# The rise of shadow AI: Navigating unregulated technologies in business



As businesses increasingly embrace artificial intelligence (AI) to enhance their operations and maintain a competitive edge, they face emerging challenges associated with the unregulated use of these technologies. A particular area of concern is the phenomenon known as 'shadow AI', which refers to the unauthorised application of AI tools within organisations without the oversight of IT or security departments.

The use of shadow AI can be witnessed in various forms, ranging from a developer employing ChatGPT to assist in coding tasks to a salesperson utilising an AI-powered meeting transcription tool without going through the official channels. The prevalence of such tools presents significant security risks due to their lack of proper oversight and security controls, which can jeopardise sensitive company information.

Identifying and managing shadow AI poses unique challenges. Unlike traditional shadow IT, where unauthorised applications can often be pinpointed through network monitoring—tracking IP addresses and domain names—shadow AI tools often integrate seamlessly into approved business applications through copilot features. This means they could easily escape detection since they share the same IP address or domain with legitimate applications.

Moreover, employees might opt to use standalone AI solutions linked to personal accounts. While not directly connected to corporate infrastructure, this still raises concerns, as employees may inadvertently input confidential data into these channels, increasing the risk of data leaks.

The implications of shadow AI are stark. Research has highlighted that approximately 15% of employees may inadvertently expose company data to such tools. As generative AI models learn from user interactions, there is a potential risk that sensitive information could be disseminated to unauthorised users or be misrepresented, leading to misinformation.

To address these challenges, companies like Reco are emerging with solutions aimed at detecting and cataloguing shadow AI usage within their SaaS environments. Reco employs a series of methodologies including Active Directory integration to compile approved applications, as well as analysing email metadata to identify communications with unapproved tools. Additionally, its generative AI module leverages natural language processing to clean and match identities with the corresponding applications, ultimately producing an inventory of both sanctioned and unsanctioned AI tools.

Once shadow AI tools are identified, Reco provides a detailed analysis of several factors, including which SaaS applications are currently in use, which are incorporating AI assistants, and the identities of users accessing these tools, along with their respective permission levels. The system allows companies to understand connections between applications and helps in managing identity and access governance via a centralized platform.

Despite its capabilities, Reco operates in a read-only capacity and does not enforce direct policy changes. For instance, it cannot prevent employees from entering sensitive data into unauthorised applications or block the use of shadow AI tools. Instead, its purpose is to enhance visibility and alert security teams to potential vulnerabilities, enabling them to act on detected risks appropriately.

With the rise of shadow AI, businesses need to balance the advantages that AI applications can offer while carefully managing the associated security challenges. Through tools like Reco, organisations can gain insights into their SaaS environments and better understand the implications of the AI technologies that have become an integral part of modern business practice.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.walkme.com/blog/shadow-ai/> - Explains what shadow AI is, including its definition as AI applications and tools used without the explicit knowledge or control of an organization’s IT department.
2. <https://www.harmonic.security/blog-posts/how-to-detect-and-mitigate-shadow-ai-in-your-organization> - Provides examples of shadow AI, such as the unapproved use of generative AI tools, independent adoption of AI solutions, and unvetted AI coding assistants, highlighting the associated risks.
3. <https://growthtribe.io/blog/shadow-ai-explained> - Describes shadow AI as the use of AI tools in a company without approval from IT or other legal departments, and outlines the risks including data security vulnerabilities and compliance violations.
4. <https://www.birchwoodu.org/what-is-shadow-ai-protect-your-business-from-its-threat/> - Discusses the urgency to address shadow AI due to its potential to cause significant harm, including data breaches, regulatory fines, and reputational damage.
5. <https://www.walkme.com/blog/shadow-ai/> - Explains how shadow AI differs from shadow IT and the specific risks associated with AI-driven tools, such as non-compliant decision-making and data leaks.
6. <https://growthtribe.io/blog/shadow-ai-explained> - Highlights that employees use shadow AI for rapid problem-solving and to leverage cutting-edge AI capabilities without waiting for corporate approval, and the risks this poses.
7. <https://www.harmonic.security/blog-posts/how-to-detect-and-mitigate-shadow-ai-in-your-organization> - Details the challenges in identifying and managing shadow AI, including the integration of these tools into approved business applications and the use of personal accounts.
8. <https://www.birchwoodu.org/what-is-shadow-ai-protect-your-business-from-its-threat/> - Mentions the risks of employees inadvertently exposing company data to shadow AI tools and the potential for sensitive information to be disseminated to unauthorized users.
9. <https://growthtribe.io/blog/shadow-ai-explained> - Explains how shadow AI can lead to significant risks, including data security vulnerabilities, compliance violations, and operational instability.
10. <https://www.walkme.com/blog/shadow-ai/> - Discusses the potential greater risks of shadow AI compared to shadow IT due to the complexity and unpredictability of AI systems.
11. <https://www.harmonic.security/blog-posts/how-to-detect-and-mitigate-shadow-ai-in-your-organization> - Provides insights into how to detect and mitigate shadow AI, including examples of real-world scenarios and the need for oversight and governance controls.
12. <https://news.google.com/rss/articles/CBMifEFVX3lxTFB0STEzQUktdEdqbVBsb0VTSm00Y2NpUXlCcGNRNGR1dmI1ak0xaXdIVldjT0hGM0VXWTZOckJrWmJoQ0IzUFVFcmMxcER2VFhNOUE2eHhleUlQRExJbjFHU1o4NG9QZE5ubzNxT3ZlRTJpT0xQQXJUZkZ3WGc?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data