# What Is Shadow AI And Why It Is A Growing Risk For Enterprises

What is Shadow AI, and are you ahead or behind this trend? How vigilant is your IT department in handling it? You could be walking on thin ice when it comes to compliance and potential regulatory violations.

Research from a McKinsey report, entitled “[AI in the Workplace - A Report for 2025](https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work),” shows employees are using GenAI more than their leaders. Beyond a doubt, Shadow AI is now becoming a high-priority risk for CIOs, CTOs, and HR leaders.

This article provides an in-depth look at ShadowAI. It explains why it is spreading and outlines the business risks it poses to enterprises. Learn how you can respond as an IT or HR leader with secure, governed AI strategies.

## What Is Shadow AI?

The term, Shadow AI, refers to the use of artificial intelligence tools or systems within an organization without formal IT approval, governance, or oversight. These could be items such as:

* Apps
* Large Language Models (LLMs)
* Plugins
* Tools

[Generative AI](https://en.wikipedia.org/wiki/Generative_artificial_intelligence) (GenAI) has taken enterprises by storm. You can’t blame your employees for using AI. Employees want to use it to make their work easier. The two most common reasons are to complete tasks more quickly and to automate them.

Is this good for business, as surely it can lead to higher productivity rates? Yes and no. Productivity may increase in the short term. But over the longer term, Shadow AI will cause serious problems unless you have IT oversight.

### Real-World Examples of Shadow AI

It can be hard to think of a time when we were not using some form of AI in our lives. As its usage becomes more commonplace, people are becoming more used to it. That is why Shadow AI has become such an issue. Here are some examples:

* Developers are using AI code assistants like Copilot and GitHub without obtaining a license.
* HR teams are generating interview questions or feedback summaries using free AI tools.
* Marketing teams are using ChatGPT to write all their content across different platforms.

## What Is The Difference Between Shadow AI and Shadow IT?

You might have heard the term Shadow IT as well and wondered what the difference is between the two. The difference is:

* Shadow AI is an unauthorized *intelligent system* that can make or influence decisions.
* Shadow IT is unauthorized software or hardware.

### Why is Shadow AI More Dangerous?

Both are challenging for IT and HR leaders to manage, but Shadow AI is far more dangerous than Shadow IT. It's because the outputs from Shadow AI could be acted on directly in your organization.

Think about areas in your business such as AI-generated emails, policies, and reports. Additionally, AI learns from inputs, and this can raise various long-term privacy and IP issues.

If you have not considered Shadow AI in your leadership role, it’s time to take it seriously. Indeed, the same report from McKinsey found 47% of the C-suite felt they were developing GenAI too slowly, although 69% invested more than a year ago.

## 

## 

## Why Shadow AI Is Growing in Enterprises

There are several reasons why Shadow AI is growing in enterprises. Here are five of the most common reasons, so you can understand how to assess them in your organization:

### Fragmented Understanding of Risk

Not every employee in your organization is going to have the same understanding of the AI tools. Consequently, some employees do not have a grasp of the risks the company could face.

### Innovation Pressure from Leadership

“*Be more productive*,” “*Automate more*,” “*Do more with less.*” Do these sound familiar? It can be challenging being a CIO or CTO when pressure comes from the top. Sadly, this pressure can lead to quick decisions with no proactive planning.

### Lack of Internal AI Strategy or Approved Tools

At [ReadyAI.dev](https://readyai.dev/), we understand your dilemma. AI feels like yet another level of work you must urgently attend to. However, when you are busy, an internal AI strategy might start sliding down your list of urgent things to do.

Indeed, we find most companies do not have a formal AI governance plan or secure alternatives. It’s a challenging situation to be in. We work closely with IT leaders in your position daily to help them resolve it.

### Rapid Accessibility of Generative AI Tools

Free, user-friendly, browser-based tools are everywhere. Understandably, your employees are seeking ways to enhance their productivity and alleviate stress. Ironically, their actions to take on AI quickly are causing more harm than good.

### Remote and Hybrid Work

A post-COVID environment has changed the working environment for employees. Now, with hybrid and remote work in nearly every business. There is less visibility into employee tools and their behaviour when they use them.

## The Key Risks of Shadow AI

While innovation continues to advance at a rapid pace, so do the risks. The rise of employees using GenAI might begin with good intentions. But ungoverned AI can create serious business risks. Here are five areas to consider:

### Data Leakage

Employees are inputting sensitive information (client names, internal documents, code) into AI tools. Many AI tools store or learn from this data unless the settings are changed. There is a high risk of confidential information appearing in future model outputs.

### Regulatory Non-Compliance

Unvetted AI tools in your organization might be violating:

* GDPR
* HIPAA
* Industry-specific compliance (e.g., in financial reporting)

Additionally, you might not have any audit trails, consent logs, or data usage documentation. Also, it’s important to note that liability can fall on the organization, not on the employees.

### Operational Silos and Inconsistency

Teams might be adopting different tools, but there is no central control. It can lead to inconsistent decision-making, duplicated AI efforts, and conflicting outputs. There is also [a high risk of the productivity paradox](https://www.afr.com/policy/economy/how-ai-risks-repeating-the-it-productivity-paradox-20250727-p5mi5j), with fast but fragmented operations.

### Security Vulnerabilities

### Unknown vendors or plugins might introduce malware, phishing, or create backdoor risks. You could have a lack of endpoint control or tool visibility for IT. You also have no clear way to track model versioning, data flow, or your threat exposure.

### Trust and Reputational Damage

Your errors or AI-generated hallucinations could become public knowledge. For example, big law firms are now facing legal issues because they are submitting court filings with [made-up citations from AI chatbots.](https://www.reuters.com/legal/government/trouble-with-ai-hallucinations-spreads-big-law-firms-2025-05-23/)

There have also been cases of AI-generated customer communications with incorrect or biased information. All these instances can lead to a loss of stakeholder trust when data misuse goes public.

## The Cost of Ignoring Shadow AI

It has reached a point where Shadow AI is too important to ignore. As Reid Hoffman, the Co-Founder of LinkedIn, said, “*AI is going to reshape every industry and every job*.” Given this situation, it is essential to know the costs of ignoring it:

**Direct Costs**

There could be the costs of breach containment or internal investigations (or both). Also, fines for regulatory breaches.

**Indirect Costs**:

It could cause internal disruption because of the sudden freezing of all AI tools. Additionally, morale could go down due to overly restrictive AI policies.

**Real-World Scenario:**

To put the costs into perspective, consider the case of three Samsung engineers who [used ChatGPT to fix proprietary code](https://www.pcmag.com/news/samsung-bans-chatgpt-after-engineers-use-it-to-fix-proprietary-code). This action resulted in a total ban of ChatGPT and other GenAI tools across the company.

## How To Identify and Govern Shadow AI Use

Now that you understand what Shadow AI is and how it can drastically affect your business. Here are five steps you can follow to start identifying and governing Shadow AI use in your organization.

### **Step 1: Acknowledge It Is Already Happening**

Accept that Shadow AI is already in use in your enterprise. This acceptance will help you to start from a place of transparency, not punishment.

### **Step 2: Audit and Monitor Employee AI Usage**

Use endpoint monitoring via surveys or employee interviews. This process will help you map which employees are using what tools and why.

### **Step 3: Develop a Clear AI Governance Policy**

First, you must define:

1. What tools are approved
2. What data employees can and cannot use
3. What roles are responsible for AI oversight

Next, include some guidelines for experimentation vs. operational use

Finally, to create a clear AI governance policy, you must integrate the compliance, IT, legal, and department heads.

### **Step 4: Offer Secure, Compliant Alternatives**

Provide vetted AI platforms in your enterprise that are:

* + Auditable
  + GDPR-compliant
  + Integrated with enterprise workflows

For example, [ReadyAI.dev’s secure enterprise AI platform](https://readyai.dev/solutions/security) has built-in data safeguards for GDPR, SOC II, and HIPAA.

### **Step 5: Train Employees and Enable Responsible Use**

Offer AI literacy and training for all employees so they can understand what they can and cannot do, and more importantly, why.

Also, do not forget to keep encouraging innovation. Your role as an IT or HR leader is to promote innovation and growth within the company, but within set guardrails.

## Why Secure Enterprise AI Platforms Are Essential

To achieve the level of security you need, you must work with a secure AI platform that has the following:

* Admin oversight and usage analytics
* Data segregation
* End-to-end encryption
* Role-based access control

In comparison to a public tool, you will have:

* Consistent performance and policy alignment
* Full audit trails
* Safer data input/output

## From Shadow AI to Strategic AI

You are in a powerful position as an IT or HR leader to make a real difference in your organization. It’s about empowering your employees to use the full potential of AI but in a safe and organized manner.

Shadow AI is not a fringe issue that might become a problem. It’s an enterprise-wide reality. However, if you use the right approach with governance, visibility, and a secure platform, you will manage it.

The future of enterprise AI is not about banning tools but about building trust and control. We can help you bring GenAI under enterprise control. [Book a demo](https://readyai.dev/contact) to see ReadyAI.dev in action and learn how it can support your AI strategy.

## Sources:

1. AI in the Workplace: A report for 2025 - [McKinsey](https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work)
2. Generative Artificial Intelligence - [Wikipedia](https://en.wikipedia.org/wiki/Generative_artificial_intelligence)
3. How AI Risks Repeating the IT Productivity Paradox - [Financial Review](https://www.afr.com/policy/economy/how-ai-risks-repeating-the-it-productivity-paradox-20250727-p5mi5j)
4. Trouble With AI Hallucinations Spreads To Big Law Firms - [Reuters](https://www.reuters.com/legal/government/trouble-with-ai-hallucinations-spreads-big-law-firms-2025-05-23/)
5. Samsung Bans ChatGPT After Engineers Use it to Fix Proprietary Code - [PC Mag](https://www.pcmag.com/news/samsung-bans-chatgpt-after-engineers-use-it-to-fix-proprietary-code)