# Cloud data exposed to AI risks as shadow applications and ghost users undermine security



Recent findings from the 2025 State of Data Security Report by Varonis paint a stark picture of cloud security challenges exacerbated by the widespread adoption of artificial intelligence (AI) tools. The report, which analysed 1,000 IT environments, highlights alarming gaps in governance that leave sensitive data perilously exposed. Among its most striking revelations, an overwhelming 99% of organisations reported that sensitive information was accessible to various AI applications, underscoring a critical risk in the current digital landscape.

These vulnerabilities extend to the use of unverified and unsanctioned applications—dubbed 'shadow AI'—with 98% of enterprises admitting to operating these tools, which bypass standard security protocols. The extensive reliance on these applications raises concerns about potential data leaks and unauthorised access. Further compounding the problem, a staggering 88% of organisations still have dormant user accounts, often referred to as ghost users, which remain active and can be exploited by malicious actors to pivot and infiltrate deeper into corporate systems.

The report accentuates that poor identity management practices, combined with insufficient enforcement of security measures—such as multifactor authentication (MFA)—create a precarious environment where breaches can occur with alarming ease. Notably, the absence of MFA enforcement, recorded in 14% of organisations, has already been linked to significant security breaches in recent years. Many companies also struggle with inadequate data governance, as only 10% of organisations employ proper file labeling, which is crucial for effective access control and compliance.

The pervasive nature of AI within corporate structures further complicates security protocols. As Varonis points out, the very benefits that AI tools offer—enhanced productivity and data insights—can also serve as a double-edged sword. “AI acts like a hungry Pac-Man, scanning and analysing all the data it can grab. If AI surfaces critical data where it doesn't belong, it's game over,” the company articulated in a related blog post. Addressing this requires a robust approach to management that not only embraces AI’s opportunities but also defines stringent frameworks around data protection.

Insights gleaned from the growing menace of shadow AI emphasise the significance of recognising and safeguarding the ‘crown jewels’ of data. As experts like Brian Vecci of Varonis note, comprehensive data management strategies are essential to prevent breaches stemming from unauthorised applications. This theme resonates beyond corporate entities, echoing among federal agencies grappling with similar security dilemmas. A data-centric security posture is increasingly deemed necessary to protect sensitive information amidst the complexities introduced by AI and cloud environments.

The ongoing surge in data breaches linked to generative AI tools showcases a pressing need for organisations to fortify their security measures. A pertinent case was highlighted where a former employee used a generative AI copilot to access and exfiltrate sensitive customer data, reiterating the tangible risks that such tools can pose without rigorous oversight and security frameworks.

Consequently, the report urges organisations to confront their exposure levels, adopt stringent access controls, and treat data security as fundamental to responsible AI application. As AI's role in the workplace continues to evolve, the interplay between convenience and security must be delicately balanced to safeguard sensitive information effectively.

For those keen on developing a holistic approach to their data governance and security, investing in advanced data lifecycle management, enhanced classification capabilities, and automated compliance monitoring tools will be pivotal as the landscape of AI continues to reshape security paradigms.

## Reference Map:

* Paragraph 1 – [[1]](https://thejournal.com/articles/2025/05/27/data-security-report-identifies-cloud-governance-gaps-ai-impact.aspx), [[4]](https://www.varonis.com/blog/federal-data-security-challenges)
* Paragraph 2 – [[1]](https://thejournal.com/articles/2025/05/27/data-security-report-identifies-cloud-governance-gaps-ai-impact.aspx), [[2]](https://www.varonis.com/blog/how-to-prevent-your-first-ai-data-breach), [[3]](https://siliconangle.com/2025/05/02/data-security-varonis-cna-shadow-ai-rsac/)
* Paragraph 3 – [[1]](https://thejournal.com/articles/2025/05/27/data-security-report-identifies-cloud-governance-gaps-ai-impact.aspx), [[6]](https://www.globenewswire.com/news-release/2025/02/25/3032089/0/en/Varonis-at-the-2025-Gartner-Security-Risk-Management-Summit-Securing-Data-in-the-Age-of-AI.html)
* Paragraph 4 – [[3]](https://siliconangle.com/2025/05/02/data-security-varonis-cna-shadow-ai-rsac/), [[5]](https://www.varonis.com/blog/whats-new-in-varonis-march-2025)
* Paragraph 5 – [[2]](https://www.varonis.com/blog/how-to-prevent-your-first-ai-data-breach), [[1]](https://thejournal.com/articles/2025/05/27/data-security-report-identifies-cloud-governance-gaps-ai-impact.aspx)
* Paragraph 6 – [[3]](https://siliconangle.com/2025/05/02/data-security-varonis-cna-shadow-ai-rsac/), [[6]](https://www.globenewswire.com/news-release/2025/02/25/3032089/0/en/Varonis-at-the-2025-Gartner-Security-Risk-Management-Summit-Securing-Data-in-the-Age-of-AI.html)

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

## Bibliography

1. <https://thejournal.com/articles/2025/05/27/data-security-report-identifies-cloud-governance-gaps-ai-impact.aspx> - Please view link - unable to able to access data
2. <https://www.varonis.com/blog/how-to-prevent-your-first-ai-data-breach> - This article discusses the increasing risk of data breaches due to the widespread use of generative AI tools, known as 'copilots', in organizations. It highlights a case where a former employee used a generative AI copilot to access and exfiltrate sensitive customer data, leading to a breach. The piece emphasizes the need for organizations to secure their data in the era of generative AI and outlines strategies to prevent such breaches, including proper data classification, access controls, and monitoring of AI tool usage.
3. <https://siliconangle.com/2025/05/02/data-security-varonis-cna-shadow-ai-rsac/> - This article highlights the growing threat of 'shadow AI'—unsanctioned AI tools used by employees—that poses significant risks to data security. It features insights from Varonis' Brian Vecci and CNA's Rizwan Jan, who discuss the challenges organizations face in protecting sensitive data from unauthorized AI applications. The piece underscores the importance of understanding and securing 'crown jewels' of data to prevent potential breaches and emphasizes the need for comprehensive data management strategies in the age of AI.
4. <https://www.varonis.com/blog/federal-data-security-challenges> - This blog post addresses the data security challenges faced by federal agencies in the age of AI. It discusses the exponential growth of data and the risks associated with exposing sensitive information to AI tools. The article emphasizes the necessity for government agencies to adopt a data-centric approach to security, ensuring that critical information remains protected amidst the complexities introduced by AI and cloud technologies.
5. <https://www.varonis.com/blog/whats-new-in-varonis-march-2025> - This article outlines the latest updates from Varonis as of March 2025, focusing on new features designed to enhance data governance, labeling, and AI security capabilities. It introduces Data Lifecycle Automation, Salesforce Agentforce discovery, and automated AWS service tag application, among other functionalities. The piece highlights Varonis' commitment to providing comprehensive solutions that help organizations enforce governance and compliance policies, create custom integrations, and improve data security in the evolving digital landscape.
6. <https://www.globenewswire.com/news-release/2025/02/25/3032089/0/en/Varonis-at-the-2025-Gartner-Security-Risk-Management-Summit-Securing-Data-in-the-Age-of-AI.html> - This press release announces Varonis' participation as a Premier Exhibitor at the 2025 Gartner Security & Risk Management Summit, scheduled for March 3–4 in Sydney, Australia. It details Varonis' activities at the summit, including a panel session titled 'Executive's Guide to Securing Data in a New Era of Risk', where experts will discuss strategies for protecting sensitive data in the age of AI. The release underscores Varonis' focus on addressing AI's impact on data security, compliance, and risk reduction.
7. <https://www.aiwithchris.com/ai-tutorials/varonis-rsac-2025-data-security-ai> - This article provides an overview of Varonis' data security platform as presented at the RSA Conference 2025. It highlights key features such as continuous data discovery and classification, automated threat detection, and reduction of data exposures. The piece emphasizes how Varonis' AI-driven automation proactively identifies critical data and swiftly removes vulnerabilities within digital infrastructures, equipping organizations to manage data security risks effectively in the evolving digital landscape.