BUILT BY A TEAM THAT HAS SECURED MAJOR FINANCIAL INSTITUTIONS WORLDWIDE FOR 25 YEARS.

ARGENT FOR AI CODING AGENTS

CODING AGENTS RUN YOUR SHELL. ARGENT DECIDES WHAT THEY MAY DO.

Argent Strategic Intelligence puts every AI coding agent that works through Argent behind one gateway. One command, argent connect, ties Claude Code, Codex, Cursor or six other tools to a named agent with a human owner, keeps its Argent key in the OS keychain and points the tool at Argent. Your AI provider key stays in your vault.

Every action is checked before it runs. The Argent hook asks the gateway about each shell command, file read or write, web fetch and tool call. Your rules allow it, ask a person or deny it, and an action with no rule is denied. Secrets are removed from prompts, new MCP tools wait for an admin's approval, and every decision is a signed record.



SEE.
Every coding agent, its owner and its sessions.



PROVE.
A signed record of every action and decision.



STOP.
Denied commands and unapproved tools are refused.

FIVE CONTROLS FOR EVERY CODING AGENT

1	**Owned identity** A coding agent runs on a key nobody owns.	argent connect registers each tool as its own agent under the signed-in developer, an active, named person. When that person leaves, their agents are refused on the next request. IT can pin Claude Code fleets to Argent with managed settings.
2	**No AI key in config** Fifty laptops, fifty copies of the AI key.	The agent holds only its own Argent key, kept in the OS keychain. The company's provider key stays in your vault and the gateway attaches it on the way out. A provider key the agent sends anyway is removed at the gateway.
3	**Rules for actions** An agent runs a destructive shell command.	The Argent hook checks each shell command, file read or write, web fetch and MCP call against your rules: allow, ask a person, or deny. An action with no matching rule is denied, and if the check cannot run, the hook fails closed.
4	**Secrets out of prompts** A pasted .env file heads to the model.	About **60** credential rules (AWS, GitHub, Stripe, OpenAI, private keys and more) find secrets in prompts and redact them before the model sees them. With reply checks on, a secret the model echoes back is removed too.
5	**Approved tools only** A new MCP tool appears overnight.	Every MCP tool call needs a scope the agent holds, and on a server the MCP Gate enforces a new tool waits for an admin's approval. Tool descriptions are scanned for hidden instructions, and tool output is fenced off from your instructions.

WHY IT MATTERS NOW

AI tools are standard in development. **84%** of developers surveyed use or plan to use AI tools.[1] Claude Code-assisted commits leaked secrets at **3.2%**, versus a **1.5%** baseline on public GitHub.[2]

Agents act with real privileges. OWASP's Top 10 for Agentic Applications names tool misuse, and identity and privilege abuse, where leaked credentials let agents act beyond their scope.[3]

HOW A TEAM STARTS

1. Connect. Each developer runs argent connect for their tool; IT can push the Argent proxy and certificate to every managed machine.

2. Watch. In watch mode Argent records what it would refuse while the work goes on.

3. Enforce. Switch on action rules, the MCP Gate and secret redaction, area by area.

BOOK A DEMO. WE WILL SHOW YOU ARGENT GOVERNING YOUR OWN CODING AGENTS ON YOUR OWN CODE.

NYEDIS.AI/DEMO

Sources. 1 Stack Overflow, 2025 Developer Survey: AI, survey.stackoverflow.co/2025/ai. 2 GitGuardian, The State of Secrets Sprawl 2026, March 17, 2026, blog.gitguardian.com. 3 OWASP GenAI Security Project, OWASP Top 10 for Agentic Applications, December 9, 2025, genai.owasp.org.