# 5 Warning Signs Your Teams Are Using Shadow AI Tools

According to PwC’s “[2024 Cloud and AI Business Survey,”](https://www.pwc.com/us/en/tech-effect/cloud/cloud-ai-business-survey.html) 67% of top-performing companies are already realizing the value of using Generative AI (GenAI). AI is helping teams move faster, but is your organization keeping up?

In the rush to adopt GenAI, many employees are using tools without IT approval. This precarious situation is known as Shadow AI. These tools can introduce significant risks into your business, such as compliance breaches, data leaks, and operational chaos.

This article reveals five key warning signs that Shadow AI may already be active in your organization. Also, learn how you can take a proactive approach and respond to these threats before anything goes wrong.

\*\*\* Not sure what Shadow AI is? Start here: [What is Shadow AI and Why It Is A Growing Risk For Enterprises](https://readyai.dev/insights/what-is-shadow-ai) \*\*\*

## 5 Warning Signs of Shadow AI In Your Enterprise

Here are five warning signs you can monitor to check if Shadow AI is in your enterprise. It might surprise you to know it is already in your business.

### Sudden Spikes in Content Volume or Productivity

The company experiences a sudden spike in content generation, such as designs, emails, and reports. The alarm bells should certainly ring if this coincides with no new hires in the company.

**Why This Matters:**

Your employees could be using AI content generators, such as [ChatGPT](https://chatgpt.com/) and [Jasper](https://www.jasper.ai/), without any guidance.

**Risk To The Organization:**

The quality of the content could become inconsistent, the content generators might create hallucinated facts, and the outputs could go live without a review.

### Employees Start Asking Vague Tech-Related Questions In Chat

A dead giveaway is employees asking random tech-related questions in work chat or forums. It could be along the lines of, “*Anyone else using the XYZ tool?*” or “*How do I hide browser extensions?”.*

**Why This Matters:**

This trend indicates that employees are experimenting with unapproved tools on company time and work devices.

**Risk To The Organization:**

The tools might not be compliant with your company policies or privacy regulations, such as those related to [GDPR](https://gdpr-info.eu/), [HIPAA](https://www.hhs.gov/hipaa/index.html), etc.

### Data Leakage or Anomalies in Usage Logs

The usage logs will start to look different. You might notice sensitive prompts popping up in browser histories, and there could be unexpected traffic to AI APIs.

**Why This Matters:**

Your sensitive business data could be entering third-party AI models. Also, it could happen without encryption or consent.

**Risk To The Organization:**

It could lead to a permanent exposure of trade secrets from the company, personal data, or IP.

### Strange or Inconsistent File Formats in Deliverables

You might start receiving documents that have unusual formatting, or the responses and work feel robotic or generic.

**Why This Matters:**

It could indicate that employees are using AI tools that export, or it could be copy-paste content.

**Risk To The Organization:**

The AI-generated content could bypass existing approval processes or brand voice checks.

### A Growing Gap Between IT-Sanctioned Tools And Reality

For example, your marketing team could be using one AI tool, your product team another one, and the IT department has approved neither of them.

**Why This Matters:**

When employees feel that internal tools are slow or limited, Shadow AI starts to emerge.

**Risk To The Organization:**

The risk is that it creates data silos, can break integration workflows, and also increases vendor risk.

## What Can You Do To Counter Shadow AI

As soon as you see examples of these situations, you must take action. Here are several things you can do to counter Shadow AI in your business.

### Educate Your Employees Instead Of Punishing Them

It’s important to remember your employees are not using GenAI maliciously. It’s your job as an IT or HR leader to help your teams understand the risks and benefits of AI. You can achieve this by offering regular training to your employees.

### Implement a Safe AI Use Policy

Create a framework for employees to follow that lays out acceptable AI usage. Remember to link the framework to business goals and compliance standards. It will enable you to have a comprehensive, safe AI use policy.

### Create a Culture of Innovation

You want to promote a culture of innovation, but at the same time, be careful that you maintain balance. You can do this by encouraging AI experimentation, but within guardrails set by IT and legal.

### Audit Tools and Behaviors

An audit of the tools and employee behaviors will give you vital insights. Use work logs, surveys, and Shadow IT detection software to uncover unsanctioned use by your employees. It will provide you with a greater understanding of your situation.

### Offer Secure Alternatives

Provide your employees with approved, secure AI tools that meet all your employees’ needs. It will stop them from browsing and using other platforms. At [ReadyAI.dev](https://readyai.dev/), our enterprise-grade platform helps you put all your AI solutions together.

## Catch Shadow AI Before It Spreads

Shadow AI is not just a tech issue; it’s far more than that. It’s a business risk that is hiding in plain sight. As an IT or HR leader, recognizing these early warning signs gives you a chance to respond proactively.

You must also think strategically about GenAI so you can protect your data and empower your people to use AI safely. At ReadyAI.dev, we act as a human-first bridge to help enterprises secure AI in their organizations.

ReadyAI.dev’s enterprise-grade AI platform was built by a global tech leader and is trusted by Fortune 500s and governments. [Talk to one of our Enterprise AI Advisors for expert advice.](https://readyai.dev/contact)

\*\*\* Want to learn more about the roots of the problem? You can read our full breakdown in this article: [What Is Shadow AI and Why It’s a Growing Risk for Enterprises](https://readyai.dev/insights/what-is-shadow-ai). \*\*\*

## Sources:

1. 2024 Cloud and AI Business Survey - [PwC](https://www.pwc.com/us/en/tech-effect/cloud/cloud-ai-business-survey.html)
2. What is Shadow AI and Why It Is A Growing Risk For Enterprises - [ReadyAI.dev](https://readyai.dev/insights/what-is-shadow-ai)
3. ChatGPT platform - [ChatGPT](https://chatgpt.com/)
4. Jasper platform - [Jasper](https://www.jasper.ai/)
5. General Data Protection Regulation - [GDPR](https://gdpr-info.eu/)
6. Health Insurance Portability and Accountability Act (HIPAA) - [US Department of Health and Human Services](https://www.hhs.gov/hipaa/index.html)