

Anatomy of an AI Agent: Memory, Tools, and Goals

FREE EDUCATIONAL BRIEF · LEARN AI. UNCOVER THE DATA. PROTECT THE TRUTH.

“Agent” is the most abused word in AI marketing. Strip the gloss and a real agent is a language model wrapped in four specific capabilities: a persistent goal, tools it can call, memory that survives steps, and a loop that plans, acts, and checks. Knowing the anatomy lets you judge whether a product is an agent or a chatbot in a trench coat.

THE FOUR COMPONENTS

» Goal & planning

The agent decomposes an objective into steps and revises the plan as results come in — not a script, a loop.

» Tools

Function calls to real systems: search, calendars, CRMs, spreadsheets, payments. Tool quality and scope define what the agent can actually do.

» Memory

Short-term working state for the current task plus long-term recall of preferences and past outcomes; without it every step starts amnesiac.

» Reflection

Self-checks between steps — did the action succeed? does the output satisfy the goal? — which separate reliable agents from flailing ones.

THE RELIABILITY MATH NOBODY QUOTES

Chained steps multiply error. A model that's right 95% of the time per step completes a 10-step task correctly about 60% of the time. Production agents fight this with verification after each step, retries, narrow scopes, and human checkpoints — which is why “fully autonomous” claims deserve suspicion and why the best deployments look more like supervised delegation.

QUESTIONS THAT EXPOSE THE TRUTH

What tools can it call, and what is it barred from? Where does its memory live and who can read it? What happens on step failure? Which actions require human approval? A vendor with crisp answers has built an agent; a vendor with adjectives has built a demo.

INVESTIGATOR'S TAKEAWAYS

- Agent = model + goal loop + tools + memory + self-checking.
- Per-step error compounds; long chains need verification and retries.
- Tool scope defines capability — and blast radius.
- Memory location is a security question, not a feature bullet.
- “What happens when a step fails?” is the fastest vendor filter.