

Coding Agent Governance

The security layer for the agentic SDLC

AI coding agents now write code, install dependencies, and act on external systems autonomously, leaving security teams blind to what is in use. Coding Agent Governance surfaces every agent, model, and MCP server, and enforces deterministic policy before risky actions turn into security incidents.

Every

AI coding agent, model, MCP server, and skill in use, discovered

Live

blocking of destructive commands, sensitive file access, and unauthorized MCP servers

Zero

parallel tools: extends the AURI policy engine security teams already use

How it works

SEE

Every agent in your environment

- Discover every AI coding agent, model, MCP server, and skill, approved and unapproved.
- Centralize visibility across Cursor, Claude Code, Copilot, and other harnesses.
- Catch shadow AI before auditors, customers, or examiners find it first.

ENFORCE

Policy on what agents can do

- Block destructive shell commands, sensitive file access, and unauthorized MCP servers in real time.
- Deterministic enforcement: policy holds regardless of what the model decides.
- Role-aware policies fit how each team works, without one heavy-handed rule.

PROVE

Audit-ready evidence on AI activity

- Searchable audit log of every agent action: commands, file access, tool calls, installs.
- Meet EU AI Act, ISO AI governance, and customer security review expectations.
- Cut assembling AI governance evidence from weeks per cycle to minutes.

CUSTOMER VOICE

Built for teams shipping with AI

Fast-growing AI companies already run Endor Labs inside their AI-native development stacks. Coding Agent Governance extends the same platform to the agents themselves: visibility, policy, and audit evidence in one place.

“As a fast-growing AI company, we prioritize feature velocity without compromising security. Endor Labs’ unique reachability-based analysis and native integrations into our AI-native software development stack keep our developers focused on rapidly finding and fixing real risks in the SDLC, so we ship faster with confidence.”

– Sunil Agrawal, CISO @ Glean