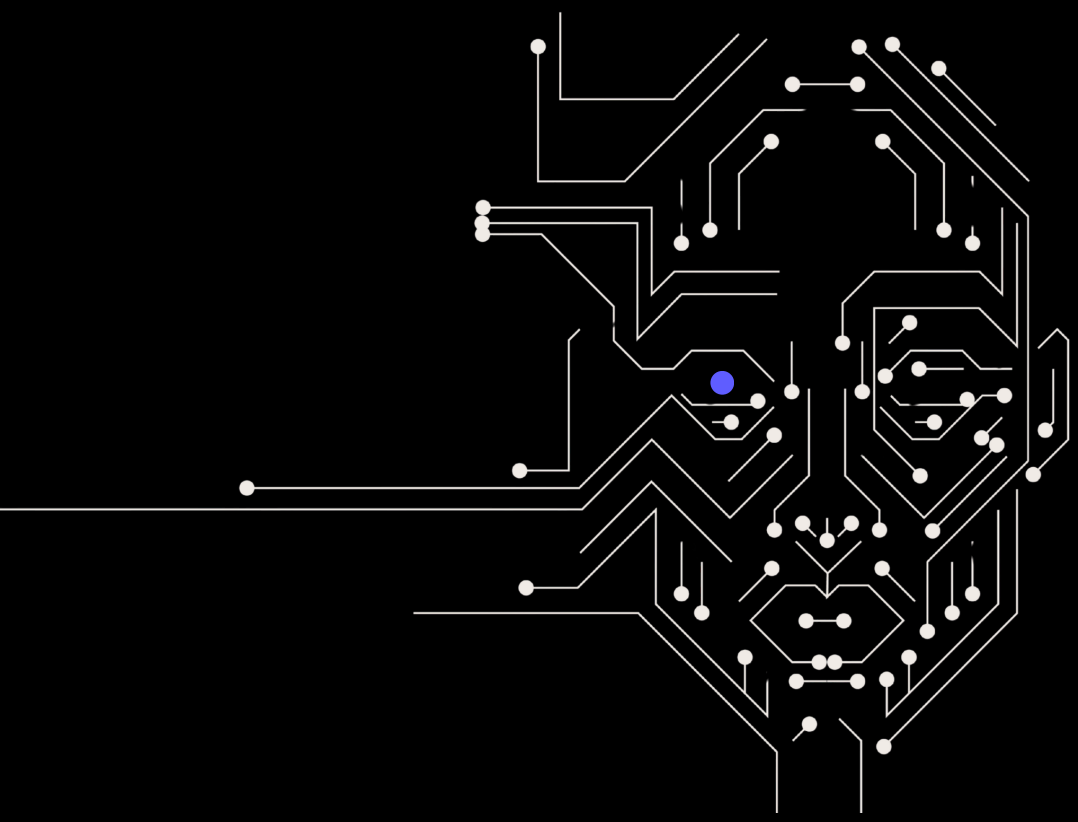
Starseer

STARSEER.AI

@STARSEERAI



How to build your AI Assurance

A STEP-BY-STEP GUIDE

Starting or want to enhance an AI assurance process? Find out where to begin and how to achieve success.

About Us

STARSEER: DISCOVER, ENFORCE, ASSURE, & MANAGE AI

Starseer delivers unified AI Assurance and Exposure Management by combining its powerful AI Platform with an advanced Risk Engine, enabling teams to quickly build an AI Census of all AI assets.

The platform discovers, classifies, and mitigates risks across every AI system or service, whether approved or shadow AI. By applying runtime protections, proxy controls, and eliminating model weaknesses, Starseer transforms these insights into clear, actionable controls that empower organizations to manage, enforce policies, and assure the trustworthiness of their AI, enabling secure, compliant, and confident AI deployment at scale.

OVERVIEW

3 reasons why you must improve AI assurance

Strengthening AI assurance uncovers risks, enforces responsible use, accelerates compliant adoption, and turns innovation into secure, measurable outcomes.

3 reasons why you must improve AI assurance

1. REDUCE SHADOW AI AND NON-COMPLIANT USAGE.

Approximately 20% of data breaches in regulated industries like finance, healthcare, and energy now stem from unapproved "Shadow AI" tools, increasing breach costs by an average of $670,000. These tools evade governance and security controls, risking data leakage, bias, and regulatory violations.

By implementing AI Assurance programs for centralized discovery, usage mapping, and policy-enforcing guardrails, organizations can reduce uncontrolled AI use by 30–40%, significantly shrinking the attack surface and potentially saving millions annually in breach-related costs and compliance penalties.

2. IMPROVE AI-DRIVEN DECISION INTEGRITY.

According to Gartner 2025, 35% of enterprise AI models/agents experience performance drift or unintended bias within their first year, resulting in incorrect outputs or compliance issues that can disrupt decision-making, fraud detection, or customer service automation.

AI Assurance proactively monitors and validates these AI assets, detecting problems like unapproved usage, unapproved access, prompt injection, jailbreaks, bias, and more before they impact critical workflows, cutting remediation time by up to 50% and preventing costly downstream losses while safeguarding business integrity and customer trust.

3. ACCELERATE TRUSTED AI ADOPTION.

Enterprises with defined AI governance and assurance frameworks achieve 25–40% faster AI adoption rates and reduce audit preparation costs by up to 30%, according to IDC 2024, by aligning with standards like NIST AI RMF, EU AI Act, and ISO/IEC 42001.

AI Assurance delivers standards-aligned reporting, audit-ready evidence, and integrated guardrails, enabling teams to prove safe and compliant AI use, which accelerates responsible adoption, streamlines regulatory reporting, minimizes legal and operational risks, and maximizes ROI on AI investments.

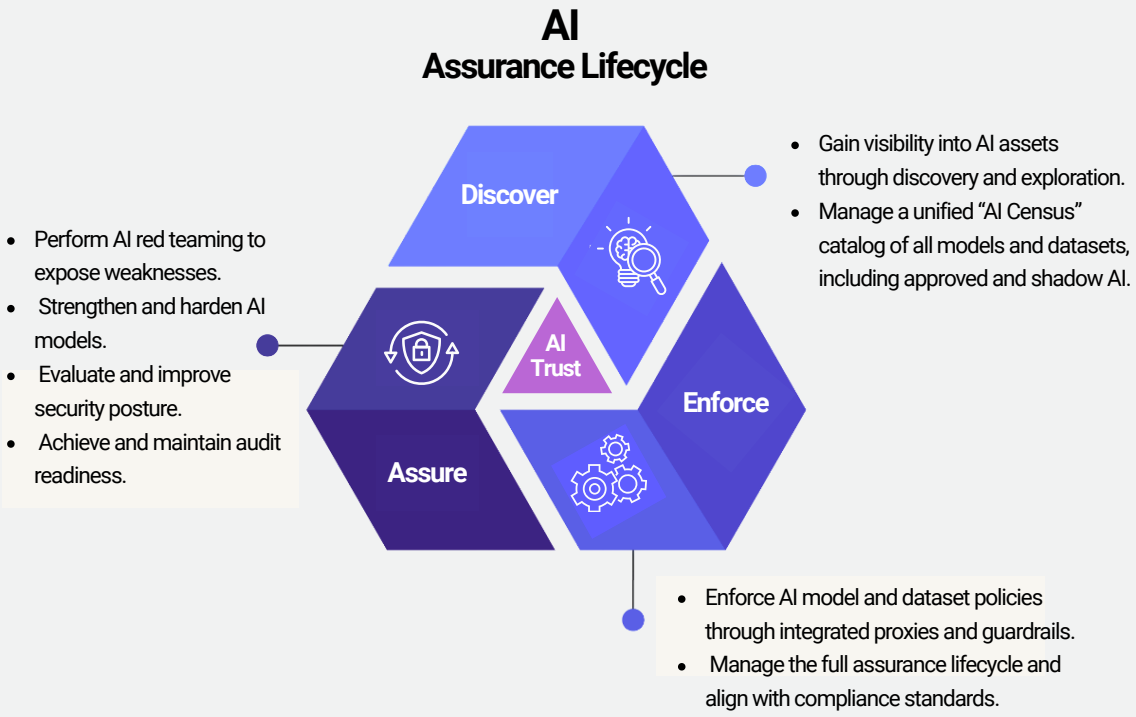
THE AI ASSURANCE LIFECYCLE

the essential phases of AI assurance

AI assurance is a lifecycle: discover assets, assess risks, harden models, and enforce policies to build trust and resilience at scale.

AI Assurance Lifecycle

It's no secret that AI has quickly transitioned from experimentation to a critical enterprise tool and enabler, driving decisions in customer interactions, operations, and safety, yet most organizations lack the visibility and control needed for secure and responsible deployment. The essential AI assurance lifecycle comprises three key stages: Discover, Enforce, Assure, and Manage.



AI ASSET DISCOVERY >> USAGE, POLICY, & ACCESS ENFORCEMENT >> AI HARDENING

HERE'S HOW IT WORKS

Discover involves identifying all AI tools, models, and data flows within an organization to ensure full visibility and eliminate blind spots like Shadow AI. Enforce establishes governance by implementing policies and guardrails to align AI usage with security standards and regulations, such as NIST AI RMF or EU AI Act, preventing risks like data leakage or bias.

Assure focuses on continuous monitoring, validation, and audit-ready reporting to confirm AI systems perform as intended, mitigating issues like performance drift or compliance violations, thus fostering trust and maximizing the value of your AI asset investments.

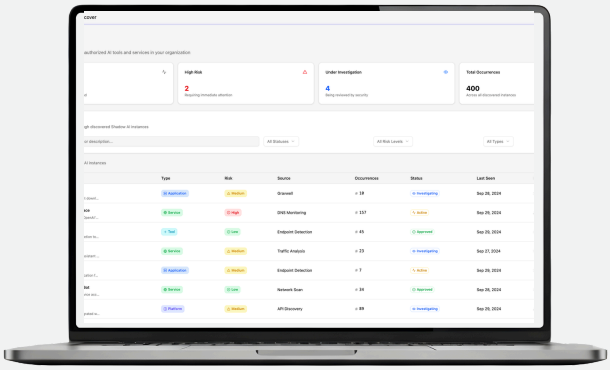
Discover: Build and Maintain an AI Census

You can't manage what you can't see. The first and most critical step is to discover and continuously catalog your entire AI ecosystem. This means maintaining a live AI Census, a dynamic, continuously updated inventory of all AI assets, including models, services such as ChatGPT or Gemini, and agents deployed across the enterprise.

Without an AI Census, organizations face significant blind spots. Shadow AI — unapproved or hidden tools — introduces untracked risks that can undermine compliance, security, and business outcomes.

Team must:

- BUILD AND CONTINUOUSLY UPDATE AN AI CENSUS THAT INVENTORIES EVERY AI MODEL, SERVICE, AND AGENT IN USE
- DETECT SHADOW AI OR UNAPPROVED TOOLS BEFORE THEY CREATE EXPOSURE
- CLASSIFY AND PRIORITIZE RISKS EARLY IN THE AI LIFECYCLE



The establishment of a living AI Census, which dynamically tracks and catalogs all AI tools, models, data flows, and usage within an organization, serves as the foundational infrastructure for every downstream decision, delivering profound long-term benefits across policy enforcement, assurance, and audit readiness. By providing comprehensive visibility into AI deployments, the census eliminates blind spots such as Shadow AI, enabling organizations to enforce governance policies consistently.

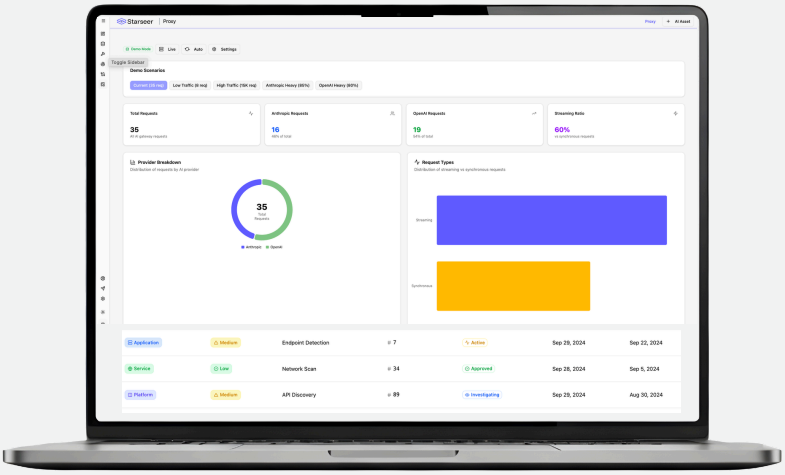
Moreover, the census streamlines audit preparation, reducing costs by up to 30% (IDC 2024), while accelerating AI adoption by 25–40%, fostering innovation without compromising security. By maintaining an up-to-date, actionable inventory, the AI Census ensures sustained trust from stakeholders, enhances operational resilience, and positions organizations to adapt swiftly to evolving regulations and technological advancements, maximizing the strategic value of AI investments for years to come.

Enforce: Control Usage, Apply Policies & Monitor

Once you know what is running, the next step is to decide what should be allowed and enforce it consistently.

Team must:

- EVALUATE AND APPROVE OR BLOCK AI MODELS AND SERVICES BASED ON RISK AND COMPLIANCE POSTURE
- APPLY POLICIES AND GUARDRAILS TO ENSURE DATA PRIVACY, RESPONSIBLE USAGE, AND ADHERENCE TO REGULATIONS
- USE THE AI PROXY TO ENFORCE WHO CAN ACCESS WHICH AI ASSETS, ENSURING CONSISTENT APPLICATION OF POLICIES
- GAIN VISIBILITY INTO COSTS BY DEPARTMENT, TEAM, OR INDIVIDUAL USERS, ALLOWING ORGANIZATIONS TO OPTIMIZE CONSUMPTION AND REDUCE UNNECESSARY SPEND



By combining policy enforcement with the visibility and control provided by the Proxy, organizations can minimize unintended exposures, prevent costly misuse, and stop risky deployments before they reach production.

Assure: Test, Secure and Build Trust

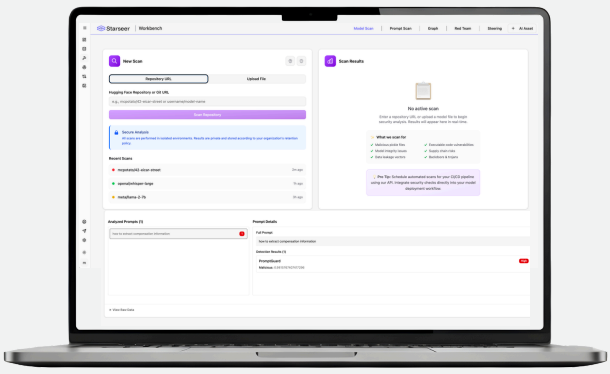
Discovery and enforcement are not enough without assurance. AI systems must be tested, hardened, and continuously protected to maintain trustworthiness.

Team must:

- DEPLOY AUTOMATED RED-TEAMING AND SECURITY POSTURE ASSESSMENTS FOR MODELS AND PROMPTS
- ADD RUNTIME PROTECTIONS TO DETECT AND BLOCK TAMPERED OR MALICIOUS BEHAVIOR
- PERFORM MODEL HARDENING TO CLOSE VULNERABILITIES AND MITIGATE RISKS SUCH AS BACKDOORS, BIAS, AND DRIFT

70 %
reduction in breach risk

47 %
reduction in identity & PII incidents



600%
saved on every dollar spent on AI risk management, avoiding $6 in reactive remediation costs

Assurance is not a one-time effort. It is an ongoing process to ensure every AI system operates safely and as intended.

Manage: Govern and Stay Audit-Ready

Finally, AI programs need continuous oversight to maintain compliance and transparency.

Team must:

- TRACK POLICY ADHERENCE AND MODEL LIFECYCLE EVENTS FROM REQUEST TO RETIREMENT
- MAINTAIN AUDIT-READY RECORDS MAPPED TO FRAMEWORKS LIKE NIST AI RMF, ISO 42001, OWASP AI TOP 10, AND THE EU AI ACT
- PROVIDE EXECUTIVE-LEVEL ASSURANCE REPORTING TO STAKEHOLDERS, CUSTOMERS, AND REGULATORS

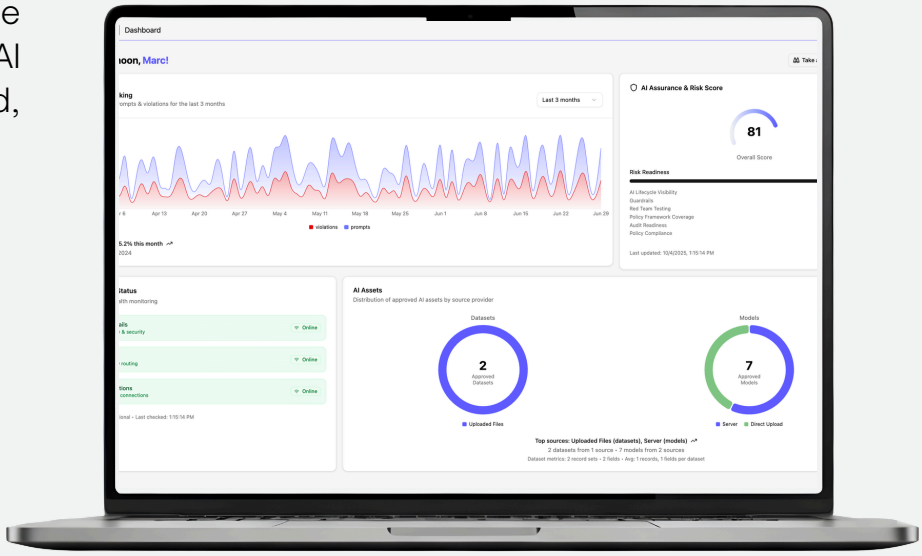
40 %

faster adoption of trusted AI

7 %

company revenue risk reduction

Management closes the loop, turning ad-hoc AI adoption into a disciplined, sustainable practice.



SUMMARY

why this matters now

As AI adoption accelerates, unmanaged risks can derail progress—acting now ensures safer innovation and lasting trust.

The reality for organizations

AI's benefits are undeniable, but so are its risks, especially when unapproved models, weak prompts, or tampered systems go undetected. Discover Enforce Assure Manage is not just a framework, it is the minimum viable foundation for trustworthy AI adoption.

Starseer recommends and helps organizations:

GAIN VISIBILITY INTO EVERY AI SERVICE AND MODEL THROUGH A CONTINUOUS AI CENSUS.

ENFORCE POLICIES AND OPTIMIZE COSTS WITH PROXY-ENABLED ACCESS CONTROLS.

ASSURE TRUST AND SECURITY THROUGH CONTINUOUS TESTING AND PROTECTION.

MAINTAIN CONFIDENCE AND COMPLIANCE AT SCALE.

The future of enterprise AI will belong to teams that can innovate securely, with clarity and confidence. Starseer's AI Security and Exposure Management and AI Assurance solutions make that future achievable today.

Learn more at **starseer.ai.**

Starseer, Inc.

8 The Green
Ste #18344
Dover, DE 19901

About Starseer

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

Starseer

For information, email contact@starseer.ai.