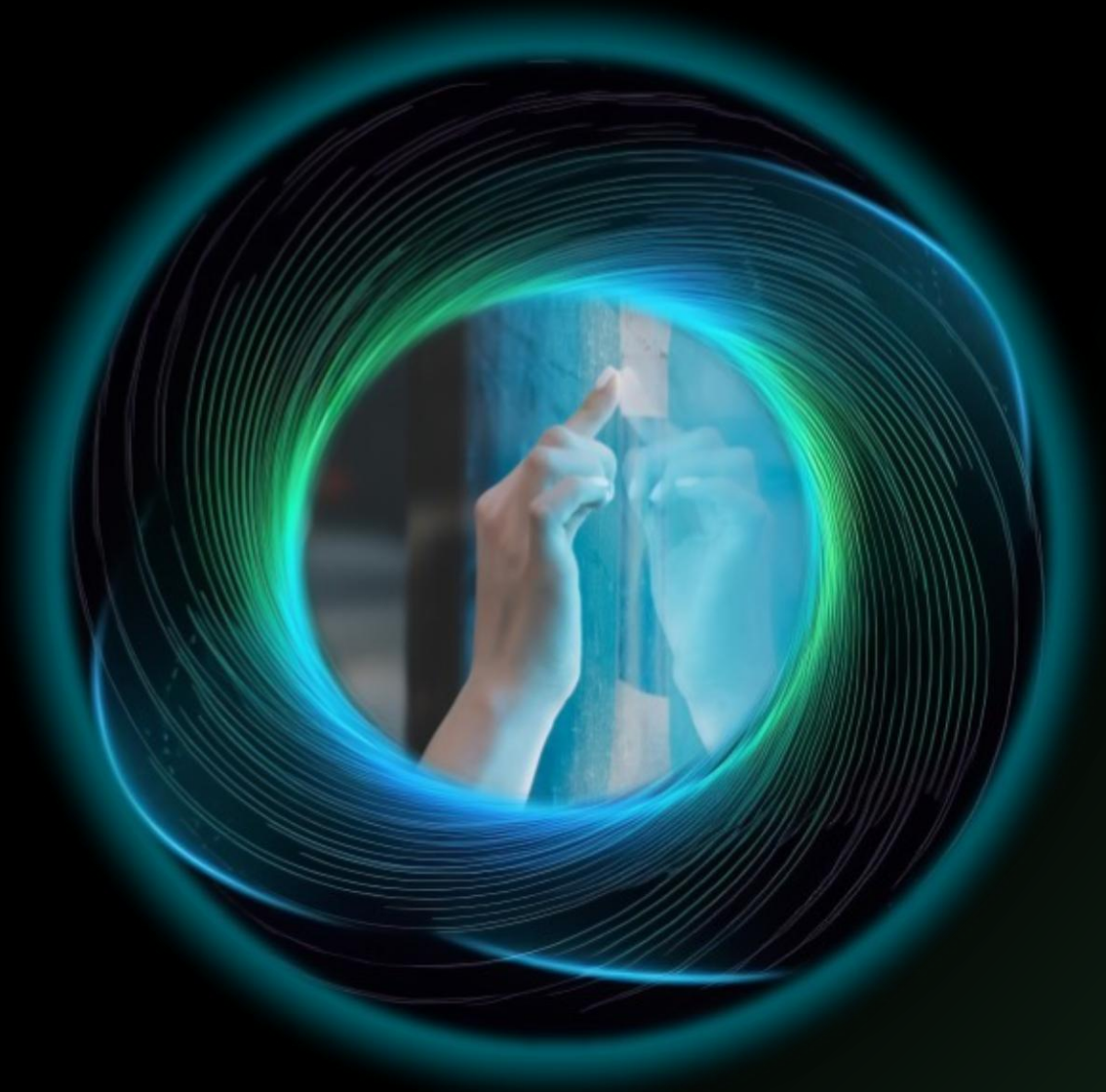
Deloitte.

Together makes progress



Shadow AI: What’s hiding in plain sight

October 2026

Deloitte.

Together makes progress

Introduction

Introduction	1
Setting the scene	2
How shadow AI takes root	3
Where and how would you find Shadow AI?	4
The multi-layered risks of Shadow AI	5
Why traditional governance falls short	6
A proactive approach: before the shadow darkens the room	7
Closing thoughts	9

Deloitte.
Together makes progress

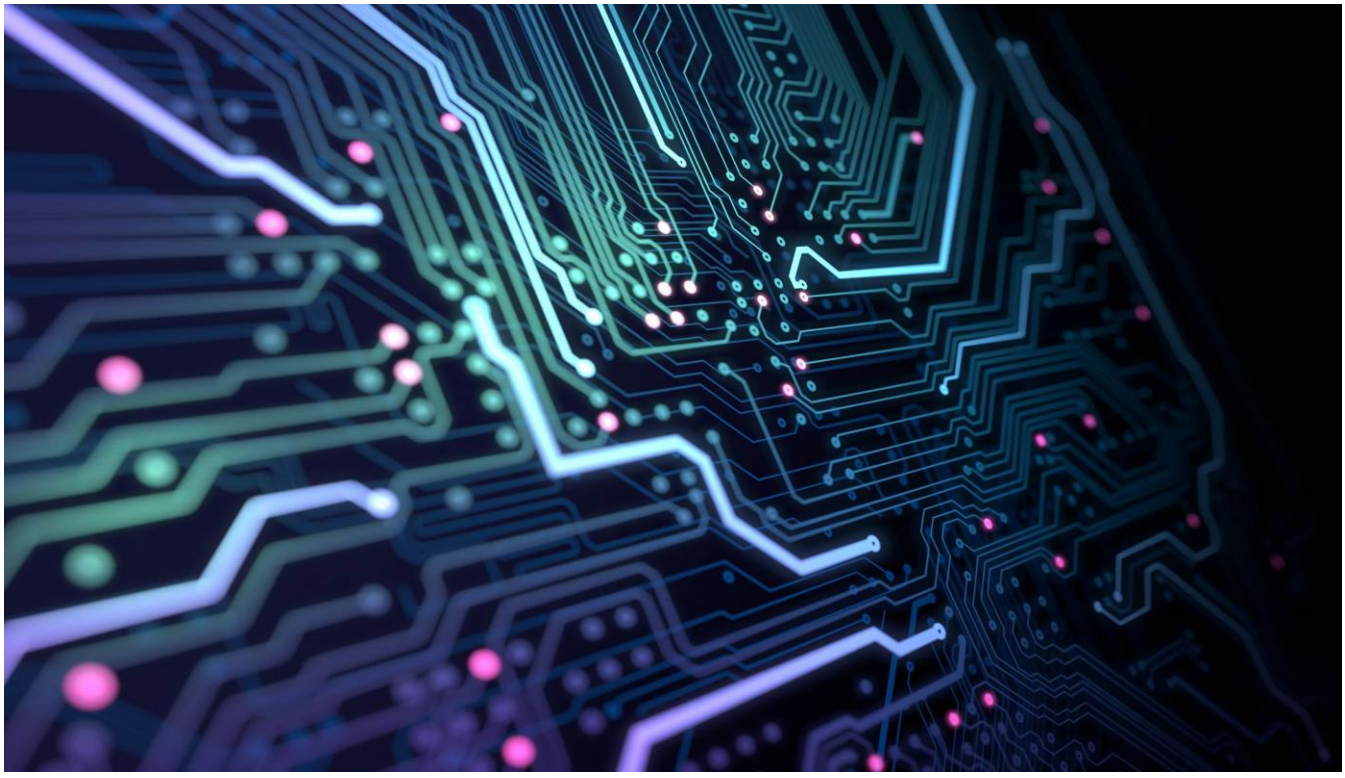
Setting the scene

The rise of Artificial Intelligence has transformed the way employees work. With powerful AI tools accessible at the click of a button, employees across all levels are adopting AI solutions to enhance productivity, often without the knowledge or approval of relevant governance stakeholders such as IT, legal, and compliance functions.

This phenomenon, commonly referred to as **Shadow AI**, is similar to the Shadow IT wave that organizations struggled to govern decades ago.

However, the risks today are significantly higher. Shadow AI introduces a complex layer of exposure where sensitive data being processed by third-party AI tools is beyond the organization's control.

As international regulations such as the EU AI Act[1] take effect and competent authorities such as KSA's SDAIA, UAE's Minister of State for Artificial Intelligence, Digital Economy, and Remote Work Applications Office, and Qatar's MCIT intensify their governance of AI, the question is no longer whether Shadow AI exists within your organization, but whether your organization is prepared to respond.



Deloitte.
Together makes progress

How shadow AI takes root

Shadow AI stems from employees seeking faster ways to get their work done, whether through drafting financial reports or screening candidates' CVs for hiring decisions. Free and accessible generative AI tools with no IT provisioning have become the preferrable option, often replacing the slower option of formally requesting access to such tools.

According to Gartner[2], by 2027, more than 40% of AI-related data leakage incidents will be caused by the misuse of generative AI tools by employees. The rate at which such tools are being used in daily operations has significantly outpaced the organization's ability to govern them, and that gap is precisely where Shadow AI takes root.



Deloitte.
Together makes progress

Where and how would you find Shadow AI?

Shadow AI is invisible by nature, but not undetectable. Organizations will likely find it in areas where workload pressure is highest and where the approved list of tools is perceived as insufficient. Common departments include finance, legal and HR, which use AI tools in their day-to-day operations.

More often, Shadow AI is not accessed through corporate systems at all; rather, employees use their personal devices, such as their mobile phones or personal laptops, to use unapproved generative AI tools. For instance, sensitive data is manually retyped into an external AI platform on one's phone.

Shadow AI is also found in browser extensions and plugins. Extensions with generative AI features can process what is displayed in the browser, potentially disclosing sensitive information without the organization's approval and causing a data breach. Since browser extensions run in user environments rather than in company systems, standard detection methods are insufficient.

From a detection point of view, there are several signs that can surface Shadow AI activity. Network traffic analysis and data loss prevention (DLP) solutions are important components of a broader monitoring and governance capability to detect abnormal outbound traffic to known AI service endpoints and flag unsafe or inappropriate sharing of sensitive information though they are not sufficient on their own. Organizations should pay attention to their third-party app integrations, as Shadow AI usually enters the organization not as a standalone application, but as a plug-in or extension that connects to existing applications. Tackling Shadow AI depends on building a culture of trust within the organization, backed by technical controls and clear processes that make it easy for employees to access approved, risk managed AI tools. When employees have access to the relevant AI tools, they no longer need to seek it out through unapproved methods.

Deloitte.
Together makes progress

The multi-layered risks of Shadow AI

The risks of Shadow AI go beyond operational disruption. It also affects how company data is handled when it is outside of the company's control. When employees use external AI tools with company data, solution providers may use such data to train their models, often without any contractual or technical controls in place.

Algorithmic bias is a crucial risk introduced by Shadow AI. As mentioned before, these tools are not governed by IT and hence organizations have no visibility whether bias exists. This blind spot can be dangerous in critical processes such as in HR decision-making and customer profiling where biased outputs can directly affect individuals' rights and futures.

Both risks carry risks of non-compliance with regulatory requirements. The EU AI Act places responsibilities on organizations that deploy AI systems, with assumptions that organizations have visibility over the AI systems in use. Shadow AI breaks that assumption due to unawareness of the tools being used. The same blind spot creates non-compliance with data protection laws such as GDPR and KSA PDPL, which regulate the conditions under which personal data may be processed using AI. In practice, employees using external AI tools may unknowingly share sensitive information, such as customer details, with third parties, leading to regulatory non-compliance and potential data breaches.



Deloitte.
Together makes progress

Why traditional governance falls short

Organizations around the world have made significant investments in cybersecurity, data governance, and privacy compliance initiatives, particularly with regard to third-party due diligence. However, the traditional path of adopting a tool, which involves contract review, vendor selection, IT provisioning, and legal sign-off, has been completely disrupted by Shadow AI. Shadow AI often bypasses centralized procurement and governance, creating visibility gaps even when some form of vendor agreement exists. A tool may already be deeply integrated into an employee's daily routine and may have processed extensive amounts of organizational data by the time compliance or legal teams learn about its use. The NIST AI Risk Management Framework[3] emphasizes the need for a different approach that is proactive and integrated throughout the organization. The pace of AI innovation will only amplify this challenge, making it difficult for organizations to improve their governance models.



Deloitte.
Together makes progress

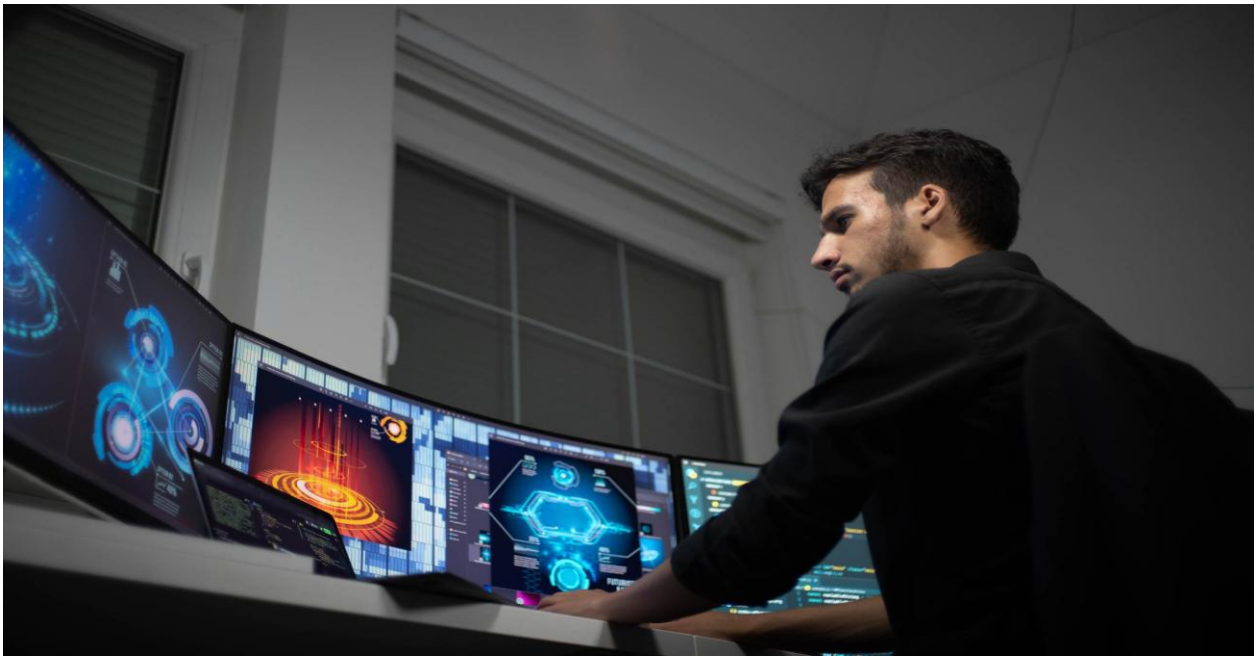
A proactive approach: before the shadow darkens the room

Simply waiting for a data breach or regulatory non-compliance penalty to detect Shadow AI is not a strategy; it is a reactive approach built on accepting risks by default. Proactive organizations have better chances of containing the risks, ensuring regulatory compliance, and building a culture of responsible AI use. The following measures outline a proactive and practical approach:

- **Develop Shadow AI discovery program.** Before implementing any mitigating controls, organizations should assess the current usage of Shadow AI. This can be done by conducting discoveries through reviewing DLP configuration, analyzing network traffic, conducting workshops with business units, and leveraging specialized AI discovery and SaaS security tools capable of detecting unauthorized AI usage by monitoring browser activity, API calls, data transfers, and integrations with generative AI platforms. The goal of this discovery is not to audit employees, but rather to understand how AI is used across the organization.
- **Conduct proper due diligence.** Before onboarding AI tools, organizations should verify whether an appropriate agreement with the AI provider is in place and whether the intended use is covered by that agreement. Where personal data is processed, organizations should assess the provider's data governance practices, including where data is stored and processed, how long it is retained, whether it may be used to train AI models, and whether appropriate contractual and data protection safeguards are in place. Where applicable, requirements relating to cross-border data transfers should also be considered.
- **Involve cybersecurity teams early.** It is essential to involve cybersecurity teams early when approving new AI tools. They need to thoroughly evaluate each tool, examine system access, understand how data is transmitted and where it goes and any possible security risks. Getting cybersecurity involved from the beginning is particularly crucial for tools that connect to enterprise systems or use company data.

Deloitte.
Together makes progress

- **Build policy infrastructure and employee awareness.** Organizations need to set clear, simple rules for using AI. These should explain which tools employees can use, when to use them and what data is allowed to be used. As AI evolves, update these rules and keep a list of approved tools, chosen by IT, legal, and privacy teams working together. However, rules alone are not enough. To reduce the risk of Shadow AI, ensure that employees understand the risks, have approved tools that meet their professional needs, and feel comfortable raising concerns. Awareness campaigns, targeted training, and strong leadership support are all key to long-term success.
- **Implement continuous monitoring.** Managing Shadow AI is not a one-time exercise. As new tools appear and employee habits change, organizations need to stay aware by keeping up-to-date AI tool lists, running regular audits, and using automated monitoring tools. Review your governance frameworks at set times and update them to match changes in regulations, including updates from the EU AI Act's phased rollout.
- **Provide a secure alternative.** Shadow AI can emerge from unmet business needs rather than malicious intent. Organizations should therefore consider developing or deploying an internal enterprise-level AI solution. This would allow for positive gain from AI without exposing sensitive data.



Deloitte.
Together makes progress

Closing thoughts

Shadow AI is not a risk to be monitored from afar; it already exists in nearly every organization. With new compliance rules from the EU AI Act and AI governance initiatives emerging across the Gulf, expectations for responsible AI use are now clearer. Organizations should adopt a proactive approach to identify and govern the adoption of AI tools to better position themselves in building trust, resilience and accountability in how AI is used.

The shadow is already in the room. The question is whether organizations choose to turn on the light.

Authors



Eliza Lozan
Partner
Digital Trust & Privacy
ellozan@deloitte.com



Aws Al-Masri
Senior Consultant
Digital Trust & Privacy
awalmasri@deloitte.com

Deloitte.
Together makes progress

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

[2] Gartner Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027

[3] NIST AI Risk Management Framework

This document is confidential and prepared solely for your information and that of other beneficiaries of our advice listed in our engagement letter. Therefore, you should not, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. In any event, no other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Deloitte Middle East" or "DME" refers to Deloitte & Touche (M.E.) which is the affiliate for the territories of Bahrain, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, Palestinian Ruled Territories, Qatar, Saudi Arabia, United Arab Emirates.

Deloitte EMEA BV, a limited liability company incorporated under the laws of Belgium (Deloitte EMEA), is a Member Firm of Deloitte Touche Tohmatsu Limited (DTTL). Deloitte Middle East, or their affiliates are shareholders in Deloitte EMEA. Deloitte EMEA and DTTL do not provide services to clients.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides leading professional services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets and enable clients to transform and thrive. Building on its 180+year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's over 470,000 people worldwide work together every day to make an impact that matters at www.deloitte.com.

DME is a leading professional services organization established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides services through 26 offices across 14 countries with more than 7,000 partners, directors and staff.

© 2026. For information, contact Deloitte United Arab Emirates All rights reserved.