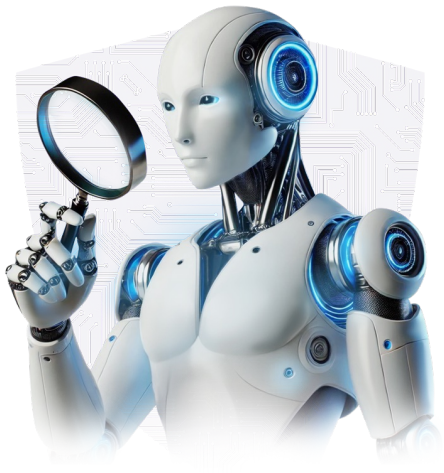
PointGuard AI Discovery

Part of a comprehensive AI Security & Governance Platform

AI Discovery | AI Security Posture | Automated Red Teaming | AI Detection & Response

AI Governance Starts with Discovery and Visibility

As AI adoption accelerates, organizations need visibility into their AI projects to manage risks effectively. PointGuard AI Discovery provides insights into AI resources including models, datasets, MLOps, notebooks, and agents, ensuring security and compliance. Rather than blocking AI initiatives and losing competitive advantage, companies can use AI Discovery to integrate governance, security, and oversight, preventing costly incidents and maintaining trust.



Discover AI Resources on MLOps Platforms

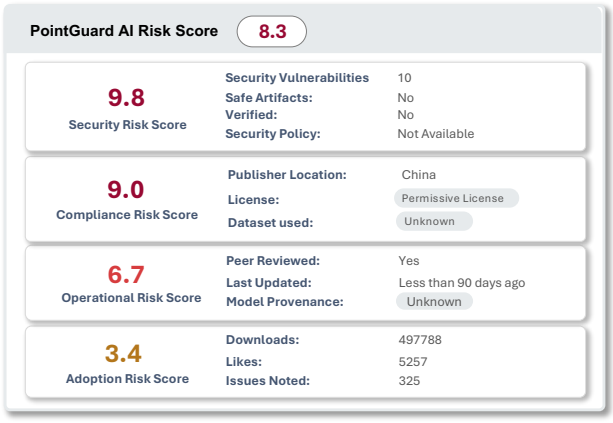
PointGuard provides deep integration with leading AI platforms from Databricks, Azure, AWS, Google, OpenAI, GitHub, and others, and automatically identifies and catalogues resources such as models, notebooks, datasets, clusters, and more to ensure thorough oversight.

- **Integrates with leading AI development platforms**
- **Provides visibility into MLOps pipelines**
- **Discovers models, dataset, notebooks, and more**

Inventory Your AI Assets

PointGuard creates inventories of AI tools, including models, datasets, notebooks, clusters, endpoints, and API connectors. AI assets are tracked and monitored to ensure visibility, acceptability, and compliance.

- **Maintains a dynamic inventory of all AI resources**
- **Tracks approved assets with risk ratings**
- **Associates AI resources with connected applications**



PointGuard AI Knowledge Base Sample Risk Scoring

Manage AI Model Supply Chains

With a comprehensive knowledge base of open-source models from major sources like Hugging Face, PointGuard helps to identify high-risk models, ensure licensing, and track lineage for models and datasets.

- **Leverages model knowledge base with risk ratings**
- **Tracks model sources, licensing, and lineage**
- **Manages AI bill-of-materials (BOM)**

Streamline Approval Workflows

As AI assets are discovered, automated multi-level workflows track and ensure approval. Managers can see at-a-glance details on models, provenance, risk ratings, and applications connected to proposed AI assets.

- **Automates approval and exception workflows**
- **Provides single view of all AI assets, provenance, and risk**
- **Streamlines compliance and reporting**

SC 2025 Awards WINNER

AI Discovery Capabilities

AI Asset Discovery	
AI Models	Includes LLMs and other ML models
Datasets	Discover datasets and their purpose such as production vs. training
AI Assets	Includes notebooks, clusters, catalogs, jobs, serving end-points, plugins, agents, API connectors
Connected Applications	Discover API calls and data connectors
Platforms Supported	Databricks, Amazon SageMaker, Amazon Bedrock, Azure AI, Azure OpenAI, Google Vertex AI
Platform Capabilities	
Mapping to Applications	Maps models, datasets, sub-resources to associated applications
Usage Approval	Alerts managers of new assets and owners with one-click approval
Exception Management	Automates approvals for exceptions and false positives to reduce redundancy and noise.
Remediation	Automates ticket creation and notifications for prioritized issues
Metrics & SLAs	Tracks metrics and team SLAs for model approvals, security findings, MTTR and more

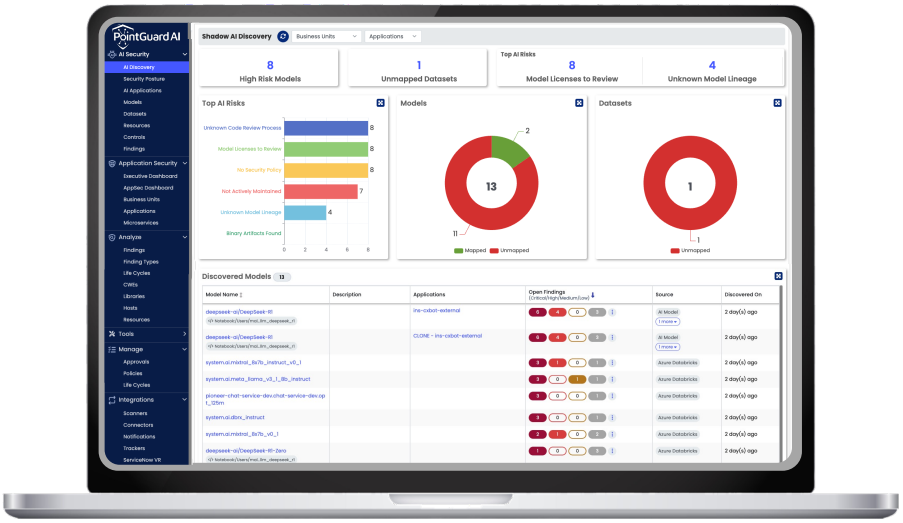
Protects AI and Supporting Applications

PointGuard is the only vendor to secure both AI systems and software applications—protecting everything from code and third-party libraries to LLM models, datasets, and MLOps. The robust platform operationalizes AI security with comprehensive dashboards, metrics, SLAs, and automated remediation workflows with ticketing systems like Jira and ServiceNow.

Get Started for Free

Try our free AI Discovery & Risk Assessment to get an overview of your AI security posture with actionable recommendations. Learn more at:

www.pointguardai.com/free-discovery



PointGuard AI Security Dashboard