KEY FINDINGS FROM OUR **2025 AI AT WORK SURVEY**

Demystifying shadow AI in the workplace

Secure your enterprise's future by providing high-quality and flexible generative AI

Fuel iX

TELUS Digital

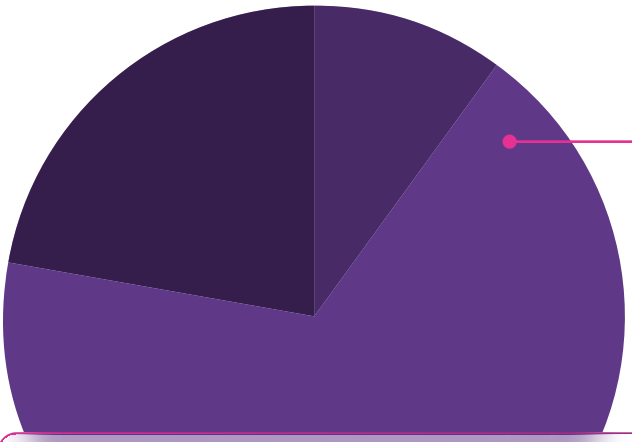
Table of Contents

Humans want to do a better job.

The impact of generative AI (GenAI) in the enterprise has undeniable value to employees. However, this enthusiasm has given rise to a new workplace challenge - shadow AI, also known as bring your own AI (BYOAI), unsanctioned AI, stealth AI and grassroots AI.

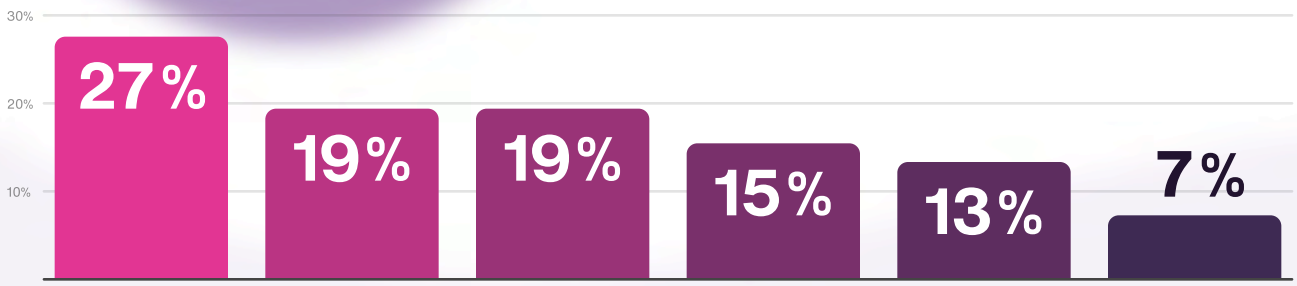
Shadow AI refers to the use of AI tools and applications within an organization without the knowledge or approval of IT departments. Of the **68%** of enterprise employees who use only public GenAI such as ChatGPT, Microsoft Copilot or Google Gemini, through their personal accounts at work, **more than half (57%)** of these employees have admitted to entering sensitive information into these AI tools.

What type of AI assistant have you used at work?



10%	An internal chatbot built by my company
68%	A publicly available chatbot (e.g., a personal ChatGPT or Google Gemini account, etc.)
22%	Both an internal chatbot and a publicly available chatbot

What sensitive information have you entered into a publicly available chatbot?



- I have not entered any of the information above into a publicly available chatbot
- Personal information (e.g., name, email, phone number, address)
- Product or project details (e.g., unreleased product designs, prototypes or launch plans)
- Company details (e.g., company name, mission statement, organizational)
- Customer information (e.g., names, contact details, order history, chat logs, emails or recorded calls)
- Confidential company financial data (e.g., revenue, profit margins, budgets or forecasts)

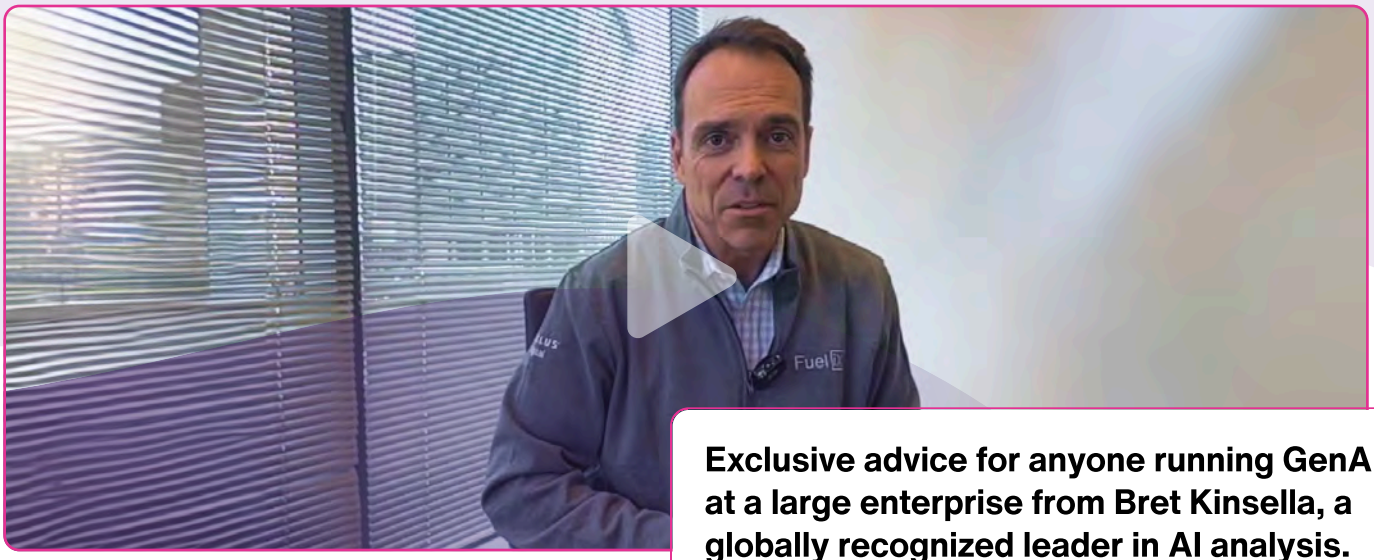
This creates a problem. Organizations cannot manage or mitigate the risks of leaking sensitive customer, employee or company information if they don't know where and how it is being shared. That means AI vendors may use sensitive data to train future models, which would embed that information in the model's knowledge that other organizations could inadvertently access.

It also means that companies may violate customer contracts or government regulations that restrict the sharing of sensitive information with third parties. You can't establish a data sharing agreement with an organization if you're unaware that they've received your protected information.

The data

To better understand the extent of shadow AI, its current risks and why employees turn to it even when they have tools provided by their company, we conducted an extensive survey among enterprise employees.

The survey included 1,835 adults aged 18+ who live in the United States, of which 1,000 work in companies with 5,000 or more employees and have experience using AI assistants such as ChatGPT, Microsoft Copilot, Google Gemini or similar/equivalent internal company chatbots at work.



Exclusive advice for anyone running GenAI at a large enterprise from Bret Kinsella, a globally recognized leader in AI analysis.

Our recent findings underscore a significant trend: there is pervasive use of personal accounts for generative AI enabled assistants within large organizations. The trend is called “shadow AI” because company leaders don’t have visibility into who is using it, what tools are involved, or how it is being used.

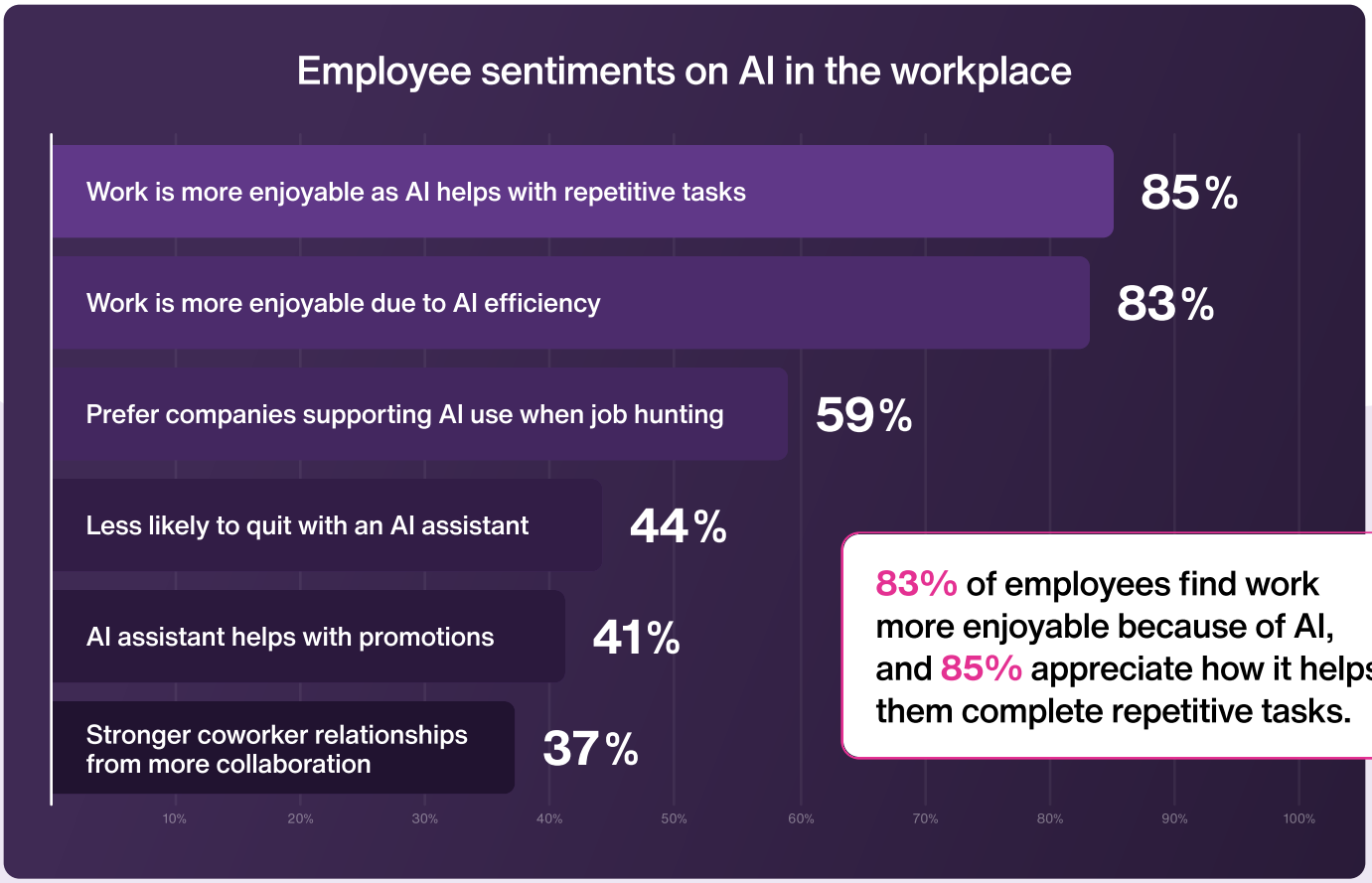
This isn't typically a matter of rogue employees, but rather a testament to the inherent value they see in these technologies. They are using generative AI to enhance their productivity because they want to do their jobs better. However, many are using these AI tools with sensitive customer and proprietary data, and that creates a problem for executives who have a responsibility to manage risk.

AI represents a significant technology transformation that will evolve over the next two decades. While no one can forecast all of the changes it will bring, our hope is that this research will shed light on an important issue faced today by organizations of all sizes. This report also provides insight into steps executives can take to capture the benefits of generative AI while mitigating emerging risks. We hope it provides practical insights and strategies to equip you to better manage the AI technology supercycle.

– Bret Kinsella

Employees are embracing AI at work

As AI reshapes the workplace, professionals are increasingly making career decisions based on an organization's technological capabilities. Our survey shows that employees prefer to work for companies that support the use of AI tools.



83% of employees find work more enjoyable because of AI, and 84.6% appreciate how it helps them complete repetitive tasks. Employees also see AI as a career advantage, with many believing it improves their chances of promotion and helps them build better relationships with coworkers by freeing up time for collaboration.

These feelings have likely contributed to shadow AI. The ease of adopting GenAI tools has exacerbated this trend. Anyone can sign up for a GenAI assistant account in seconds, with many solutions being free or inexpensive.

These tools make it easy to upload documents and process text, but this also means there are virtually no safeguards regarding what type of information is uploaded or processed.

This situation mirrors previous "shadow IT" cycles, where employees brought personal technology into the workplace. From personal computers in the 1980s and 1990s to smartphones in the 2010s, each wave of technology has presented both opportunities and challenges for organizations.

Organizations should consider the following when managing AI adoption while minimizing shadow AI risks:

- ✓ When individuals find value in a new technology, many will start employing it to help them at work without fully considering company policies or risks.
- ✓ Early in new technology adoption cycles, company leadership may not understand the breadth of potential use cases or have a sense of risk stratification across them.
- ✓ Prohibition policies and technical solutions to block usage typically have limits in terms of effectiveness.
- ✓ Providing access to “approved” solutions is an important step to bring use out of the “shadows,” into view by the organization and aligned with company standards and expectations.
- ✓ Providing “approved” solutions is necessary but often insufficient. Organizations generally need to provide solutions that are at least as capable as commonly available consumer solutions; otherwise, users will default to what they view as the “better” capability.
- ✓ Companies need to consider change management that drives the expected behavior of the “approved” solutions and also facilitates transition from the “shadow” solutions.

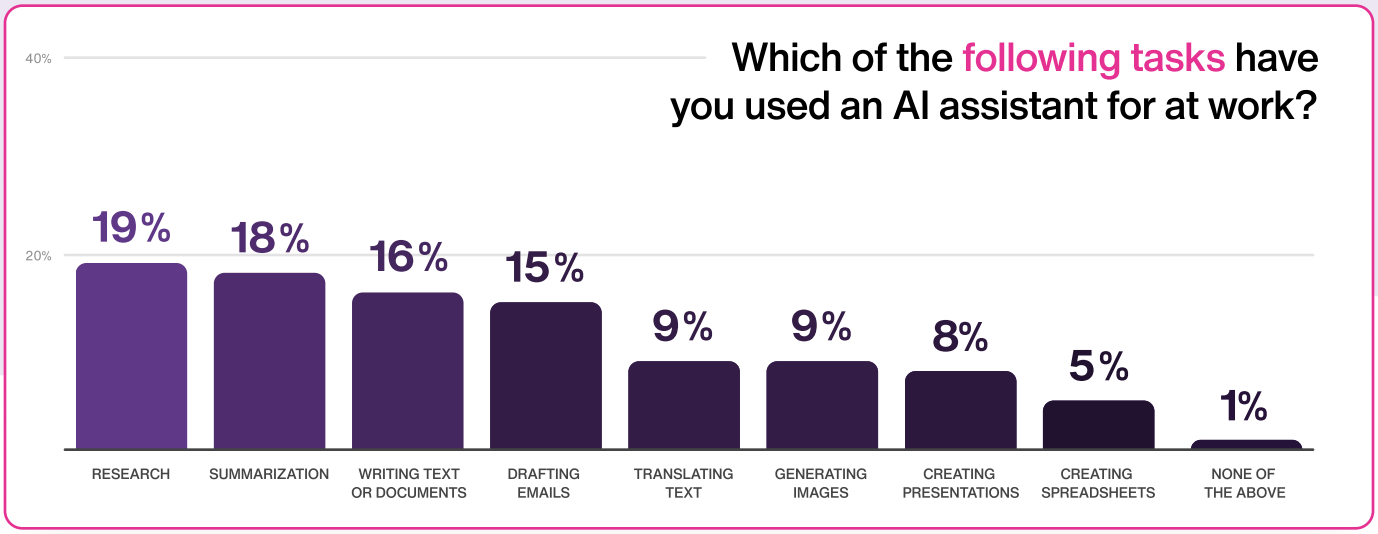
Using lessons learned from shadow IT, organizations can ensure secure and strategic AI adoption in the era of shadow AI.

- Dell Technologies, Forbes

How are employees using AI at work?

Employees have found a way to work smarter. Our survey shows that they're letting AI handle many of their information needs.

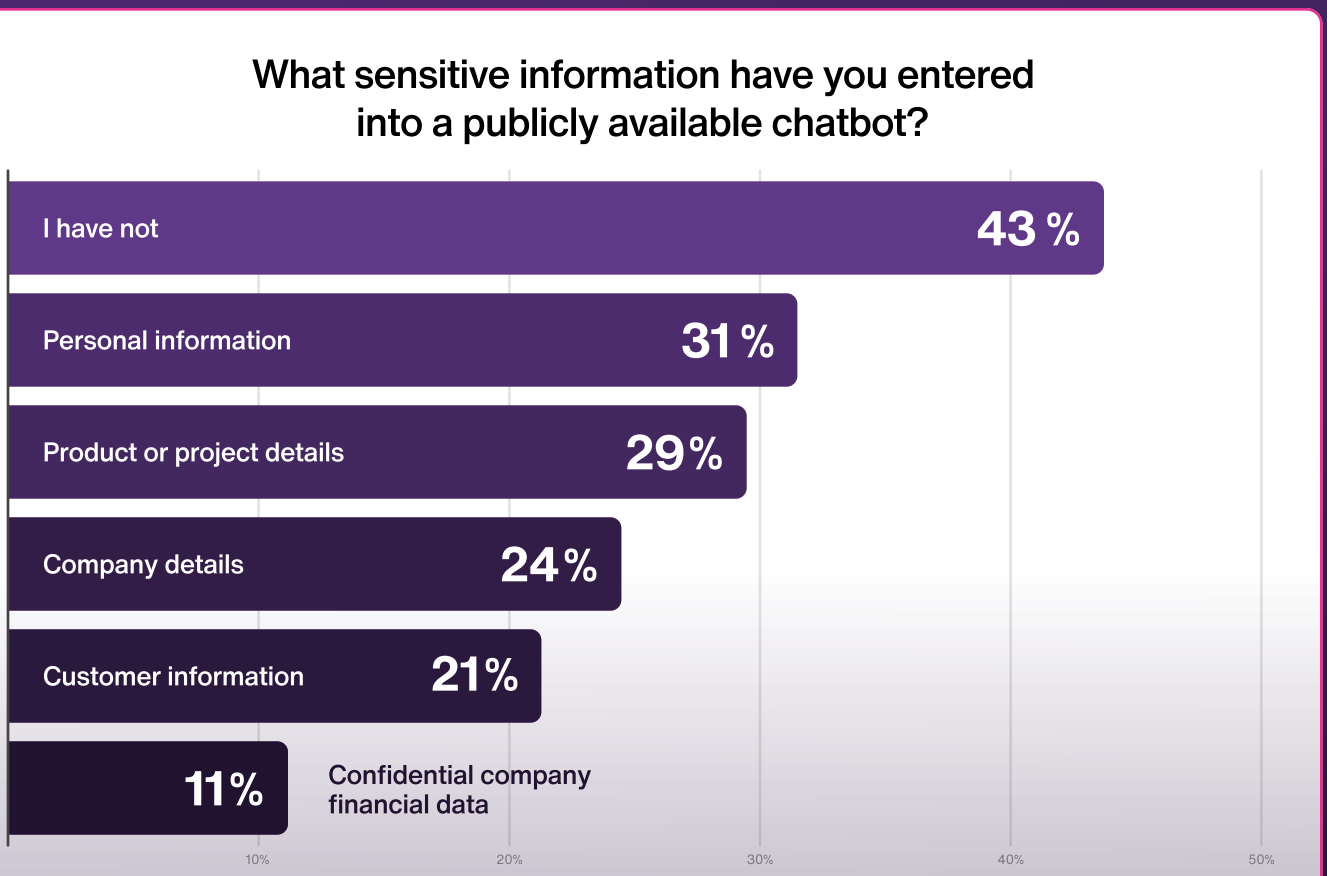
AI adoption is highest for tasks involving information processing and content creation. Research leads the way, with 58.8% of employees using AI for this purpose, followed closely by summarization at 54%. Writing tasks also feature prominently, with 49.7% using AI for writing text or documents. These high adoption rates contrast with more specialized tasks like image generation or spreadsheet creation.



The high adoption of AI for research, summarization and writing tasks signals a significant shift in how knowledge work is performed. Employees can now process information and create content more efficiently than ever. However, it also presents new challenges for organizations. As AI becomes integral to core work functions, companies must balance the benefits of increased productivity with the need for data security and proper governance. Failure to adapt to this AI-driven transformation could leave organizations struggling to remain competitive.

Given these changes, we recommend that organizations:

- ✓ Focus on implementing secure AI solutions for the most commonly used tasks, particularly research and content summarization.
- ✓ Develop clear protocols for AI usage in different types of tasks, especially those involving sensitive information.
- ✓ Offer specialized training for different AI applications, helping employees maximize the benefits while maintaining security.
- ✓ Regularly assess AI tool usage patterns to ensure provided solutions meet evolving employee needs and maintain security standards.



Shadow AI publicly exposes personal and proprietary data

It's unsurprising that employees are using personal GenAI accounts when their companies fail to offer comparable solutions. However, this enthusiasm can lead to misuse and introduce significant enterprise risk.

Of the 68% of enterprise workers who use only public GenAI tools at work, such as ChatGPT, Microsoft Copilot or Google Gemini, through their personal accounts, 57% admit to entering sensitive information into these publicly available large language models (LLMs).

The risks are significant: 33% have entered proprietary product information, 20% have shared customer information and 11% have input confidential company information into these public AI platforms.

This widespread adoption of shadow AI is leading to significant security risks and data breaches. This impact is evident in several ways:

1 Ineffectiveness of current safeguards

- Despite a $3 billion annual investment in data loss prevention, existing solutions are falling short.
- 79% of IT leaders have deployed static email DLP solutions (Egress Data Loss Prevention Report, 2021).
- 72% of organizations have two or more DLP solutions (Cloud Security Alliance report, 2023).
- However, these measures prove inadequate against shadow AI, with nearly a million end users accessing ChatGPT through corporate infrastructures in just the first half of 2023 (CSO Online).

2 High-profile incidents

- Samsung was forced to ban GenAI in 2023 after an engineer accidentally leaked sensitive internal source code by uploading it to ChatGPT.
- A financial services firm suffered a significant data breach when employees inadvertently input client financial information into a GenAI chatbot (Dark Reading, October 2024).
- An employee unknowingly exposed confidential and proprietary data by using Grammarly for communication improvement, unaware that the application could train on the data (Dark Reading, October 2024).

3 Persistent risks

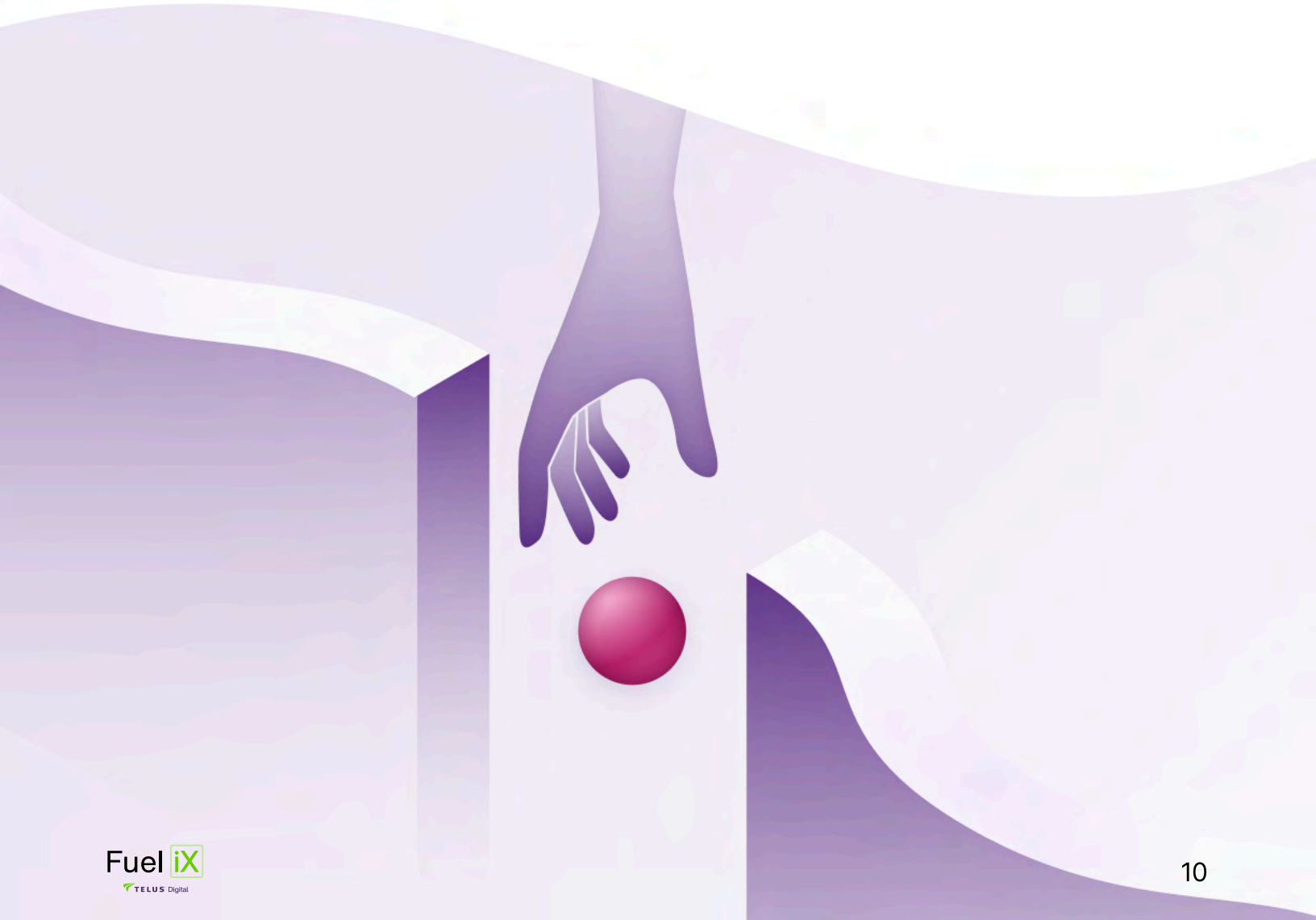
- Data shared with AI chatbots is stored on servers owned by service providers, with limited access and deletion options.
- Employees may unknowingly expose sensitive information through seemingly innocuous tools.
- The rapid adoption of new AI tools outpaces the implementation of corporate safeguards.

The traditional approach to data protection is no longer sufficient in an era where employees can easily access powerful AI tools outside of corporate oversight.

The consequences of inaction include potential data breaches, intellectual property theft and violations of data protection regulations, all of which can lead to significant financial and reputational damage.

Organizations need a comprehensive approach that acknowledges both the appeal and risks of GenAI tools:

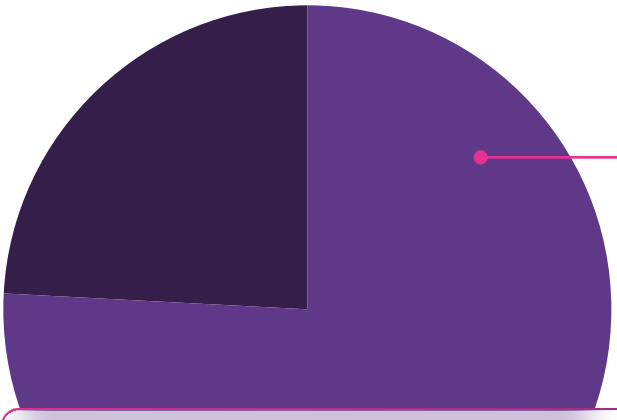
- ✓ Implement secure, company-approved AI solutions that match public tool capabilities.
- ✓ Establish clear governance policies.
- ✓ Conduct regular security audits.
- ✓ Provide employee education about risks.
- ✓ Create an environment where employees feel equipped to use approved tools efficiently.



Companies try and fail to fight shadow AI

There's a significant gap between rapid employee AI adoption and organizational readiness, with many companies lacking comprehensive AI governance structures. This disconnect leads to widespread unauthorized AI use, even when approved alternatives exist.

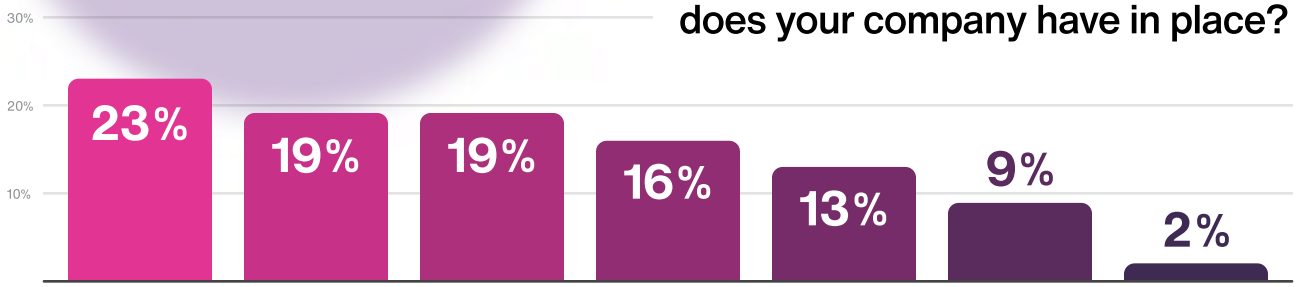
Our survey reveals some striking findings. Surprisingly, **24.2%** of organizations have no AI guidelines or policies in place at all. Among those that do, approaches vary widely: 29% prohibit inputting sensitive company information into AI assistants, 23.6% require mandatory AI training for employees, 16.4% implement content marking for AI-generated materials, 11.1% restrict access to public AI tools like ChatGPT and 2.6% completely prohibit AI use.



75.8% Companies with AI guidelines or policies

24.2% Companies with no policies

Which of the following AI guidelines/policies does your company have in place?



- Don't input company, client or other sensitive info into AI assistants
- Every employee must undergo mandatory AI assistant training
- My company does not have AI guidelines/policies in place
- I don't know if my company has AI guidelines/policies in place
- Note when content has been generated by AI
- My company does not permit the use of publicly available AI (e.g., ChatGPT)
- My company does not permit the use of AI

Despite these measures, the U.S. National Cybersecurity Alliance reports that less than half of employees receive proper AI safety training, making policy enforcement challenging. Even more concerning, **our data shows that more than two-thirds of employees report using personal GenAI assistant accounts, despite having access to company-approved alternatives.**

The impact is significant. The lack of AI governance and training creates security vulnerabilities and compliance risks for organizations. Policy enforcement becomes increasingly difficult when employees prioritize convenience and productivity over security, leading to the widespread use of unauthorized AI tools. This exposes companies to potential data breaches and undermines efforts to standardize AI usage across the enterprise.

To effectively address these challenges, organizations need to implement AI solutions that enable centralized management of GenAI applications, providing specific security and control mechanisms. These solutions should include:

Enterprise-grade security

- Privacy and data sovereignty controls.
- Enhanced security features for AI systems.
- Safe deployment in both shared and private environments.

Governance features

- Centralized control over custom and third-party AI solutions.
- Unified observability and orchestration.
- Comprehensive governance and moderation capabilities.

Flexibility and control

- Ability to switch between different LLMs and cloud providers.
- Vendor lock-in prevention.
- Standardized AI excellence across the enterprise.

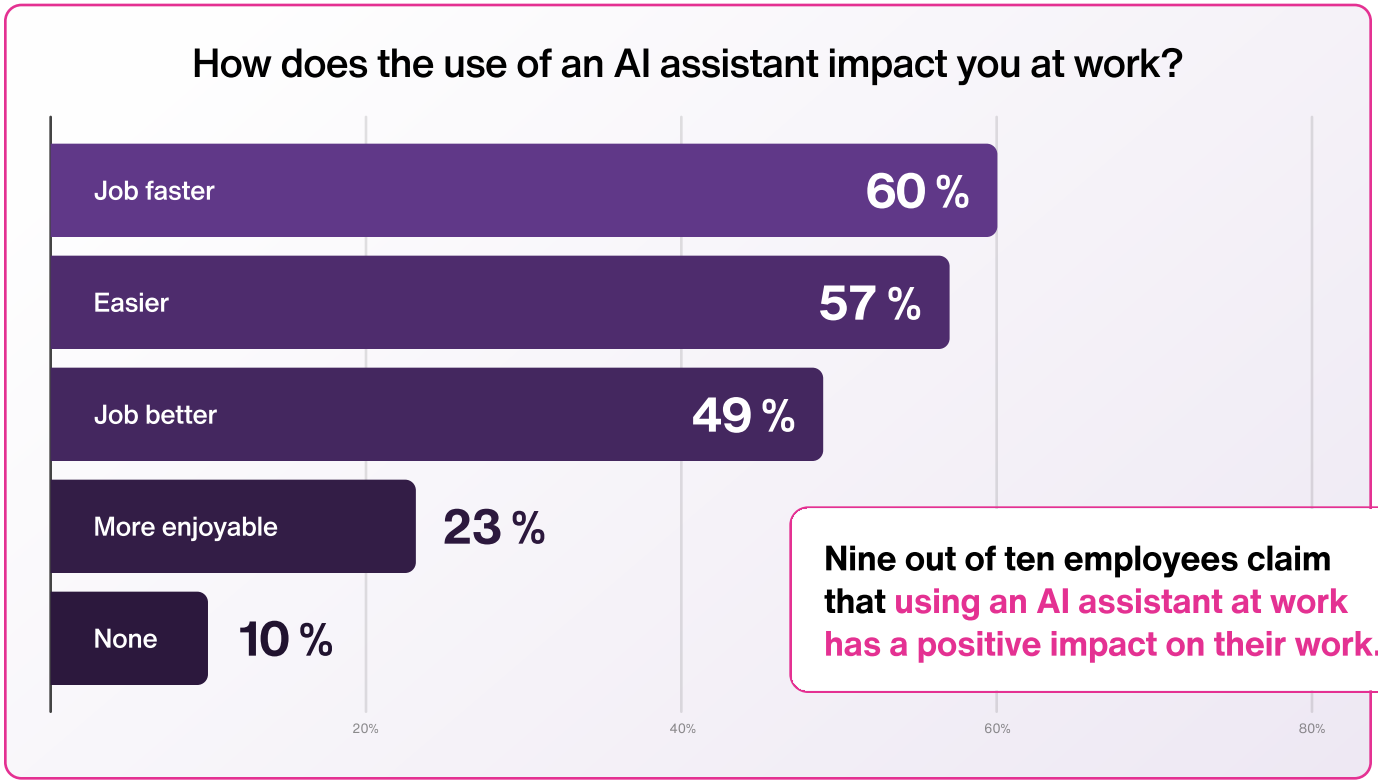
Safety features

- Automated vulnerability detection.
- Stress-testing of AI systems for safety.
- Simulation of real attacks on GenAI copilots.

This systematic approach helps organizations bridge the gap between employee AI usage and organizational readiness, providing the flexibility employees need while maintaining necessary security controls.

The benefits to employees are too great to follow the rules

Employees are not following the rules because the career benefits outweigh the risk. They want to do a good job - that means meeting deadlines and exceeding expectations. Many have also heard the adage, **“knowledge workers are less likely to be replaced by AI than by other workers using AI.”**



Our survey findings reveal the extent to which AI impacts workplace efficiency. Nine out of ten employees claim that using an AI assistant at work has a positive impact on their work. A majority of employees report that AI helps them work faster (60.1%) and makes their job easier (56.8%). Nearly half say it improves their job performance (49.1%), while 23.3% find their work more enjoyable with the help of AI.

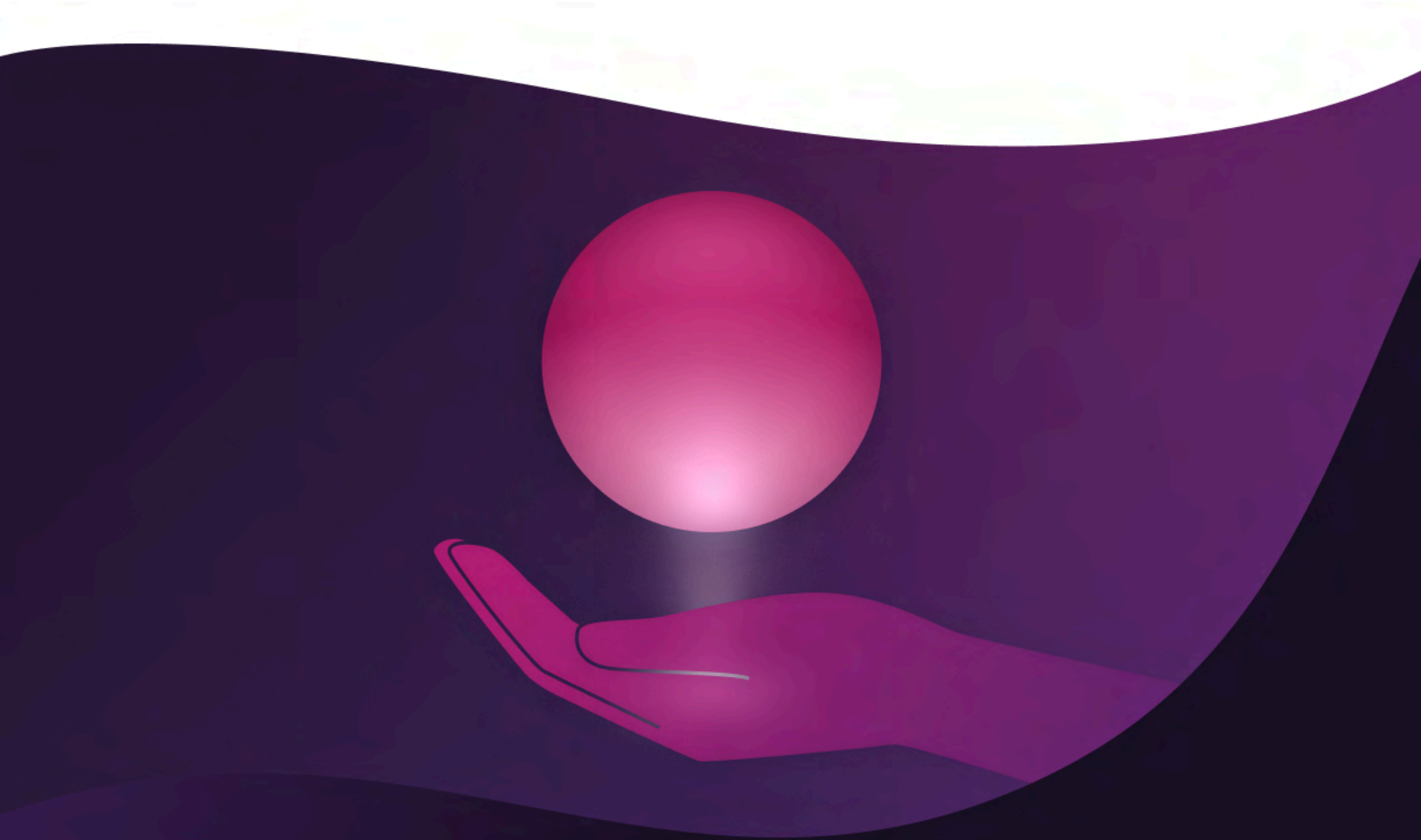
Consider a marketing team at a large enterprise like Salesforce. Before GenAI, brainstorming sessions often resulted in similar ideas being recycled. Now, team members can generate hundreds of unique content ideas in minutes. They can craft compelling narrative options and even easily create visually stunning graphics. This drives efficiency and expands creativity, which improves the odds of success.

They use AI tools for various tasks, including:

- ✓ **Generating initial drafts and outlines for blog posts.**
- ✓ **Creating social media copy.**
- ✓ **Producing email subject lines.**
- ✓ **Developing key talking points for videos.**

Companies should reassess their AI policies and tools. It's crucial to evaluate the feature parity between approved corporate solutions and publicly available AI assistants. Employees may have established expertise with particular AI tools, which could undermine the adoption rates of company-approved alternatives.

Developing AI policies that balance productivity benefits with security requirements is essential. Also, creating migration paths from unauthorized to approved AI tools that preserve workflow efficiency can help ensure compliance without sacrificing the performance gains that employees have come to rely on.



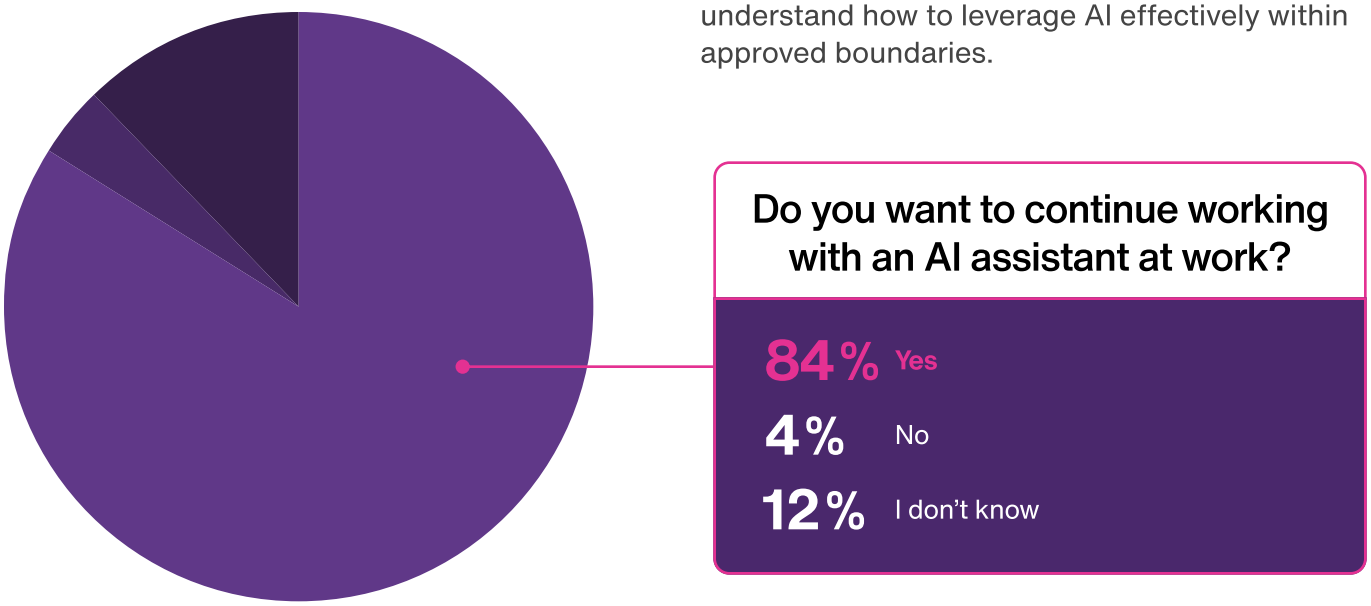
Taking AI away is not the answer

Removing AI from the workplace is counterproductive and may increase risk for organizations. The focus should be on implementing flexible usage policies and tools that enable productive use while effectively managing potential risks.

This approach is crucial, considering that a striking 85% of employees express a desire to continue using AI assistants after initial exposure. Such high adoption rates indicate that AI tools are rapidly becoming an integral part of many employees' work processes, making it essential for organizations to adapt rather than restrict.

A 2024 SHRM survey, while not providing specific percentages, indicates that limiting AI use could lead to frustration and decreased productivity. A lack of access to AI tools could increase the likelihood that employees will seek and misuse unauthorized alternatives. This could lead to security risks and compliance issues for organizations.

Organizations should implement flexible AI policies that enable productive use while managing risk, rather than imposing overly strict limitations. This approach should include providing secure, company-approved AI solutions that have been vetted for security and compliance, reducing the temptation to seek unauthorized alternatives. Clear usage guidelines are essential, helping employees understand how to leverage AI effectively within approved boundaries.



Supporting these policies with comprehensive training ensures employees can maximize the benefits of approved AI tools while adhering to company policies. Additionally, regular feedback channels allow employees to provide input on AI tools and their needs, helping organizations stay responsive to evolving requirements and maintain employee satisfaction. **By embracing AI as a strategic asset in this way, organizations can enhance job satisfaction, drive innovation and mitigate the risks associated with shadow AI use.**

Strategic recommendations for complete shadow AI management

Core strategic approach

- Implement flexible AI policies that balance productivity with risk management.
- Provide enterprise solutions that match or exceed public alternatives.
- Create environments where employees naturally choose sanctioned tools.
- Transform potential security challenges into strategic advantages through proactive management.

Employee engagement & training

- Deliver specialized training programs for approved AI tools.
- Establish clear usage guidelines and documentation.
- Create regular feedback channels for tool improvement.
- Implement robust change management programs.
- Provide continuous education about sensitive information risks.
- Maintain ongoing training for sanctioned solutions.

Technical implementation requirements

- Support safe deployment in both shared and private environments.
- Enable flexibility to switch between different LLMs and cloud providers.
- Implement automated vulnerability detection systems.
- Conduct regular stress-testing of AI systems.
- Perform simulated attack scenarios on GenAI copilots.

Security & governance framework

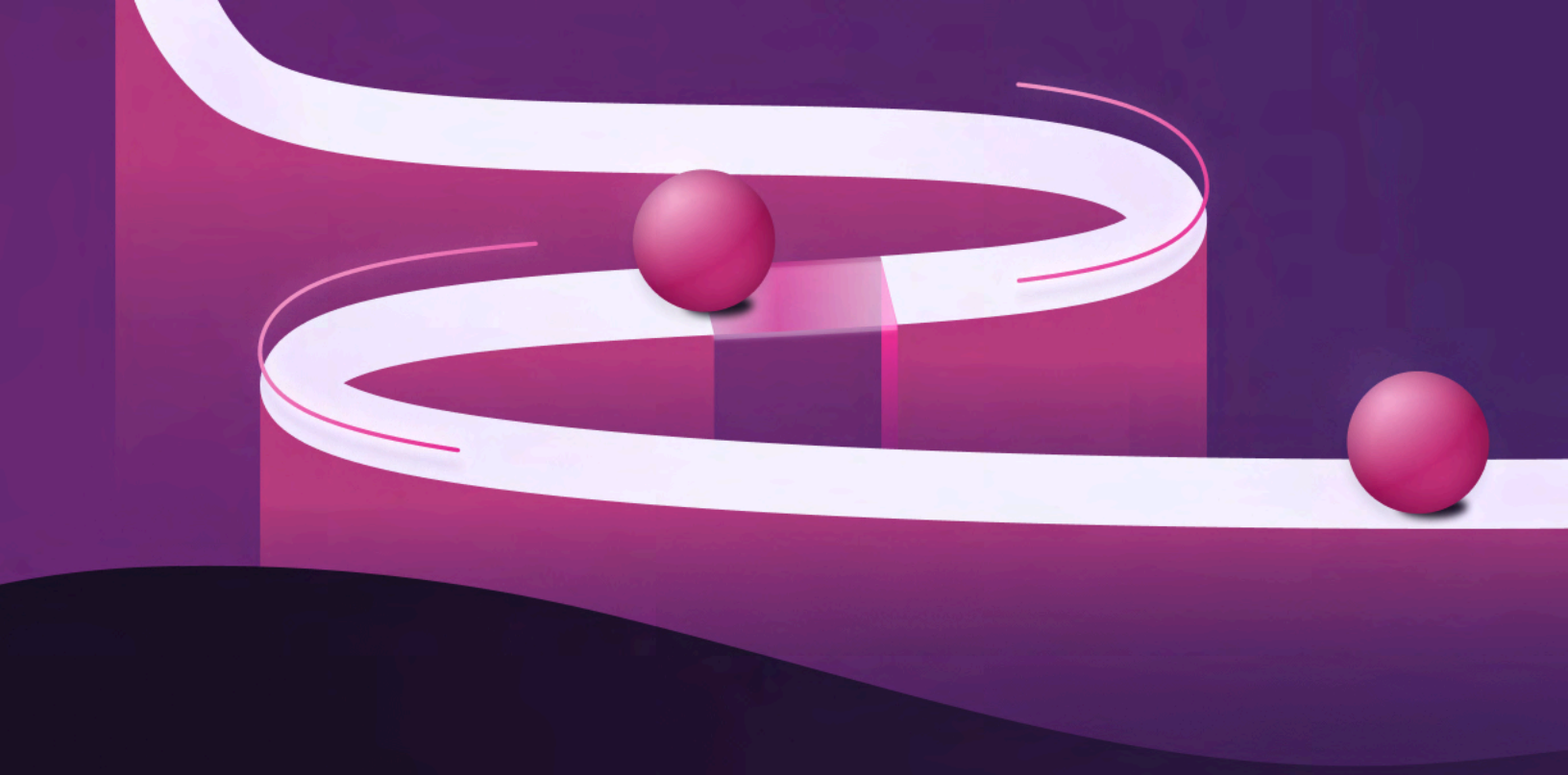
- Extend beyond traditional DLP solutions.
- Maintain centralized control over custom and third-party AI solutions.
- Establish unified observability mechanisms.
- Implement comprehensive orchestration protocols.
- Conduct regular security audits.
- Develop vendor-agnostic architecture.

Risk management & monitoring

- Assess AI tool usage patterns continuously.
- Monitor emerging security threats.
- Conduct regular policy reviews.
- Ensure compliance with data protection regulations.
- Perform security standard assessments.
- Track effectiveness of approved solutions.
- Adapt to evolving security challenges.

Critical success factors

- Maintain feature parity with consumer alternatives.
- Balance security requirements with productivity needs.
- Communicate policies and risks clearly.
- Foster supportive environment for approved AI adoption.



Fuel iX was designed to fight shadow AI

The importance of balancing security with democratization cannot be overstated. Fuel iX's GenAI platform achieves this balance by offering robust security and compliance measures alongside advanced capabilities. This approach enables enterprise leaders to foster productive AI usage while effectively mitigating shadow AI risks.

- **Model flexibility:** Integrates various AI models and tools seamlessly, reducing the need for unauthorized AI.
- **Collaborative copilots:** The unique ability to share copilots and information across the organization prevents employees from using personal AI tools to solve problems. This enhances internal collaboration and learning, mitigating the risks of shadow AI.
- **Enhanced security:** Provides robust security measures to protect data and ensure compliance.
- **Comprehensive governance:** Supports safe, responsible AI management aligned with policies and ethical standards.
- **No vendor, cloud or platform lock-in:** Allows flexibility and control without being tied to a specific vendor.
- **Proven success:** Demonstrated success in large enterprises like TELUS, saving significant time and resources.
- **Employee satisfaction:** Encourages the use of approved tools, which boosts job satisfaction and reduces shadow AI risks.

How TELUS combated shadow AI

TELUS tackled the shadow AI challenge head-on with an enterprise-wide strategy using Fuel iX. By providing universal access across their global workforce, TELUS ensured every employee had access to the latest LLM technology within a secure environment. The platform's robust tool-calling capabilities and intuitive copilot customization features enabled teams to create AI copilots tailored to specific needs, tasks, and domains. Critical to their success was the ability to securely ground responses in company data, eliminating the need for employees to seek external AI solutions.

Key Outcomes through early 2025:

- Created over 7,000 custom GenAI employee assistants across more than 50,000 global employees.
- Saved employees over 500,000 hours, reducing time spent per task by over 40 minutes.
- Enhanced productivity and innovation while maintaining privacy and security guardrails.

How TELUS built a flexible enterprise AI solution that empowers 50,000+ employees

READ MORE ON THE BLOG

Fuel iX is an enterprise AI platform developed through the collaborative efforts of TELUS and TELUS Digital. The platform seamlessly integrates company infrastructure with an extensive library of LLM models and generative AI applications, providing complete observability and control throughout the process. Designed to address a critical gap in the GenAI landscape, Fuel iX enables enterprise-scale management of AI applications, foundation models and data sources within a framework built to deliver safe, responsible and accurate AI-powered experiences.

The platform's model-agnostic approach serves over 50,000 users enterprise-wide, with its excellence recognized through the Responsible AI Institute's Outstanding Organization 2023 prize. TELUS's GenAI Customer Support tool, powered by Fuel iX, became the world's first to achieve ISO 31700-1 Privacy by Design Certification.

VISIT US AT FUELIX.AI

Fuel iX

TELUS Digital