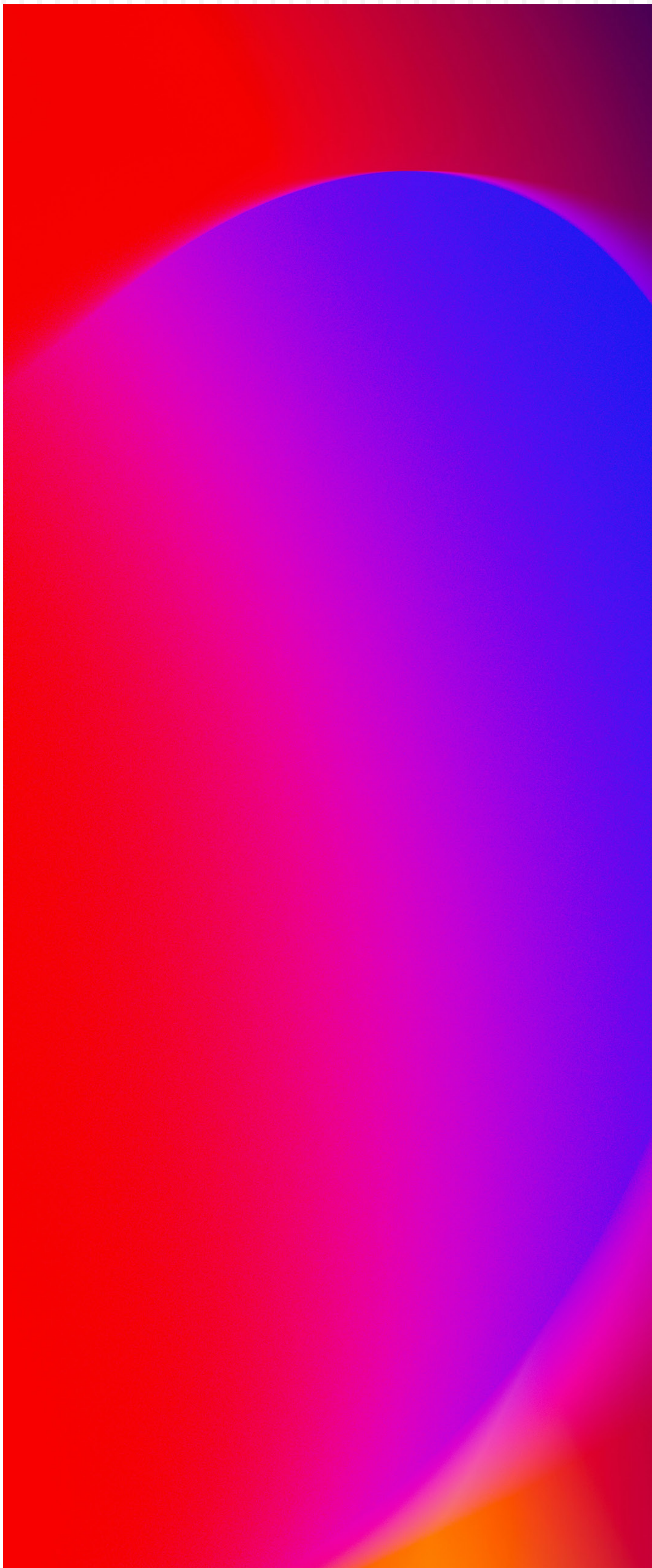
2025 WHITE PAPER

Unmasking Shadow AI: Managing Hidden Risks & Strengthening Governance with BigID

A detailed overview of the risks, regulatory challenges, and best practices for tackling Shadow AI—while highlighting how BigID can empower enterprises to discover, classify, and manage AI-driven data risks.



2025 White Paper
Unmasking Shadow AI: Managing Hidden Risks & Strengthening Governance with BigID

2025 White Paper

Unmasking Shadow AI: Managing Hidden Risks & Strengthening Governance with BigID

As artificial intelligence (AI) adoption accelerates, organizations are facing an emerging challenge—Shadow AI. Much like Shadow IT, where unauthorized technology solutions proliferate outside official oversight, Shadow AI refers to the unsanctioned or unmanaged use of AI tools, models, and applications within an enterprise. Employees may leverage third-party AI solutions, train models on sensitive data, or deploy AI systems outside governance frameworks—all without proper security controls, compliance measures, or visibility from IT, privacy, and security teams.

The risks of Shadow AI extend beyond simple policy violations. Unregulated AI usage can introduce data security vulnerabilities, compliance failures, and ethical concerns, undermining an organization's ability to manage data privacy, intellectual property, and responsible AI governance. This guide explores the risks, regulatory challenges, and best practices for tackling Shadow AI—while highlighting how BigID can empower enterprises to discover, classify, and manage AI-driven data risks.

Understanding Shadow AI: The Hidden Threat in AI Adoption

What is Shadow AI?

Shadow AI encompasses any artificial intelligence or machine learning (ML) tools that operate outside of an organization's official governance framework. Employees, departments, or external vendors may adopt AI-powered solutions independently—often for productivity, automation, or analysis—without IT, privacy, or security team approval.

Common Examples of Shadow AI

- **Use of unauthorized AI tools** (e.g., ChatGPT, Midjourney, Bard) for business tasks involving sensitive data.
- **Training AI models on proprietary or personal data** without proper governance.
- **Deploying AI applications outside of security controls**, leading to data exposure.
- **Use of external AI-powered SaaS solutions** without IT approval.
- **Integration of AI tools with corporate systems** without security vetting.

Shadow IT versus Shadow AI

To grasp the impact of shadow AI, it's important to differentiate it from shadow IT.

Shadow IT	Shadow AI
Shadow IT encompasses the use of software, hardware, or information technology within an enterprise network without the approval, awareness, or oversight of the IT department or CIO. Employees may resort to unauthorized AI tools when they find existing solutions inadequate or perceive approved options as too slow. Typical examples include utilizing personal cloud storage services or unapproved project management tools.	While shadow IT encompasses any unauthorized application or service, shadow AI specifically pertains to unapproved AI tools, platforms, and use cases. For example, an employee might leverage a large language model (LLM) to generate a research report without considering potential security risks. The primary distinction lies in the type of technology involved—shadow AI revolves around the unauthorized use of artificial intelligence, raising unique challenges related to data management, model outputs, and decision-making.

Why is Shadow AI a Growing Concern?

The 2024 Work Trend Index Annual Report from Microsoft and LinkedIn reveals that at least 75% of global knowledge workers use generative AI. As a matter of fact, to highlight the prevalence of the most widely used generative AI tool, ChatGPT set a record for the fastest-growing user base at 100 million weekly users.

Unlike traditional software, AI models learn and adapt based on the data they process, making their impact on **privacy, security, and compliance more complex.** While its capabilities offer significant productivity and personalization benefits, its use poses privacy and security risks. Key risks include:

- **Data Privacy Violations** – AI models trained on sensitive, regulated, or personally identifiable information (PII) may inadvertently expose confidential and sensitive data.
- **Regulatory Non-Compliance** – AI systems that process personal data without governance may violate GDPR, CCPA, NIS2, and AI-specific laws like the EU AI Act.
- **Security Risks & Data Leaks** – Without proper security controls, AI-generated insights, prompts, and outputs may leak proprietary or classified information.
- **Intellectual Property Exposure** – AI tools trained on enterprise data may retain sensitive information, leading to potential IP loss.
- **Bias & Ethical Issues** – Shadow AI models can reinforce biases without proper risk assessment and mitigation strategies.

Organizations need a proactive approach to **discover, monitor, and secure** AI-related data usage—before it leads to compliance failures and reputational damage.

Regulatory Landscape: How AI Governance is Evolving

According to The 2024 Global Report on Generative AI, 73% of organizations lack full confidence in meeting future AI regulations and data compliance requirements. This is a clear indication that there are growing concerns about aligning with upcoming AI regulations and compliance, which make navigating an already complex landscape even more difficult, making generative AI a top priority for many executives.

Governments and regulatory bodies worldwide are tightening AI compliance standards to prevent the risks associated with uncontrolled AI deployments. Some key regulations include:

EU AI Act

- Bans **"unacceptable risk" AI** applications, including manipulative AI and social scoring.
- Requires **high-risk AI systems** to implement transparency, accountability, and data governance measures.
- Mandates compliance with **GDPR**, ensuring AI systems respect **data privacy, retention, and security requirements.**

NIST AI Risk Management Framework

- Emphasizes **trustworthy AI principles,** including explainability, fairness, and continuous monitoring.
- Encourages organizations to adopt AI lifecycle governance to manage risks across training, deployment, and operations.

GDPR & CCPA

- Requires organizations to ensure AI systems comply with **data minimization, purpose limitation, and privacy-by-design principles.**
- Mandates transparency in **automated decision-making processes** impacting individuals.

Failure to comply with these regulations can result in heavy fines, reputational damage, and legal action—making AI governance a business-critical priority.

How BigID Helps Organizations Manage Shadow AI & Strengthen AI Governance

Shadow AI is no longer an isolated IT concern—it is a business-wide challenge that demands immediate action. Organizations must proactively discover, manage, and secure AI data usage to prevent security breaches, compliance failures, and reputational harm.

BigID provides the visibility, governance, and automation needed to unlock the benefits of AI while minimizing its risks. Whether it's detecting unauthorized AI applications, enforcing compliance, or securing AI-generated data, BigID helps organizations stay ahead of evolving AI governance challenges.

With BigID, organizations can:

1. Detect Model Files in Unstructured Data Sources
BigID automatically scans your data repositories—including S3 buckets, file stores, and databases—to detect files and binaries associated with AI models (e.g., PyTorch,

TensorFlow). This process helps to identify deployments that have bypassed formal IT channels, flagging potential instances of unauthorized LLM usage.

2. Scrape Emails for AI Service Communications
BigID scrapes email systems (Gmail, Outlook, etc.) for registration or usage notifications related to external AI services such as DeepSeek, OpenAI, Claude, Gemini, and more. By pinpointing these communications, you can reveal instances where employees might be leveraging unsanctioned tools, potentially exposing sensitive data or violating internal policies.

3. Scan Code Repositories
BigID scans code repositories and analyzes source code for embedded API keys or calls to external AI services. Detect unauthorized integrations and flag potential supply chain vulnerabilities by gaining insight into which datasets were used and ensuring they are neither biased nor poisoned.

4. Monitor Native AI-Platform Deployments
BigID monitors deployments to classify and analyze underlying models. With BigID, you can detect sensitive data in training sets, identify rogue models bypassing standard approval channels, and continuously verify the supply chain and training datasets. This process safeguards against unintended bias and data poisoning while triggering policy enforcement actions for non-compliant usage when using public AI platforms (e.g., Hugging Face, Azure AI, OpenAI, Google Cloud AI).

5. Map Datasets and Models to AI Assets
BigID maps every discovered dataset and model to your AI asset inventory, ensuring you comply with mandates like those in the EU AI Act. This comprehensive inventory lets you track every AI component, supporting governance and providing the necessary documentation required by global regulations.

6. Initiate and Manage AI Risk Assessments
BigID automates the AI risk assessment process by classifying each AI asset against regulatory standards. Organizations can maintain an up-to-date risk assessment inventory, allowing you to quickly identify risks associated with each model and comply with evolving AI regulations. BigID helps you remediate compliance and data vulnerabilities by cleaning training datasets based on organizational policies, enforcing strict access controls, and ensuring that only authorized usage persists—mitigating potential threats.

7. Map to Regulations and Security Frameworks
BigID continuously maps your AI deployments against relevant security or privacy frameworks, such as the NIST AI Risk Management Framework (AI RMF), and regulatory requirements. By regularly reviewing which controls may be failing, you can proactively address gaps and maintain robust AI governance.

Ready to Tackle Shadow AI?

Let BigID help you discover, manage, and protect your AI-driven data—before it becomes a risk. Request a demo today!

About BigID

BigID enables security, compliance, privacy, & AI data management for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining overnance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 4 consecutive years; the Deloitte 500 for 4 consecutive years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at https://bigid.com.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • AI Data Management

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

> **Tools like BigID are the future.**
> Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.

IDC

Ryan O'Leary
Future of Trust: Battling Data Discovery Confusion