

AI Certification

Designing Internal AI Assistants



AI Certification



Saahil Kamath

Head of AI
Eltropy



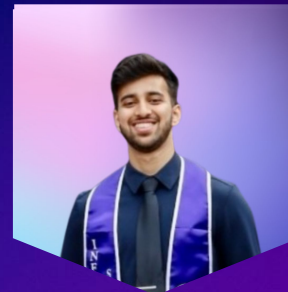
Rahul Prakash

Head of Engineering (AI)
Eltropy



Dheeraj Anikar

Implementation Manager
Eltropy



Anay Deshpande

Implementation Manager
Eltropy

EMERGE

Agenda

Introduction to AI (more like crash course)

Building AI Assistant & Intelligence

SafeAI Framework (Cutting edge that does not cut corners)

Q&A



What is AI?

‘Artificial Intelligence’

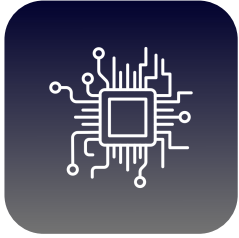
1950s

*“The science and
engineering of making
intelligent machines”*

– John McCarthy



Types of AI by Capability



Narrow AI (Weak AI)

Trained for specific tasks



General AI (Strong AI)

Human-like intelligence



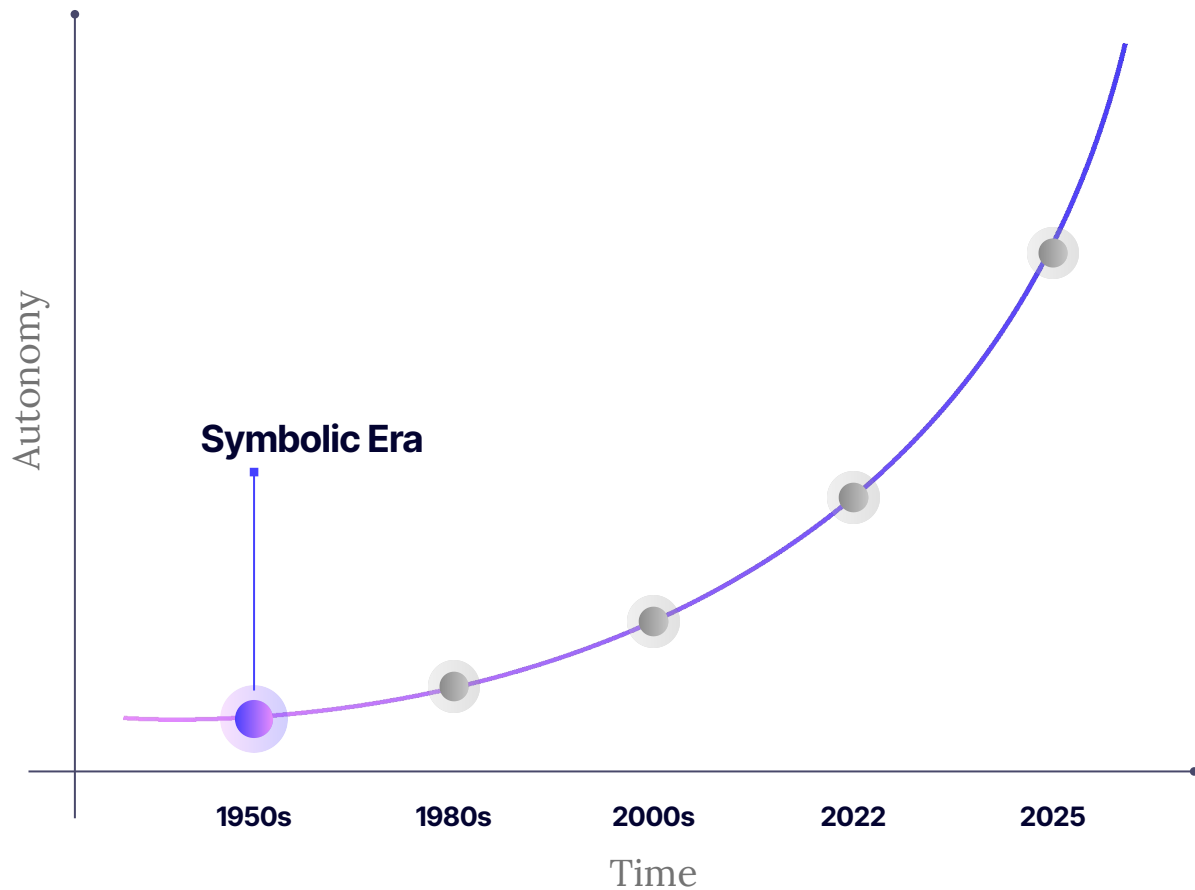
Super-Intelligent AI

Surpasses Human
Intelligence

Evolution of AI - Symbolic AI Era

No learning — Everything encoded by experts

Handcrafted rules, logic programming, symbolic reasoning



ELIZA

He says I am depressed much of the time.

I AM SORRY TO HEAR YOU ARE DEPRESSED

INPUT

It's true. I am unhappy.

DO YOU THINK COMING HERE WILL HELP YOU NOT TO BE UNHAPPY

INPUT

I need some help, that much seems certain.

WHAT WOULD IT MEAN TO YOU IF YOU GOT SOME HELP

INPUT

Perhaps I could learn to get along with my mother.

TELL ME MORE ABOUT YOUR FAMILY

INPUT

My mother takes care of me.

WHO ELSE IN YOUR FAMILY TAKES CARE OF YOU

INPUT

My father.

YOUR FATHER

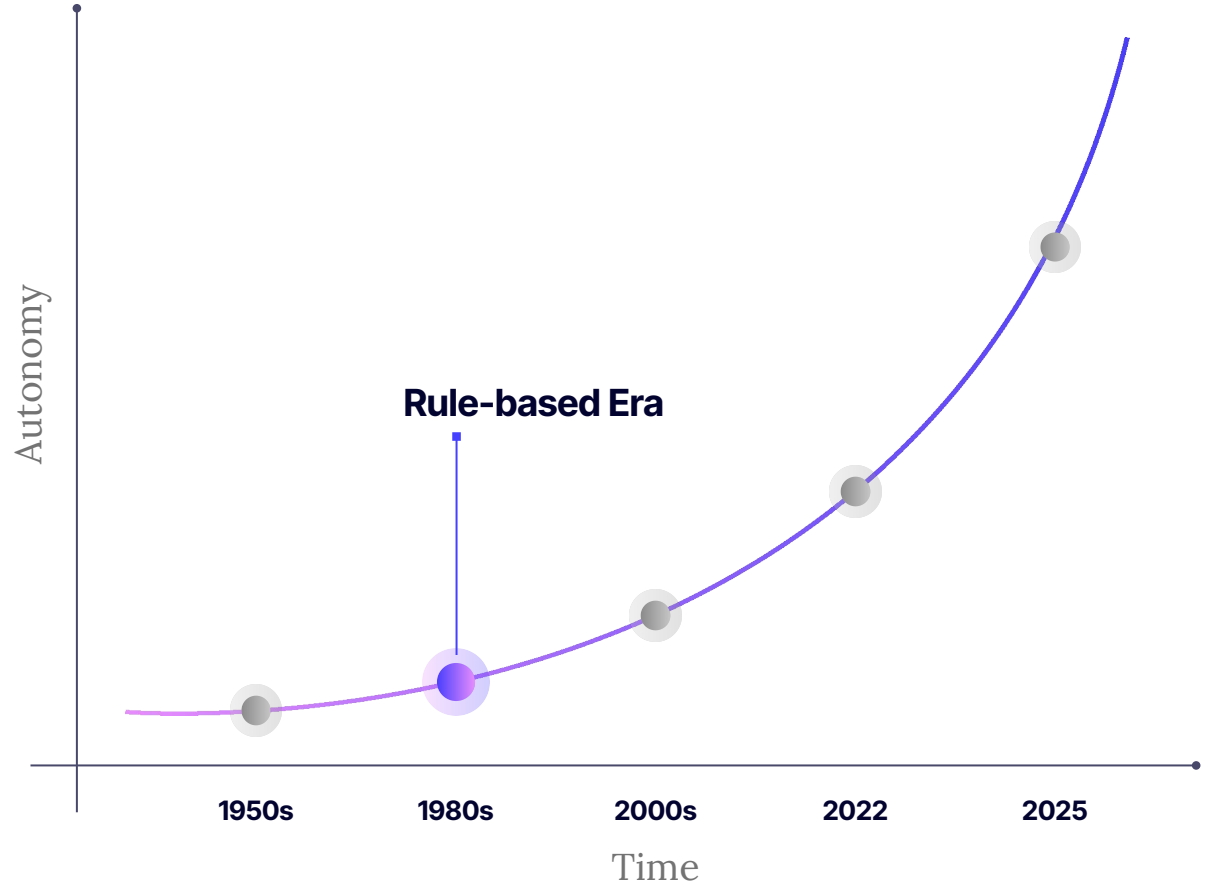
INPUT

Evolution of AI - Rule based AI Era

Still **entirely rule-driven**, no true adaptation

Scripted decision trees, DTMF menus, basic speech prompt interfaces

Knowledge based "if-then" systems in industry (and IVR on the phone)





DELTA

IVR

**Interactive Voice Response
For Reservations**

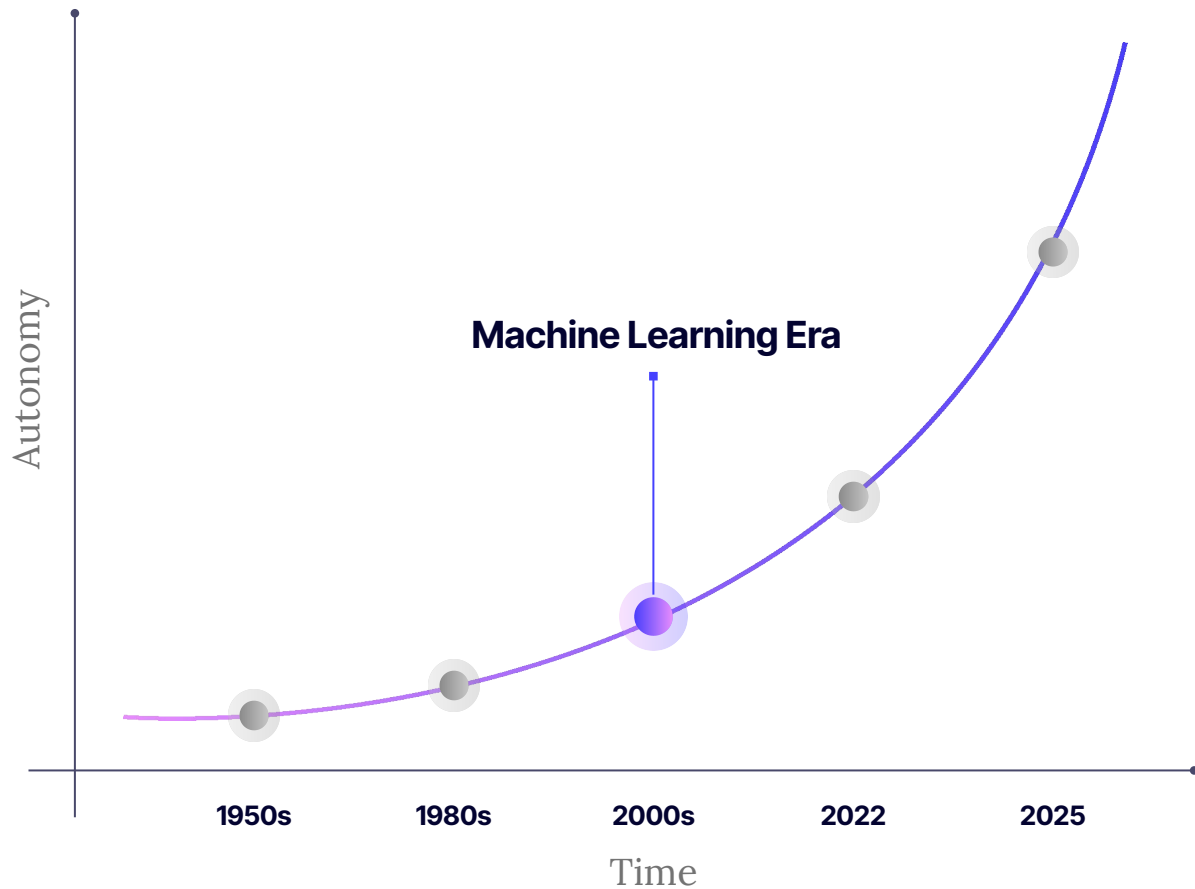
**Say: "What can I
help you with?"**

Evolution of AI - Machine & Deep Learning Era

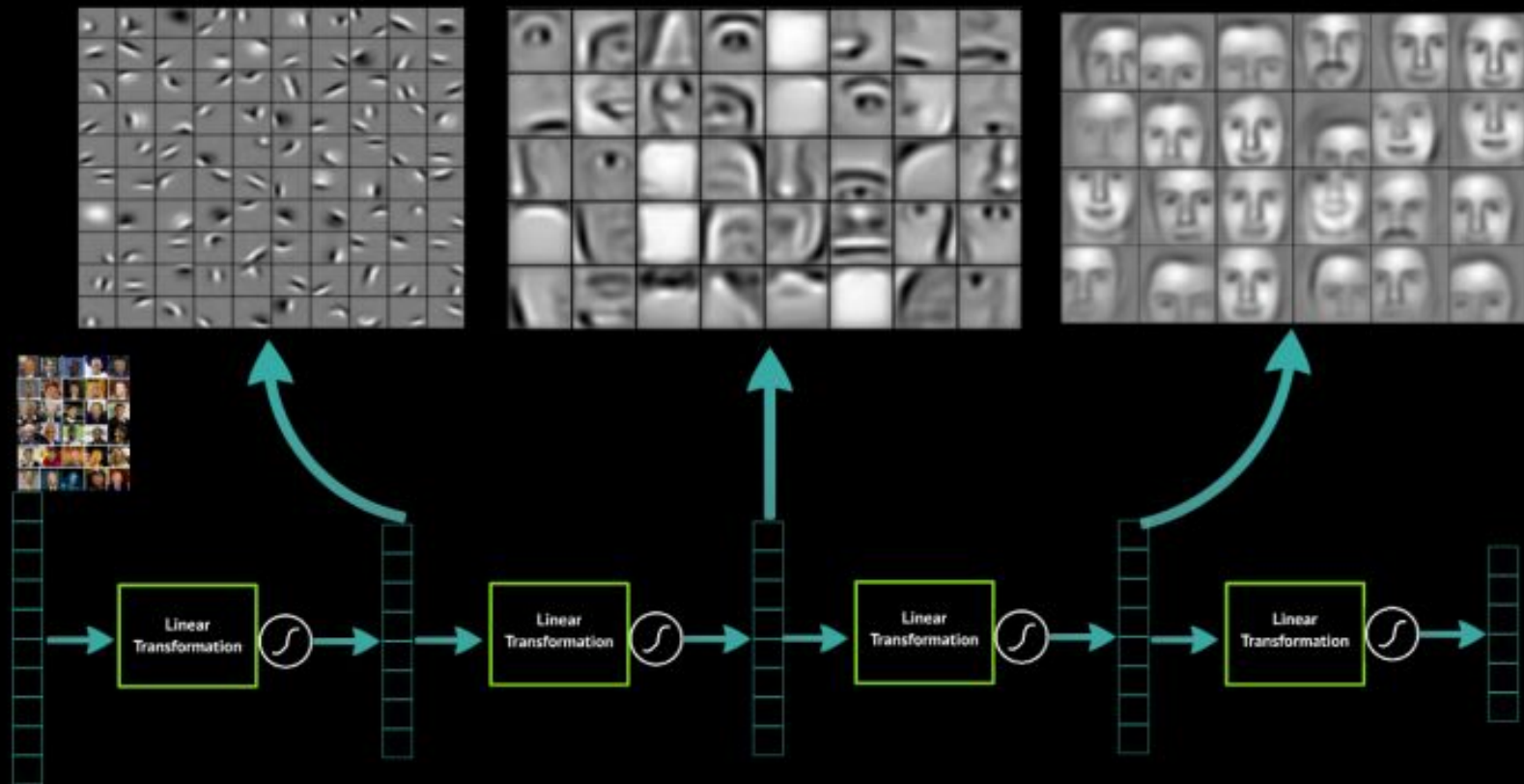
Statistical NLP for intent classification & entity extraction

Data-driven models: SVMs
HMMs, random forests, early neural nets

Early virtual assistants (Siri, Watson, early Google Assistant)



Deep Learning learns layers of features



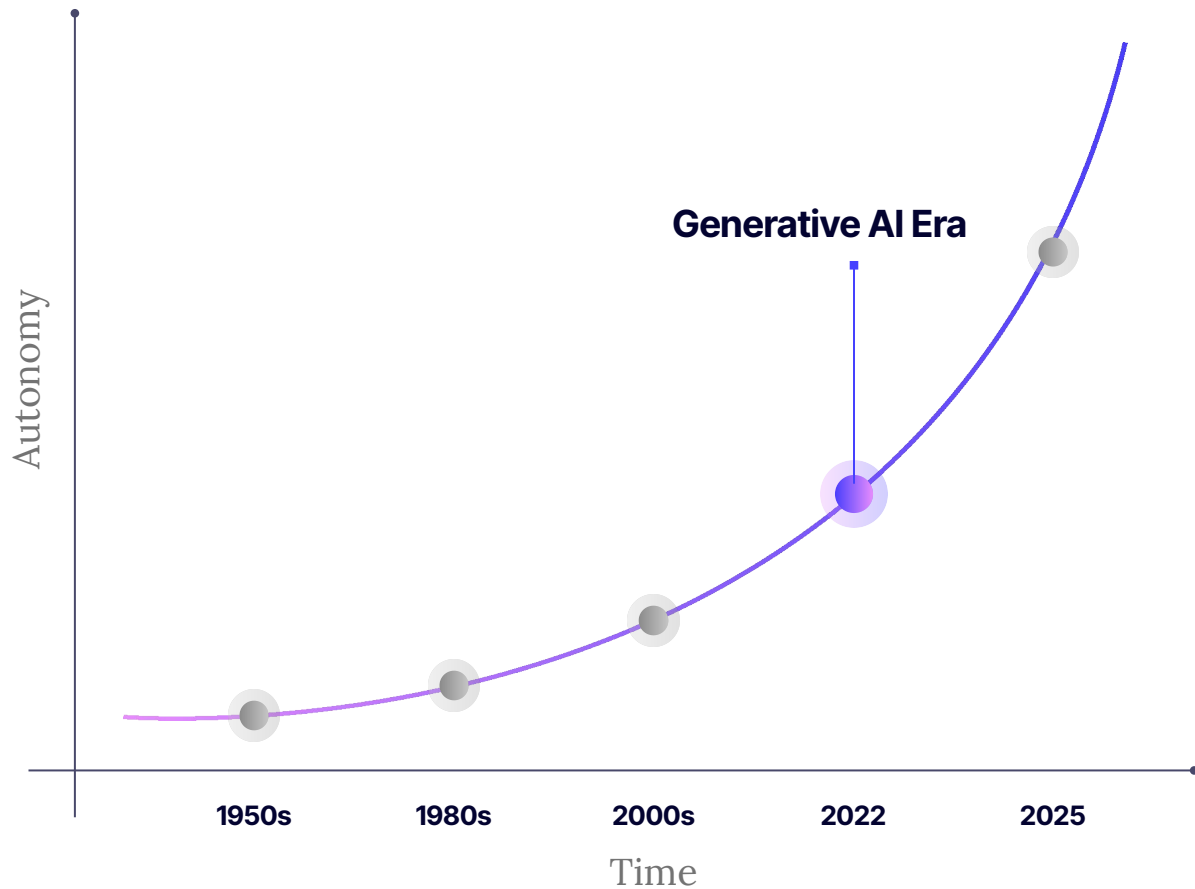


Evolution of AI - Generative AI Era

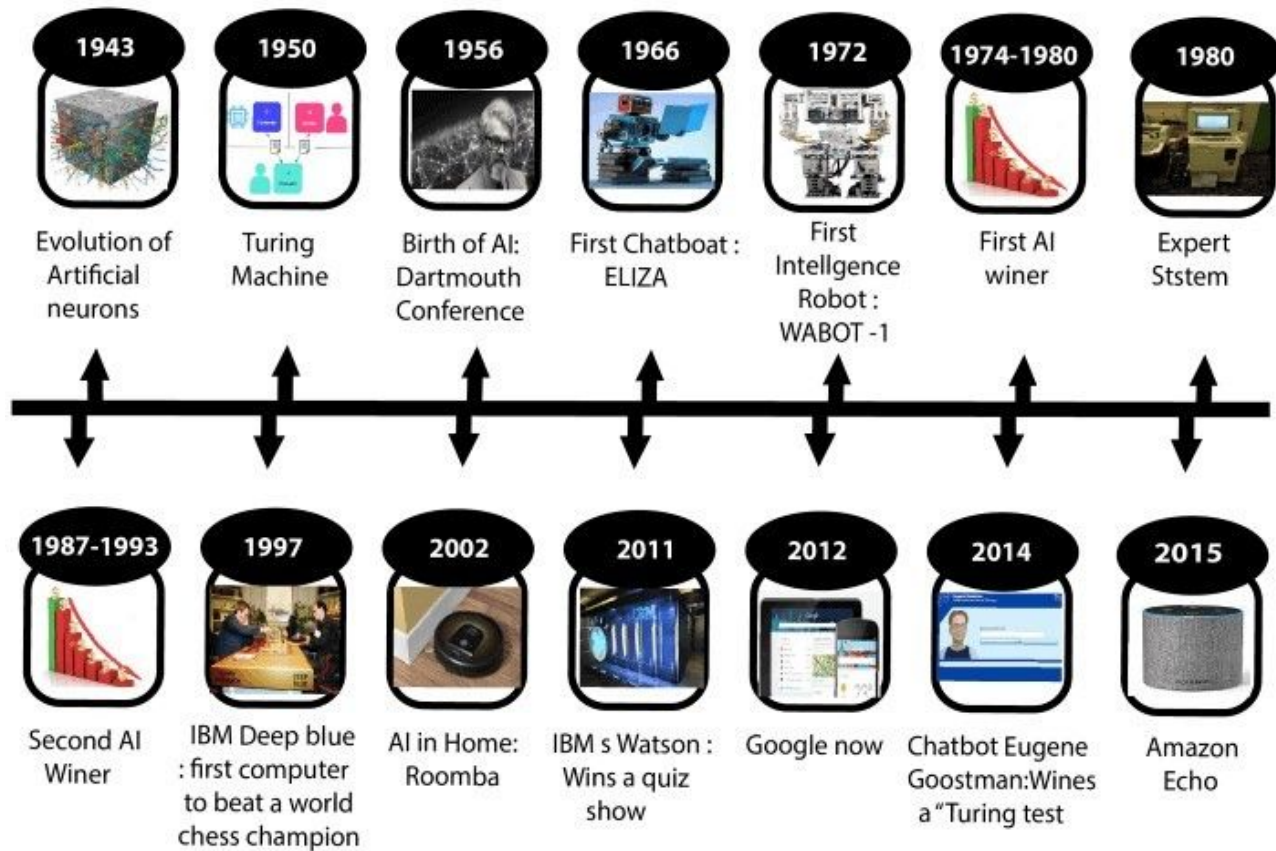
Large generative models for text, images, code (LLMs, diffusion models)

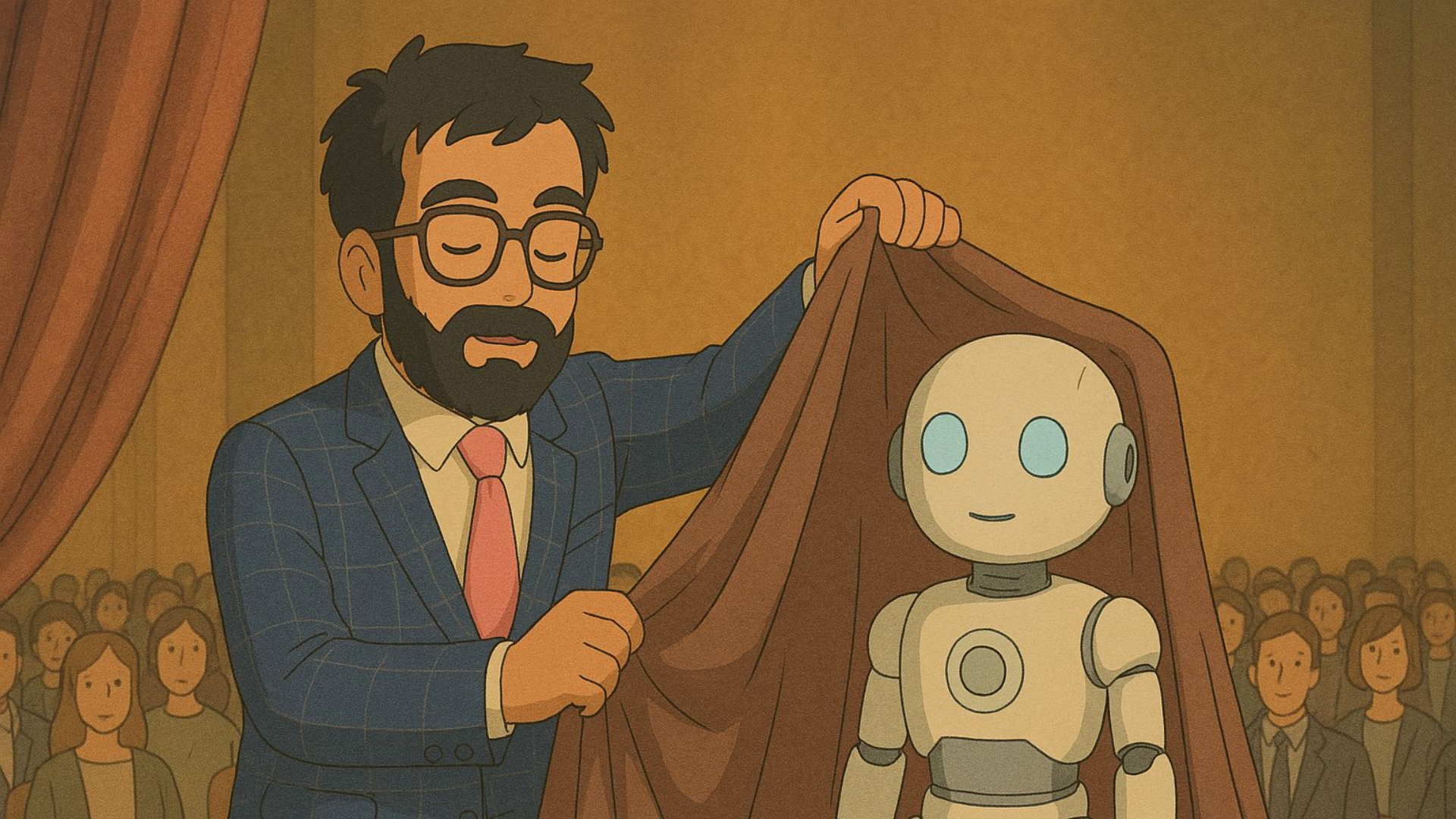
Prompt-driven content creation, multi-modal capabilities

RAG based pipelines



History of AI





Generative AI



Applications (ChatGPT)

ChatGPT is an example of an application built on GPT LLM architecture.

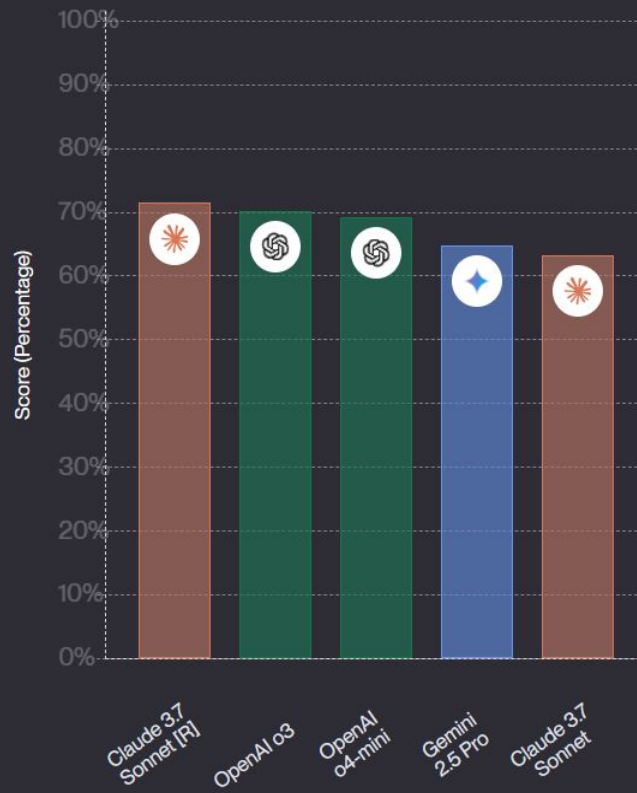
Large Language Model (LLM)

LLM refers to a class of models, such as GPT-3, that are pre-trained on massive amounts of text data to understand and generate human-like text.

Foundation Model

Foundation model is trained on a huge amount of unstructured data in an unsupervised manner.

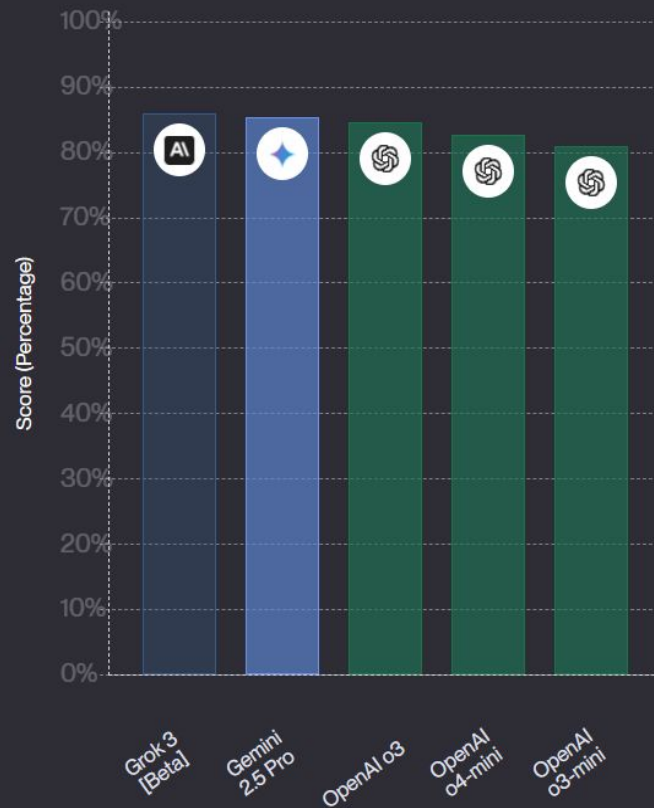
Best in Agentic Coding (SWE Bench) ⓘ



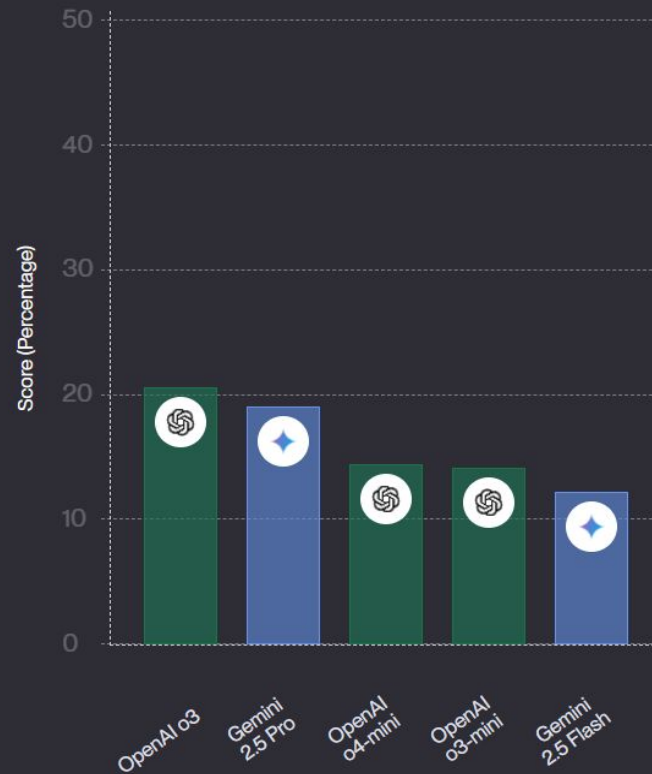
Best in High School Math (AIME 2024) ⓘ



Best in Reasoning (GPQA Diamond) ⓘ



Best Overall (Humanity's Last Exam) ⓘ



Classics

Question:



Here is a representation of a Roman inscription, originally found on a tombstone. Provide a translation for the Palmyrene script. A transliteration of the text is provided: RGYN^o BT HRY BR ^cT^o HBL

Henry T
Merton College, Oxford

Ecology

Question:

Hummingbirds within Apodiformes uniquely have a bilaterally paired oval bone, a sesamoid embedded in the caudolateral portion of the expanded, cruciate aponeurosis of insertion of m. depressor caudae. How many paired tendons are supported by this sesamoid bone? Answer with a number.

Edward V
Massachusetts Institute of Technology



OpenAI

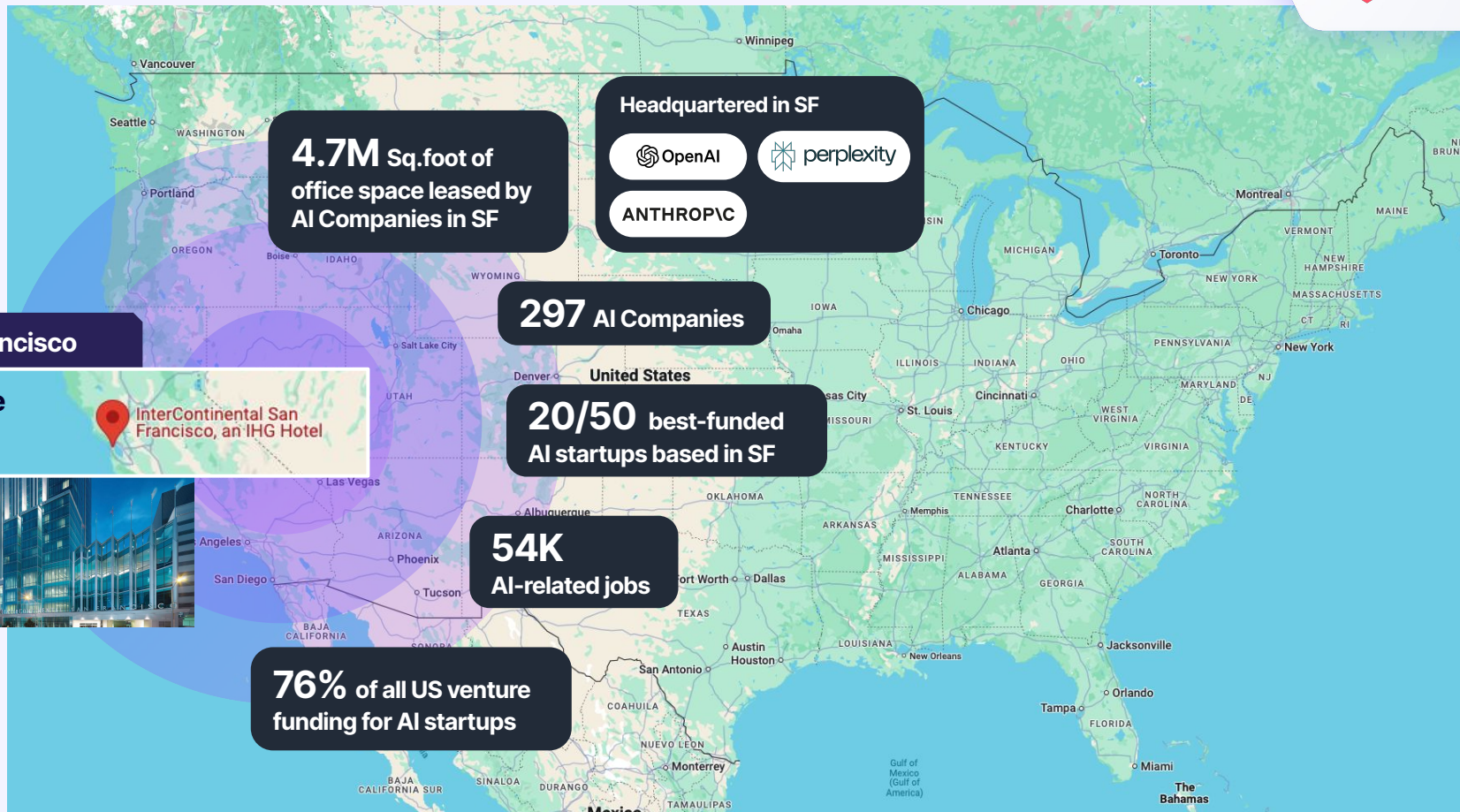


Google



Microsoft

The AI war has begun..

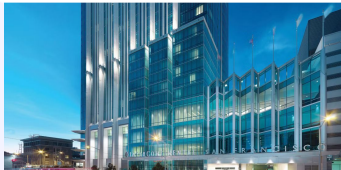


San Francisco

You are Here



InterContinental San Francisco, an IHG Hotel



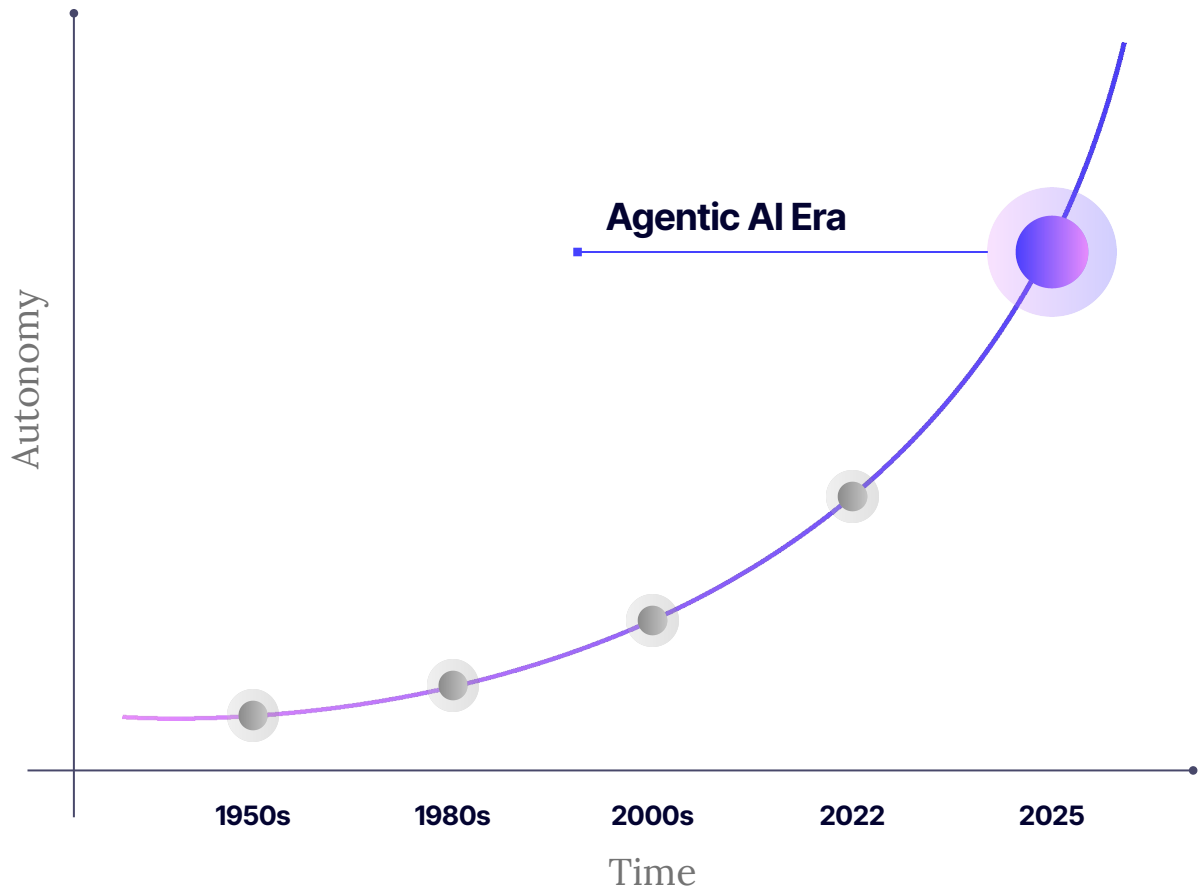


Evolution of AI - Agentic AI Era

Autonomous agents that plan on-the-fly and invoke the right tools

Context-aware, multi-step workflows with self-monitoring

Minimal human designer intervention: Continuous learning loops



What is Agentic AI?



What is Agentic AI?

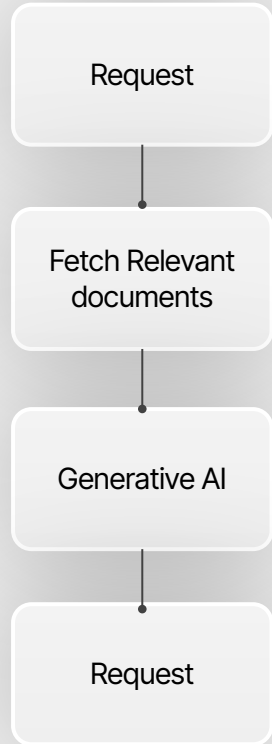


Artificial intelligence systems that
*can act autonomously with
goal-directed behavior.*

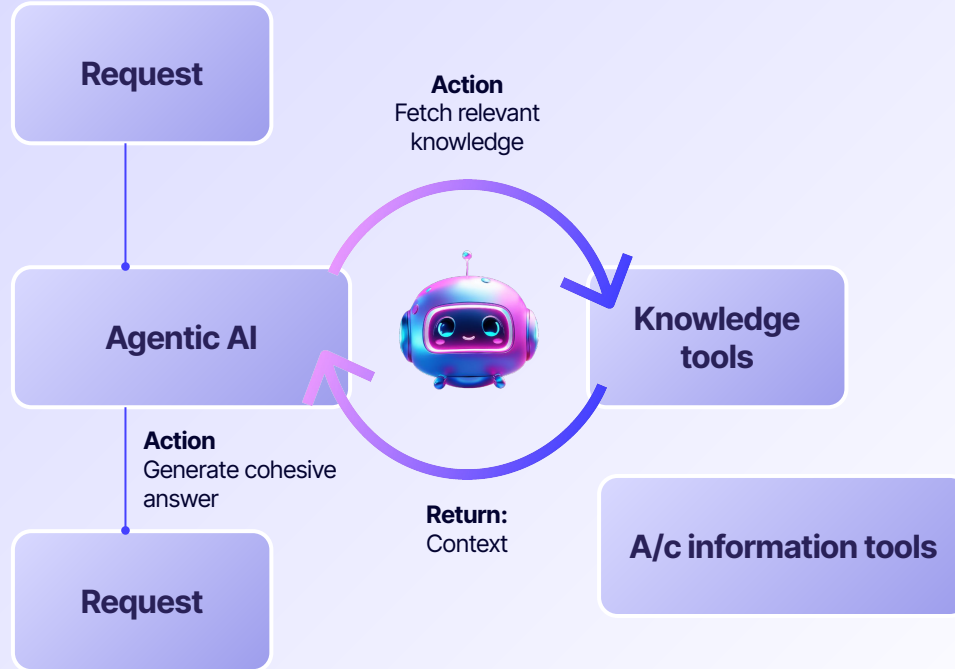


What is giving Agency mean?

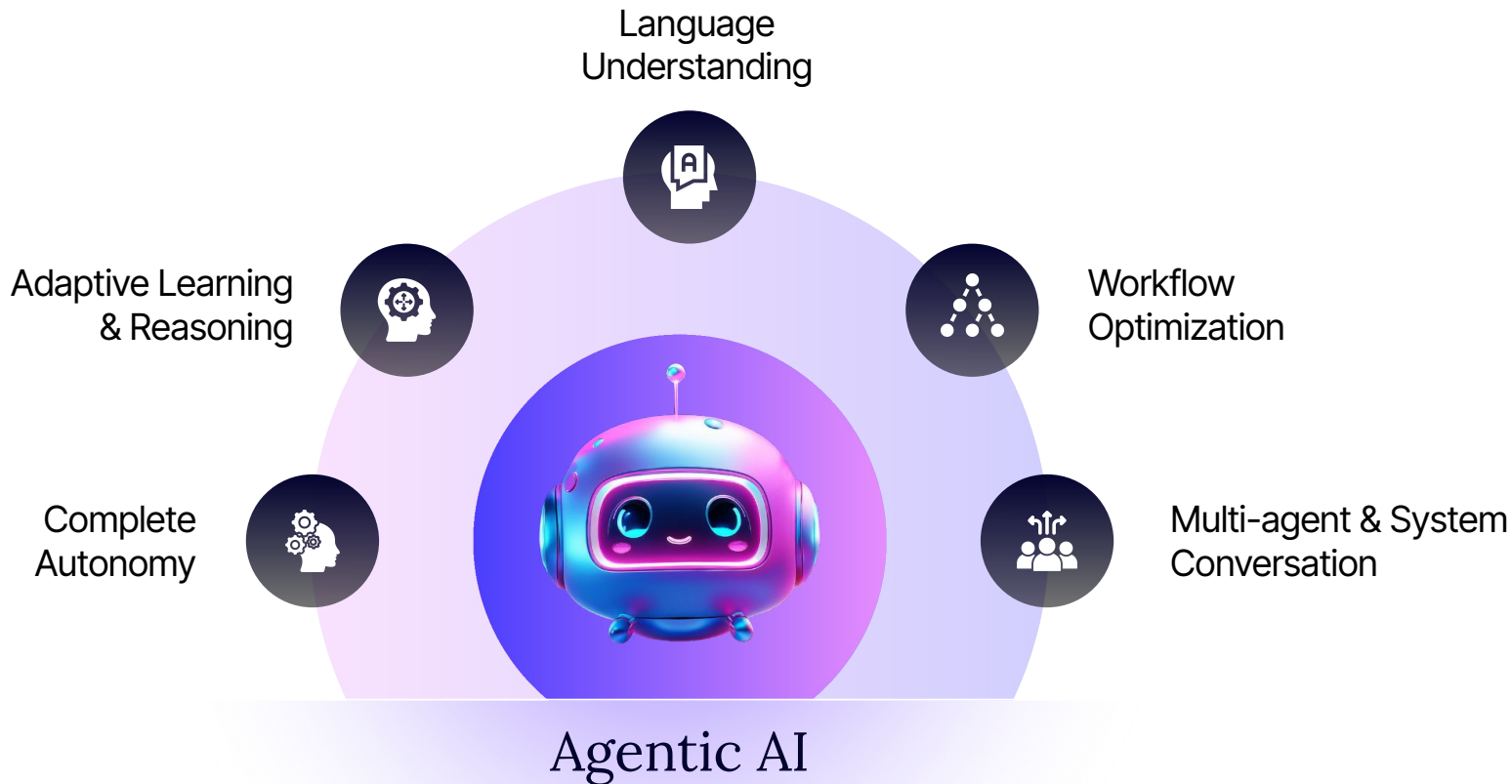
Generative AI



Agentic AI



What is **Agentic AI** Era



Enabling AI Agents

Why do Tools Matter ?

Extend an agent's "hands and eyes" beyond pure LLM text.

Enable real-world actions:
database queries, API calls,
document retrieval, etc.



BYOA

Bring Your Own
Appetizer



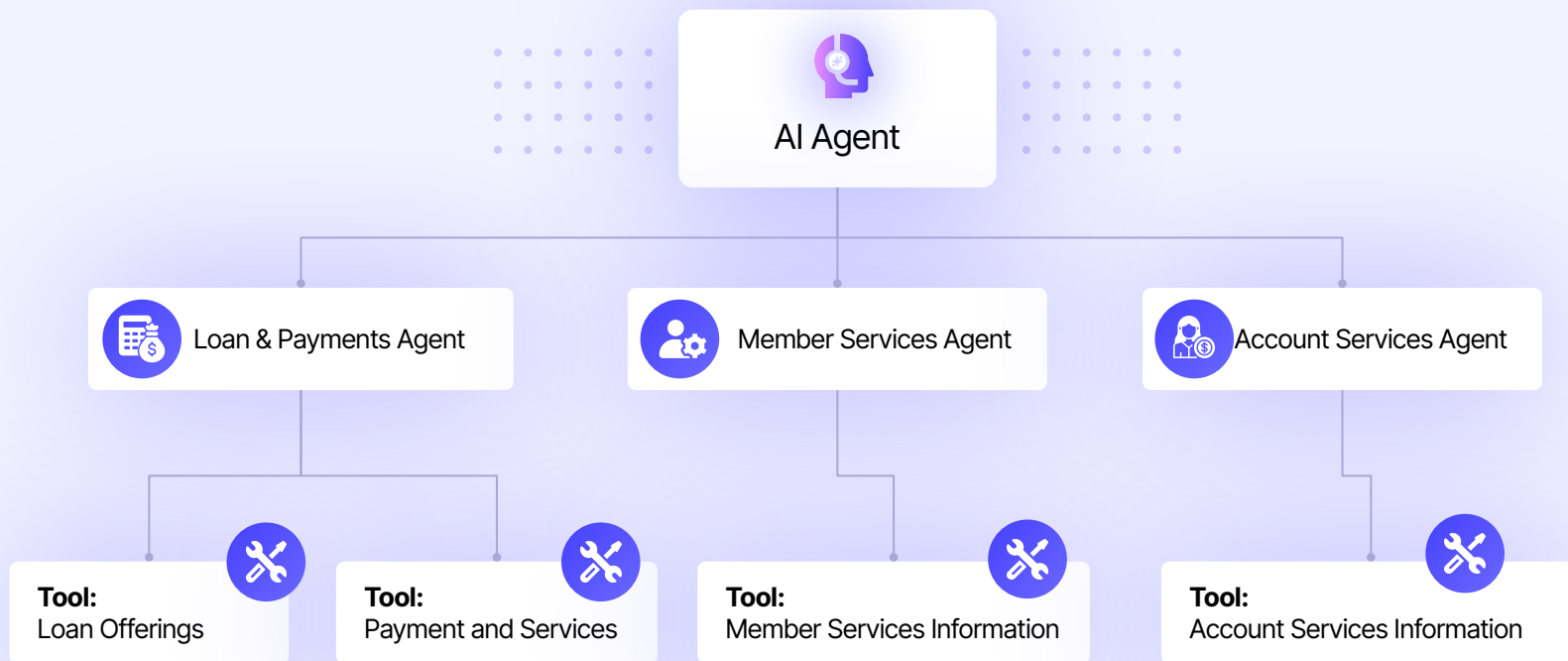
BYOA

A stands for "Assistant"..



Revision time!





AI Assistant

Ask AI Assistant →

Knowledge

Starred

History

Groups Access ⓘ

All Knowledge Group

General Policies

Lending Team

AJ Test Group

Ask AI Assistant

The AI Assistant is your go-to resource for navigating credit union policies and procedures. It provides quick, accurate answers to your questions, helps you stay compliant, and offers tailored guidance...

Select an assistant or type @ to select a different assistant



AI Assistant



Document



Default



AI Assistant is capable of answering any queries within the scope of documents uploaded. For further information contact your supervisor.



Conversations

Steve Kamath +1 669-309-2719

Saahil Kamath (Agent) Complete

Conversations Workflows Co-browse Consumer details

Preferred Language : English

Saahil Kamath (Agent) (You)
Thank you, Steve!
Could you also provide your email?
Translate to English 9:12 AM

Steve Kamath
Steve@eltpoxy.com
Translate to English 9:15 AM

Saahil Kamath (Agent) (You)
World's Best CU: Dear Steve K, in order to resolve your auto-loan account issues, please click on the link here:
<https://saahil.eltpoxy.com/sh/zHbKbl>.
Reply STOP to opt-out of these messages.
Translate to English 9:15 AM

Text

Type your message | Tip: Press Enter to send the message or Shift + Enter to switch to a new line | Max 1000 characters

Transfer English AI Compose

Conversations

Inbox

Departments

Chat (0)

Text (1)

SK

Steve Kamath

Mientras investigamos la...

Central...

3m

Steve Kamath

+1 669-309-2719

SK

Saahil Kamath (Agent)

Complete

Conversations

Workflows

Co-browse

Consumer details

Preferred Language : English

Steve Kamath

Will this account still be considered past you while the dispute is under investigation?

Translate to English

9:18 AM

Steve Kamath

I lost my job, but Support, can you offer me?

Translate to English

9:18 AM

Steve Kamath

How will a settlement affect my credit report?

Translate to English

9:19 AM

Steve Kamath

Will this account continue to be considered overdue while the dispute is under investigation?

Show Original Message

9:23 AM

Text

Click Shift + Enter to add a new line.

Yes, the account will be placed in a temporary hold status while the dispute is investigated.

Transfer

Aa

English

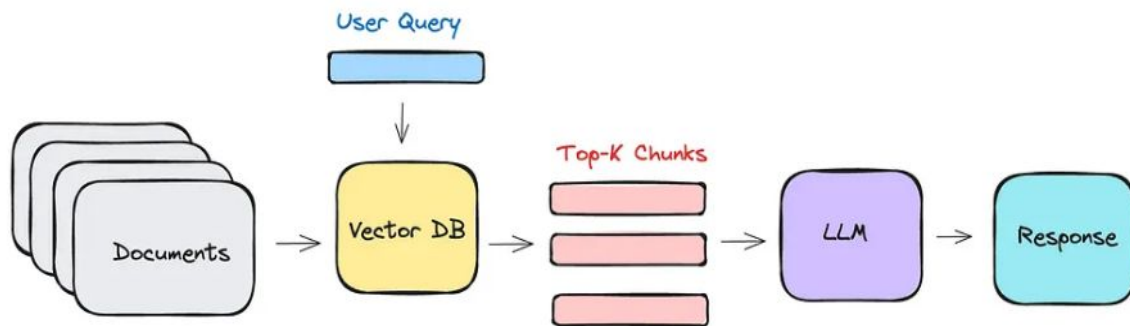
AI Compose

How does it all work?



RAG

Basic RAG Pipeline

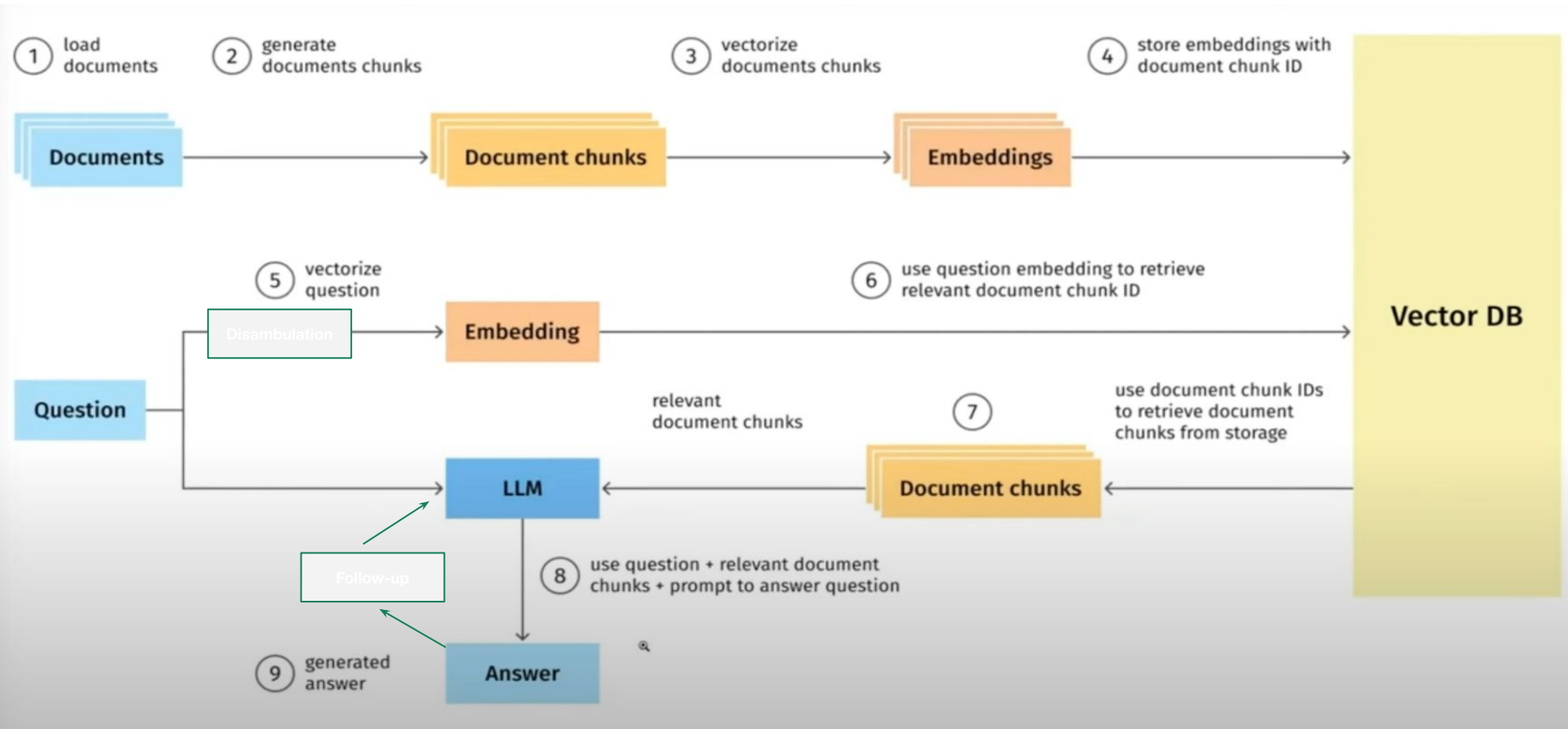


Step 1: Data Indexing

Step 2: Data Retrieval & Generation

Basic RAG Pipeline consists of 2 parts: Data Indexing and Data Retrieval & Generation

Knowledge Retriever Architecture



Knowledge In, Answer out?

Best practices

Avoid Large PDFs: **"Divide to Conquer"**

Use Simple Text Formatting: **"Text Talks"**

Maintain Clear Structure: **"Structure = Strength"**

Table Formatting: **"Keep Data Table Tidy"**

Eliminate Duplicate Content: **"One Truth, One File"**

Grouping of similar topics: **"Stack the Facts"**



BAD DOCUMENT

You request a list of seniors who can speak Spanish and the computer prints it out. You seat yourself at a console and in seconds you see on a TV screen before you a student's permanent record which had been updated electronically on videotape only moments before. With the touch of a button you have a transcript on paper. These examples may seem poles apart but they are all within the spectrum of "information storage and retrieval" when the term is loosely applied. It is within this broad concept of information retrieval that your committee on New Developments and Techniques has asked me to address my remarks. So let's begin with the storage and retrieval of hard copy--"paper" as we used to call it. **HARD COPY STORAGE AND RETRIEVAL** The data assembled and filed by admissions and registrars offices might be classified as entrance data, student description data, historical academic data, and statistical data. Every office will have its own groupings of files and arrangements under which to store this data, but this paper assumes that the following five files are typical: 1. Admissions Files. Include applications for admissions and all supporting papers and evaluation work sheets. One file folder for each applicant. May be consolidated with registration papers upon registration of the applicants. 2. Admissions Reference Card Files. Contain limited entrance and student identification information. 3. Registration Case Files. Contain most or all of the admission papers, supplemented by registration and other information about the student since his enrollment, other than his permanent record. One file folder for each applicant. Approved For Release 2001/03/02 : CIA-RDP74-00005R000200080057-3 4. Permanent Record Files. Historical record of courses taken and grades received. One or several letter size sheets per student serving as the source of transcript information. 5. Statistical Files. Computer print-outs or other statistical tabulations and reports, filed by subject. Of course there will be other files such as registration card files, general administrative subject files, class rosters, final class lists, and others. But the five are presumed to be the most typical and basic of the records maintained, and it is in this context that the comments in this paper are made. Misfiles Audits have shown that the typical office struggles along with nearly 3 percent of its papers or folders physically misfiled. This is too high. How much lower the figure should be depends on the kind of file involved and the impact of "can't find" and delayed findings. For the files in question, there is little excuse for misfiles of more than 1/2 of 1 percent. If it is higher, check first to see if you have fixed responsibility on someone for the files and barred all others from pulling or replacing folders or papers in the file. Too many cooks spoil the broth in filing as well as in cooking. Misfiles can also be substantially reduced and retrieval made more certain by a variety of techniques we will discuss. Time Required In most subject files, it should normally take no more than 2 to 3 minutes to locate any item requested from the file. In case or card files arranged in name or number sequence, the figure should be scaled down to less than a minute depending on the proximity and size of the file and the finding aids employed. Parenthetically, we might note here that only the most expensive automated systems are faster than manual retrieval systems when the object is to find a folder by name or number, if the name or number is known at the outset. Filing Arrangements The most common filing arrangements are by name, number, or subject. The rule for selection is simple--file by the feature most often known when the records are needed. The users are more likely to know the student's name than his identification number, then file by surname. To take care of those instances, if numerous, in which the number is known but not the exact name, you may need an "Index" in number sequence. Our rule, to file by the feature most often known, is simple and logical, but it is surprising how many people have been persuaded to file by number because they have heard that it is faster and more. Approved For Release 2001/03/02 : CIA-RDP74-00005R000200080057-3



GOOD DOCUMENT

3.5.6.2 Indefinite Articles

Use the customary pronunciation of the abbreviation to determine which [indefinite article](#) to use: *a* or *an*.

- Use *a* before an abbreviation (or any word) that begins with a consonant sound. For example, write "a RID" (an acronym pronounced as "rid") or "a GSE requirement" (an initialism pronounced by saying each letter).
- Use *an* before an abbreviation (or any word) that begins with a vowel sound. For example, write "an ANSI standard" (an acronym pronounced as "an-se") or "an LRU" (an initialism pronounced by saying each letter).

3.5.7 Periods, Spaces, and Mixed Cases with Abbreviations

Observe the following conventions for [periods](#), spaces, and mixed cases with abbreviations:

- Write most initialisms and [contractions](#) without periods or spaces, but because exceptions exist, follow the guidance of the authority that presides over the particular abbreviation. The organization's website is often a good source. Noteworthy exceptions are *Certificate of Compliance* (or *Certificate of Conformance*), which is usually abbreviated as *C of C*; *Page and Pages*, which are abbreviated as *p.* and *pp.*, respectively; and *United States*, which is always abbreviated as *U.S.*
- With the exception of *inch*, **don't** add a period to abbreviations of units of measure. The use of a period is essential for avoiding a miscue between the abbreviation of *inch* and the word *in*, as in the following: "Use a 3 in. test strip in the first run. Increase the length to 4 in. in the second run." Omit the period when you abbreviate *square inch* as *in²* or *cubic inch* as *in³*.
- Try to reflect mixed-case abbreviations (those that combine uppercase and lowercase letters) accurately. Try to avoid starting a sentence with an abbreviation that begins with a lowercase letter.



A white arrow originates from the top-left corner of the slide and points towards the "Wifi:" text.

Wifi: **IHG ONE REWARDS**

Password: **ENCORE**

Domain: **wbcu.eltropy.com**

Time to Build!



Knowledge

- Loan Policies and procedures
- Account services and procedures
- HR policies
- IT policies



Time to Test!



Prompt Engineering

- Prompt engineering means **finding the best way to phrase your request to an AI** so it understands what you want and provides a helpful answer.
- Well-crafted prompts lead to better results because **clear instructions help the AI give you exactly what you need** and save time.

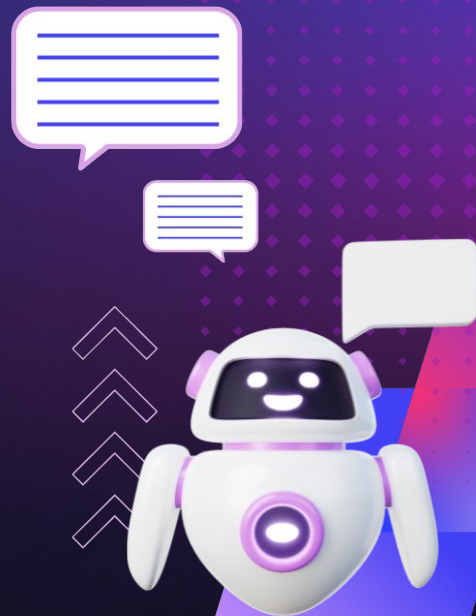


Prompt Engineering

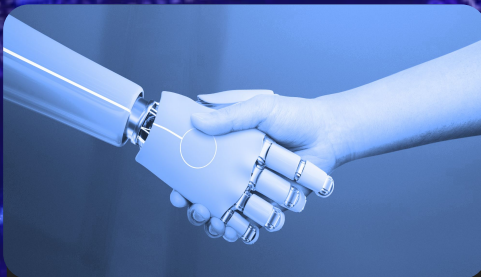
Zero shot prompting

Few shot prompting

Chain of thought prompting



Conversational Intelligence



Supercharge
Intelligence




















































































Interaction List

Observatory

Eleveo (Cisco Call Manager)

Analytics

 Export data Choose date range

	Start time	Queue/Department	Contact info	Handled by	Status	Interaction Id	Conversation Id	AI Score	Alerts	Survey score	Stats
 	09/24/24 01:10:33 PM	Loans and Lending	Collin	 Ishank Vaish	Closed	 	 	6/10 		5/5	 
 	09/20/24 09:43:01 AM	Loans and Lending	Collin	 Agent Demo	Closed	 	 	8/10 	--	--	 
 	09/20/24 09:26:20 AM	Loans and Lending	Collin	 Agent Demo	Closed	 	 	6/10 		--	 
 	09/20/24 12:23:15 AM	Loans and Lending	Collin	 Ishank Vaish	Closed	 	 	0/10 	--	--	 
 	09/20/24 12:19:57 AM	Loans and Lending	Collin	 Ishank Vaish	Closed	 	 	0/10 	--	--	 
 	09/20/24 12:14:34 AM	Loans and Lending	Collin	 Ishank Vaish	Closed	 	 	8/10 		--	 
 	09/20/24 12:06:23 AM	Loans and Lending	Collin	 Agent Demo	Closed	 	 	5/10 	--	--	 
 	09/19/24 11:58:03 PM	Loans and Lending	Collin	 Agent Demo	Closed	 	 	5/10 	--	--	 



The word "Safe" is written in a large, white, serif font. To its right, the letters "AI" are rendered in a large, 3D, isometric style with a blue-to-purple gradient. A thin white line with a small arrowhead points towards the "S" in "Safe".

Safe AI

Responsible use of AI

SafeAI Strategy for every Stakeholder

Developing Responsible AI applications while understanding the

Risks, Limitation & Unintended consequences.



Risks, limitations & unintended consequences

Content
Filtering and
Moderation



Bias Detection



Ethical
Guardrails



User Feedback
and Iteration



Privacy
Protection



Fairness and
Diversity Risk



Contextual
Awareness Risk



Control
Interfaces



Legal and
Regulatory



Continuous
Monitoring and
Improvement



What is SafeAI

SafeAI is about mitigating risks, ensuring compliance and be able to provide business value.



SafeAI

Safe AI Framework

A thin white vertical line with a small dot at the bottom, connecting the title to the four pillars below.

Transparency



Fairness

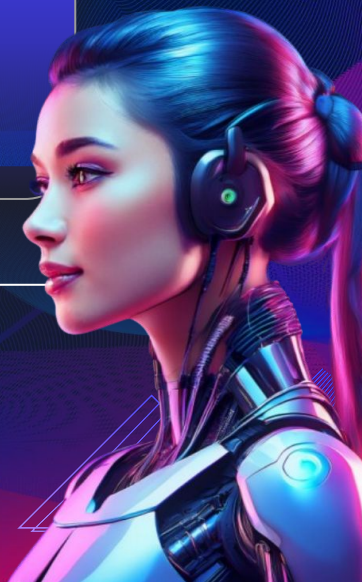


Accountability



Privacy

Powering Responsible AI

A thin white vertical line with a small dot at the top, extending from the text area down to the bottom of the slide.

AI Guardrails



Product Positioning Layer



Application Design Layer



Programmable Guardrail Layer



Model Layer

Risk Mitigation

Usage and best practices guide
Limitations and Usage Policy
User Responsibility

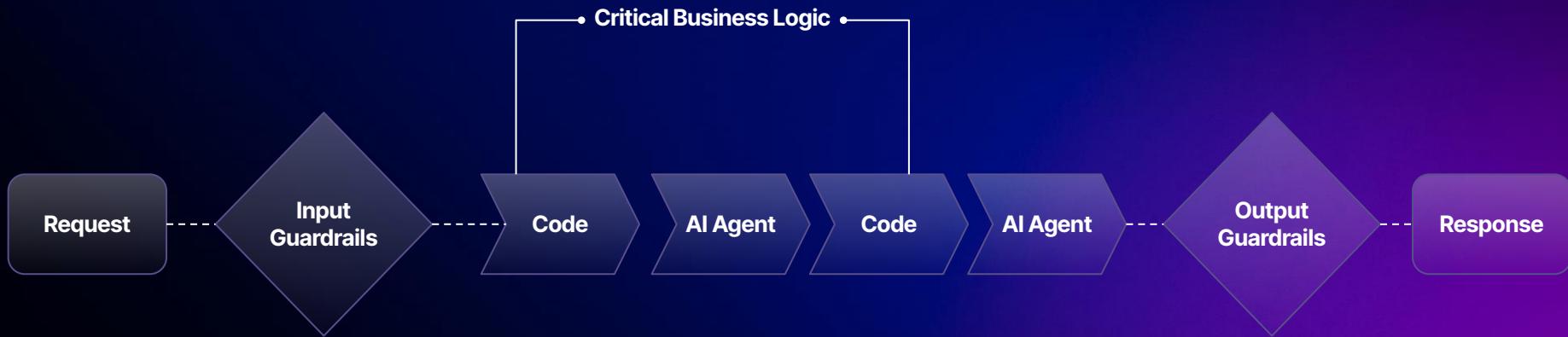
Disambiguation, Augmentation over Automation
Human Feedback Mechanism
Provide Citations

PII redaction, Profanity Detection
Deny Harmful/ Non Relevant Topics
Output Relevancy Checks
Mitigate Prompt Injection

Harmful Content Filters, Bias Mitigation.
Measures taken to reduce Hallucinations
Fine Tuning and Alignment Process

Constrained Agents (Programmable Guardrail)

Safe AI ensures that our agents are designed with certain constraints in mind ensuring critical parts of the flow like authentication, escalations are handled outside of the AI Agent Scope



Safe 

Grounding (Application Design Guardrail)

Ensuring it is used in a factually verifiable domain



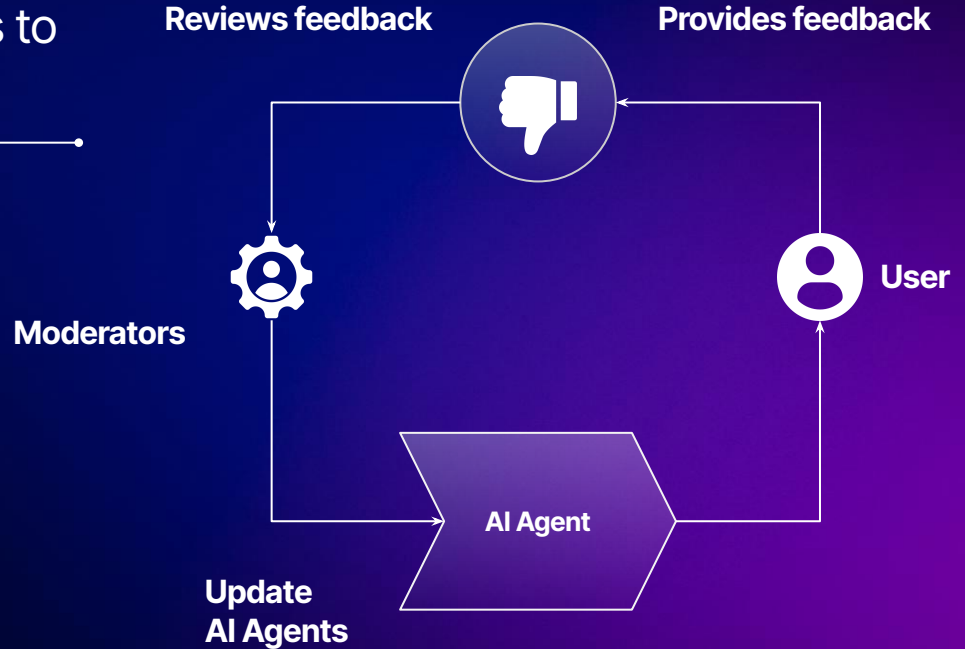
Safe

Feedback (Application Design Guardrail)

Ensure that the users are aware they are interacting with an AI Agent

Provide an easy mechanism for users to provide feedback

Provide a mechanism to escalate (where applicable)

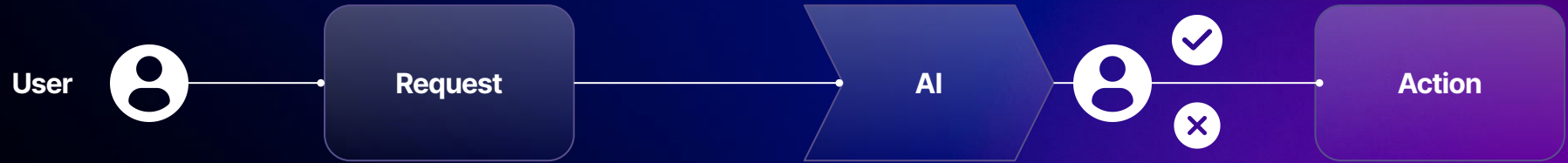


Safe 

Human in the loop (Application Design Guardrail)

Ensure that humans are always kept in loop with AI.

AI systems will be designed to assist users take a decision and will not be allowed to take a decision without explicit consent from the user.



Safe 

AI Guardrails

Bring Responsible AI to Life



Safe

Unified Conversations Platform

Intelligence

AI Intelligence & Analytics

Automation

AI Agents (Digital & Voice) & AI Assistants

Communication

Video, Text, Chat, Voice, Co-browse



**Safe AI
Framework
& Guardrails**



**Compliance
& Security**



Workflows

Integrations



Core



Lending



Collections



AOS



Marketing



Call Center



CRM



Q&A