Geordie

AI AGENT SECURITY & OPERATIONS

The agentic enterprise, under your control



Understand, secure and control your agentic operations, with the confidence to transform how your business works.

As more work happens through agents, every enterprise needs its own understanding of a new operating environment, from which agents are working and what they can access to how they behave as they work. Because that activity spans cloud, code, endpoint and browser, approaches built around a single surface see only part of it.

Geordie builds a continuous understanding of how each agent operates across goals, decisions, tools, data and actions, giving teams the evidence to set operating boundaries, shape behavior and improve how agents work over time.

FITS HOW YOU WORK

Deploys in about 10 minutes
Via API, code scan or endpoint

Vendor agnostic
Every agent platform and tool type

Works alongside your stack
Gateways, native controls and SIEM

Built for security, AI, IT and finance leaders.

One understanding of every agent and the work it does

Know what you have

Vendor-agnostic discovery finds agents where they operate, with owners and tools attached.

Understand behavior

Decisions, tool calls and actions read in the context of the whole agent, with an immutable audit trail.

Shape what happens

Beam acts through the agent's own context to monitor, guide, confirm or enforce.

Priority and risk	Severity	Agents
1. Non-corporate Git repository	Critical	3
2. MCP server on an open port	Critical	2
3. Credential leakage to external service	High	1
4. Supply chain worm in repository hooks	High	1
5. Unapproved AI platform in use	High	41

Agent inventory — By owner

JS	John Smith	314 agents	Low
BK	Brenda Kowalski	37 agents	Medium
MG	Maria Gonzalez	24 agents	Low
?	Unsanctioned	19 agents	Critical

Figure 1. Risks ranked by priority and severity, alongside the agent inventory by owner, including unsanctioned agents.

> "There are very few platforms that give you that real holistic view, whether it's from the frontier models' APIs or from the endpoints themselves. Having value, cost, risk and security all tied together in one platform makes Geordie a really powerful tool.



GRAEME CANTU-PARK · CISO and CIO, Matillion

HOW IT WORKS

Built where agents work

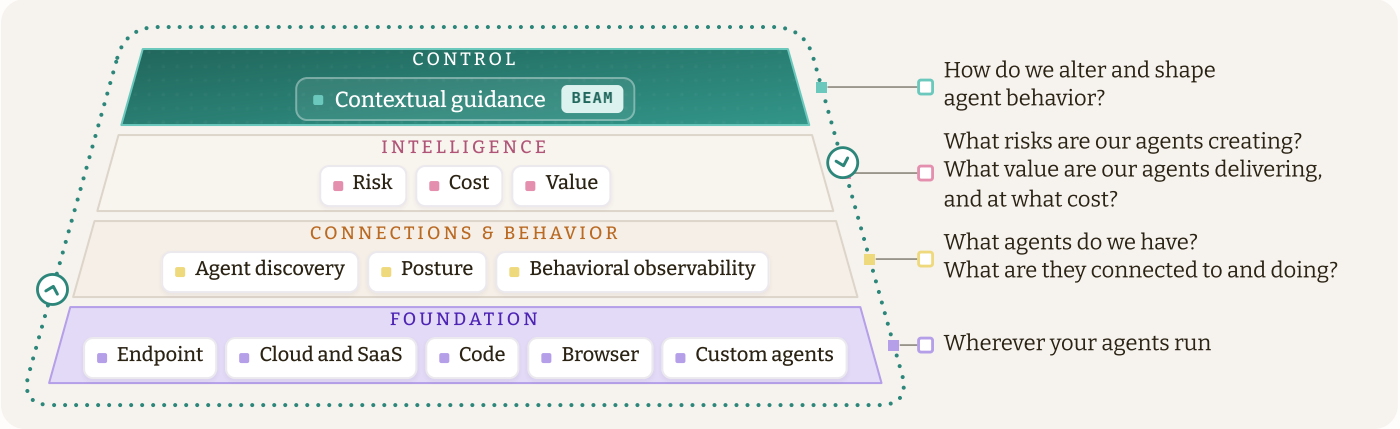


Figure 2. Read from the base up. Control sits on top, shaping agent behavior with everything the layers beneath it know.

From agent activity to controls that hold

01 Collect at the source

A sensor, APIs and telemetry, repository scans and a browser extension, each closest to the agent.

02 Map the relationship graph

Each agent tied to its owner, identity, model, tools, data and permissions, tracked as access changes.

03 Classify risk and value

Risk rated from configuration plus behavior, and spend tied to the owners behind it.

04 Act through Beam

Beam

Deterministic controls that monitor, guide, confirm and enforce through the agent's own context.

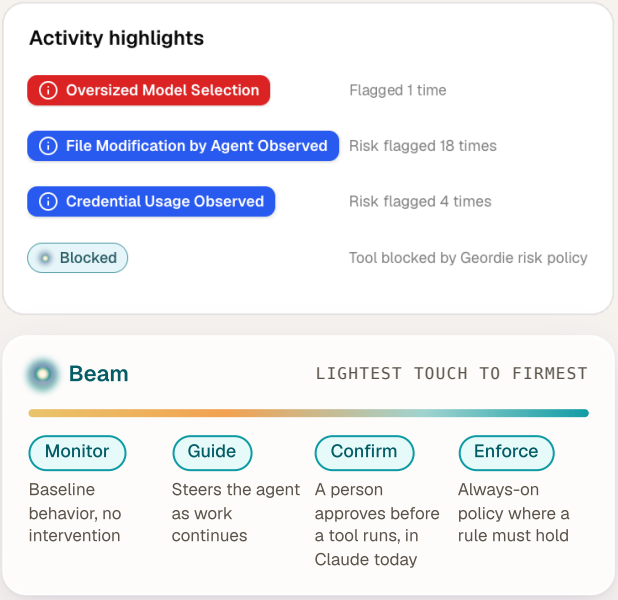


Figure 3. Activity highlights from one coding agent session, and the range of responses Beam applies.

What customers found

327%
more agents than expected

OWKIN · CASE STUDY →

Found in a single proof of concept that also surfaced three critical CVEs and avoided about $13M in exposure.

98%
inventory accuracy

WOOD PARTNERS · CASE STUDY →

Its estimate for one inventory of agents from multiple platforms, with Beam enforcing policy on critical risks.

Approve more agents, with evidence

Connect Geordie where your agents already run, and see what they can reach and how they behave, with controls that keep the work moving.

See Geordie in action at geordie.ai/book-a-demo →