervising defined actions and managing exceptions.

PRIORITY 06

Measure outcomes, not automation volume

The success of the autonomous digital workplace should not be measured by how many tasks are automated.

Organizations should measure whether autonomy improves work.

That includes tracking disruption prevented, time recovered, support tickets avoided, errors corrected, overrides required, employee trust, customer impact and business outcomes.

The goal is not more automation for its own sake. The goal is a digital workplace that works more intelligently, proactively and reliably.

Conclusion

The autonomous digital workplace will be defined by systems that can detect needs, evaluate conditions and take action within clear boundaries. But autonomy does not mean removing people from work. It means changing where human judgment is applied.

People should not have to check every output, approve every routine action or react to every disruption after it occurs. As trusted systems take on more defined activity, people can focus on the work that requires creativity, judgment, empathy, strategy and accountability.

The path to autonomy is not about handing over control. It is about giving trusted systems the authority to act within clear boundaries, so people have more time and energy for higher-value work.



TeamViewer (XETRA: TMV) resolves digital friction before it disrupts productivity. As AI compounds the sprawl of machines, applications, and agents beyond human reach, TeamViewer restores control: observing endpoint health in real time, acting autonomously to keep technology in its desired state, and guiding operators when human judgment is needed. Its TeamViewer ONE platform unifies endpoint management, digital employee experience, and agentic remote support to lead the shift to autonomous endpoint management (AEM). Built on a structural data advantage from millions of AI-captured expert resolutions, the platform powers self-healing technology and grows more capable with every issue it fixes. More than 600,000 customers, from small businesses to the world’s largest enterprises, rely on TeamViewer to keep their digital and physical operations running. Learn more at www.teamviewer.com.

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Germany

TeamViewer US Inc.
3600 Midtown Drive
Suite 1200
Tampa, FL 33607
USA

Stay Connected



www.teamviewer.com