

A practical guide to building agents

Contents

What is an agent?

When should you build an agent?

Agent design foundations

Guardrails

Conclusion

2

4

5

7

24

32

Practical guide to building agents

Introduction

Large language models are becoming increasingly capable of handling complex, multi-step tasks. Advances in reasoning, multimodality, and tool use have unlocked a new category of LLM-powered systems known as agents.

This guide is designed for product and engineering teams exploring how to build their first agent, distilling insights from numerous customer deployments into practical and actionable best practices. It includes frameworks for identifying promising use cases, clear patterns for designing agent logic and orchestration, and best practices to ensure your agents run safely, predictably, and effectively.

After reading this guide, you'll have the foundational knowledge you need to confidently start building your first agent.

What is an agent?

While conventional software enables users to streamline and automate workflows, agents are designed to perform the same workflows on the users' behalf with a high degree of independence.

Agents are systems that independently accomplish tasks on your behalf.

A workflow is a sequence of steps that must be executed to meet the user's goal, whether that's resolving a customer service issue, booking a restaurant reservation, committing a code change, or generating a report.

Applications that integrate LLMs but don't use them to control workflow execution—think simple chatbots, single-turn LLMs, or sentiment classifiers—are not agents.

More concretely, an agent possesses core characteristics that allow it to act reliably and consistently on behalf of a user.