Shadow AI Discovery

Uncover Hidden AI Models, Risky Datasets, and Unapproved AI Usage

Shadow AI Discovery

Shadow AI Discovery

Overview

AI is spreading fast across the enterprise—but many security teams have no visibility into what models are running, what data they're using, or where that usage violates policy. The result: Shadow AI. These unmanaged models often operate without oversight and frequently rely on sensitive or regulated data—creating major risk.

BigID's Shadow AI Discovery gives organizations a way to detect, investigate, and act on shadow AI activity. Security and governance teams can automatically discover rogue models, pinpoint risky data use, and take enforcement actions directly in-platform. With full context around access, behavior, and exposure, BigID helps enterprises reduce AI risk—fast.

- Discover unauthorized AI models and deployments across your environment
- Identify sensitive, personal, or regulated data used in AI workflows
- Investigate risky AI usage across cloud, SaaS, developer, and collaboration tools
- Correlate AI activity with underlying data and users for actionable insight
- Take direct action with built-in enforcement and remediation workflows

Key Outcomes

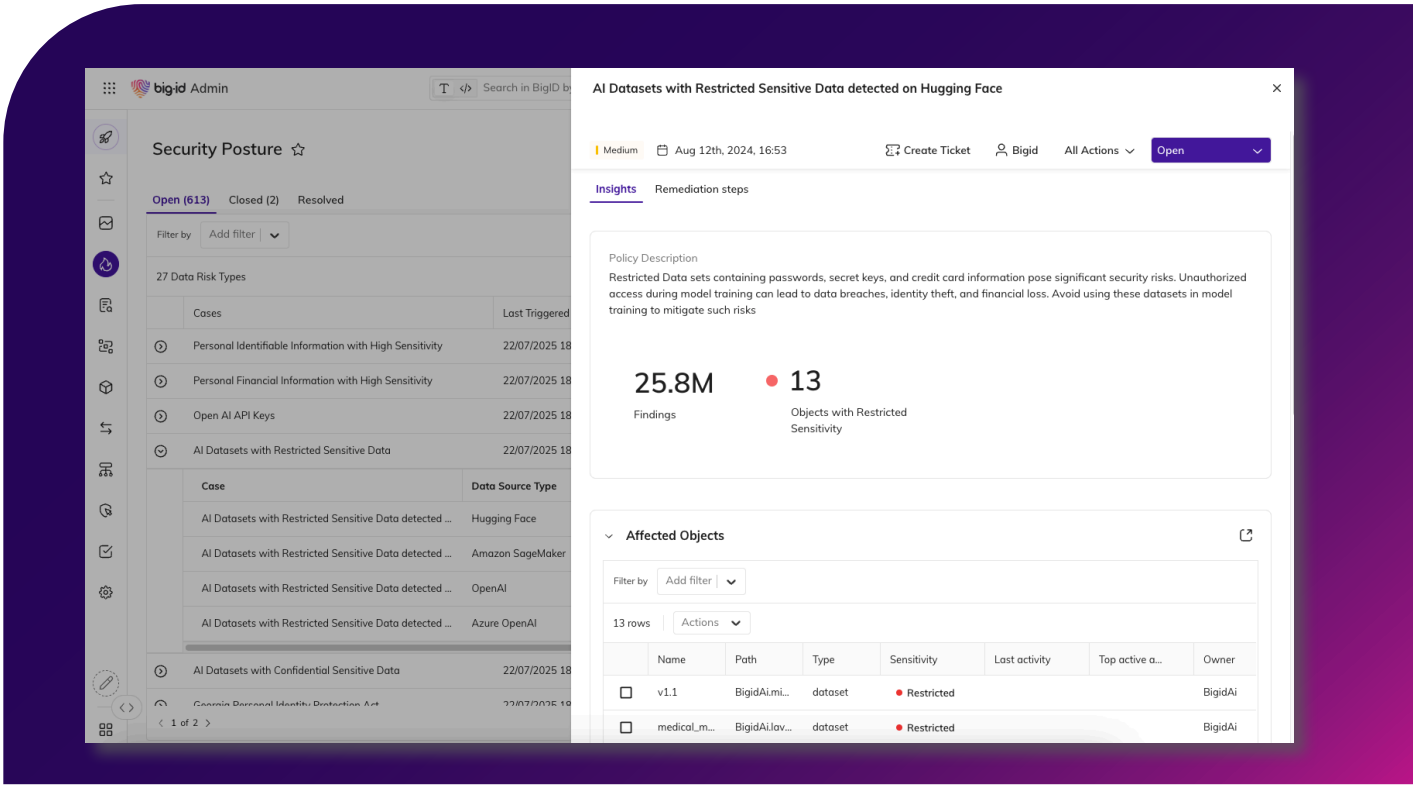
Expose Hidden AI Threats
Uncover unauthorized, unmanaged, or rogue AI models operating outside official oversight.

Detect Sensitive Data Use
Identify personal, proprietary, or regulated data in AI pipelines—before it's exposed or misused.

Investigate with Full Context
See where AI models live, what data they touch, and who's behind them—so you can prioritize response.

Take Action, Not Just Inventory
Trigger alerts, restrict access, apply labels, or launch remediation—all within BigID.

Operationalize AI Governance
Move from theory to action by tying governance policies to model discovery and data controls.



Key Capabilities

AI Model Discovery Across Cloud & SaaS
Automatically detect deployed, unmanaged, or unauthorized AI models across cloud platforms, SaaS applications, developer tools, and internal systems. BigID continuously scans your environment to identify shadow models that may be operating outside governance and security oversight. This gives security teams the complete picture of their AI landscape—no blind spots.

Sensitive Dataset Detection for AI
Uncover when personal, regulated, or proprietary data is used in AI training, inference, or prompt pipelines. BigID identifies sensitive datasets that pose compliance or security risks when consumed by AI systems. By exposing high-risk data use, teams can take early action to mitigate exposure and avoid downstream AI misuse.

Model-to-Data & User Correlation
Correlate discovered models to the data they access and the users or teams responsible for them. BigID combines identity-aware data mapping with model metadata to show how AI is used, who's behind it, and what data is at risk. This context enables targeted investigations and policy enforcement based on real-world usage.

Unstructured & Collaborative Environment Support
Go beyond structured data by discovering AI usage hidden in documents, PDFs, emails, Slack messages, SharePoint, GitHub, and other collaboration tools. BigID scans unstructured and semi-structured sources to detect informal or decentralized AI activity that traditional tools miss. This ensures you catch shadow AI no matter where it lives.

Enforcement & Remediation Built-In
Move from discovery to action with integrated workflows that let you respond in-platform. Automatically trigger alerts, apply labels, restrict access, or initiate remediation when shadow AI activity is detected. BigID enables teams to operationalize governance by embedding enforcement directly into their data and model oversight processes.

About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.

Connect the Dots Across Data & AI

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