PointGuard AI

AI Discovery & Inventory

Proactive Visibility for Models, Agents, and AI Supply Chains

AI Security Starts with Discovery

AI adoption is moving faster than security and governance teams can track. Models, agents, datasets, and AI services often appear through cloud platforms, developer workflows, and runtime behavior without formal approval, creating security and compliance risk.

PointGuard AI Discovery provides continuous visibility across code, cloud, and runtime. Instead of reacting after deployment or incidents, teams identify AI usage early, assess risk in context, and govern AI confidently without slowing innovation.

Dynamic Inventory of AI Assets

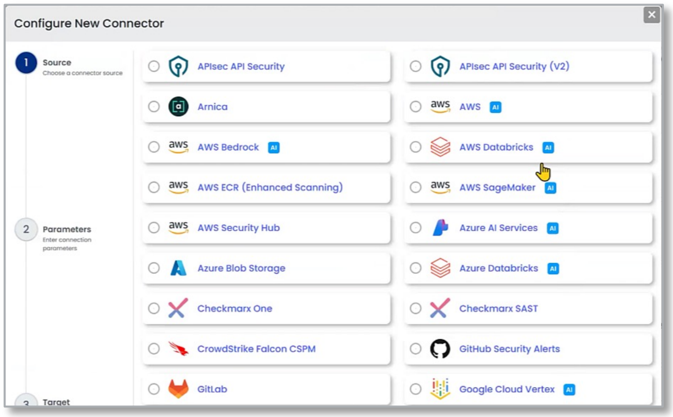
PointGuard builds the most complete inventory of AI assets across your organization and automatically updates it as systems grow and change. This includes:

- **Models, datasets, and notebooks**
- **Agents, MCP servers, and connected applications**
- **Infrastructure and endpoints**
- **External AI services and supply chains**

Discovery Across AI Platforms

AI development spans multiple cloud providers and MLOps tools, making manual tracking nearly impossible. PointGuard integrates directly with leading AI platforms to automatically identify and catalog AI resources across development and production environments including:

- **Databricks, AWS, Azure, Google, Copilot Studio**
- **Discovers AI assets, servers, and endpoints**
- **Provides continuous visibility across AI pipelines**



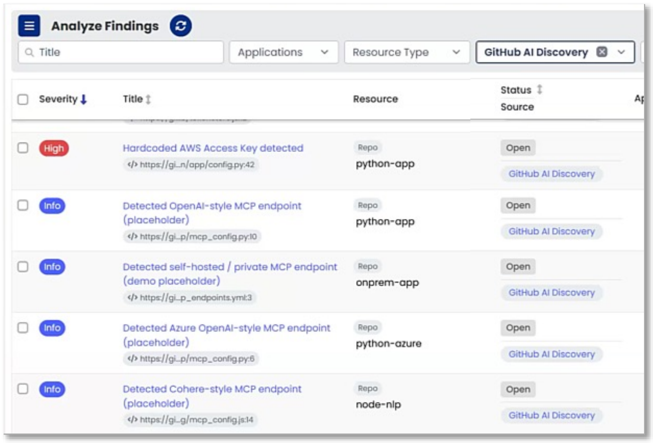
Configure New Connector

1 Source
Choose a connector source

2 Parameters
Enter connection parameters

3 Target

○ APIsec API Security
○ APIsec API Security (V2)
○ Arnica
○ AWS AI
○ AWS Bedrock AI
○ AWS Databricks AI
○ AWS ECR (Enhanced Scanning)
○ AWS SageMaker AI
○ AWS Security Hub
○ Azure AI Services AI
○ Azure Blob Storage
○ Azure Databricks AI
○ Checkmarx One
○ Checkmarx SAST
○ CrowdStrike Falcon CSPM
○ GitHub Security Alerts
○ GitLab
○ Google Cloud Vertex AI



Analyze Findings

Title | Applications | Resource Type | GitHub AI Discovery

□	Severity	Title	Resource	Status Source
□	High	Hardcoded AWS Access Key detected https://gi...n/app/config.py:42	Repo python-app	Open GitHub AI Discovery
□	Info	Detected OpenAI-style MCP endpoint (placeholder) https://gi...p/mcp_config.py:10	Repo python-app	Open GitHub AI Discovery
□	Info	Detected self-hosted / private MCP endpoint (demo placeholder) https://gi...p_endpoints.yml:3	Repo onprem-app	Open GitHub AI Discovery
□	Info	Detected Azure OpenAI-style MCP endpoint (placeholder) https://gi...p/mcp_config.py:6	Repo python-azure	Open GitHub AI Discovery
□	Info	Detected Cohere-style MCP endpoint (placeholder) https://gi...g/mcp_config.js:14	Repo node-nlp	Open GitHub AI Discovery

Find AI Assets in Code Repositories

Many AI risks originate in developer code long before applications reach production. PointGuard scans source code repositories to identify AI usage early allowing teams to address risk before AI systems are deployed or exposed to users and data. The solution:

- **Detects models, agents, chatbots, and MCP references in code**
- **Identifies calls to external AI services and APIs**
- **Flags hard-coded secrets used by AI components**

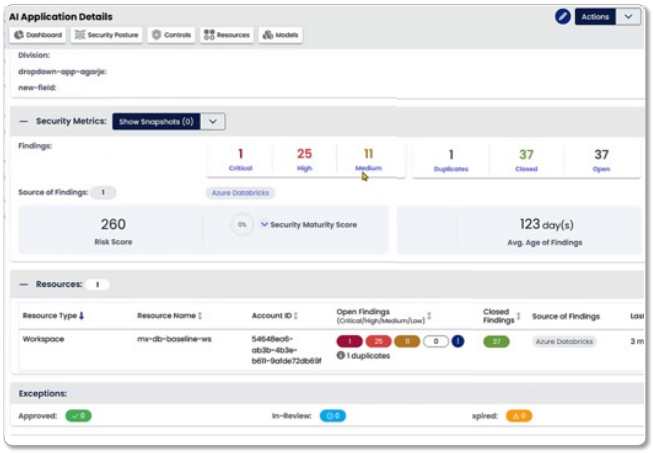
www.pointguardai.com   info@pointguardai.com

AI Discovery & Inventory

Map AI Assets to Applications

AI assets rarely operate in isolation. PointGuard AI Discovery maps discovered resources into applications, providing the context needed to understand real-world risk and business impact. This application-centric view transforms fragmented AI findings into actionable governance insights.

- **Maps models, agents, datasets, and resources to applications**
- **Aggregates findings for all application components**
- **Provides application-level AI risk posture**



AI Application Details

Division:
dropdown-app-agarje:
new-field:

Security Metrics: Show Snapshots (0)

Findings: 1 Critical | 25 High | 11 Medium | 1 Duplicates | 37 Closed | 37 Open

Source of Findings: 1 | Azure Databricks

260 Risk Score | 0% Security Maturity Score | 123 day(s) Avg. Age of Findings

Resources: 1

Resource Type	Resource Name	Account ID	Open Findings (Critical/High/Medium/Low)	Closed Findings	Source of Findings	Last
Workspace	mx-db-baseline-ws	54648ea6-ab3b-4b3e-b611-9afde72db69f	1 25 11 0 1 duplicates	37	Azure Databricks	3 m

Exceptions:
Approved: 0 In-Review: 0 xpired: 0

Manage Risk in AI Supply Chains

As organizations adopt agentic AI, risk shifts from individual models to interconnected AI supply chains. Agents, MCP servers, tools, and datasets introduce new dependencies that must be governed together. PointGuard AI Discovery delivers supply chain visibility designed for modern AI architectures.

- **Tracks lineage across models, agents, datasets, and MCP servers**
- **Identifies dependencies and connected systems**
- **Supports SBOM-style visibility for AI environments**

Leverage the Trusted MCP Directory

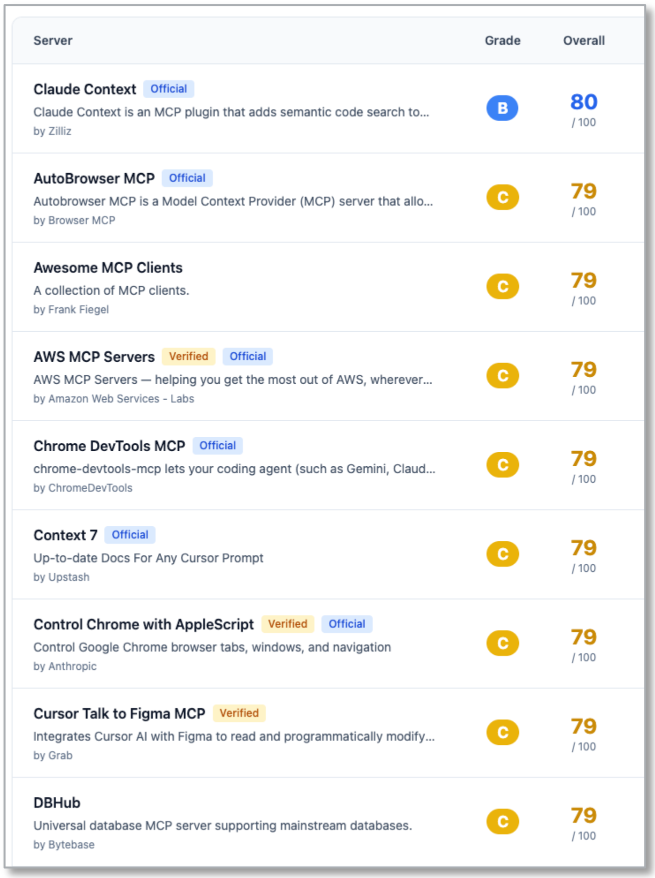
The PointGuard AI Trusted MCP Directory evaluates MCP servers across security, operational, and adoption maturity to help teams identify trustworthy, production-ready MCP services before they are integrated into AI agents and workflows.

- **Vulnerabilities, secrets, malicious prompts, policies**
- **Publisher trust, licensing, responsiveness**
- **Adoption, likes, stars, forks**

Manage Risk in AI Supply Chains

As organizations adopt agentic AI, risk shifts from individual models to interconnected AI supply chains. Agents, MCP servers, tools, and datasets introduce new dependencies that must be governed together. PointGuard AI Discovery delivers supply chain visibility designed for modern AI architectures.

- **Tracks lineage across models, agents, datasets, and MCP servers**
- **Identifies dependencies and connected systems**
- **Supports SBOM-style visibility for AI environments**



Server	Grade	Overall
Claude Context Official Claude Context is an MCP plugin that adds semantic code search to... by Zilliz	B	80 / 100
AutoBrowser MCP Official Autobrowser MCP is a Model Context Provider (MCP) server that allo... by Browser MCP	C	79 / 100
Awesome MCP Clients A collection of MCP clients. by Frank Fiegel	C	79 / 100
AWS MCP Servers Verified Official AWS MCP Servers — helping you get the most out of AWS, wherever... by Amazon Web Services - Labs	C	79 / 100
Chrome DevTools MCP Official chrome-devtools-mcp lets your coding agent (such as Gemini, Claud... by ChromeDevTools	C	79 / 100
Context 7 Official Up-to-date Docs For Any Cursor Prompt by Upstash	C	79 / 100
Control Chrome with AppleScript Verified Official Control Google Chrome browser tabs, windows, and navigation by Anthropic	C	79 / 100
Cursor Talk to Figma MCP Verified Integrates Cursor AI with Figma to read and programmatically modify... by Grab	C	79 / 100
DBHub Universal database MCP server supporting mainstream databases. by Bytebase	C	79 / 100

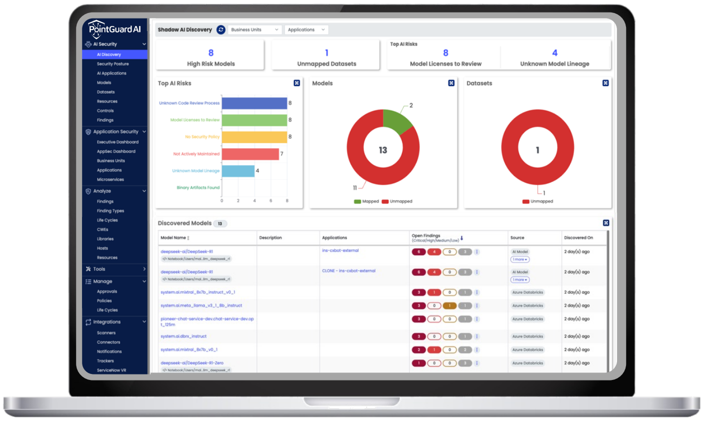
Trusted MCP Directory

AI Discovery & Inventory

Unified Dashboard Reporting

Intuitive dashboards summarize critical findings, AI behavior, and testing frequency, as well as recommendations for remediations and compliance. Technical and compliance dashboards include:

- **High risk models, agents, and MCP servers**
- **Top AI risks mapped to AI frameworks**
- **Drill-downs to full details for every asset**



Discovered Models 13

Model Name	Description	Applications	Open Findings (Critical/High/Medium/Low)	Source	Discovered On
deepseek-ai/DeepSeek-R1 </> Notebook:/Users/mal...llm_deepseek_r1		ins-cxbot-external	6 4 0 3	AI Model 1 more	2 day(s) ago
deepseek-ai/DeepSeek-R1 </> Notebook:/Users/mal...llm_deepseek_r1		CLONE - ins-cxbot-external	6 4 0 3	AI Model 1 more	2 day(s) ago
system.ai.mixtral_8x7b_instruct_v0_1			3 1 0 1	Azure Databricks	2 day(s) ago
system.ai.meta_llama_v3_1_8b_instruct			3 0 1 1	Azure Databricks	2 day(s) ago
pioneer-chat-service-dev.chat-service-dev.opt_125m			3 0 0 1	Azure Databricks	2 day(s) ago
system.ai.dbrx_instruct			3 0 0 1	Azure Databricks	2 day(s) ago
system.ai.mixtral_8x7b_v0_1			2 1 0 2	Azure Databricks	2 day(s) ago
deepseek-ai/DeepSeek-R1-Zero </> Notebook:/Users/mal...llm_deepseek_r1			1 0 0 3	Azure Databricks	2 day(s) ago

Streamlined Approval and Governance

As AI assets are discovered, the platform automates governance workflows that scale with enterprise environments. Teams can approve, track, and remediate AI usage without slowing development or overwhelming security operations, including:

- **Automated alerts for new AI assets**
- **One-click approvals and exceptions**
- **Application-aware approval context**
- **Jira, Slack, and ticketing integrations**
- **Centralized reporting for audits**

Part of the PointGuard AI Platform

PointGuard AI uniquely secures both AI systems and software applications. Through a single, unified management console all components work seamlessly together to secure the complete AI lifecycle, from discovery to data protection.

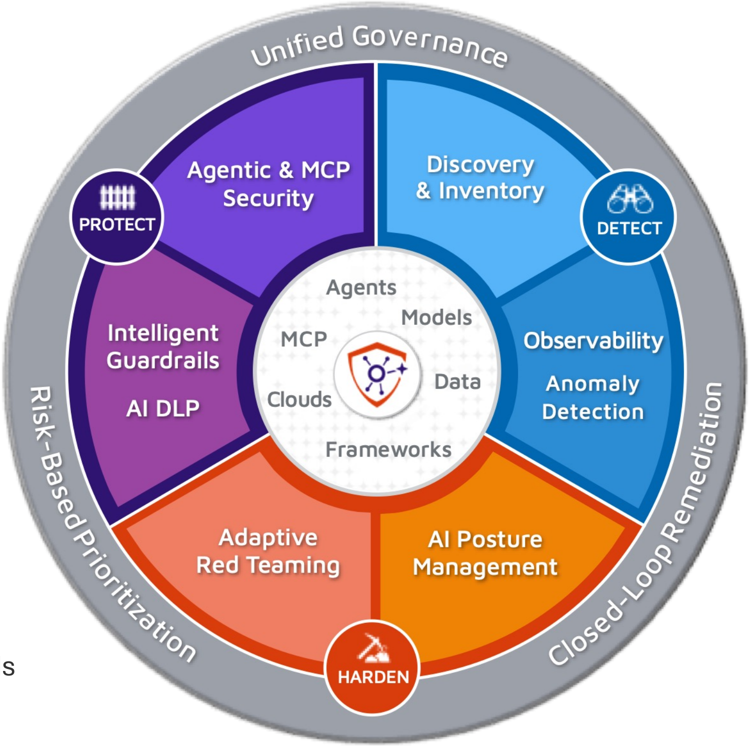
Built for the Agentic Era

As AI systems evolve into autonomous, interconnected agents, security testing must evolve with them. PointGuard AI Discovery deliver context-aware, policy-driven protection designed for today's AI systems and tomorrow's agentic environments.

Get Started

View demos and detailed technical content on our website or schedule a call to discuss your specific needs with our security experts.

www.pointguardai.com/contact



AI Discovery & Inventory Capabilities

AI Asset Discovery	
AI Models	LLMs and ML models across platforms
Datasets & Knowledge Bases	Training, inference, and RAG data sources
AI Agents	Agents discovered via platforms, code, and runtime
MCP Servers & Tools	MCP servers, tools, and connected systems
AI Assets	Notebooks, clusters, jobs, endpoints, plugins
External AI Services	SaaS and hosted AI APIs used by applications
Discovery Sources	
Cloud Platform APIs	Databricks, AWS, Azure, Google, Copilot Studio
Code Repositories	GitHub and similar repositories
Runtime Telemetry	OpenTelemetry-based discovery of active AI usage
Model Risk Scoring Knowledge Base	
Security Risk	Vulnerabilities, secrets exposure, misconfigurations
Compliance Risk	Licensing, publisher location, dataset sensitivity
Operational Risk	Provenance, maintenance, update frequency
Adoption Risk	Popularity, community trust, reported issues
MCP Server Testing and Knowledge Base	
Security Maturity	Direct testing of MCP servers for vulnerabilities, hardcoded secrets, malicious prompts, and availability of security policies
Operational Maturity	Details verified publishers, location, license compliance, issue resolution and peer review status
Adoption Maturity	Tracks community support, usage metrics, and long-term viability
Governance & Workflows	
Application Mapping	Maps AI assets to business applications
Usage Approval	Automated approvals and exception handling
Exception Management	Automates approvals for exceptions and false positives to reduce noise.
Remediation	Ticketing and notifications for prioritized issues
Reporting	Centralized audit and compliance reporting
Metrics & SLAs	Tracks metrics and SLAs for model approvals, security findings, MTTR