How to Build an Agent

From scratch in Python

Srinivas Neppalli
H2O.ai

2025-10-16

AGENDA

1. What is an Agent?
2. Types of Agents
3. Build an Agent
4. Agents in H2oGPTe
5. What's Next?

H2O.ai

What is an Agent?

What is an Agent?

A chatbot that answers customer questions by retrieving information from a knowledge base and responding conversationally.

What is an Agent?

An AI system that monitors your calendar, reads your emails, and automatically schedules meetings by finding available times and sending calendar invites to participants without asking for permission each time.

What is an Agent?

A spam filter that analyzes incoming emails and moves suspicious messages to a spam folder.

What is an Agent?

An AI assistant that is given the task "research competitors and create a market analysis report" and then autonomously searches the web, gathers data, analyzes it, creates visualizations, and produces a final document.

What is an Agent?

A recommendation algorithm that suggests movies based on your viewing history.

What is an Agent?

An AI system that monitors a smart home: it learns your preferences, adjusts temperature and lighting throughout the day, orders groceries when supplies run low by checking your pantry cam, and schedules HVAC maintenance when it detects issues.

What is an Agent?

GitHub Copilot that suggests code completions as you type.

What is an Agent?

An AI coding assistant that you tell "build me a todo app" and it then autonomously writes code, tests it, debugs errors it encounters, searches documentation when stuck, and iterates until the app works.

What is an Agent?

An autopilot system in a car that maintains lane position and speed on the highway.

What is an Agent?

An AI system that manages your company's social media: it monitors trending topics, creates relevant posts aligned with brand voice, responds to comments and messages, analyzes engagement metrics, and adjusts its strategy over time.

What is an Agent?

01
Autonomy

Acts without constant human intervention

02
Goal-directed

Works toward specific objectives

03
Perceives environment

Takes in information from its surroundings

04
Takes actions

Does things that affect its environment

05
Adapts

Can adjust behavior based on feedback or changing conditions

Types of Agents

Types of Agents

Autonomous Agents

Orchestrate multiple tools and sub-agents with high-level planning to achieve complex goals with minimal human intervention.

MCP Agents

Dynamically connect to external data sources (databases, APIs, files) to enrich context with fresh, private information.

Tool Calling Agents

Extend capabilities by invoking external tools (calculators, search, code interpreters) when needed to complete tasks.

Agents with Self Reflection

Evaluate and critique their own outputs, then iterate and improve without external feedback.

Spectrum of Autonomy

H2O.ai

01 RPA Workflows

Low Autonomy
- Pre-defined rules & scripts
- Same steps every time
- No adaptation to changes

02 Tool-Calling Agents

Medium Autonomy
- Selects appropriate tools
- Basic decision-making
- Extends core capabilities

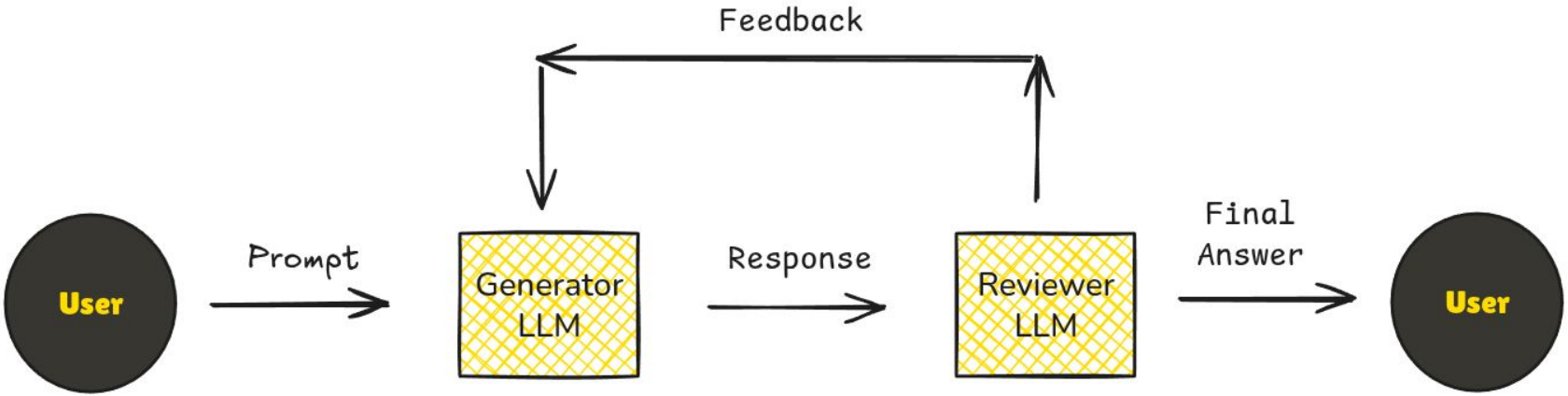
03 Planning Agents

High Autonomy
- Creates action strategies
- Multi-step reasoning
- Goal-oriented behavior

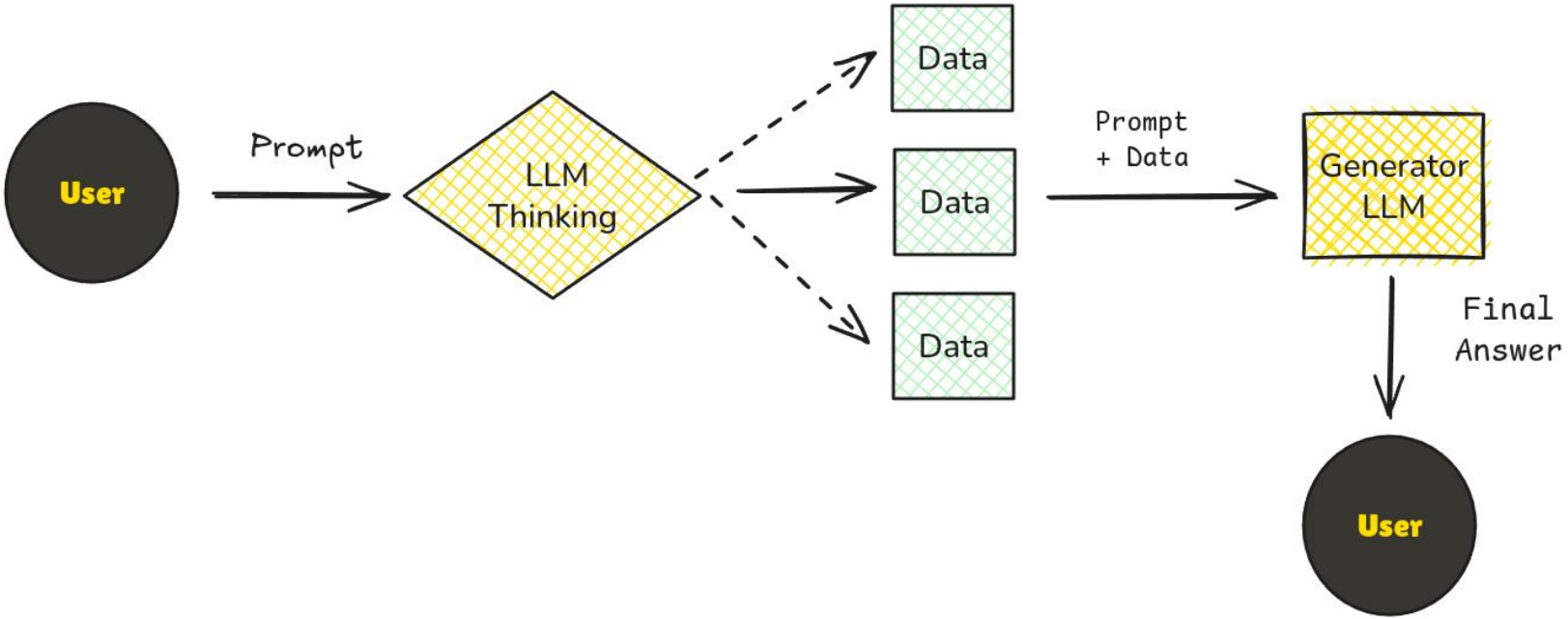
04 Autonomous Agents

Full Autonomy
- High-level goal interpretation
- Self-correction & learning
- Orchestrates sub-agents

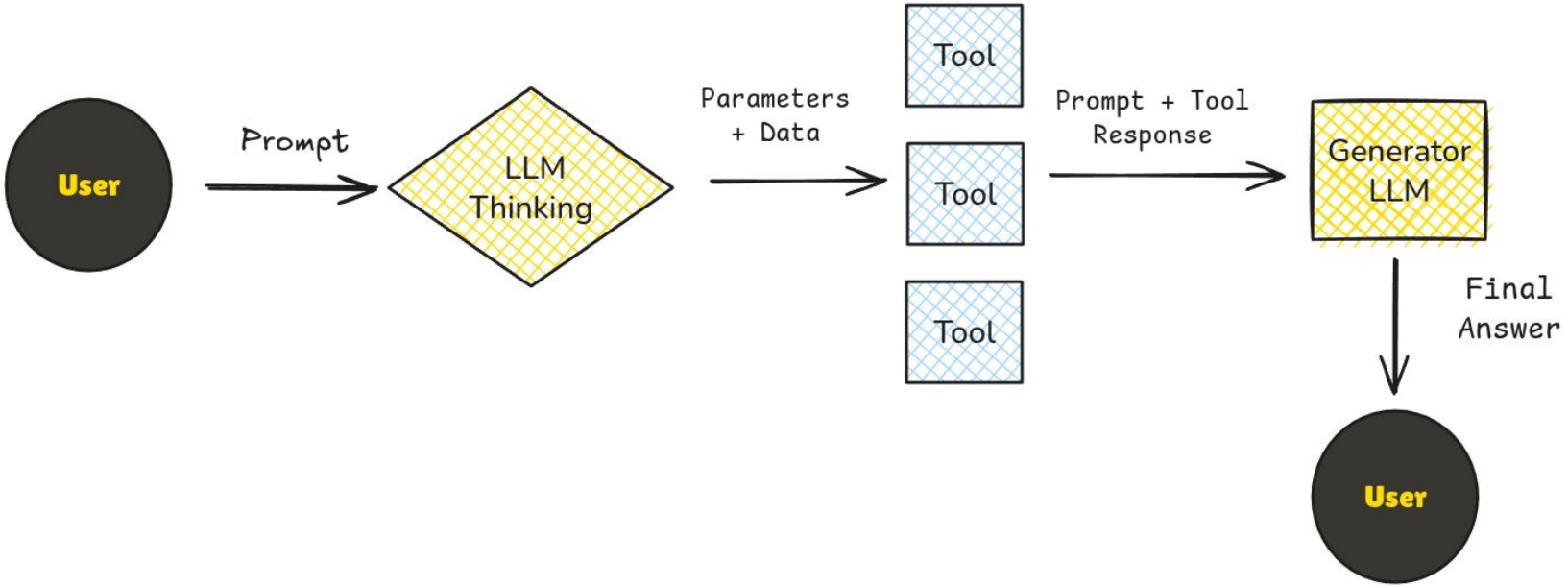
Agent with Reflection



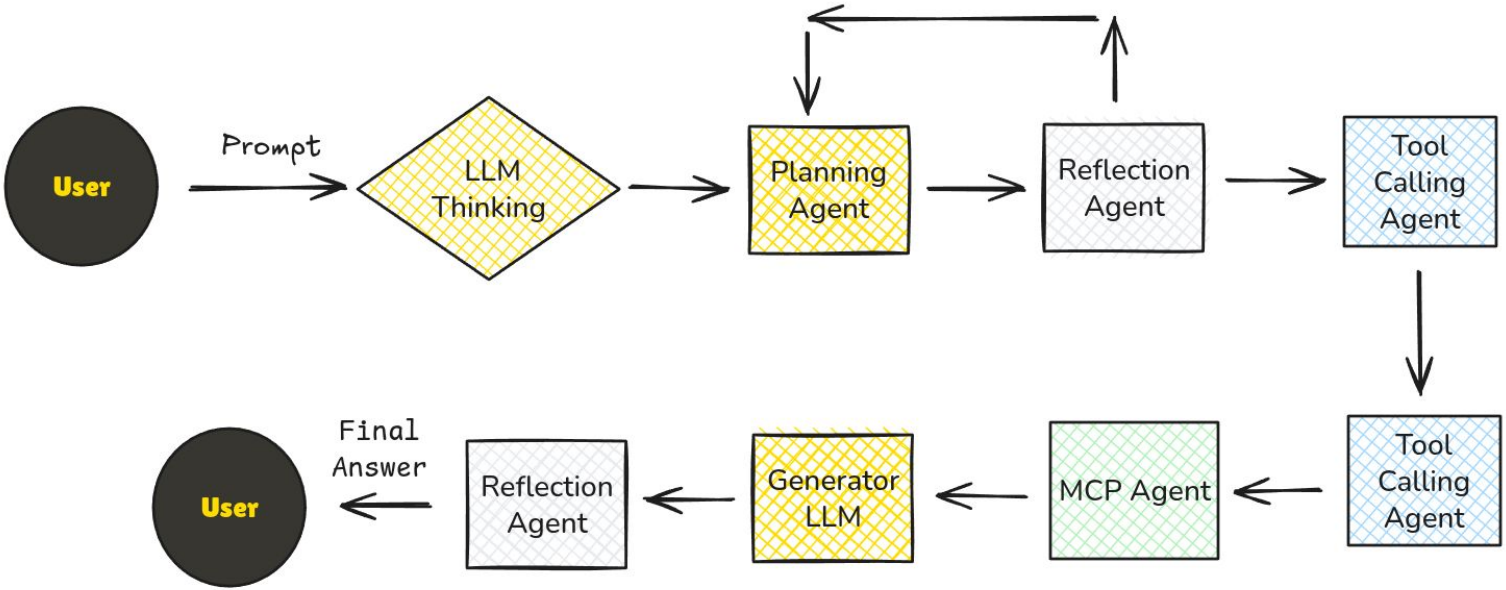
MCP Agent


User
Prompt
LLM
Thinking
Data
Data
Data
Prompt
+ Data
Generator
LLM
Final
Answer
User

Tool Calling Agent



Autonomous Agent



H2O.ai

Build an Agent

Agents in H2oGPTe

H2O.ai delivers a complete set of capabilities to support Agentic AI workflows

Agentic AI

Vertical Agents for Banking and Financial Crime

Domain-specific, intelligent chat and function calling features

Predictive AI Agent

AutoML

Easy–to-use, low-code, machine learning algorithms

MCPs

Environment to manage, deploy, govern, and monitor models

Generative AI

Data Prep

No-code apps to streamline data curation

Agentic AI

Out-of-the-box agents and reusable vertical task agents ready to be customized

Fine Tuning

Models that provide cost efficiency and flexibility

Data Extraction

Intelligent data extraction and classification from unstructured data

On-Prem — DEPLOYMENTS — Cloud

OUR VALUE

Automate and scale entire workflows using the world's best deep research and AI talent.

Brings together Predictive AI, Generative AI, and Agentic AI into **one sovereign platform** that runs on-premise, air-gapped, or in the cloud.

Deploy agents securely in your own environment.

We provide an **end-to-end platform** with:

- **AutoML** to automate machine learning and feature engineering
- **Distillation and Fine-tuning** of small models that can be customized
- **Data Prep and Data Extraction** for curating and processing unstructured data.
- **MCPs (model context protocol)** for managing, deploying, and governing models at scale.

Enables national, regulated, or private-sector **AI sovereignty** with full compliance and guardrails.

We deliver ready-to-use vertical agents that can be customized with your data, tools, and models for faster time to value.

H2O.ai

OUT-OF-THE-BOX AGENTS, READY TO BE CUSTOMIZED

- General AI Assistant
- Deep Research
- Workflow & Task Management
- Web Search
- Tool Builder
- MCP-Only Runner

VERTICAL TASK AGENTS

- Code Agent
- Data Science Agent
- Data Extraction Agent
- Data Assembly Agent
- Data Ingress Agent
- Data Egress Agent
- Data Enrichment Agent
- Data Quality Assurance Agent
- Data Load Agent
- Requirements Analysis Agent
- FinCrime Agent
- Procurement Agent
- Fraud Agent
- Cyber Security Agent

Use your agent as is, or customize for your exact needs:

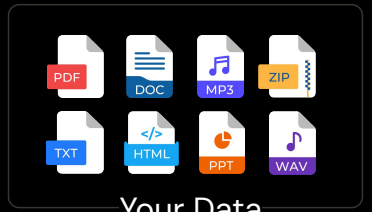
- Modify the System Prompt to push for specific tasks and goals
- Enable and disable any of 25+ out-of-the-box tools
- Add your own tools:
  - Existing MCP servers
  - Custom MCP servers
  - Browser tools
  - Prompting + python tools
- Choose if you want to emphasis speed / low cost or accuracy
- Choose your LLM:
  - Bring your own external model
  - Use local models like oss-gpt, llama 4 scout and more
- Enable guardrails, PII detection

Save the settings so that any users that come to this use case get an agent that works just how you want it to

- Role based access control to make sure the right people can use or modify each use case
- Access from the H2O UI or integrate with Rest and Python APIs

How We Do It

On-Premise and Air Gapped Agentic AI Platform supporting multiple enterprise use-cases



WORLD'S BEST AGENTIC AI & AWARD WINNING PREDICTIVE AI

Distillation & Fine-Tuning of SLMs on Your Private Data

H2O DOCUMENT AI | H2O EVAL STUDIO | H2O MRM | Workplace Apps

Enterprise h2oGPTe | APIs

Agentic AI | RAG | Deep Research | Guardrails

Predictive AI

H2O LABEL GENIE | H2O DRIVERLESSAI | H2O HYDROGEN TORCH

H2O Enterprise LLM STUDIO

H2O DANUBE | H2OVL MISSISSIPPI | LlaMA | Qwen | deepseek

H2O Platform

VERTICAL TASK AGENTS

- Data Extraction Agent
- Data Enrichment Agent
- Agentic Contact Center
- AML Investigation Agent
- Transaction Reconciliation
- AI Workforce: BDR Agent
- Financial Crime Agent
- Audit & Assurance Agent

H2O.ai COMPANY OVERVIEW

- **RANKED #1** ON GAIA BENCHMARK JUNE 2025
- **Visionary** in Gartner Magic Quadrant Data Science Machine Learning **2025**
- **Leader** in CB Insights Best Large Language Model (LLM) Application Development **2024**
- **Leader** in Forrester Wave Computer Vision Tools **2024**
- **Visionary** in Gartner Magic Quadrant Cloud AI Developer Services **2024**
- **Top 8** Constellation Research Cloud AI Developer Services Shortlist **2024**
- CRN AI 100 List **2025**

FOUNDED	FUNDRAISED	COMMUNITY	KAGGLE GRANDMASTERS
2012	$256M	2M	15

GLOBAL HQ

Mountain View, CA

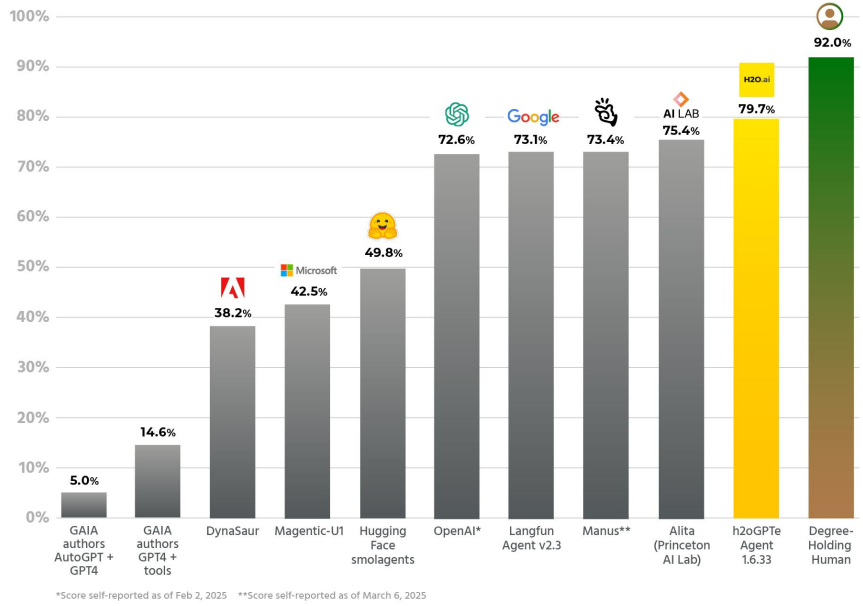
INVESTORS

CBA, Goldman Sachs, Wells Fargo, Capital One, Nexus, New York Life, NVIDIA

The **World's Best** Deep Research

H2O.ai

H2O.ai h2oGPTe Agentic AI Tops GAIA
June 2025



*Score self-reported as of Feb 2, 2025 **Score self-reported as of March 6, 2025

TECHNOLOGY PARTNERS

DELL Technologies · NVIDIA · snowflake · aws · Google Cloud

H2oGPTe Demo

What's Next?

Resources

- https://h2ogpte.genai.h2o.ai
- Building effective agents - Anthropic Blog
- 12-Factor Agents: Patterns of reliable LLM applications — Dex Horthy, HumanLayer - YouTube
- A Comprehensive Survey of Self-Evolving AI Agents - https://arxiv.org/pdf/2508.07407
- Agents White Paper - https://www.kaggle.com/whitepaper-agents
- DeepLearning.AI
- FastMCP - https://gofastmcp.com

H2O.ai

Thank You!