ManageEngine

The Shadow AI Surge in Enterprises

Insights from the US and Canadian workplace

Index

Introduction

While IT departments race to implement AI governance frameworks, many employees have already opened a back door for AI. Shadow AI, the use of unauthorized AI tools, has quietly infiltrated organizations across North America, creating blind spots that even the most vigilant IT leaders struggle to detect.

This report reveals a critical disconnect: the gap between IT perception and employee reality in North American enterprises. Based on insights from over 700 IT decision-makers and employees across the US and Canada, this study reveals that Shadow AI isn't just a compliance problem—it's a leadership alignment crisis.

The data points to a clear policy-practice gap: 91% of organizations claim to have AI policies in place governing employee use of AI tools, yet 70% of IT leaders have identified unauthorized AI use in their organizations, and 78% of employees report coworkers using unapproved tools.

Shadow AI is more than just unsanctioned software use. It is a reflection of systemic gaps in governance, communication, and security culture. While employee experimentation with AI may be well-intentioned, the risks to data integrity, regulatory compliance, and organizational reputation cannot be overlooked. This report aims to guide enterprise IT and business leaders toward a more structured and secure AI future.

Respondents profile

In May 2025, 700 IT decision-makers and working professionals across the United States (US) and Canada (CA) answered questions a range of Shadow AI issues for ManageEngine. Respondents fell into the following two categories:

1

Sample one:

350 IT decision-makers (from managers to C-suite) across the US and CA (250 in the US and 100 in CA) who work in companies that generate at least $10 million in annual revenue and have at least 500 employees.

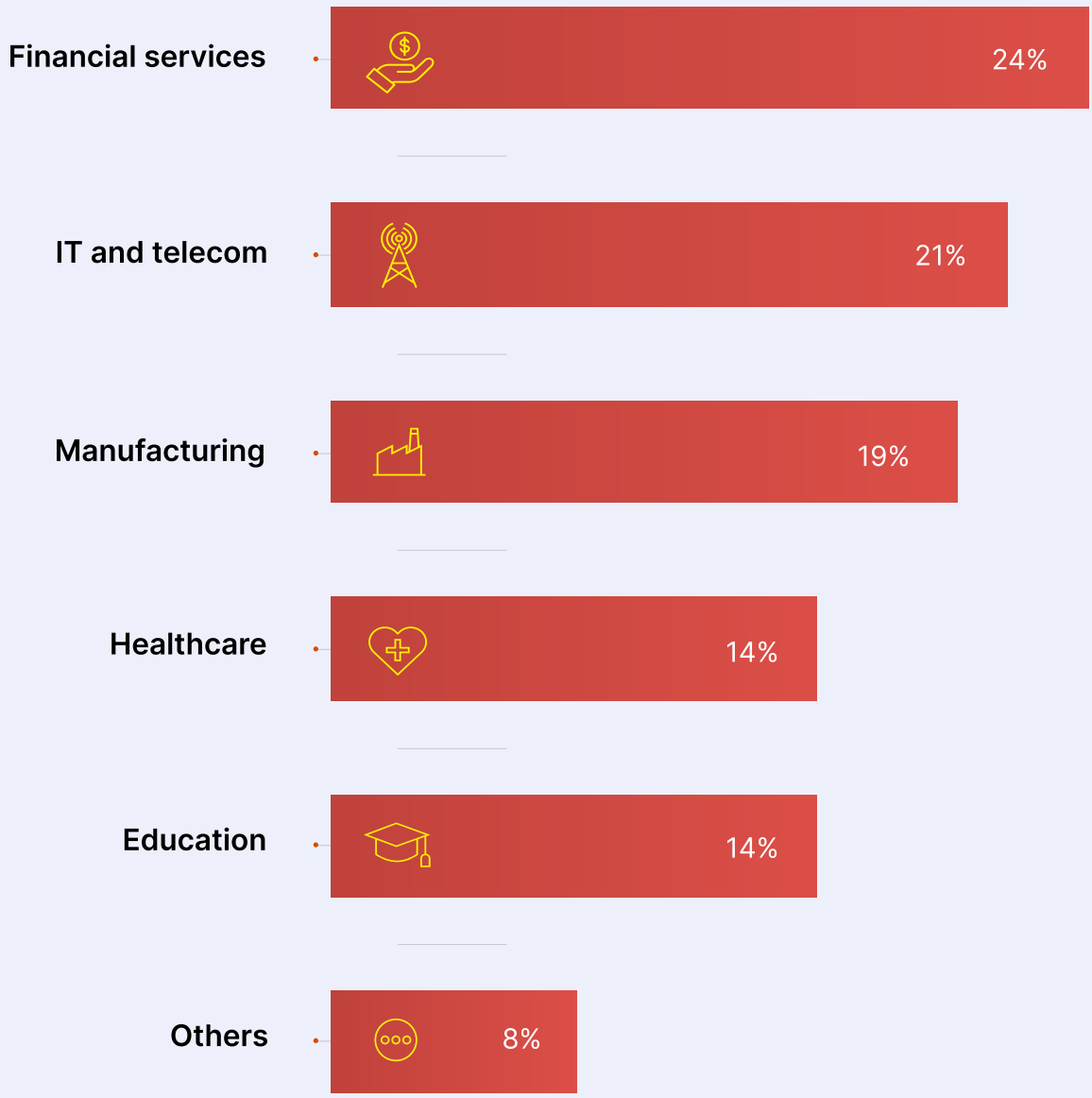
2

Sample two:

350 (250 in the US and 100 in CA) working professionals, working across HR, marketing, finance, sales, and operations in companies with at least $10 million in revenue and at least 500 employees.

This dual-perspective approach, gathering insights from both policy enforcers and technology users, ensures that the findings reflect the real-world complexity of AI deployment in mid-sized and enterprise environments.

Respondents by industry



The rise of unauthorized AI use

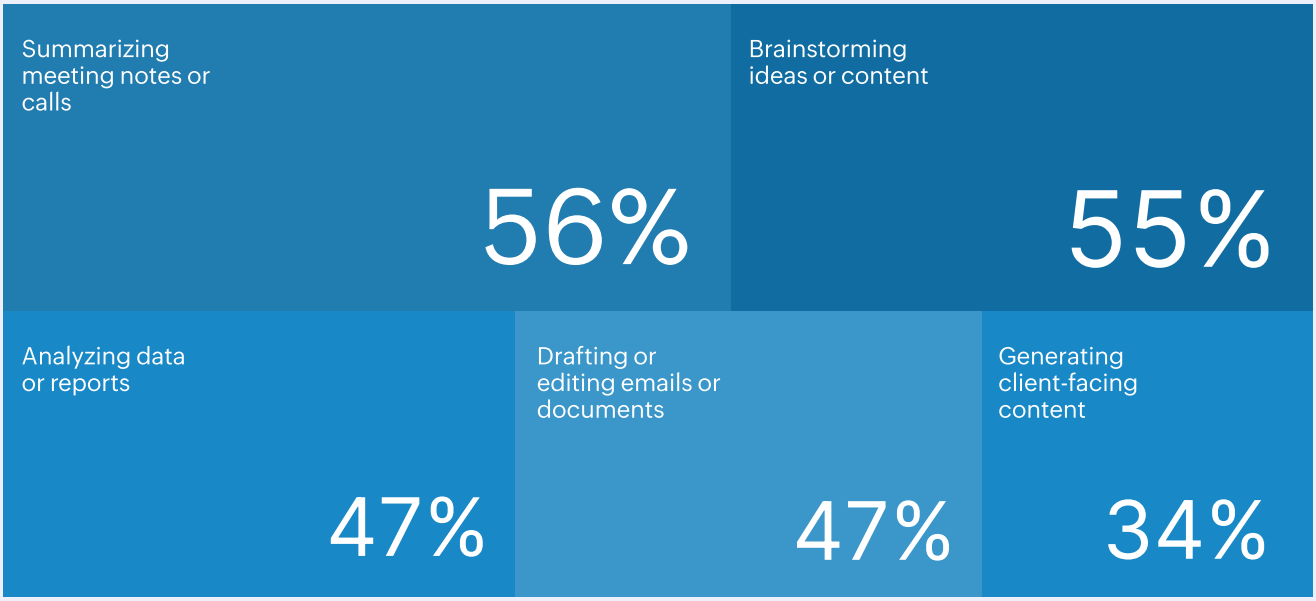
Despite formal guidelines and sanctioned tools, shadow AI has become the norm rather than the exception:

- **70%** of IT decision-makers have identified unauthorized AI use within their organizations.
- **93%** of working professionals admit to inputting information into an AI tool without approval.
- **60%** of employees admit their use of unapproved AI tools has increased in the past year.
- **82%** of US-based employees know coworkers who are using AI tools without IT authorization.

These aren't isolated incidents. Rather, they represent a fundamental shift in workplace behavior. Shadow AI has evolved from experimentation to integration, becoming embedded in daily workflows across departments.

What employees are actually doing:
The most common unauthorized AI activities reveal how deeply these tools are embedded in routine work:

Top unauthorized use cases



While these use cases may appear harmless, they introduce significant risk when data privacy, security protocols, and regulatory compliance aren't considered. The gap between perception and reality becomes more concerning when examining what information employees are sharing with these unauthorized tools.

Drivers behind unauthorized use and the confidence paradox

This study, gathering perspective from both IT leaders and employees, reveals that shadow AI is driven by more than convenience or productivity benefits. The real story lies in organizational system failures that create conditions for unauthorized AI use to thrive.

Employee justifications reveal organizational gaps
Contrary to assumptions about deliberate defiance, the data reveals shadow AI is driven more by confusion, convenience, and misplaced confidence than rebellion:

Top justifications for unauthorized use

These responses expose three critical organizational gaps:

Knowledge gap

90% of employees trust unauthorized AI tools to protect their data, while 50% believe there's little to no risk in using unapproved tools. This false sense of security stems from fundamental employee misunderstandings about how AI models process and potentially retain information.

Process gap

According to **48%** of IT decision-makers, employees are bypassing formal approval processes when adopting new tools. This suggests that official channels may be perceived as too slow, unclear, or disconnected from employees' day-to-day needs.

Leadership gap

Only **31%** of IT decision-makers believe senior leaders from other departments fully understand shadow AI risks, creating a governance vacuum where policies lack organizational support and enforcement.

IT leadership confidence in governance:
Ninety-six percent of IT decision-makers believe their governance frameworks will hold steady or improve with adjustments over the next year. This represents significant organizational confidence in AI governance capabilities. Organizations in the US and Canada are positioning themselves as early adopters of mature AI governance.

However, confidence doesn't equal execution:

85%

of IT leaders agree that employees are adopting AI faster than IT teams can assess them.

82%

agree that it's challenging to control unauthorized AI use by employees.

95%

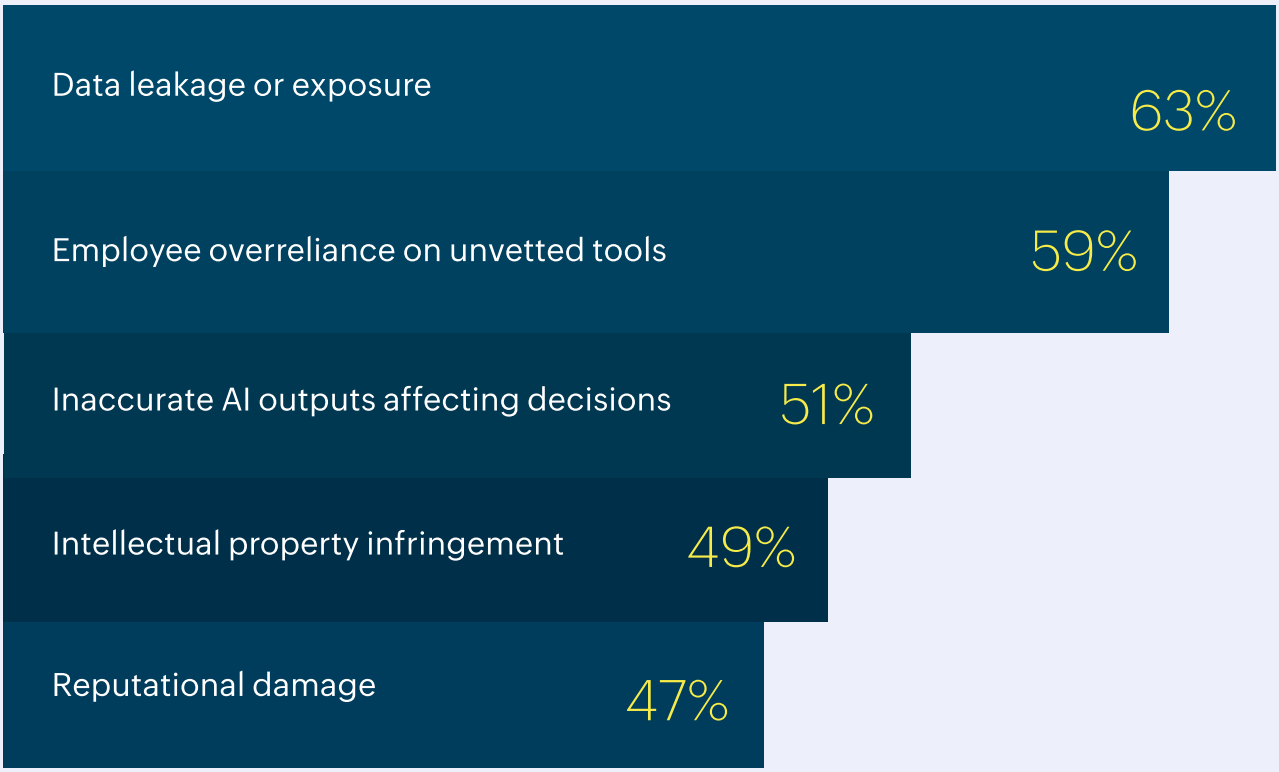
acknowledge organizational blind spots exist, primarily due to employees lacking awareness of AI-related security risks.

only 5%

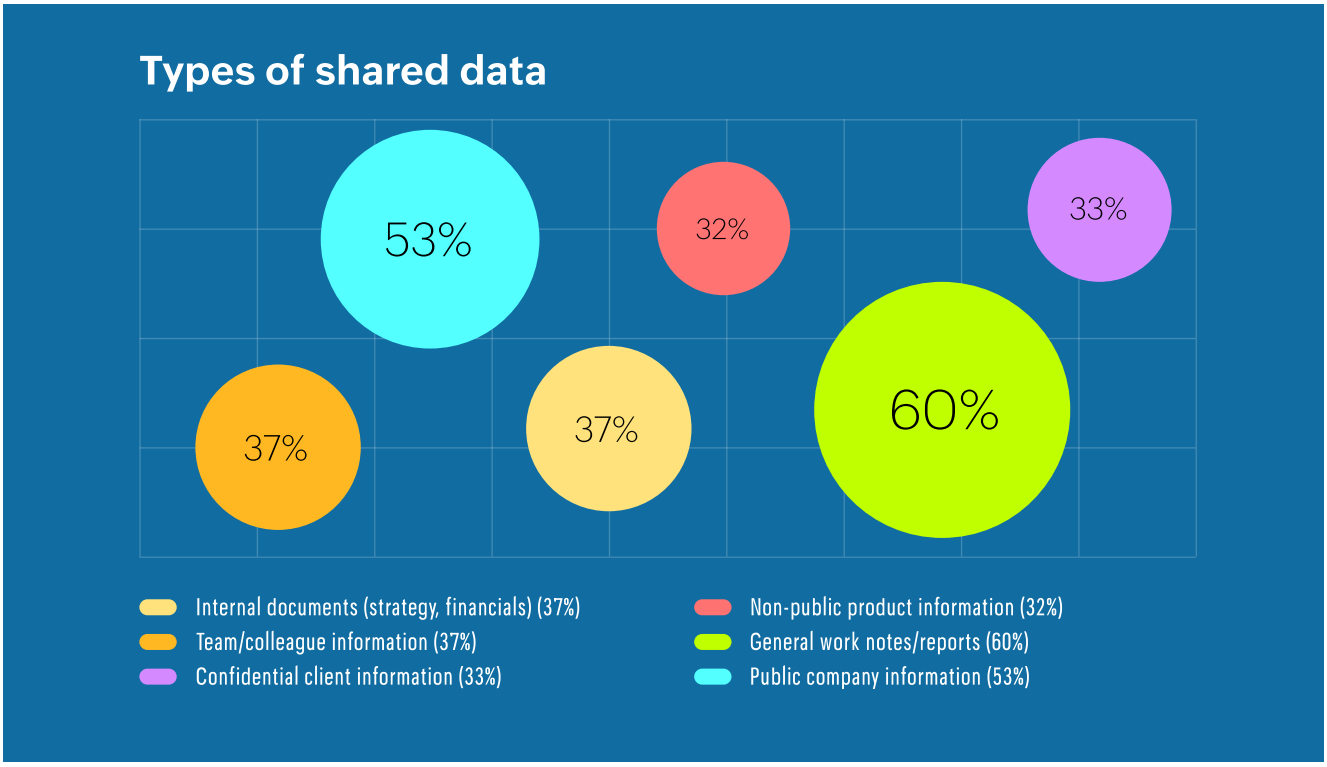
of IT decision-makers claim they have zero blind spots in their organization created by AI.

This confidence-execution gap presents both an opportunity and a warning for IT leaders. The question isn't whether organizations believe they can solve shadow AI, it's whether they're implementing the right solutions.

Top risks identified by IT leaders



What's being shared without authorization: More than one-third of employees admit to sharing sensitive information with unauthorized AI tools:



When employees use AI tools outside the organization's visibility, they're not just bypassing IT, they're bypassing decades of security protocols and compliance frameworks. In the AI era, trust in the tools must be matched by an equal trust in processes.

— **Ramprakash Ramamoorthy, Director of AI Research, ManageEngine**

Leadership blind spots, governance gaps, and organizational fallout

The persistence of shadow AI reveals deeper organizational disconnects that extend beyond IT departments, creating leadership blind spots and governance gaps.

The leadership challenge
Organizations face a complex challenge that spans multiple levels of leadership:

The visibility problem
While 91% of organizations reported having established AI governance policies—with 55% claiming clear, enforced guidelines—shadow AI continues to proliferate. This paradox points to critical blind spots in how policies are communicated, implemented, and monitored.

Key governance disconnects:

65%
of IT leaders say non-IT senior leaders underestimate shadow AI risks.

57%
of IT leaders believe their current governance models will remain enforceable within a year.

39%
report inconsistent policy enforcement across their organizations.

The enforcement challenge
Despite having policies in place, organizations struggle with practical implementation. The gap between policy creation and behavioral change suggests that traditional top-down approaches aren't sufficient for managing AI adoption in the modern workplace.

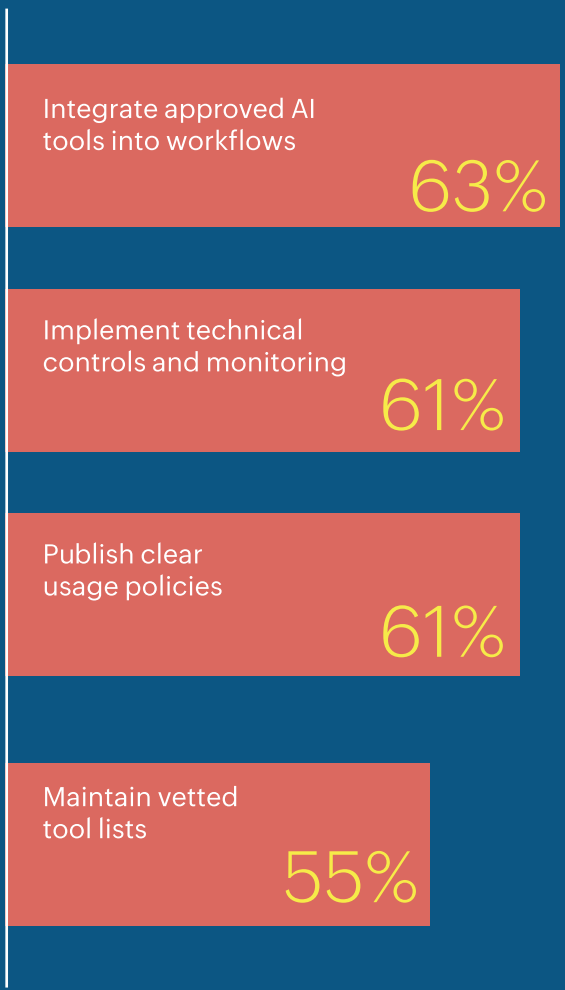
This misalignment can create a dangerous cycle: Employees continue using unauthorized tools because they don't understand the risks, while leadership focuses on policy creation rather than education and enablement.

How IT leaders are responding

Organizations have an opportunity to establish strategic AI enablement. The data shows these organizations are positioned to move beyond reactive policies toward competitive advantage through intelligent AI governance.

Building a smarter response
There is no one-size-fits-all fix. But both IT leaders and employees agree on some of the changes needed to address Shadow AI.

What IT leaders are doing to reduce shadow AI



What employees report they need

The alignment between these lists suggests a path forward, but the employee emphasis on practical and relevant policies indicates that governance success depends on usability, not just security.

The AI governance blueprint
Based on the dual-perspective data, successful shadow AI management requires addressing three specific organizational dynamics:

Leadership-IT alignment

Close the 65% gap between IT understanding and senior leadership awareness through executive education and cross-functional governance teams.

Policy-reality integration

Move beyond the 91% policy implementation rate to focus on practical enforcement and user-centric design.

Confidence-execution matching

Leverage the strong confidence in governance (96%) to build proactive rather than reactive AI strategies.

Strategic enablement over restriction:
Organizations have an opportunity to redefine a new approach to shadow AI—one that channels employee initiative rather than restricting it:

- **Rapid tool provisioning:**
  Beat employees to emerging AI tools rather than blocking access after adoption.
- **Innovation sandboxes:**
  Create safe spaces for AI experimentation within governance frameworks.
- **Competitive intelligence:**
  Use shadow AI patterns to identify market opportunities and workflow improvements.
- **Cultural integration:**
  Make AI governance a business enabler rather than a compliance burden.

The path forward

The shadow AI challenge represents both organizations' greatest AI governance risk and a strategic opportunity for those that can effectively channel employee AI innovation while maintaining security. While 85% of IT leaders agree that employees adopt AI faster than teams can assess tools, this acceleration also positions forward-thinking organizations ahead of more cautious competitors—when managed properly.

Organizations that will thrive are those that reframe shadow AI from a security threat to a strategic indicator. Employee AI adoption patterns reveal genuine business needs and competitive opportunities that restrictive policies miss entirely.

Strategic imperatives for leaders:

1. **Transform IT from gatekeeper to enabler**
   Use organizational confidence in governance evolution to build proactive rather than reactive frameworks.

2. **Leverage the leadership gap**
   Close the disconnect between IT and senior leadership to create organization-wide AI alignment.

3. **Channel innovation energy**
   Use employee AI usage patterns to guide official enablement.

4. **Build adaptive governance**
   Create frameworks that evolve with AI advancement rather than restricting access.

Shadow AI isn't merely evidence of employee recklessness—it's proof of workplace innovation culture. The organizations that will lead the AI economy are those that harness this initiative rather than suppress it.

The question isn't whether shadow AI will continue. The question is whether organizations will use their position to establish the governance models that enable safe, strategic AI adoption at scale.

Methodology

This report is based on a study conducted in May 2025 by Censuswide, commissioned by ManageEngine. The study surveyed 700 full-time IT decision-makers and working professionals employed across the United States (500) and Canada (200). Among the respondents, 442 worked at large enterprises and 258 at mid-sized organizations. All participants were employed at companies with over $10 million in annual revenue and at least 500 employees. The research complies with ESOMAR and British Polling Council standards.