Shadow AI Security Risks: Facts for CISOs

AI Security Snapshot

As new AI technologies transform business operations, security leaders at midsized companies must be aware of the dangers of "shadow AI." Similar to how the cloud introduced shadow IT problems, CISOs should plan for how to mitigate the risks of unsanctioned AI usage. Consider that according to a recent Gartner® survey:

Only **16%** of organizations report that they block GenAI use by default for public GenAI.[1]

72% of respondents report a struggle to maintain visibility of embedded AI.[1]

52% of organizations suspect or have evidence that employees are building custom GenAI without including cybersecurity risk evaluation.[1]

69% of organizations suspect or have evidence that employees are using prohibited public GenAI.[1]

Shadow AI Security Concerns

Data Privacy
AI tools require access to large datasets, increasing risk of breaches and compliance issues (GDPR, CCPA, HIPAA).

Third-Party/Vendor Risk
CISOs must vet all AI vendors and related third-parties, as many lack robust security certifications.

Insider Threats
Whether it's intentional or unintentional, shadow AI can lead to data leaks and policy violations.

AI-Powered Attacks
Criminal hackers are leveraging AI for sophisticated phishing, model poisoning, and manipulating outputs.

Best Practices

- Promote AI usage policies that balance innovation with security.
- Encrypt sensitive data and limit API exposure used by AI.
- Educate employees to recognize AI security risks while balancing visibility, providing secure alternatives, and offering real-time coaching.
- Regularly audit AI systems and monitor for drift or anomalies.
- Establish clear governance to align AI use with company values and regulations.
- Foster open AI communities that surface risky uses, share approved cases, and coach employees toward safer adoption.

Adopting AI securely means balancing innovation with vigilance and policy.
Smart CISOs can learn how to harness AI's benefits while managing the risks of shadow AI with a complimentary copy of the Gartner report, **CISOs Must Bring Shadow AI Into the Light:**

blue mantis

Download the Report

Gartner, CISOs Must Bring Shadow AI Into the Light, By Andrew Walls, Jeremy D'Hoinne, John Watts, 4 July 2025 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

References:

[1] 2025 Gartner Cybersecurity Innovations in AI Risk Management and Use Survey: This survey was conducted to understand how organizations are managing the cybersecurity risks of generative AI (GenAI) and AI techniques that support it. The research was conducted online from 21 March through 9 May 2025 among 302 cybersecurity leaders in the North America (n = 181), EMEA (n = 71) and Asia/Pacific (n = 50) regions. Qualifying organizations reported enterprise-wide revenue of at least $250 million or equivalent for fiscal 2024 and were senior cybersecurity management involved in activities related to AI cybersecurity risk management within their organization. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.