# Shadow AI threatens UK productivity gains unless firms act on governance



Generative AI is already in daily use for an estimated seven million UK workers, with tasks from email triage to research benefiting from automation. TechRadar Pro reports that 58% of organisations believe AI could narrow the productivity gap — yet “shadow AI” is rising just as fast.

Surveys by Salesforce show that nearly 40% of employees using AI tools do so via apps their employer has banned, while Cyberhaven telemetry recorded a 485% year-on-year jump in corporate data being fed into public models, often from personal accounts. IBM’s 2025 Cost of a Data Breach report found AI-related breaches added an average US$670,000 to incident costs, with poor access controls a major factor.

Analysts say the fix is clear:

* **Inventory AI use** and track data flows to uncover unsanctioned activity.
* **Apply zero-trust principles** to model access, matching permissions to role and purpose.
* **Enforce DLP and access controls** to limit what sensitive data reaches external tools.
* **Offer secure, approved AI services** so staff aren’t tempted to “bring their own”.
* **Train staff in safe, ethical AI use**, backed by clear policy.
* **Automate SOC workflows** with SOAR to detect and contain incidents faster.
* **Monitor and adapt controls** as tools and risks evolve.

The goal, experts stress, is not to block innovation but to channel it. With transparent governance, secure tooling and embedded trust, UK firms can capture AI’s productivity promise while protecting the data and reputation on which long-term competitiveness depends.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.techradar.com/pro/tackling-shadow-ai-how-uk-businesses-can-mitigate-the-risks> - Please view link - unable to able to access data
2. <https://www.salesforce.com/news/stories/ai-at-work-research/> - Salesforce’s Generative AI at Work research surveyed over 14,000 workers across 14 countries and reveals rapid, unsanctioned adoption of generative AI in the workplace. Roughly 28% of respondents reported using generative AI on the job, and more than half of those users relied on tools that lacked formal employer approval. The study also found that around 40% had used tools explicitly banned by their organisations, while 64% admitted to passing off AI-generated content as their own. Importantly, many employees reported little or no training on safe, ethical or compliant AI usage, highlighting a governance gap employers must urgently address now.
3. <https://www.prnewswire.com/news-releases/cyberhaven-report-surge-in-shadow-ai-accounts-poses-fresh-risks-to-corporate-data-302151221.html> - Cyberhaven’s AI Adoption and Risk report analysed anonymised activity from millions of employees and documents explosive growth in unsanctioned AI use. Between March 2023 and March 2024 the amount of corporate data placed into AI tools rose by 485%, while the proportion of sensitive inputs climbed markedly. The firm found most usage occurred through personal, non‑corporate accounts — for example nearly three-quarters of ChatGPT activity — increasing exposure of confidential information to public models. Cyberhaven warns that without visibility and controls, organisations risk data leakage, compliance breaches and reputational harm, urging monitoring and governance to mitigate these emergent threats now.
4. <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai> - IBM’s annual Cost of a Data Breach report examines breaches across hundreds of organisations and highlights a widening AI oversight gap. Findings include that 97% of organisations suffering AI‑related incidents lacked proper AI access controls and that shadow AI incidents increased the average breach cost by roughly US$670,000. The study also reports that 13% of breaches involved AI models or applications and that mature use of AI and automation in security can materially reduce detection and containment times and lower breach costs. IBM advises stronger governance, access controls and AI-aware incident response to manage these risks across all sectors now.
5. <https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026> - Gartner’s research warns that generative AI adoption will accelerate sharply, predicting that more than 80% of enterprises will have used generative AI APIs or deployed generative AI-enabled applications by 2026. The analysis highlights rising demand for APIs and platform services to integrate large language models into enterprise products, with technology service providers playing a central role. Gartner advises organisations to evaluate GenAI use cases carefully, assess risks such as inaccuracy or hallucination, and embed trust, risk and security measures as part of product design. The briefing underscores how GenAI is poised to reshape application development and enterprise workflows globally quickly.
6. <https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture> - The NIST NCCoE’s Implementing a Zero Trust Architecture project provides detailed, practical guidance to help organisations build zero‑trust environments. Its practice guide (NIST SP 1800‑35) and companion materials describe nineteen example implementations using commercial technologies, outlining architecture patterns, configuration details and mappings to established security frameworks. The resource explains zero‑trust principles — verify explicitly, use least privilege and assume breach — and offers step‑by‑step advice for identity, device and data protection. It is intended to remove complexity and accelerate adoption, enabling security teams to design adaptable defences that reduce internal attack surfaces and protect sensitive information in hybrid cloud settings.
7. <https://www.techtarget.com/searchsecurity/definition/SOAR/> - Security Orchestration, Automation and Response (SOAR) platforms centralise security alerts, automate repetitive tasks and co‑ordinate incident response across disparate tools, improving SOC efficiency. By enriching events with contextual threat intelligence, SOAR reduces analyst workload and shortens mean time to detect and respond through repeatable automated playbooks. Organisations deploying SOAR report faster containment, more consistent remediation and better cross‑team collaboration, while mitigating alert fatigue. SOAR also enables scalability for security operations, integrates with SIEM and threat feeds, and supports case management. Adoption of SOAR is recommended as part of modernising security operations to handle high telemetry volumes and scarce skilled personnel.