AI Agents

Customer Agent

Goal: Interface with customer to answer/confirm delivery

User request: Urgent delivery of medication

Response: confirms delivery for next day

(1) First check inventory
(2) Then check delivery schedules and confirm

Uses Llama model

(1)

(2)

Inventory Agent

Goal: tracks inventory levels in warehouse

Uses Claude LLM model

Delivery Agent

Goal: Checks routes and manages delivery schedules

Uses Gemini LLM model

Sandeep Arora

www.trilyen.com

2025 is the year of AI Agents

https://www.youtube.com/watch?v=Vy3OkbtUa5k

A lot of what we are focused on is giving every creator and every small business the ability to create AI Agents for themselves….these are huge spaces….there are hundreds of millions of small businesses in the world. In a few taps they will be able to create AI agents like customer support agents for themselves – *Mark Zukerberg*
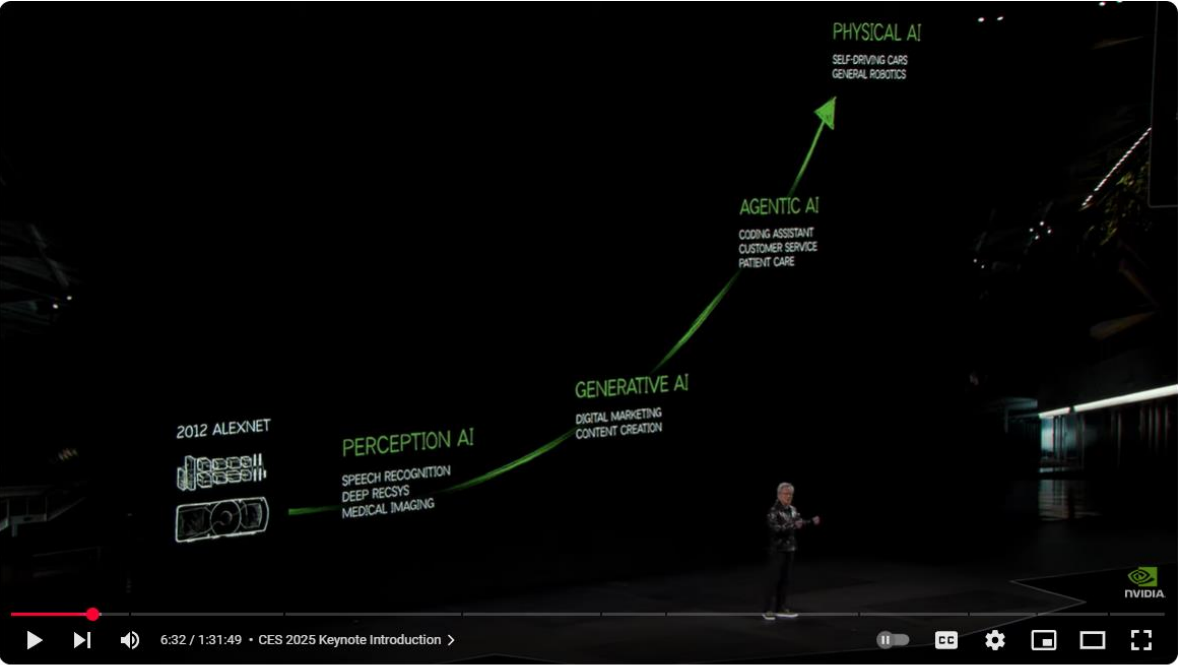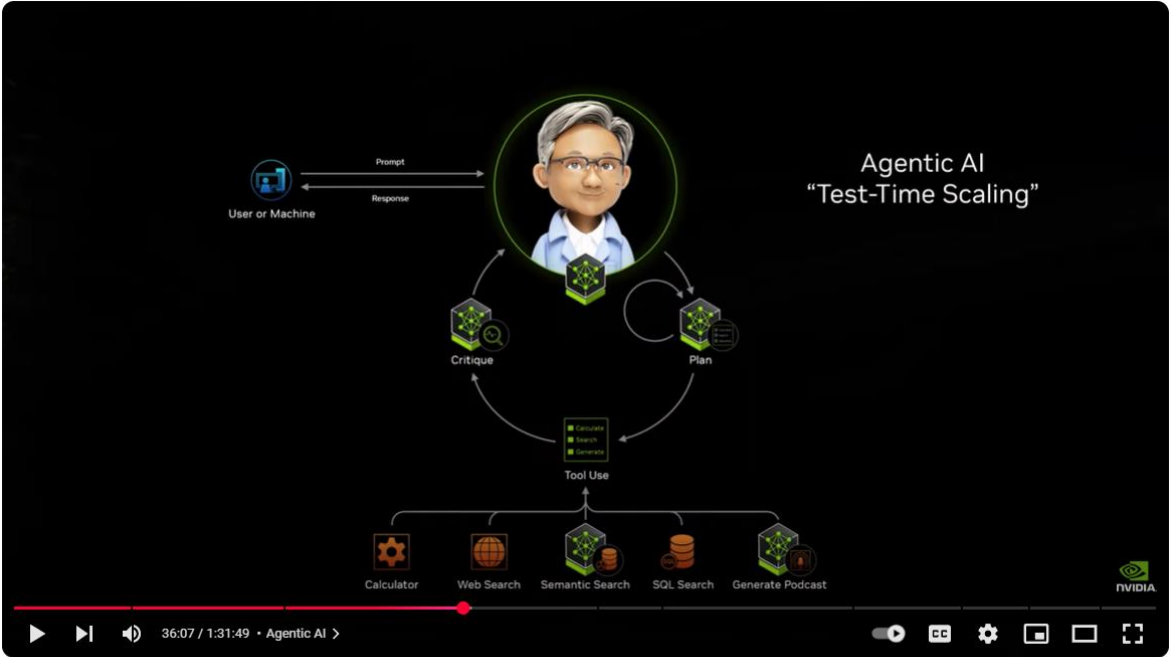

Salesforce is calling it "Digital Labor"

… now we are in an age of Agentic AI, AI's which can perceive, reason, plan and act…
– Jensen Huang, CEO of Nvidia

https://www.youtube.com/watch?v=k82RwXqZHY8

What is an AI Agent

AI Agents can be defined in several ways

- **AI agent is a software program that can complete a task using LLMs, with minimal to zero supervision**

or

- **An AI Agent is a type of software program, that uses LLM's to achieve a goal. It can run autonomously, reason, plan and make decisions to complete a goal. The AI agent can be triggered by a human, or by an event or by another agent. If it needs input or cannot complete a task it reaches out to a human for input or guidance**

Travel AI Agent

creates a custom itinerary for a group of traveler's having mobility issues, translates it to multiple languages and sends it to each member of the travel group.

Finance AI Agent

A finance AI Agent, searches the web for all news related to a portfolio of stocks , summarizes it and sends it to finance analyst.
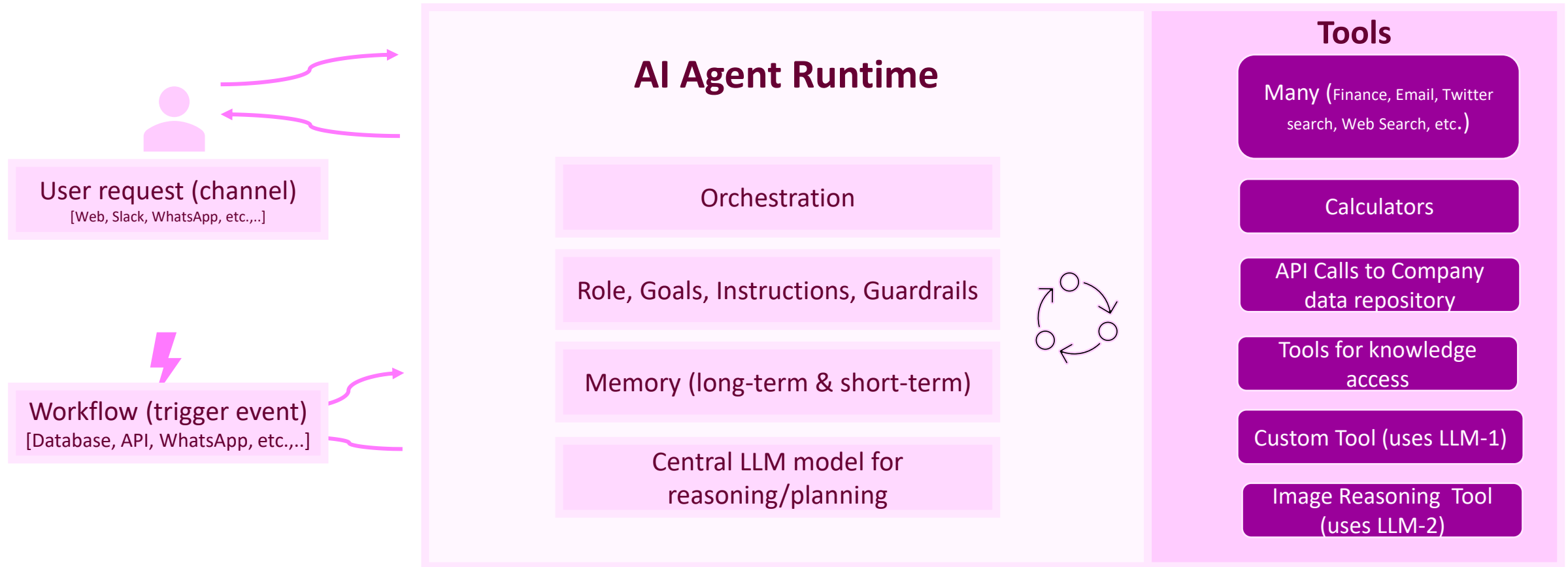
Difference between LLM model and AI Agent

- **LLMs process input and provide a result. Like when you use ChatGPT, you prompt and get an answer.**
- **AI Agents: Take input, understand it, then create a plan and then use tools to achieve the goal**

Feature	LLM (Large Language Model)	Agentic AI
Role	The Thinker	Complete a Goal using one or more LLMs
Main Function	Understands and generate content	Solves problems and takes actions
Reactivity	Waits for user input. Request and response pattern.	Can act independently once triggered by a human or event
Goal Orientation	Generate content. Request response in a realtime manner	Executes tasks to achieve a goal which could take some time
Tool	Tool usage limited	Uses tools (APIs, databases, etc.) to achieve goals and complete tasks
Autonomy	Needs direct instructions to operate	Can plan and act based on objectives
Decision-Making	No, only provides information	Yes, makes decisions to achieve goals

How do AI Agents work

When a user or workflow makes a request, the AI agent uses a LLM to understand the request. It then reasons and plans which tools to use, in what order and what data to pass to each tool. The AI Agent runtime then executes the plan, to achieve the goal and return the results to the user. The AI agent has a goal or a mission. It has guardrails on what it can do or cannot do. The Agent Runtime also has a memory to main context as it executes the various steps.

User request (channel)
[Web, Slack, WhatsApp, etc.,...]

Workflow (trigger event)
[Database, API, WhatsApp, etc.,...]

AI Agent Runtime

Orchestration

Role, Goals, Instructions, Guardrails

Memory (long-term & short-term)

Central LLM model for reasoning/planning

Tools

Many (Finance, Email, Twitter search, Web Search, etc.)

Calculators

API Calls to Company data repository

Tools for knowledge access

Custom Tool (uses LLM-1)

Image Reasoning Tool (uses LLM-2)

Components of Agentic AI

User request (channel) [Web, Slack, WhatsApp, etc.,..]	The channel (Web, Slack, WhatsApp, etc.,..) where humans interact with the agent
Orchestration	The orchestration engine that makes sure all steps are completed, and goal is achieved.
Role, Goals, Instructions, Guardrails	Describes the Goal, Roles and instructions the Agent must follow. Also put guardrails on what the agent cannot do or when it should reach out to human if it gets stuck
Memory (long-term & short-term)	Context and memory needed for the life of one instance of process. The long-term memory refers to on-going learning for personalization and so that it gets smarter over time.
Central LLM Model for reasoning/planning	The LLM Model (or Models) that will be act as the centralized decision maker for agent processes. They are reasoning models.

Components of Agentic AI

Tools

Many (Finance, Email, Twitter search, Web Search, etc.)

Calculators

API Calls to Company data repository

Custom Tools for knowledge access

Custom Tool (uses LLM-1)

Image Reasoning Tool (uses LLM-2)

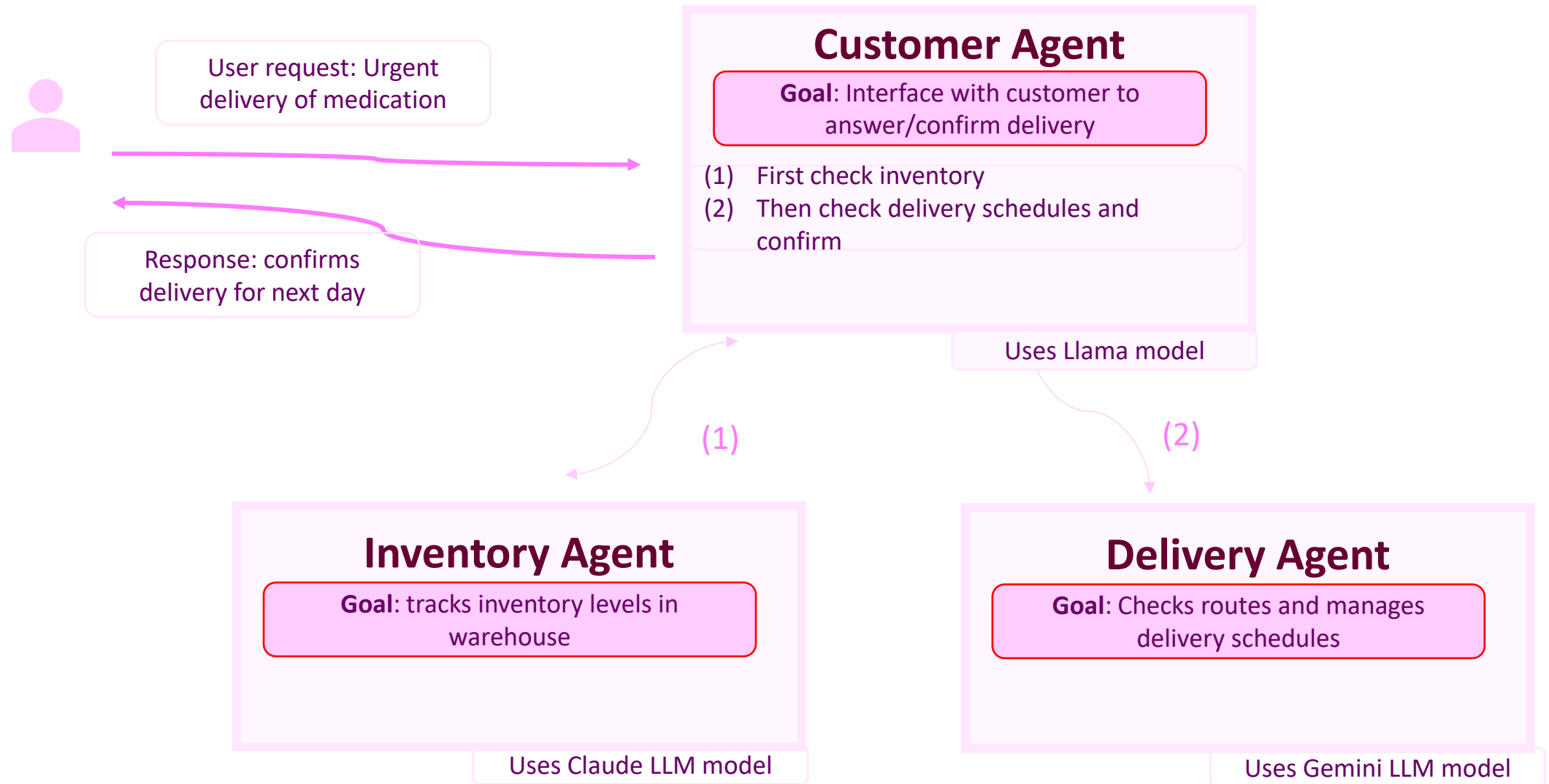Depending on the type of Agent, it will need access to various tools to accomplish mission.
- A research assistant may need Web Search tool to search the web.
- A financial analysis agent will need access to data analysis tool and an image reasoning LLM
- To access enterprise data, you can build custom tools and invoke them from the AI agent.

Tools enable Agents to interact with the outside world. Agents will also use one or more LLMs to complete the goal.

To summarize, by attaching agents with tools, we unlock vast potential of use cases for agents - not only understand the world but also act upon it, opening doors for an array of new applications and use cases.

Multi-Agent Conversation

In certain use cases – Agents may invoke or collaborate with other agents to complete a goal. To give you an idea, here is a visual of a multi-agent conversation. Each agent specializes in a different task and may use a different LLM model .

User request: Urgent delivery of medication

Response: confirms delivery for next day

Customer Agent

Goal: Interface with customer to answer/confirm delivery

(1) First check inventory
(2) Then check delivery schedules and confirm

Uses Llama model

(1)

(2)

Inventory Agent

Goal: tracks inventory levels in warehouse

Uses Claude LLM model

Delivery Agent

Goal: Checks routes and manages delivery schedules

Uses Gemini LLM model

AI Agents

Think of AI Agents as a system of models, some understand and interact with the customer, some parts retrieve information from enterprise systems or knowledge bases, others search the internet or use tools, all working in synch to achieve a goal
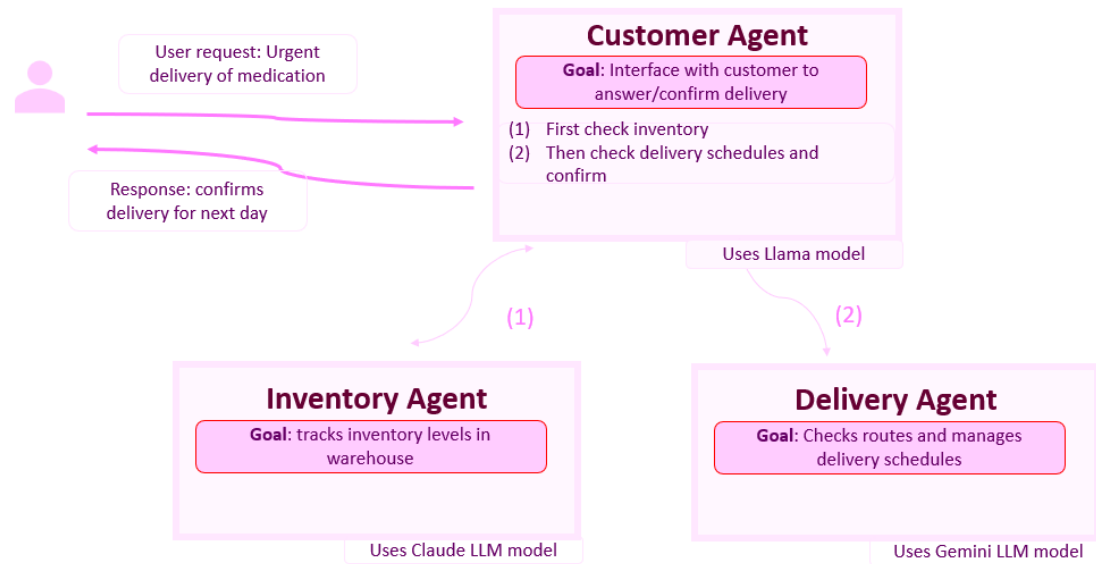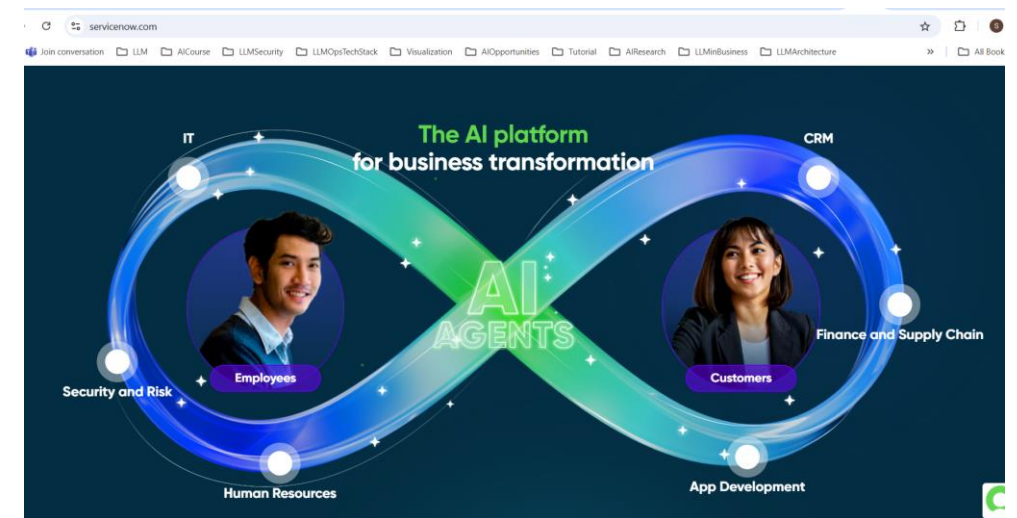
Agents Everywhere (Enterprise)

AI Agents are an application of LLMs in business. In the enterprise space, all companies are providing tools for their customers to create AI Agents on their data. Salesforce, ServiceNow, SAP, etc. all allow customers to build AI Agents on top of their data.
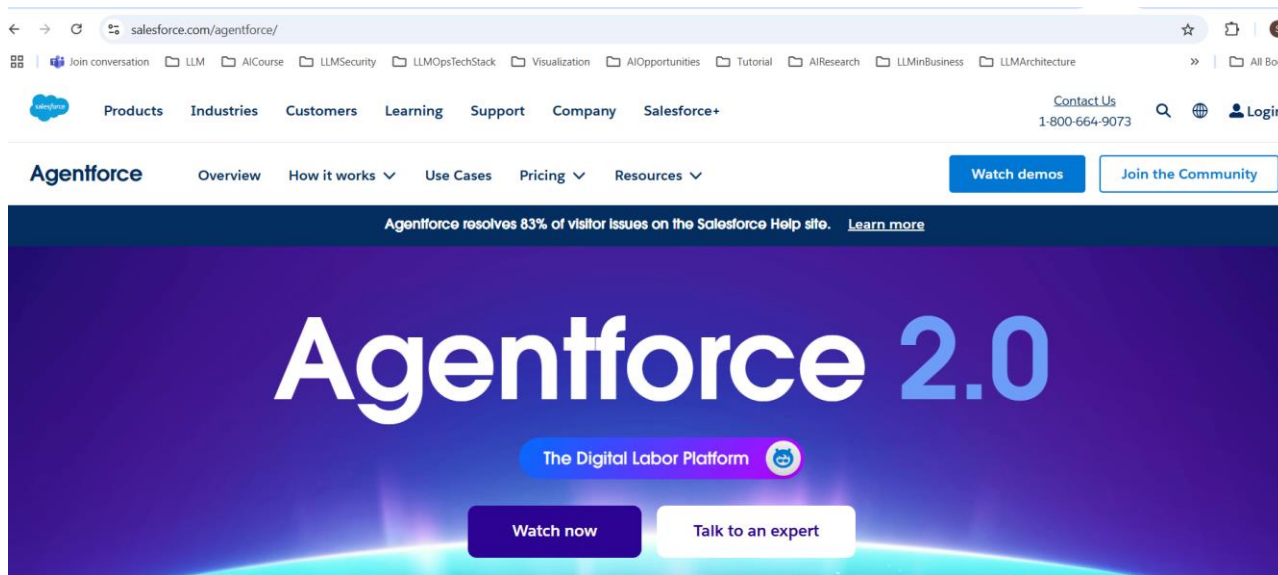

Salesforce

Service Now

Agents Everywhere (Small Business)

- **Google Agentspace is going to empower millions of small business to create different kinds of AI agents using AgentSpace.**
- **There are several no-code/ low-code frameworks emerging like Crew AI to enable everyone to leverage AI and build AI agents for their workflow.**
- **It is important to understand this evolving area of AI deeply.**
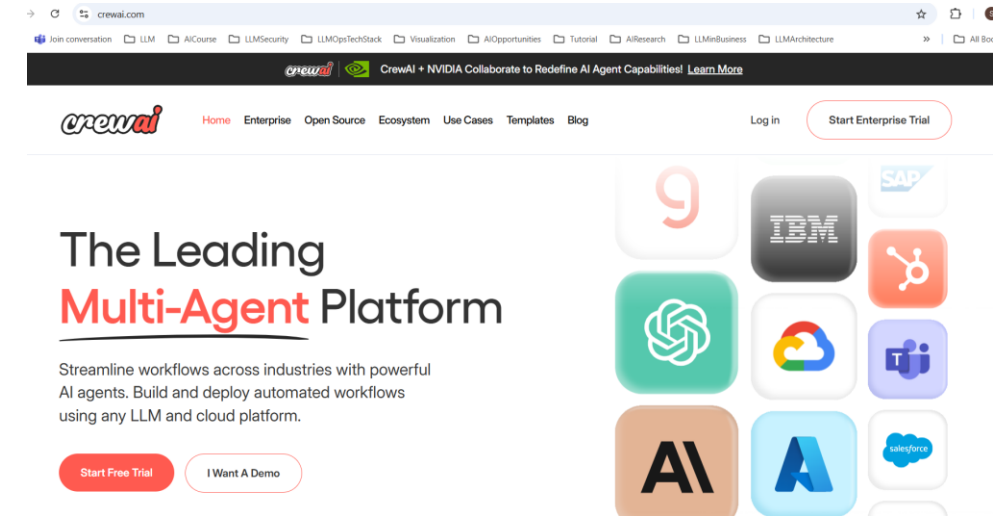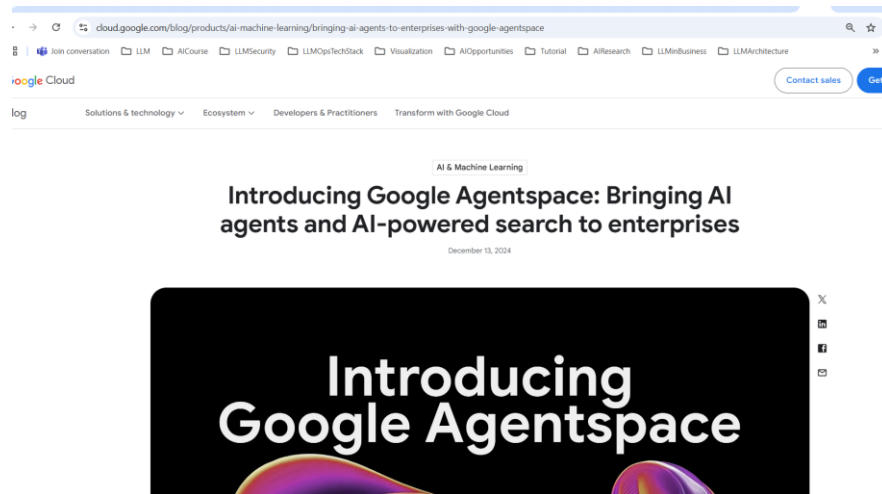
CrewAI allows business to create AI Agents

A lot of what we are focused on is giving every creator and every small business the ability to create AI Agents for themselves….these are huge spaces….there are hundreds of millions of small businesses in the world. In a few taps they will be able to create AI agents like customer support agents for themselves – *Mark Zukerberg*
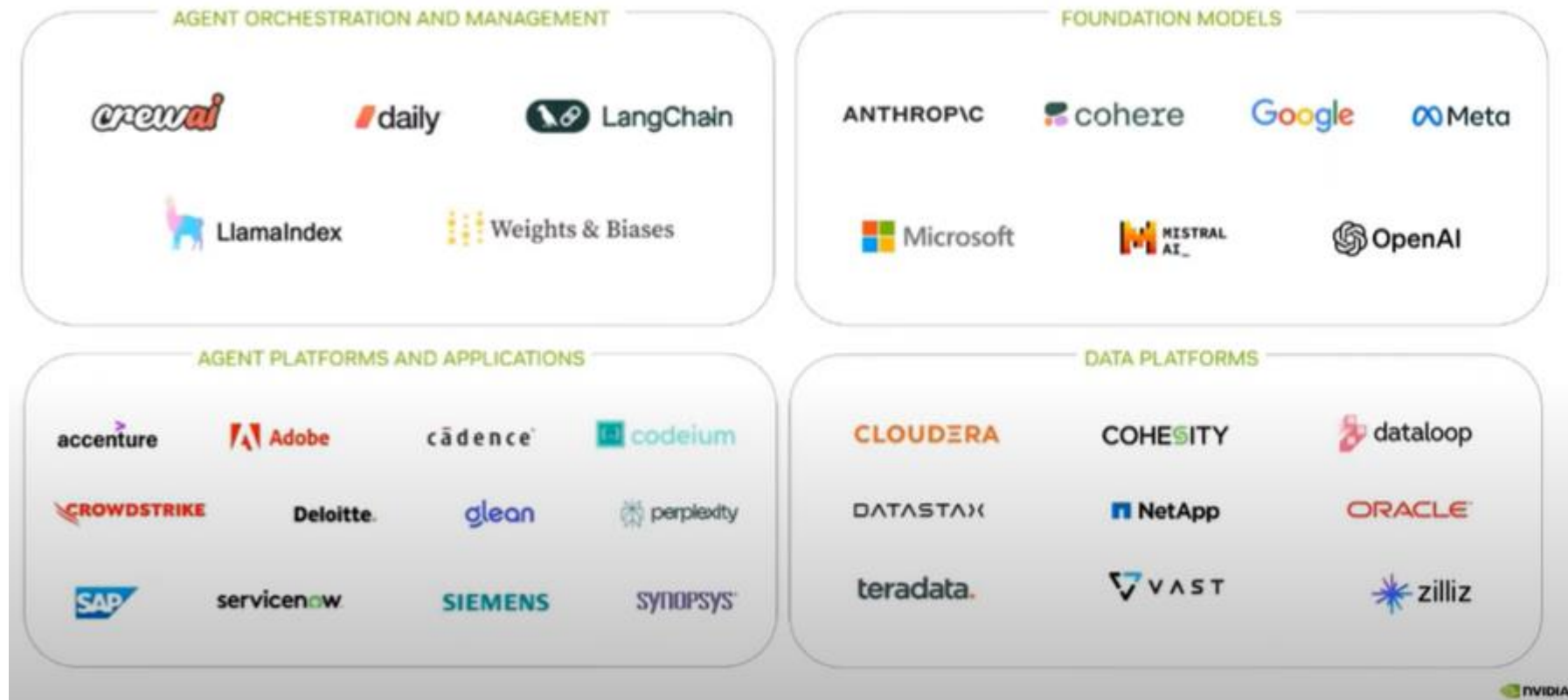
https://www.youtube.com/watch?v=Vy3OkbtUa5k
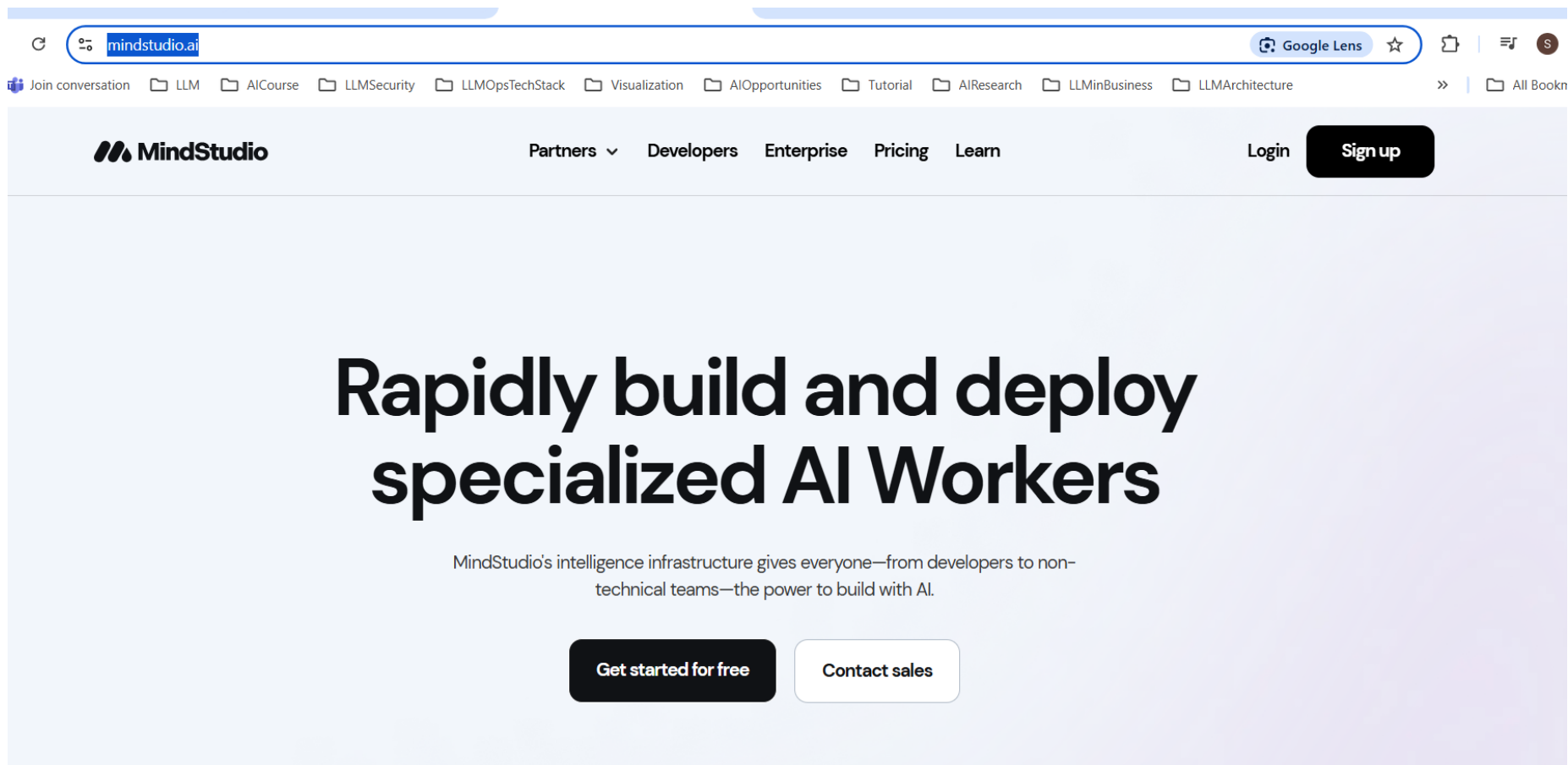
Appendix

- Tools

AI Agents

AI Agents also being called as "Digital Labor" or "AI Workers" are going to get embedded everywhere knowledge work is done. Study deeply how these agents work, how they impact your craft to stay ahead and not be caught off guard.

https://www.youtube.com/watch?v=Lt0bY8tQ52k

MindStudio's intelligence infrastructure gives everyone—from developers to non-technical teams—the power to build with AI.

Appendix - Tools

Here are a few frameworks which allow you to create Agents
- PhiData
- AutoGen
- LangChain
- Crew.ai
- LLamaIndex

Tools for AI Agents in PhiData

Here is an example of few toolkits available with PhiData Agentic AI framework to give you an idea

Toolkit	Description	Toolkit	Description
Apify	Use Apify Actors.	Arxiv	Read arXiv papers.
Calculator	Perform calculations.	CalCom	Interact with the Cal.com API.
Composio	Compose complex workflows.	Crawl4AI	Crawl web data.
CSV	Work with CSV files.	DuckDb	Run SQL using DuckDb.
DuckDuckGo	Search the web using DuckDuckGo.	Dalle	Generate images with Dalle.
Email	Send emails.	Exa	Search the web using Exa.
File	Read and write files.	Firecrawl	Crawl the web using Firecrawl.
GitHub	Interact with GitHub.	Google Search	Search Google.
HackerNews	Read Hacker News articles.	Jina Reader	Perform neural search and AI services using Jina.
Jira	Interact with Jira.	MLX Transcribe	Transcribe audio using MLX.
ModelsLabs	Generate videos using ModelsLabs.	Newspaper	Read news articles.
Newspaper4k	Read articles using Newspaper4k.	OpenBB	Search for stock data using OpenBB.
Pandas	Manipulate data using Pandas.	Postgres	Interact with PostgreSQL databases