Shadow AI

An Evolution from Shadow IT to Shadow AI

Shadow IT where employees unknowingly end up accessing the information they are not authorized to or is not part of their job or use unapproved apps or devices inside the enterprise network. An employee might use their personal Dropbox account to move files instead of the company-approved file-sharing system. Employees might also use unapproved apps or software to conduct code reviews.

Louie Orbeta, writes about Shadow IT "Employees try to improve productivity or may simply be unfamiliar with proper procedures."

Shadow IT operates outside the awareness and protection of the IT team this means; any associated vulnerabilities can go unaddressed leaving the organization exposed to risks.

With the rapid advancements in generative AI, where almost everyone is familiar with AI tools, their use and potential. Jeff Crume, an engineer at IBM , warns, *“**Shadow AI is lurking in corners at your organization**.”*

Employees at your organization might be using generative AI to streamline workflows or assist with problem solving. But are you familiar with full extent of generative AI usage within your organization? Are these tools being used in compliance with company policies? Are they integrated securely into your systems to protect sensitive data?

Gen AI can significantly enhance productivity when used appropriately, but its misuse can lead to serious repercussions stated by Tristan Marot, June 2024 article.

According to a Forbes article (August 2024), over 50% of U.S. employees already incorporate AI tools in their work—often without formal approval.

A lot of data is being exposed out there. Employers have unintentionally entered the organization’s data into external AI tools.

The 2024 *Work Trend Index Annual Report* by Microsoft & LinkedIn revealed that 75% of surveyed employees were already using generative AI in their work tasks without employer oversight.

This "scattering" of data across multiple platforms creates vulnerabilities including data leakage which can cause threat. If a threat actor gains access to these platforms, they could potentially compromise the organization's data. Organizations developing AI applications or training AI models face risks because a threat actor could Poison the dataset, causing errors in the AI system if their data is not secure.

IBM's 2023 report found that the average cost of a data breach in a U.S. company is $9.4 million.

AI-generated responses can also provide "hallucinated data," producing incorrect information. For instance, in *Parker v. Forsyth N.O. & Others*, attorneys relied solely on ChatGPT for legal research, failing to verify the AI-generated results.

So, what can organizations do to address Shadow AI? **Saying "No" Isn’t the Solution:** Outright banning AI could lead to employees continue to use them secretly, says Jeff, from IBM.

We need to bring it out of the shadows to keep organization safe. First, we need to have ‘visibility’ and ‘control’. For visibility we need to discover what’s out there and what’s being used. Identify all instances of AI use within the organization. Regularly monitor tools and platforms employees rely on and by following established frameworks for AI usage in corporate environments. We need to bring it out of the shadows to keep organization safe.

- Identify all instances of AI use within the organization.
- Follow frameworks like National Institute of Standards and Technology (NIST) AI Risk Management and OWASP® Foundation Security Guidelines.
- Develop and communicate clear policies for responsible AI use.
- Training employees on the risks and ethical implications of AI.
- Introduce company-approved AI tools that prioritize security and confidentiality.

Louie Orbeta adds *“Having a strong defense and staying vigilant is more than just complying—it’s about strengthening our defenses.”*

We need to Rethink the Protection of Data in this AI Era.