Agent Guard

Your teams already run AI agents: coding assistants, a support chatbot, a release bot in CI. Agent Guard finds them, shows what each one can reach and how badly a hijacked one could hurt, tests them against prompt injection, and proposes the least privilege each one needs. Your teams decide what changes.

> **$540K** blast radius of one CI agent with a deploy token, in the demonstration on a fictional company

WHAT AI ADDS OVER TODAY'S TOOLS

- **Lists every agent from its own config: coding assistants, MCP servers, chatbots, CI jobs**
- **Follows each tool to the credential and scope it holds**
- **Reads tool descriptions and flags private data plus untrusted input plus the power to act**
  By name
- **Tests injection in a test environment and scores the result**
- **Prices the blast radius in money**

HOW IT WORKS

Inventory	Every agent, from its own config
Reach	What each one can really touch
Rank	Blast radius, the same way every time
Test	Prompt injection, recorded
Propose	Least privilege, per finding
Brief	What to fix first

WHERE IT RUNS

- **In your environment.** Reads configs, manifests and the identity export with read-only access. Nothing leaves.
- **Masked first.** Secrets and personal data are masked before any model or person sees them.
- **Your policy.** Sensitivity levels, weights, trusted publishers and what counts as approval are yours, written down.
- **People decide.** Every scope change, revoked token and approval gate is a proposal until its owner accepts it.

PEOPLE'S HOURS A YEAR, FOUR REVIEWS OF FIVE AGENTS

By hand	210 h	$32K
Security tools and people	144 h	$22K
Agent and people	**31 h**	**$5K**

85% fewer hours than by hand; 78% fewer than with security tools and people.

WHAT IT'S WORTH

- **$540K** At risk if the CI release agent is hijacked: a tampered deploy takes Checkout ($52K an hour) and Orders ($38K an hour) down for an assumed 6 hours. Exposure, not a saving.
- **$166K** Incident cost avoided each year: Fix-now findings closed on the release agent and the support chatbot ($662K combined exposure), at an assumed 25% annual chance one is hijacked if left as is.
- **$17K** Engineer hours saved each year: 110 hours of tracing five agents' configs, tokens and scopes by hand, four times a year, replaced by checking the agent's inventory.

THE ENGAGEMENT · TESTED INVENTORY IN 1 WEEK; FIXES IN 2–3; RE-TESTED EVERY QUARTER

Days 1–2	Connect
Week 1	Inventory and test
Weeks 2–3	Fix
Every quarter	Watch

People decide. The agent finds, judges, drafts and proves. Every fix, boundary and status is a proposal until its owner accepts it, and a person signs every assessment.

Figures are estimates for a fictional company, with every assumption shown on the agent's page. Categories of tools, not products; individual tools vary. Verify against your environment.