Shadow AI: The Silent Threat to Credential Security

Understanding the Risks from Shadow AI in the Enterprise

Jennifer Gold | CISO, Risk Aperture | Dashlane Security Summit | April 1, 2025

Introduction

JANE DOE

A Well-Intentioned Employee

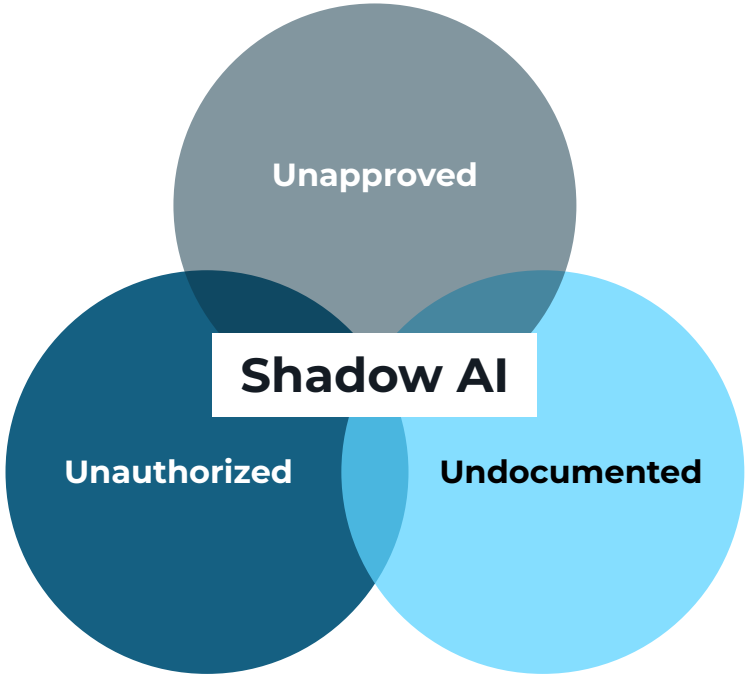
Jane Doe pastes a project report into ChatGPT to improve clarity. Unknowingly, she includes a URL to an internal dashboard and embedded API credentials. A few weeks later, those credentials appear for sale on a dark web forum. A cybercriminal purchases access, bypasses authentication, and internal systems are compromised.

- No alert was triggered.
- No policy was violated because none existed.
- No visibility. No oversight. No control.

This is Shadow AI.

What is Shadow AI?

Shadow AI is the **unauthorized**, **unapproved**, and **undocumented** use of AI powered tools and systems within an organization, without explicit approval or security oversight.

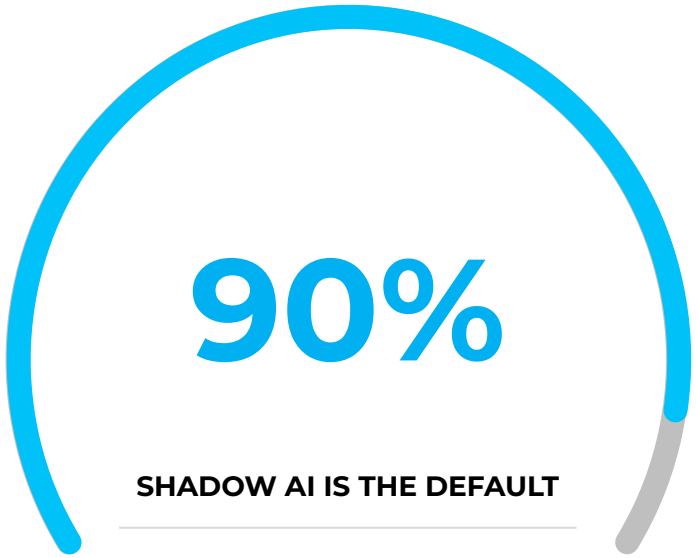


Key Characteristics:

- **Unapproved**: Implemented without formal vetting, increasing vulnerabilities
- **Unauthorized**: Operating outside security protocols, lacking encryption and access controls
- **Undocumented**: Missing integration with official systems, creating operational blind spots.

Shadow AI is Everywhere

- Shadow AI is often hiding in plain sight embedded in the workflows of nearly every business unit and sector.
- Employees across industries are using GenAI for efficiency, often outside of IT-sanctioned governance.
- Risks = security breaches, data leaks, regulatory violations



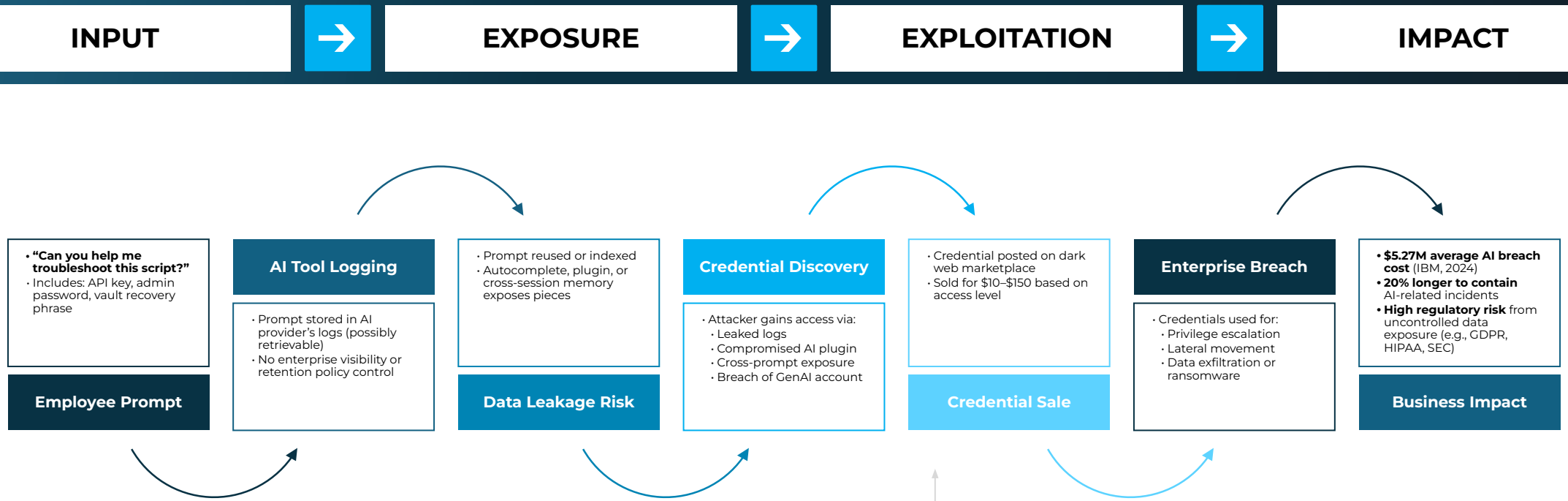
Security Blind Spots

93% of security leaders report using GenAI. Yet 1 in 3 firms lack mitigation strategies.

Shadow Data = Rising Costs

Breaches involving shadow data cost $5.27M on average and take 20% longer to contain.

From Prompt to Breach



How Credentials Are Sold
The Dark Web Economy

- Marketplaces operate like black-market Amazon
- Pricing: $10 for basics, much higher for corporate credentials
- Preferred: Bitcoin, Monero, mixing services

Assessing the Business Impact of Shadow AI

Understanding Shadow AI requires balancing business value with risk across a wide range of ungoverned use cases. This framework organizes those behaviors into four primary risk quadrants to help prioritize response and approach.

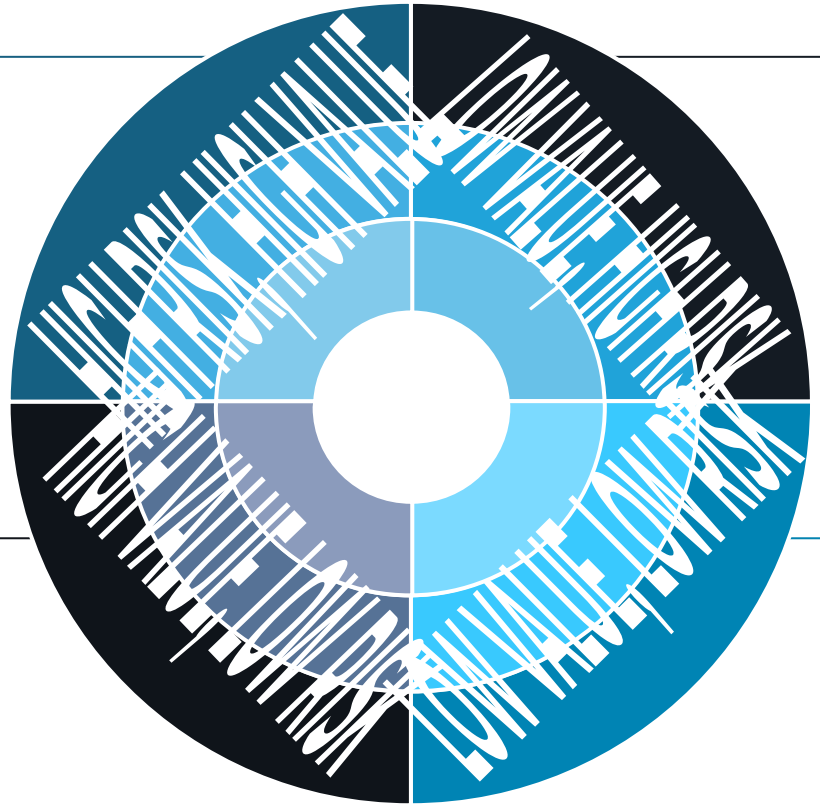
High Risk, High Value

These Shadow AI initiatives offer substantial business benefits but pose serious compliance, security, or ethical risks.

Examples: Unauthorized use of powerful generative AI tools for customer communication. Models trained on sensitive or proprietary data without oversight.
Impact: These require urgent attention and formalization. Evaluate for potential integration into official systems.

High Value, Low Risk

Relevant Factors
3. Customer Expectations, 4. Supply Chain Risks, 9. Talent Acquisition & Retention
Potential Cybersecurity Impact:
Third-party risks, insider threats due to workforce turnover, cyber resilience against vendor attacks.



Low Value, High Risk

These Shadow AI use cases boost productivity with minimal data exposure, though they remain outside formal governance.

Examples: Summarizing industry news for internal newsletters; generating mockups or diagrams for brainstorming.
Impact: Strong candidates for formal support. Provide approved tools, clear usage guidelines, and copyright awareness to sustain value and reduce risk.

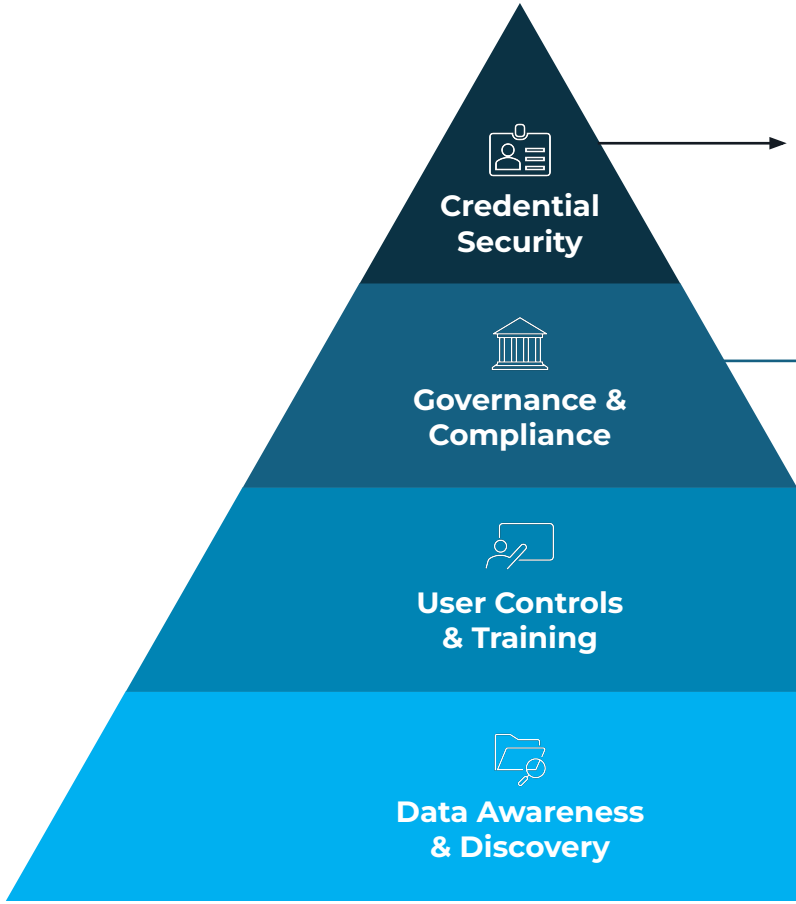
Low Value, Low Risk

These use cases are ***Apparent*** Low Risk, Low Value based on context and content.

Examples: AI tools casually used for grammar, summarizing· Employees experimenting with image generators/
Impact: May involve hidden data risks if left unchecked

Approach to Shadow AI Mitigation

A multi-layered model to support organizational resilience and proactive Shadow AI mitigation



- Use password managers to prevent GenAI credential storage.
- Monitor the dark web for AI-linked credential leaks.

- Develop and enforce enterprise-wide AI usage policies.
- Align AI governance with NIST, ISO, and AI Act standards

- Train employees on AI security risks and acceptable use
- Implement security controls, including access controls to secure data

- Discover Shadow AI usage across tools and endpoints
- Deploy prompt monitoring or usage analytics
- Audit third-party AI integrations and restrict access

AI Standards and Controls

For each category, apply the relevant standards and controls.

Governance

NIST AI RMF, ISO/IEC 38500, GDPR, HIPAA, EU AI Act

Security

NIST CSF, ISO 27001, OWASP Top 10 (for AI), CIS Controls

Data

GDPR, ISO 27701, CCPA, and privacy-enhancing techniques

Usage

SOC 2, ISO 27001, NIST AI RMF

Key Takeaways

Address Shadow AI risk with a defined strategy. Action beats reaction every single time.

Visibility

- Recognize that Shadow AI already exists in your organization
- You cannot secure what you cannot see
- Automate the discovery of AI usage

Governance

- Verify AI usage and data access
- Apply policy, least privilege, and data controls
- Govern proactively rather than reactively

Enablement

- Adapt controls to match AI speed
- Provide guardrails for safe usage
- Train employees in responsible AI use

Questions & Answers

THANK YOU

Jennifer Gold, CISO, Risk Aperture

LinkedIn

https://www.linkedin.com/in/jenniferfarrellgold/

Email

jennifer@risk-aperture.com

Additional Reading

Whitepaper, “The Hidden Threat of Shadow AI”

Statistics: Data Leaks and Security Risks

Usage & Adoption:

- 56% of U.S. employees use generative AI for work-related tasks, with nearly 10% relying on these tools daily.
- Corporate data input into AI tools surged by 485% from March 2023 to March 2024.
- 93% of cybersecurity leaders report deploying generative AI, 34% of these companies have not taken steps to mitigate security risks.

Data Leakage & Security Risks:

- 38% of employees share confidential data with AI platforms without approval (survey of 7,000 workers).
- 35% of breaches in 2024 involved data stored in unmanaged sources (shadow data).
- Breaches involving shadow data took 26.2% longer to identify and 20.2% longer to contain, averaging 291 days, with an average cost of USD 5.27 million.

Types of Data Exposed:

- Customer support information (16.3%)
- Source code (12.7%)
- Research and development materials (10.8%)
- HR and employee records (3.9%)
- Financial documents (2.3%)

Impact on Intellectual Property:

- 26.5% rise in IP theft due to attackers accessing more sensitive data during breaches.
- Cost per record of lost IP increased to USD 173 in 2024 from USD 156 in 2023 (an 11% uptick).

Sources:
1. https://www.ibm.com/think/insights/hidden-risk-shadow-data-ai-higher-costs
2. https://www.cfodive.com/news/shadow-it-surge-threatens-corporate-data-report/716686/
3. https://cloudsecurityalliance.org/blog/2025/03/04/ai-gone-wild-why-shadow-ai-is-your-it-team-s-worst-nightmare
4. https://versa-networks.com/blog/shadow-ai-data-leakage-how-to-secure-generative-ai-at-work/

Data at Risk from Shadow AI Use

Customer Records	*PII, contact info, CRM exports*
Source Code	*Including proprietary algorithms, scripts, GitHub repo links*
HR Documents	*Resumes, employee data, performance reviews*
Financial Reports	*Forecasts, internal dashboards, budgets*
Access Credentials	*Passwords, API keys, recovery phrases, MFA reset links*
Intellectual Property (IP)	*Product designs, roadmaps, trade secrets*
Legal & Contract Language	*Draft agreements, sensitive deal terms*
Medical or Regulated Data	*PHI, insurance forms, compliance risk*