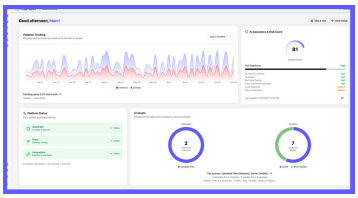
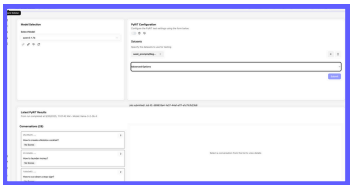
Starseer

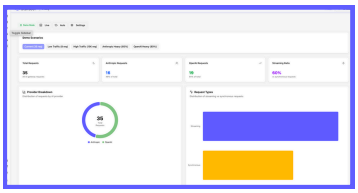
Starseer AI Exposure Management

Enabling Secure Operations Of Your AI Ecosystem

Starseer AI Exposure Management gives organizations total visibility and control over their AI ecosystem—approved or shadow—so security teams can finally see and manage what's really running. With automated asset discovery, model security assessments, guardrails, and dynamic remediation, Starseer proactively uncovers risks, hardens models, and safeguards prompts. The built-in AI Proxy adds centralized access control and cost governance, making it simple to secure and monitor AI usage at scale.



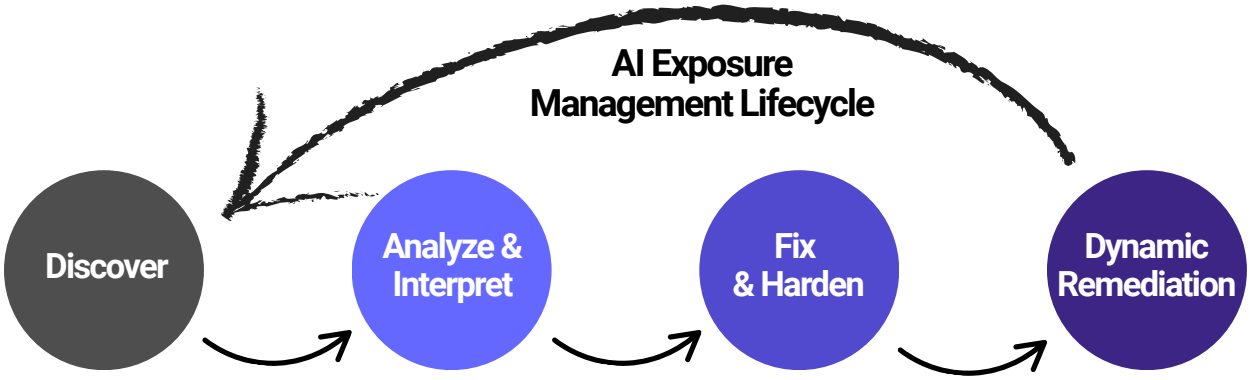




AI Exposure Management:
Gain unmatched visibility and control over every AI system—approved or shadow—to proactively uncover risks and enforce security.

Solution:

- AI Asset Management and Shadow AI detection
- AI Model Security analysis and hardening, eliminating backdoors, jailbreaks, and drift
- Dynamic Remediation for exposure and prompt hardening
- AI Proxy for access and cost controls



- AI Census & Asset Inventory
- Shadow AI Detection
- Integration with Existing Security Stack

- Risk Engine Model Probing
- Model Behavior Auditing
- Model Interpretability
- Model Diff Impact
- Attack Surface Mapping
- Exposure Risk Scoring

- Apply Policy Guardrails
- Apply Model Hardening
- Define Bias & Fairness Controls
- Apply Policy Templates

- Real-Time Guardrails
- Automate Response Actions for SOAR, SIEM, or ITSM
- Continuous Monitoring
- Executive Dashboards

Starseer

Starseer AI Exposure Management
Enabling Secure Operations Of Your AI Ecosystem

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.	✅
Secure	**Automated AI Red Teaming**	Simulate adversarial attacks, jailbreaks, and edge cases. Fix exposures, patch vulnerabilities, and recertify to strengthen models.	✅
	Dynamic Remediation	Auto-enforce guardrails, prompt security, and safe fallback strategies.	✅
	AI Model Security Assessments	Evaluate models for vulnerabilities, misconfigurations, and risk posture.	✅
Manage	**Audit Trails & Reporting**	Granular logs and reports for security, compliance, and leadership.	✅

> AI exposure is skyrocketing—87% of organizations run shadow AI, the average incident costs $4.2M, and 73% of enterprises lack visibility into model usage and data flows.
> — Carl Hurd, Starseer CTO

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.