AI AGENTS 101

WHAT ARE AI AGENTS?

AI AGENT is a system that perceives an environment, makes decisions and takes autonomous actions to achieve goals

AI is technology that enables machines to simulate human learning

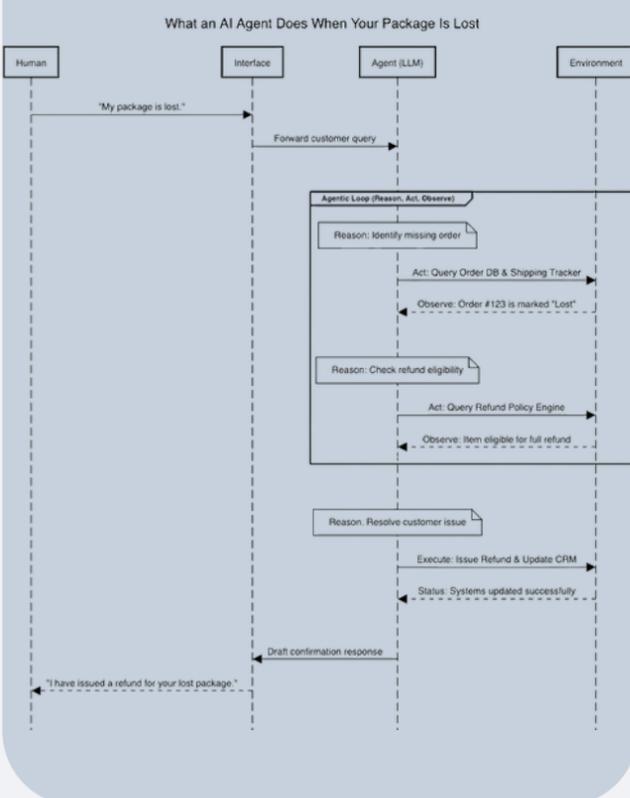**Agent** is an entity authorized to act on behalf of another

EARLY AI

- ✳ Stand alone models
- ✳ Simple and rule-based
- ✳ Followed fixed "if-then" instructions
- ✳ Couldn't handle ambiguity
- ✳ Executed predfined logic
- ✳ Require manual updates

AI NOW

- ✳ Compound systems
- ✳ Combine models with tools, memory and feedback loops
- ✳ Alternate between reasoning and taking actions
- ✳ Adaptive, interactive behavior

IF YOU USE AMAZON, YOU HAVE ALREADY INTERACTED WITH AGENTIC AI SYSTEM...

What an AI Agent Does When Your Package Is Lost

Human | Interface | Agent (LLM) | Environment

"My package is lost."

Forward customer query

Agentic Loop (Reason, Act, Observe)

Reason: Identify missing order

Act: Query Order DB & Shipping Tracker

Observe: Order #123 is marked "Lost"

Reason: Check refund eligibility

Act: Query Refund Policy Engine

Observe: Item eligible for full refund

Reason: Resolve customer issue

Execute: Issue Refund & Update CRM

Status: Systems updated successfully

Draft confirmation response

"I have issued a refund for your lost package."

WHICH SECTORS USE AI AGENTS MOST ACTIVELY?

- Software engeineeting
- Customer Service, E-commerce
- Finance & Accounting
- Cybersecurity
- Marketing & Copy writing
- Academic Research

COMPONENTS OF AN AI AGENT SYSTEM

AI agents can coordinate and automate real-world tasks. For example, an agentic system can power a smart home by controlling lighting, temperature or security devices accordingly. Research and industry implementations generally converge on a set of core architectural components that enable these capabilities.

- **Goal:** Provides task objectives
- **LLM (reasoning engine):** Interprets human language, converts it into natural language representations, and generates plans.
- **Tools:** External systems an agent can call, which include database, APIs, search engine, code execution
- **Memory:** Stores relevant context such as conversation history, user preference, prior actions
- **Controller:** Determines next step (reason, plan, act, observe, updates, and etc..)