# Is Your Company’s Data at Risk from Shadow AI?

Gartner has predicted that by 2027, [75% of employees will acquire, modify, or create technology](https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024) outside IT’s visibility. It’s a stark statistic and one that should worry you as a leader in any industry. The reality is your data is at risk from Shadow AI.

It’s not deliberate sabotage by your employees; it’s a lack of training in risk management. Putting your head in the sand is not going to make the problem go away. You must take action now to protect your enterprise for the long term.

This article explores how Shadow AI can expose your sensitive enterprise data and what you, as a leader, can do to secure your systems. Learn how you can assess your exposure and how you can implement secure, compliant AI practices.

## What is Shadow AI?

The simplest definition of Shadow AI is employees using AI tools without official approval or IT governance.

Examples of these tools are [ChatGPT](https://chatgpt.com/), [Claude](https://claude.ai/login?returnTo=%2F%3F), and [Midjourney](https://www.midjourney.com/explore?tab=video_top). Accessibility, productivity, and lack of internal AI options are some of the reasons why employees are using AI tools.

In an earlier article, we went into more detail about Shadow AI. You can read the article here to learn more: [What is Shadow AI and Why It Is a Growing Risk for Enterprises.](https://readyai.dev/insights/what-is-shadow-ai)

## Why Shadow AI Is a Data Security Threat

Data is one of the most important things in your enterprise. You are obliged by law to protect your data and that of your customers. You might have systems in place already to protect your data, but this is the next level.

Shadow AI is a data security threat for all enterprises. It is like the wild, wild west in business right now, with everybody getting on the AI bandwagon, but with no clear control. Here are three reasons why it can be so dangerous:

### Data Exposure Risks

Staff are entering customer information, internal processes, and IP addresses into public models.

Only this month, [security researchers have found a weakness in OpenAI’s connectors](https://www.wired.com/story/poisoned-document-could-leak-secret-data-chatgpt/), which let you hook up ChatGPT to other services. The danger here is that it allows them to extract data from a Google Drive without any user interaction.

### Loss of Control

As soon as your employees use that data, several things happen. Your enterprise cannot audit, retrieve, or delete the data after submission.

### Compliance Issues

Any data that leaves your organization opens your enterprise up to compliance risk. A breach could violate GDPR, HIPAA, or internal governance policies.

## How To Know If Your Organization is at Risk

It might not be easy to recognize the risks your company will face, but there are things you can start looking for in your business. Here are some examples:

* There is an increased use of external apps, but they have unknown endpoints.
* After consulting your IT framework, you might realize that you do not have any AI-specific policies.
* Your employees are unsure about the AI tools they can use and ask questions about the safety of specific apps.

In this article, we go into more detail: [5 Warning Signs Your Teams Are Using Shadow AI Tools](https://readyai.dev/insights/5-warning-sign-your-teams-are-using-shadow-ai).

## Real-World Consequences of Ignoring Shadow AI

You might be surprised to learn how easy it is for Shadow AI to take over enterprises. Employees believe they are doing the right thing for their work but are creating more harm than good.

One of your engineers might be pasting sensitive code into ChatGPT and not giving it a second thought. Your marketing team could be uploading unreleased campaign data into a free AI tool.

It could be an issue in your HR department, where they are using AI to save time to summarize performance data and are unintentionally violating privacy laws. The possibility of Shadow AI already being in your business is very high.

### Potential Fallout For Your Enterprise

The results of these innocent actions by your employees can be devastating. It could result in:

* Data leaks
* Fines
* Legal consequences
* Reputational damage

## How to Protect Your Enterprise from Shadow AI

So, what can you do as a leader to help protect your business from Shadow AI?

**1) Build an AI usage policy** that defines what they can use, what is not permitted, and also explains why this is the case.

**2) Start educating and training** your teams. You can provide training, but also run awareness campaigns, so people remember.

**3) Empower your team** and give them safe, approved AI tools. Use enterprise-grade platforms, built with compliance and security in mind.

## Why Enterprise AI Platforms Can Help

Your immediate role is to reduce Shadow AI risk in a controlled and secure manner. Using a secure enterprise AI platform, like [ReadyAI.dev](https://readyai.dev/), gives you an edge. You can get to grips with Shadow AI straight away and start taking back control.

### Key Features Your Enterprise AI Platform Must Have

Before you sign on the dotted line with any enterprise AI platform. There are some key features that your platform must have. Here are some must-haves:

* Audit trails and user management
* Custom model governance
* Data residency controls
* End-to-end encryption

For example, at ReadyAI.dev, our platform is powered by enterprise-grade AI from a global leader and trusted by Fortune 500s and government agencies worldwide. We are recognized in the industry for giving our clients the highest level of security.

## 

## What You Can Do Next To Protect Your Company’s Data

Shadow AI is a risk you cannot ignore. It’s not going away, and it will only get worse. Are you ready to take action and nip Shadow AI in the bud?

With the proper visibility and tools, your enterprise can embrace AI confidently and securely. You should immediately start auditing your AI usage now or [talk to one of our Enterprise AI Advisors](https://readyai.dev/contact) to begin assessing your Shadow AI risk.

## Sources:

1. Gartner Unveils Top Eight Cybersecurity Predictions - [Gartner](https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024)
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. A Single Poisoned Document Could Leak “Secret” Data Via ChatGPT - [Wired](https://www.wired.com/story/poisoned-document-could-leak-secret-data-chatgpt/)
4. 5 Warning Signs Your Teams Are Using Shadow AI Tools - [ReadyAI.dev](https://readyai.dev/insights/5-warning-sign-your-teams-are-using-shadow-ai)