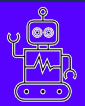
Jennifer Kaehms – Partner, Foundation Capital

Building Your First AI Agent

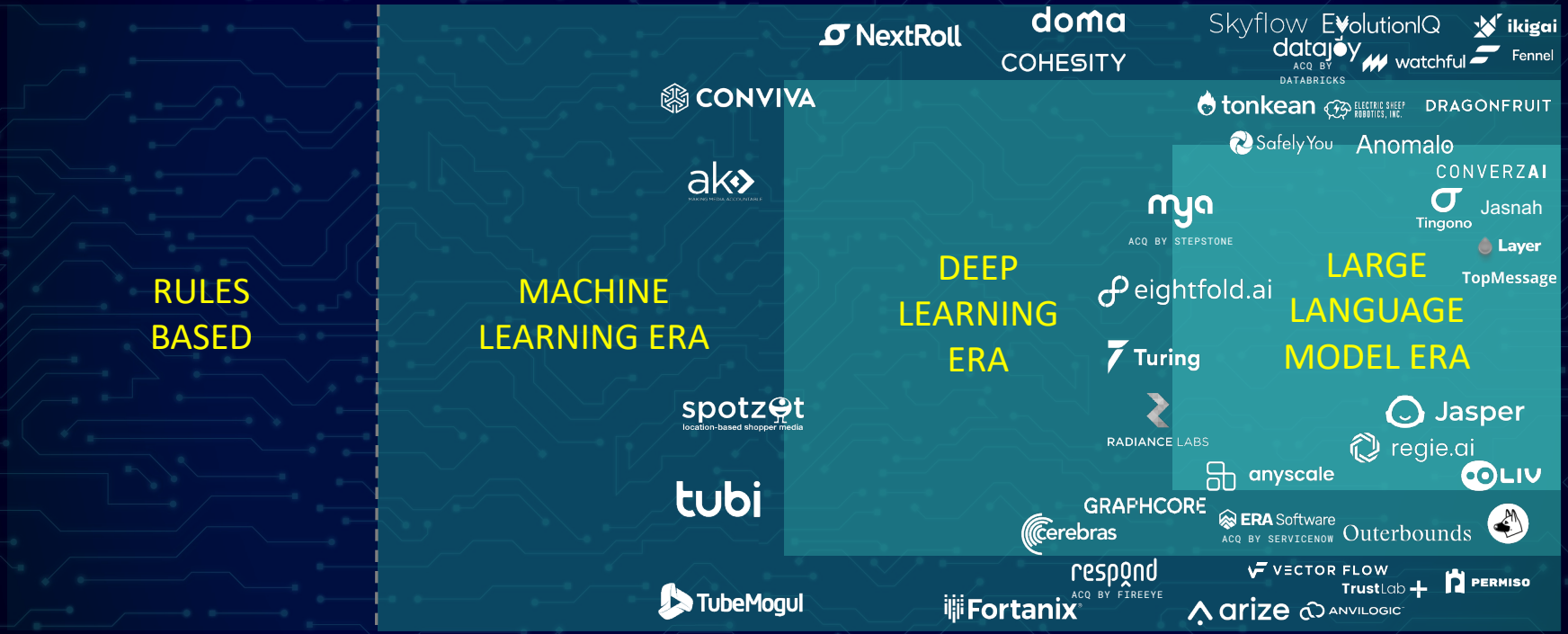
Building AI Agents with LLMs X O'Reilly



Intro

- My name is Jennifer Kaehms (@jennykaehms)
-Investing since 2016 – Luminar, Lambda Labs
- Worked at Forethought AI
- Now a partner at Foundation Capital

We've invested in multiple eras of AI starting in 2010



1960 1970 1980 1990 2000 2003 2006 2009 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

FC AI Portfolio

Intelligent Automation

AI VERTICAL APPS

Addi
doma
EvolutionIQ
SafelyYou
FAIRMATIC™

AI HORIZONTAL APPS

eightfold.ai
Jasper
Turing

Data / ML Infrastructure

cerebras
COHESITY
anyscale

Data Security

Fortanix
Skyflow
ANVILOGIC™

Building Your First AI Agent

1. **Why agents?**

   Why would you need an agent?

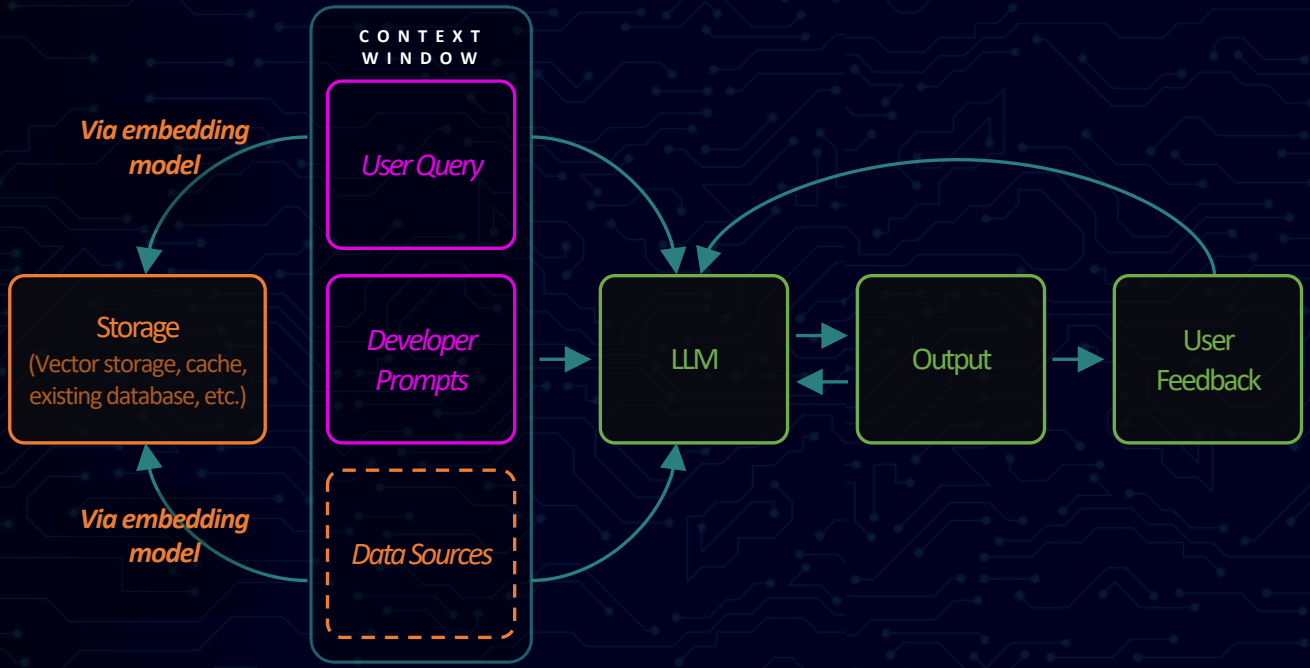
2. **Two questions to ask before starting an agent project**

   1) Is this system isolated to one app?
   2) Is this a chatbot?

3. **Demo**

   Automating my job with an AI agent

Generative AI model: automates one task in your application



1. **Prompt Engineering:** Ask better questions
2. **Retrieval:** Add more context for better responses
3. **Finetuning** Train model to give better responses through continuous iteration
   - → Outerbounds
   - → anyscale

LLM Observability — arize

Security — Fortanix, skyflow

	One context window	AI Agents
Browser Buddies	Returns an answer, not a list of links (ChatGPT)	Helps you browse the internet & take actions (OpenAI Plugins & MultiOn)
Social Media	Creates a photo for your social media (Midjourney or Lensa)	Generates a game for you to play & interact with
Legal Work	Searches for case files (Casetext)	Processes case information & generate filings

	One context window	AI Agents
Healthcare	Returns information based on query	Helps you maintain your insulin level
Education	Suggests answers to test questions & homework	Generates a lesson plan that adapts to your learning goal
Logistics	Fills out a customs form	Plans route & navigates to your desired destination

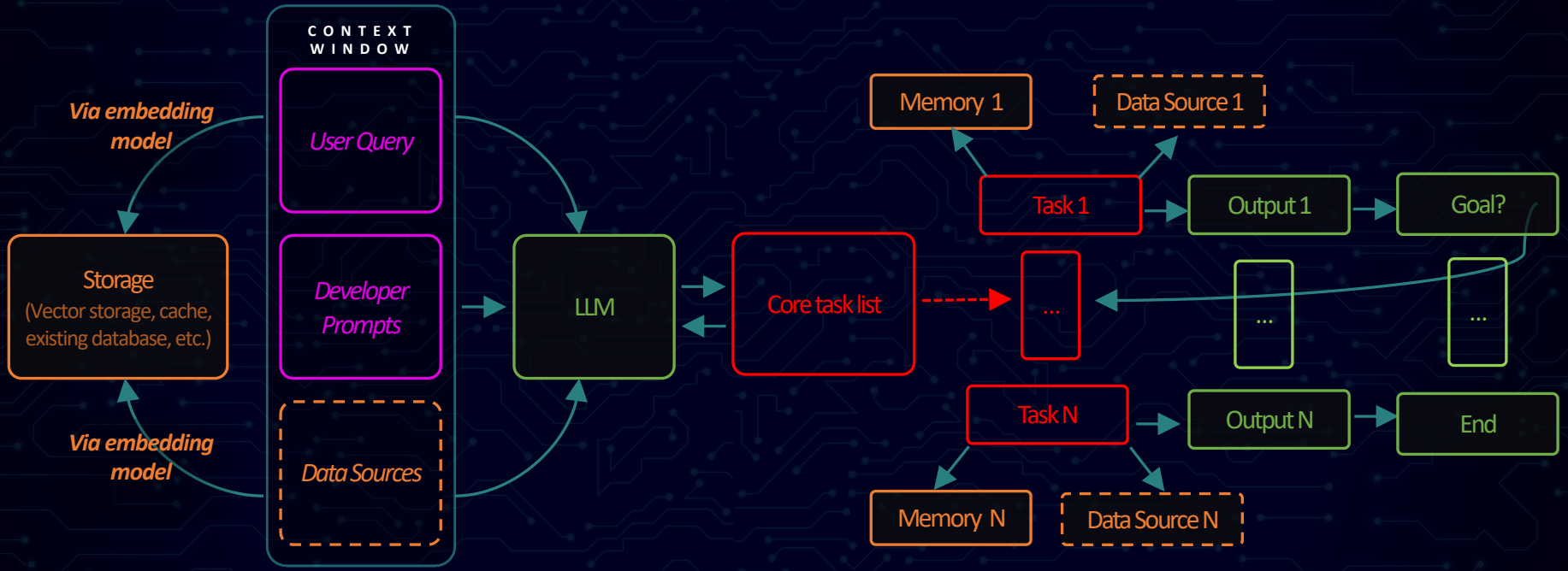
Types of Agents

Agent Adaptability

	One context window	AI Agents	
Browser Buddies	Returns an answer, not a list of links (ChatGPT)	Helps you browse the internet & take actions (OpenAI Plugins & MultiOn)	Goal Based
Social Media	Creates a photo for your social media (Midjourney or Lensa)	Generates a game for you to play & interact with	Object centric or "curious"
Legal Work	Searches for case files (Casetext)	Processes case information & generate filings	World-model based

	One context window	AI Agents	
Healthcare	Returns information based on query	Helps you maintain your insulin level	Reflex based
Education	Suggests answers to test questions & homework	Generates a lesson plan that adapts to your learning goal	Object centric or "curious"
Logistics	Fills out a customs form	Plans route & navigates to your desired destination	Utility based

Generative AI agent: automates a sequence of tasks in your application



Building Your First AI Agent

1. **Why agents?**

Why would you need an agent?

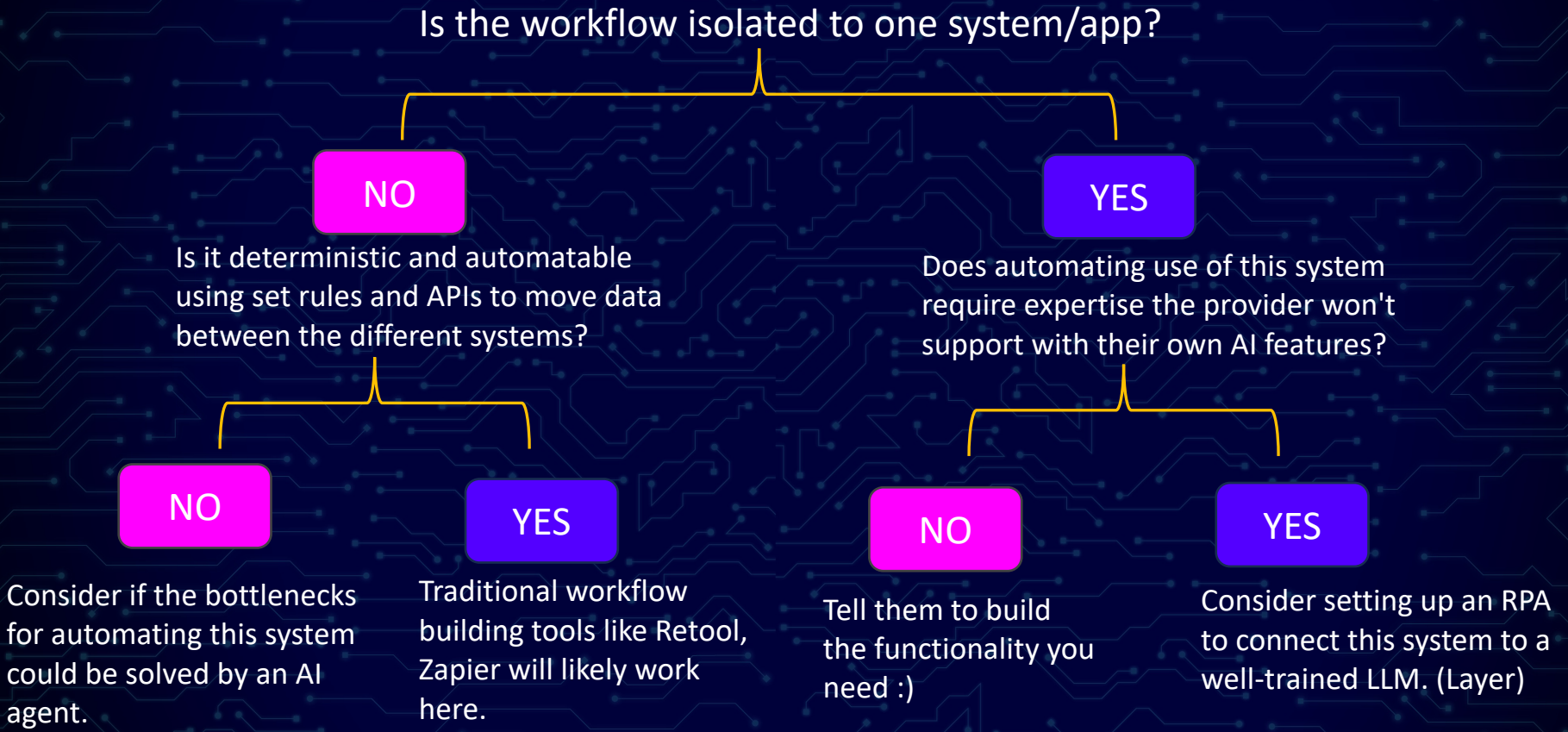
2. **Two questions to ask before starting an agent project**

1) Is this system isolated to one app?
2) Is this a chatbot?

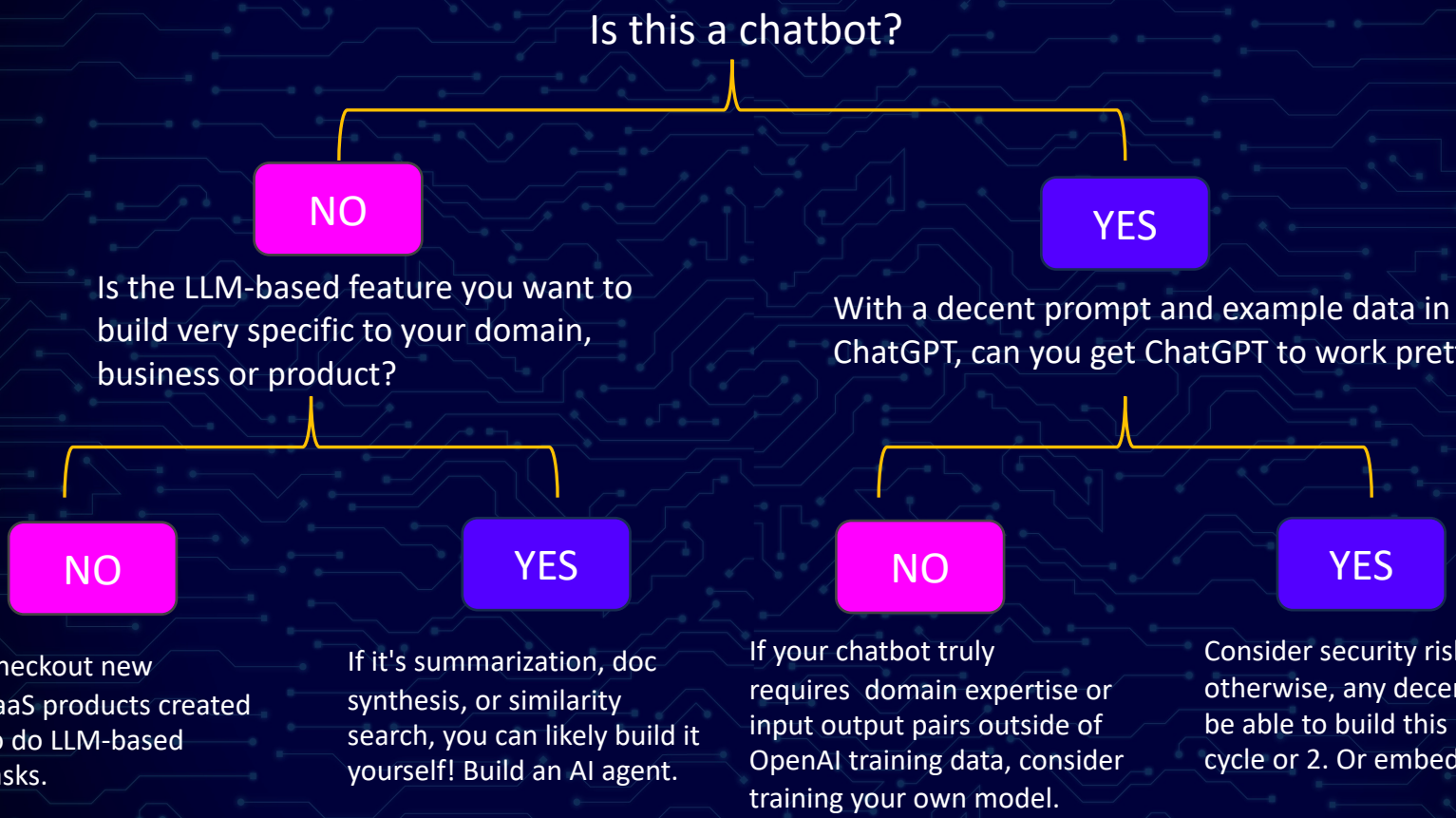
3. **Demo**

Automating my job with an AI agent

AI Agents for Internal Use Cases



AI Agents for External Use Cases



Building Your First AI Agent

1. **Why agents?**

Why would you need an agent?

2. **Two questions to ask before starting an agent project**

1) Is this system isolated to one app?
2) Is this a chatbot?

3. **Demo**

Automating my job with an AI agent

Tennr provides task observability & ensures model security

Tennr

Final Thoughts

	Method	Challenge & Restrictions Today	Considerations
Choosing an Agent Architecture	○ Reflex based ○ World-model based ○ Goal based ○ Utility based ○ Object centric or "curious"	• The more autonomy an agent has, the more likely it is to drift • Creating model-based agents requires an accurate model of the world • As you connect agents to more data sources, you must consider data security & privacy	• When creating a solution for your org, choose the simplest solution possible • It's possible to have multiple agents work together to learn & achieve goals
Security	○ Embeddings models (open source or proprietary) ○ Vector search ○ Retrieval methods	• Privacy concerns: storing customer schema / data information with vector database third parties indefinitely • Retrieval results are typically poor; high dimensionality, sparse representation, domain adaptation, out-of-vocabulary words, language coverage • Latency, hallucination, reliability challenges	• More of a "data engineering" problem vs an ML problem • Need to understand what data is relevant & how to chunk data appropriately
Reliability and Accuracy	○ Chain of thought ○ Curious replay ○ Object centric	• Can fail to generate results when inputs are vague • Model loops on a task • The "Binding Problem"	• How well does the model do on the Crafter Benchmark • For workflow tasks, chain of thought works