MOUNTAIN THEORY

We control what AI can do.

Mountain Theory controls what AI agents can do across the AI tools your organization already uses. We check each action **Anthropic's Claude Code** asks to take, before it runs, and each action an agent built on **Hermes (Nous Research)** asks to take. We also work with Anthropic's Claude, Claude Desktop and Claude Cowork, OpenAI's ChatGPT and Codex, OpenClaw, NVIDIA NemoClaw, Google's Gemini CLI, Microsoft 365 Copilot and GitHub Copilot. Each action is checked against your rules, then allowed, held for a person to decide, or blocked. The model still decides. The action does not run until it has been checked.

WHAT WE DO

For Anthropic's Claude Code and the agents your teams build, each action is checked before it runs. Rules are written in plain English by whoever owns the risk, and every decision is logged for your auditor.

CORE COMPETENCIES

- Checks each action your AI asks to take, before it runs: allow, hold for a person, or block
- Catches personal data on the way in and out
- Blocks instructions hidden in documents
- Rules in plain English, no code
- Every decision logged for your auditor

DIFFERENTIATORS

- Checks the action, not the chat
- Checks the workaround too, not just the first try
- Stops new bad behavior on day one, with no new rule needed
- Your environment or the cloud
- Tests published, misses included. Patent pending.

PAST PERFORMANCE

- A Tier 1 public research university in Texas evaluated Palo Alto's Protect AI, Cisco's DefenseClaw and Mountain Theory, and selected Mountain Theory.
- Optimo AI, design partner: its agent was blocked, then blocked again several times when it tried to reach the same result by chaining tools.

COMPANY DATA

Legal name	Mountain Theory, Inc.
NAICS	541512 (primary), 541511, 541519, 513210
Business type	Small business
Established	2024
Website	mountaintheory.ai
Contact	Mike May, CEO · mike@mountaintheory.ai

Product names are trademarks of their owners. Mountain Theory is not affiliated with or endorsed by any of them.