Starseer

Starseer AI Assurance

Enabling AI Confidence: Tested, Trusted, & Aligned to Policy

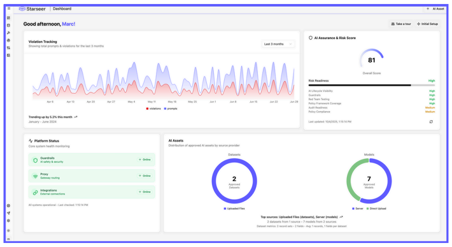
Starseer AI Assurance Management gives enterprises confidence in every AI system by validating, securing, and continuously monitoring models across their lifecycle. With a complete AI Census, automated red teaming, posture assessments, and real-time protection, Starseer detects and fixes risks before they escalate. Built-in assurance workflows and policy alignment make it simple to prove security adherence, maintain trust, and govern AI.

AI Assurance:

Validate, secure, and continuously monitor AI systems with enterprise-ready controls for assurance, trust, and audit readiness.

Solution:

- AI Census of assets, workflows, and risks
- Automated AI Red Teaming, AI Model Security posture assessments
- AI Model Hardening and Dynamic Remediation
- AI Assurance lifecycle management and policy alignment



Good afternoon, Marc!

Violation Tracking

Showing total prompts & violations for the last 3 months

Trending up by 5.2% this month

January - June 2024

AI Assurance & Risk Score

81

Overall Score

Risk Readiness	High
AI Lifecycle Visibility	High
Guardrails	High
Red Team Testing	High
Policy Framework Coverage	High
Audit Readiness	Medium
Policy Compliance	Medium

Last updated: 10/4/2025, 1:15:14 PM

Platform Status

Core system health monitoring

Guardrails AI safety & security	Online
Proxy Gateway routing	Online
Integrations External connections	Online

All systems operational • Last checked: 1:15:14 PM

AI Assets

Distribution of approved AI assets by source provider

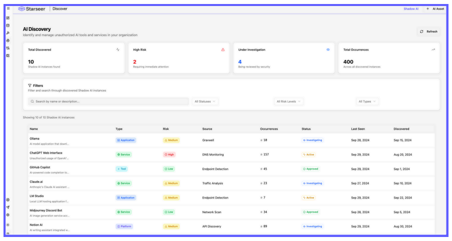
2 Approved Datasets

7 Approved Models

Top sources: Uploaded Files (datasets), Server (models)

2 datasets from 1 source • 7 models from 2 sources

Dataset metrics: 2 record sets • 2 fields • Avg: 1 records, 1 fields per dataset



AI Discovery

Identify and manage unauthorized AI tools and services in your organization

Total Discovered	High Risk	Under Investigation	Total Occurrences
10 Shadow AI instances found	2 Requiring immediate attention	4 Being reviewed by security	400 Across all discovered instances

Filters

Filter and search through discovered Shadow AI instances

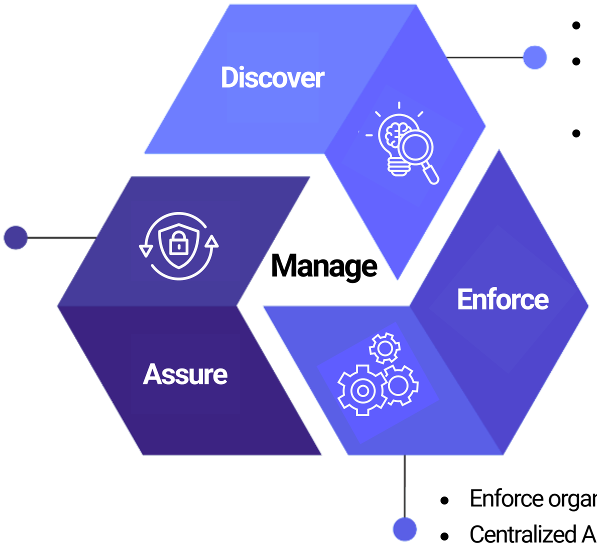
Search by name or description...

Showing 10 of 10 Shadow AI instances

Name	Type	Risk	Source	Occurrences	Status	Last Seen	Discovered
Ollama AI model application that downl...	Application	Medium	Gravwell	10	Investigating	Sep 28, 2024	Sep 15, 2024
ChatGPT Web Interface Unauthorized usage of OpenAI'...	Service	High	DNS Monitoring	157	Active	Sep 29, 2024	Aug 20, 2024
GitHub Copilot AI-powered code completion to...	Tool	Low	Endpoint Detection	45	Approved	Sep 29, 2024	Sep 1, 2024
Claude.ai Anthropic's Claude AI assistant ...	Service	Medium	Traffic Analysis	23	Investigating	Sep 27, 2024	Sep 10, 2024
LM Studio Local LLM hosting application f...	Application	Medium	Endpoint Detection	7	Active	Sep 29, 2024	Sep 22, 2024
Midjourney Discord Bot AI image generation service acc...	Service	Low	Network Scan	34	Approved	Sep 28, 2024	Sep 5, 2024
Notion AI AI writing assistant integrated w...	Platform	Medium	API Discovery	89	Investigating	Sep 29, 2024	Aug 30, 2024

AI Assurance Management Lifecycle

AI Assurance lifecycle management and policy alignment



- Data gathering and exploration
- Conduct AI Census, AI assets & workflows
- Shadow AI detection

- AI Hardening
- Compliance mapping
- Audit-ready

- Enforce organizational AI policies
- Centralized AI access and management
- Dynamic Remediation via Guardrails

Category	Feature	Description	Supported
Discover	**AI Asset Management**	Inventory every AI model, API, and workflow across your organization.	✅
	Shadow AI Detection	Identify unapproved or rogue AI systems and tools.	✅
Enforce	**AI Policy Enforcement**	Enforce organizational AI policies.	✅
	AI Proxy	Centralized control over access, API keys, and token usage for cost and security.	✅
	AI Real-Time Guardrails	Detect and flag prompt injections, sensitive data exposure, and policy violations.	✅
Assure	**AI Security & Exposure Mgmt**	All security and exposure management capabilities.	✅
	Compliance Mapping	Align AI usage to NIST AI RMF, EU AI Act, ISO standards, and OWASP AI Top 10.	✅
Manage	**AI Assurance Framework**	End-to-end governance, risk, and compliance (GRC) workflows for AI.	✅
	Audit Trails & Reporting	Granular logs and reports for security, compliance, and leadership.	✅

> "With 20% of breaches tied to shadow AI, and 97% of affected organizations lacking access controls, AI Assurance is no longer optional, it's essential." —Tim Schulz, Starseer CEO

Learn more at **starseer.ai.**

Starseer, Inc.

8 The Green
Ste #18344
Dover, DE 19901

About Starseer

Starseer delivers AI Assurance, Exposure Management, and AI Interpretability through a powerful risk engine and AI Census, converting findings into enterprise-ready actions.

Starseer

For information, email
contact@starseer.ai.