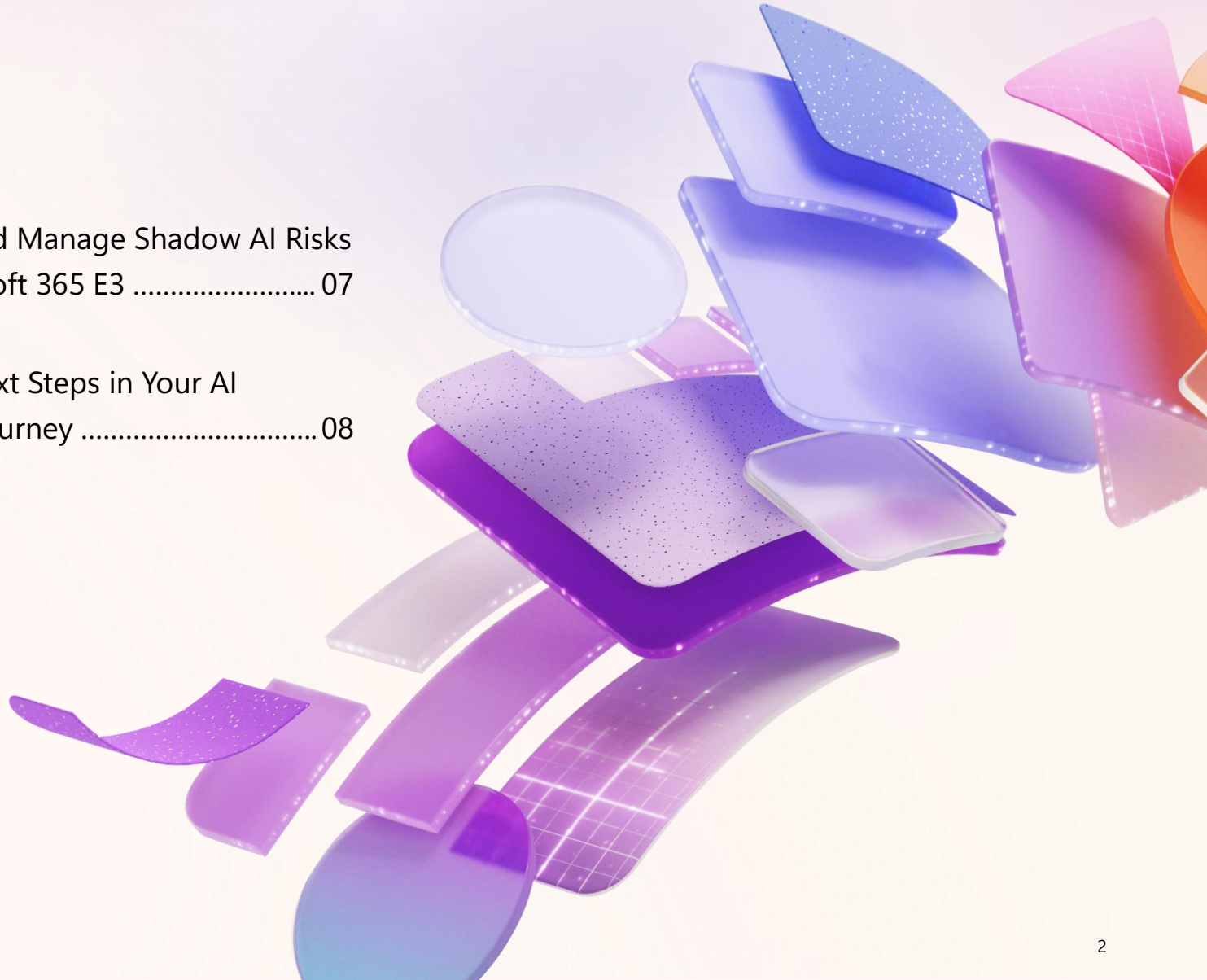
Microsoft 365

From Oversight to Insight: Managing Shadow AI Risks

Table of Contents



Introduction

In the recent Work Trend Index report, more than 80% of knowledge workers surveyed across 31 countries—including employees and leaders—reported feeling like they lacked the time or energy to do their work. In addition, more than 50% of business leaders surveyed reported that productivity needed to increase to meet goals[1]. According to the 2024 Microsoft Work Trend Index Report, many employees are seeking out generative AI tools to address this gap and aren't waiting for official IT approval before starting to use the tools.

When tools operate outside of IT's visibility, they may pose security and compliance risks for organizations. And Shadow AI – the use of AI tools without IT approval – is emerging as the latest form of Shadow IT in today's workplaces.

As AI adoption accelerates, business leaders are working to stay ahead and mitigate potential risks these tools may pose. In a recent iSMG study, more than 70% of business leaders surveyed reported that ensuring data privacy and security is the primary challenge for integrating generative AI with existing IT infrastructure[2]. In addition, more than 90% of CIOs and CTOs surveyed reported that Generative AI has already driven or will drive greater cybersecurity investments at their organization[3].

In this e-book, explore common scenarios where shadow AI is being used, understand the potential risks to organizations, get five ways to manage those risks, and see how Microsoft 365 E3 can help.

[1] **2025 Work Trend Index Annual Report,** Microsoft, Inc., April 2025. Microsoft analyzed survey data from 31,000 full-time employed or self-employed knowledge workers across 31 countries between February 6, 2025, and March 24, 2025, LinkedIn labor market trends, and trillions of Microsoft 365 productivity signals.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** Based on survey responses from more than 360 business and cybersecurity professionals in Q3 across 6 regions (North America, Europe, Asia, South Americas, Australia, and Africa)

[3] **The AI Security Balancing Act: From Risk to Innovation," NTT DATA, June 2025,** Based on data from an NTT DATA survey of more than 2,300 senior GenAI decision-makers, comprising 1,500 C-Suite leaders across 34 countries.

What is Shadow AI? And Why Does Visibility Matter?

Shadow AI refers to the use of artificial intelligence tools and applications by employees without explicit approval or oversight from IT departments, often outside the visibility of official security and compliance frameworks. As employees seek ways to enhance productivity and address the growing demands of their workloads, they may turn to these unsanctioned solutions to streamline tasks, collaborate, or generate new content—frequently without realizing the potential risks involved. Shadow AI is not visible to IT, making it difficult for organizations to know what applications are being used and which ones pose the greatest risks.

Why Visibility of Shadow AI Matters

When IT is not aware of an application or service, it cannot secure or support it. This *visibility gap* makes it difficult to accurately identify, manage, or mitigate potential threats related to sensitive data exposure, regulatory non-compliance, and loss of control over proprietary information. IT and business leaders need to gain visibility into the Shadow AI being used at their organization, address the emerging risks associated with AI use, and decide which tools should be allowed with the right guardrails. The opportunity for organizations is to transform Shadow AI from a risk into a chance to innovate how work gets done, securely. To do this, there needs to be a better balance – enabling employees to harness useful AI tools within a governed, secure framework to mitigate potential risks.

INSIGHT

You can't secure what you can't see. When IT isn't aware of an application or service being used, it cannot secure it. This is the crux of the Shadow AI problem – and it highlights why a new approach is needed. Simply banning all outside tools is not practical if employees feel these AI tools are critical to meeting their goals. Instead, organizations need to bring Shadow AI into the light – to gain visibility into what employees are using, put appropriate controls in place, and offer secure, approved alternatives that meet the needs of the organization. In short, the challenge is to empower teams with AI *without* compromising security.

Shadow AI in the Workplace: Example Scenarios and Potential Risks

Shadow AI arises from employees who may want to increase their productivity and impact or try a new technology. Below are several fictional examples to illustrate how unsanctioned AI tools may be used and the potential risks they may introduce:

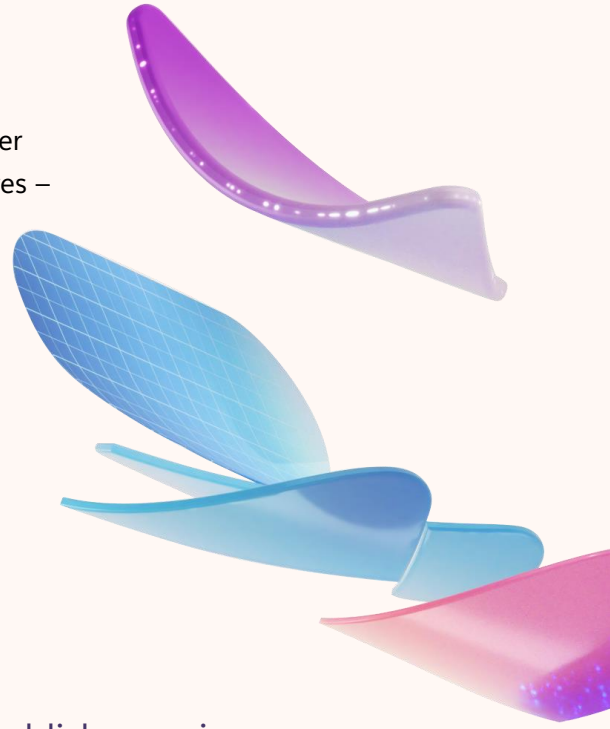
Role	Example Scenario	Potential Risk From Unsanctioned Tools
Marketing	Using a generative AI content tool to create marketing copy or designs using company brand data.	Leakage of sensitive brand or product information; loss of control over how an external AI service might store or use the company's creative assets.
Finance	Uploading corporate financials into an AI-driven analytics or visualization service for quick insights.	Exposure of confidential financial data (budgets, forecasts) to a third-party; potential compliance violations (e.g., GDPR) if customer or employee data is included without proper safeguards.
Customer Support	Sharing client data or support chat transcripts into an AI tool to draft responses or summarize cases.	Violation of privacy and data handling rules – sensitive customer information could be stored outside company systems; no guarantees on data retention or proper deletion by the AI provider.
Frontline – Retail	Store managers using AI scheduling apps on their phone to optimize employee shift rosters.	Company workforce data (employee names, schedules) uploaded to an unsanctioned app, risking privacy issues. Conflicting schedules or policy violations might occur if AI suggestions do not align with labor regulations.
Frontline – Healthcare	Nurses or doctors using an AI chatbot to help draft patient care notes or answer medical questions.	Patient health information (PHI) might be exposed to an external service without any safeguards, violating compliance and confidentiality requirements. The AI's medical advice might also be unverified, posing safety risks.

In each of the above cases, the individual employee had good intentions and was looking for a productivity boost, but the organization may inherit risks as a result.

Company information can end up scattered across unsanctioned platforms creating *data governance headaches*. Unvetted apps could introduce malware or security vulnerabilities, expanding the attack surface outside of IT's purview. There may also be compliance implications. From an IT support perspective, if something goes wrong with a Shadow AI tool, the help desk may be unable to assist end users as they have no insight into or control over it.

Five Ways To Manage Shadow AI Risks

With the right strategy and tools, you can turn shadow AI from a potential threat into an opportunity to foster a culture of secure innovation. Empower your teams with AI productivity tools *while* maintaining the oversight needed to protect your business. It's a shift from saying "no, never" to saying "yes – but with the right guardrails." The following five tips are designed to help you manage and take control of Shadow AI at your organization:



01 Discover your Shadow AI footprint to evaluate and prioritize risks

You can't protect what you can't see. Gain visibility into the applications being used at your organization through your activity logs. Once you know the apps in use, you can identify the right tools to handle sensitive data, while noting the ones that do not align with your security and compliance policies. With these insights, you can make a more informed decision on what applications you want to allow, monitor, or limit to mitigate potential risks.

02 Implement quick wins with security and compliance policies

Enable or apply policy fixes to better mitigate potential risks from Shadow AI use. You can use conditional access policies to restrict the use of high-risk applications, use data loss prevention policies for sensitive information to mitigate oversharing and data leakage, and enforce basic multi-factor authentication and device compliance for all users. These steps quickly reduce the most glaring risks even if you do not yet have full visibility into the AI applications being used.

03 Educate employees on the potential risks of Shadow AI

Often, employees are unaware of the risks using unsanctioned AI tools may pose to an organization. Communicate the risks of Shadow AI often with well-placed data loss prevention warnings, reminders of company policies, and brief trainings to help redirect users to safer practices without heavy-handed enforcement.

04 Provide approved AI tools to further mitigate risks

Where possible, offer employees approved AI tools as alternatives to unsanctioned ones. A great way to reduce Shadow AI is to fulfill the most common use cases at your organization with a sanctioned solution. This enables IT to maintain visibility and control, while providing user support for issues that arise.

05 Establish ongoing governance

Integrate checks into your IT governance routine – review activity logs and reports regularly, update policies as new AI services emerge, and keep leadership informed of progress (such as reductions in unsanctioned app usage or incidents prevented). This will help you mitigate potential risks now and into the future as the landscape evolves.

By taking the steps above, you can empower both innovation and security.

Employees are able to use approved AI solutions at work and IT maintains control and compliance over those tools.

Discover and Manage Shadow AI Risks with Microsoft 365 E3

Microsoft 365 E3 provides organizations with the capabilities to discover Shadow IT, assess potential risks, and implement security and compliance policies *without* stifling innovation. This suite of integrated productivity, security, and management capabilities can empower you to directly address Shadow AI challenges.

Microsoft 365 E3 Solution	How it helps you manage potential Shadow AI risks
Cloud App Discovery	**Discover and take action on unsanctioned applications.** Cloud App Discovery enables you to upload activity logs and create snapshot reports to gain visibility into more than 31,000 cloud apps – including over 400 generative AI applications. It lets you see what is being used in your organization, by whom, and how often. This information enables you to make informed decisions on which apps to allow or limit the use of.
Microsoft Purview Data Loss Prevention (DLP)	**Mitigate sensitive data leaks.** Microsoft Purview DLP lets you define and apply policies that detect sensitive information and block or restrict sharing across Microsoft 365 services for emails and files. For example, you can set a rule to monitor, audit, or stop users from sharing sensitive information through email or file sharing and alert the user.
Microsoft Entra ID P1	**Manage access to cloud apps.** Microsoft Entra ID P1 enables Conditional Access policies to control who can access which applications under what conditions. For example, you can choose to require multi-factor authentication or event limit log-ins with corporate credentials to apps you've determined are higher risk. Microsoft Entra ID P1 provides access to cloud resources to the right people, on compliant devices, under approved conditions - while limiting access to unapproved apps.
Microsoft Intune P1	**Enforce device and app usage policies.** Microsoft Intune P1 gives you the ability to allow managed, compliant devices to be used for work, and provides you tools to manage those devices. For example, it can prohibit installation of unapproved software on corporate PCs, or push configurations that limit access to specific websites or services.
Microsoft Defender for Endpoint P1	**Limit traffic to unapproved URLs.** Microsoft Defender for Endpoint P1 helps you reduce risks from sites that you deem risky by blocking traffic to an unapproved URL from managed devices. For example, employees trying to visit a known risky AI site on a company laptop would be prevented from accessing it.

Take the next step in your AI adoption journey →

It all starts with awareness, the right tools, and a proactive plan. Microsoft 365 E3 provides the tools to enable your organization to establish a robust security foundation and governance framework for AI solutions. You'll be able to gain visibility into unsanctioned tools, enable policies to protect sensitive data, and maintain control over both user access and device security. Get ready to shift from a reactive stance (finding and blocking Shadow AI after it appears) to a more proactive approach of guiding AI usage into secure, managed channels. Take the Security for AI Assessment and learn how you can improve your security posture for AI. Learn more about the capabilities included in Microsoft 365 for Enterprise.