LangGuard.AI

Accelerate your AI agent adoptions

with an AI Control Plane for IT and Security

Any Agent. Any Tool. Monitored.

LangGuard At-a-Glance

Agent Accountability

Review, Approve & *Provision* AI agents (pilot → production) using a **live agent registry**.

Agent Traceability

Gain visibility into *how* and *why* the AI agent is behaving the way it does with **behavioral analytics** and **activity monitoring** enriched with enterprise integration contexts.

Agent Auditability

Record and *Replay* AI agent actions with immutable **audit logging** and **reporting** to support compliance – ISO 42001, NIST AI-RMF, EU AI Act, SOX

AI agent Adoption Challenges

- *Product and business teams are rushing to deploy homegrown and 3rd party AI agents into existing enterprise processes*
- *IT manual reviews and approvals are unable to keep up the dynamic AI agent needs*
- *Growing concerns with AI agent token spend quickly getting out of hand*

Strategic Outcomes for CIOs

- ✓ **Onboard Securely:** Only approved tools and data are ever used by your AI agents.
- ✓ **Go Live Faster:** Deploy and scale your AI agents quickly with governance built-in from day one.
- ✓ **Always Compliant:** Automatically trace, observe, and enforce policies while your AI agents are running.

LangGuard adds enterprise context to every AI agent run behavior, making run-time governance and compliance measurable and demonstrable.

Key Use Cases

Ai Asset Discovery & Attribution

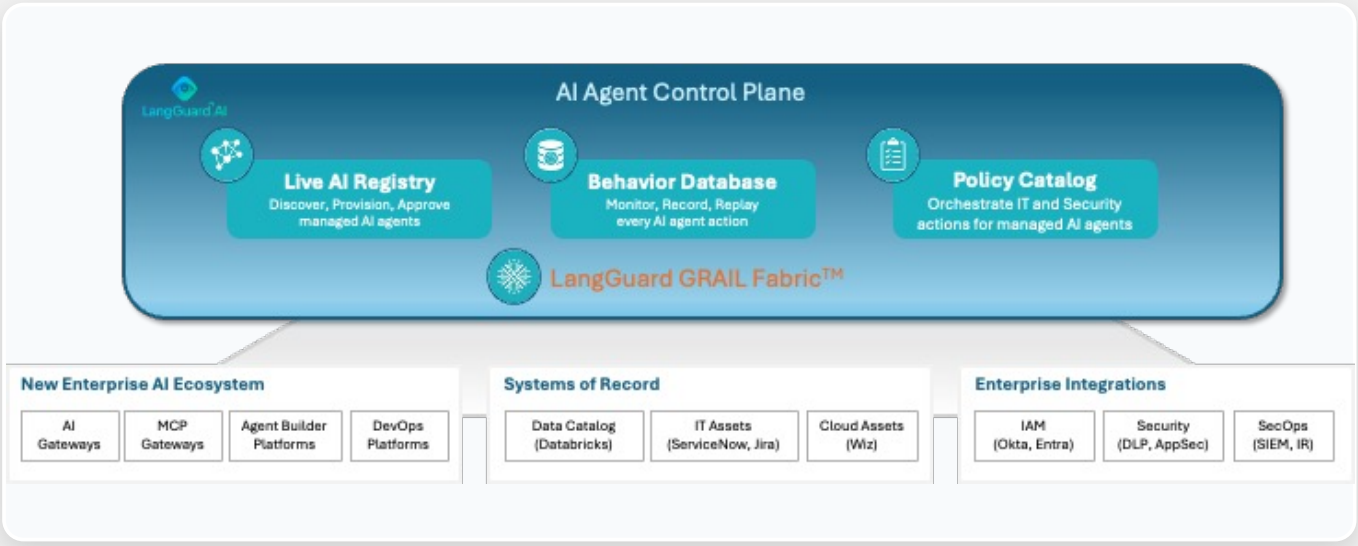
LangGuard discovers AI assets with an extensible plug-ins, classifies and categorizes AI agents so that IT can gain visibility into AI agents that are not in any systems of record.

AI Agent Provisioning & Approval

LangGuard provisions and approve “IT-vetted” AI agents (known, controlled) for use within the enterprise. Action any issues using tickets in ServiceNow/Jira.

Enable Continuous Evidence & Audit

LangGuard continuously scans AI agent behavior to action any incidents and audit findings Provide behavioral analytics, deep activity monitoring, audit log retention and replays.



"90% of AI agent projects are stuck in pilots."

Source: The State of AI in 2025, McKinsey, November 2025

How does LangGuard work

1. **Interprets** AI agent *intent* at run-time.
2. **Evaluates** that *intent* against enterprise policy ground truth.
3. **Decides** whether the *action* should be allowed, modified, or blocked.
4. **Enforces** controls on access, tools, data, identity, and cost.

Email Us

To learn how LangGuard can accelerate adoption of AI agents, reach out to us today!

info@langguard.ai

About LangGuard

LangGuard is a North America based startup building and delivering enterprise-grade solution to help organizations adopt AI Agents confidently and realize intended business value.

Founded by industry veterans in Cybersecurity, IT Services Management, and Cloud, this team is embarked on solving the #1 challenge for Enterprise AI adoption.

To learn more, visit langguard.ai or follow us on LinkedIn.

LangGuard Inc.

US | Canada

(512) 200-4345