

CREATE YOUR OWN PRIVATE GPT





ABOUT ME



- IAM Expert
- 9 Years Of Experience in Cyber Security
- Scripting Aficionado
- AI Hobbyist



**HOW MANY
OF YOU USE
CHAT GPT?**





**HOW MANY
OF YOU HATE
CHAT GPT?**



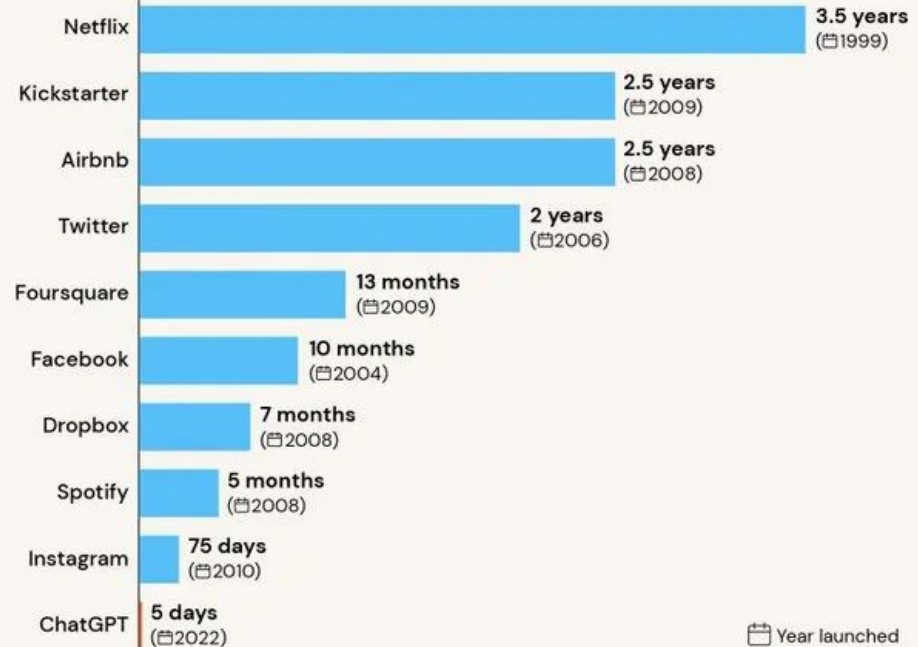
GROWTH & POPULARITY



Released in 2022

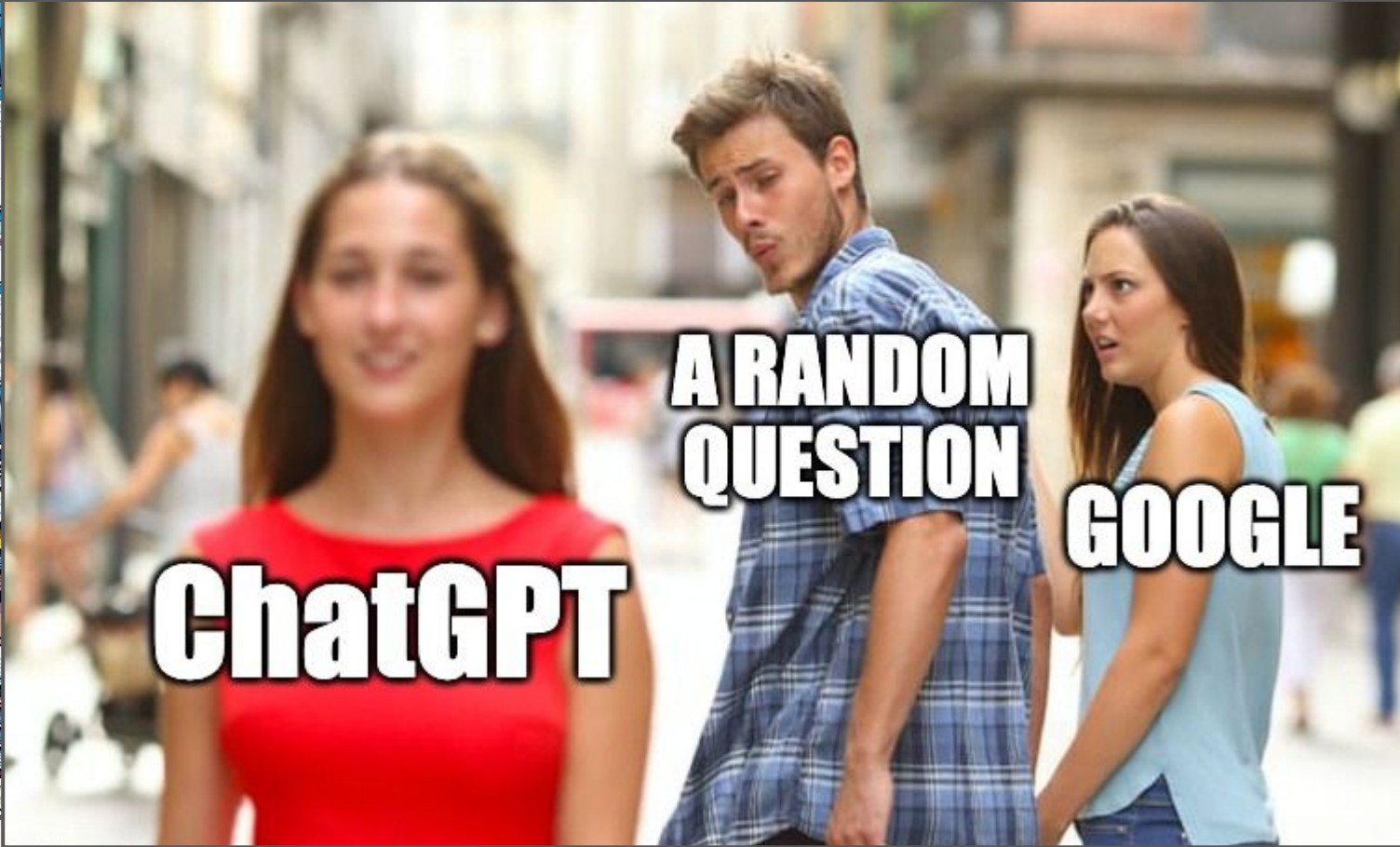
Released to general public on Nov 30 2022, having worked on it since **2018**

1 Million users in 5 days





**WHAT MAKES IT SO
POPULAR?**



ChatGPT

**A RANDOM
QUESTION**

GOOGLE





P You
can you breakdown thi

[a-z0-9!#\$%&'*/=?^`{|}~-]+(?:\.

P You
can you breakdown how chatgpt works?

CAN YOU FIGURE OUT WHAT DOES THIS REGEX DO?

```
/(?:[a-z0-9!#$%&'*/=?^`{|}~-]+(?:\.|(?!\.)(?:[a-z0-9!#$%&'*/=?^`{|}~-]+)*|"(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.|(?:[a-z0-9-]*[a-z0-9])?|\[(?:(?25[0-5]|2[0-4][0-9]||01?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]||01?[0-9][0-9]?)|[a-z0-9-]*[a-z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+\.)\)/i
```

including ASCII control characters and escaping for characters. This allows for special characters and spaces in the local part when quoted.

3. '@' **Symbol:** This is the literal at symbol '@' that separates the local part of the email from the domain part.

your question or continue the conversation. It's like making a mini-puzzle each time it replies to you.

5. **Learning from Feedback:** Just as a puzzle solver gets better with practice, ChatGPT learns from the interactions it has. If it makes mistakes or gets new information, it uses that to improve how it

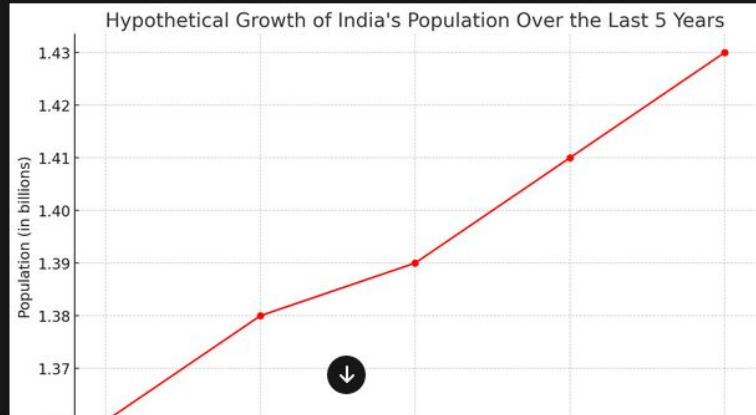
ChatGPT

To analyze the growth of India's population over the last 5 years and present it in a graph, we'll use hypothetical data. Real population growth can be influenced by various factors, including birth rates, death rates, and migration patterns. The actual data would be available from official sources like the World Bank, the United Nations, or India's Office of the Registrar General & Census Commissioner.

Let's assume the following hypothetical population figures for India from the last 5 years:

- 2019: 1.36 billion
- 2020: 1.38 billion
- 2021: 1.39 billion
- 2022: 1.41 billion
- 2023: 1.43 billion

Now, let's create a graph to visually represent this growth.



ChatGPT

To analyze and showcase the growth of ChatGPT, we can consider various metrics such as user base growth, the number of interactions over time, or the expansion of its capabilities and features. Since I don't have access to real-time or specific proprietary data about ChatGPT's growth, I'll create a hypothetical example to illustrate how one might visualize the growth of ChatGPT using user base growth as the metric.

Let's assume the following hypothetical data points representing the number of users (in millions) at different points in time since ChatGPT's launch:

- Month 1: 1 million users
- Month 2: 2 million users
- Month 3: 4 million users
- Month 4: 7 million users
- Month 5: 12 million users
- Month 6: 20 million users

Now, I'll create a graph to visually represent this growth.

Finished analyzing



WHY IS IT SO POPULAR?



SAVES YOU TIME

A GOOD LEARNING TOOL

HELPS YOU ANALYZE DATA

SPEEDY ANSWERS





WHAT ARE THE
DRAWBACKS?

Samsung announce
ChatGPT after the
uploaded sensitive

Goldman Sachs has restricted employees from using ChatGPT to
avoid compliance issues around

is from
accessible from
risk of losing

Apple said AI could lead to a potential leak of confidential data



Deutsche Bank
workpl:

Spotify has reportedly restricted its workers from using ChatGPT





AG

How many letters are there in the word "nineteen"?

Before Chat GPT

After Chat GPT



How recent is your training data?



My training data was collected and used to create my programming before September 2021. I do not have access to any new information or updates since that time and my knowledge is based on the data that was available at the time of my training. As a language model, I am not able to browse the internet or access new information, so I am unable to provide information about events or developments that have occurred after my training data was collected. However, I can provide general knowledge and information about a wide range of topics that were current at the time of my training. If you have any specific questions, please don't hesitate to ask and I will do my best to provide helpful and accurate information.





ChatGPT-maker OpenAI accused of string of data protection breaches in GDPR complaint filed by privacy researcher

Natasha Lomas @riptari / 10:31 PM GMT+5:30 • August 30, 2023

Comment

sed

edit

LEAD LATER



WHAT ARE THE DRAWBACKS?



COMPLIANCE

DATA PRIVACY

LESS CONTROL

INACCURATE INFORMATION

THE GOOD

SAVES YOU TIME

A GOOD LEARNING TOOL

HELPS YOU ANALYZE DATA

SPEEDY ANSWERS

THE BAD

COMPLIANCE

DATA PRIVACY

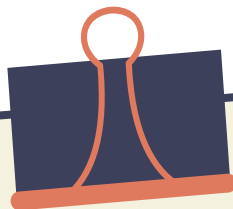
LESS CONTROL

INACCURATE INFORMATION





01



**HOW DO WE
LEVERAGE THIS FOR
TEAMS & CUSTOMERS?**



POTENTIAL USE-CASES

**SEARCHABLE
DOCS AND
WIKIS**



**INTERNAL
LEARNING
TOOL**



**INTERNAL
TOOL FOR
DATA
ANALYSIS**



**AI DRIVEN
REPORTING
SYSTEM**



**LOW LEVEL
SUPPORT
BOT**





**HOW DO WE NOT
COMPROMISE WITH
SECURITY?**

02



RUN YOUR OWN PRIVATE GPT



**SO WHAT ARE OUR
OPTIONS?**

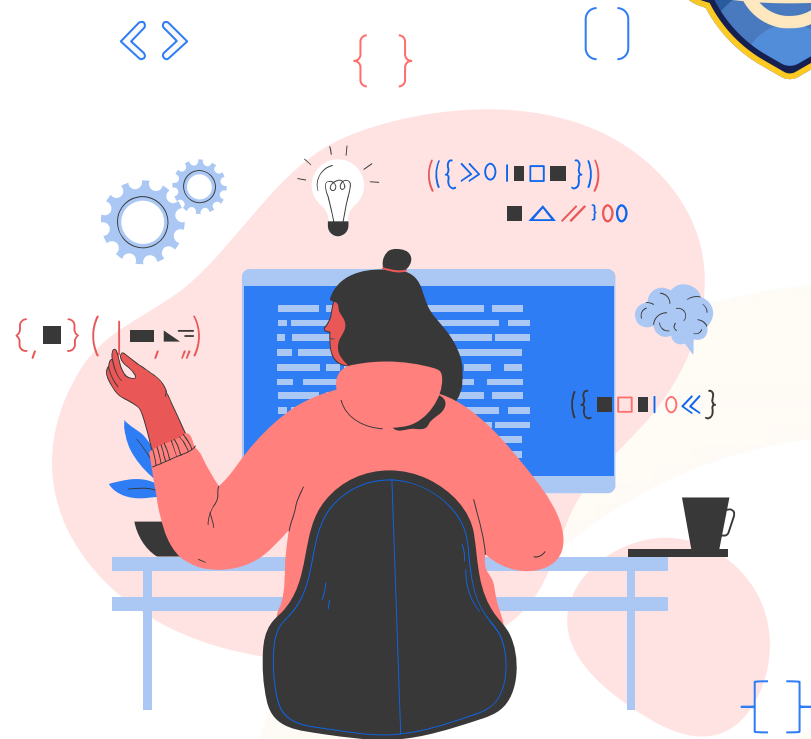


<https://t.ly/ox-qr>



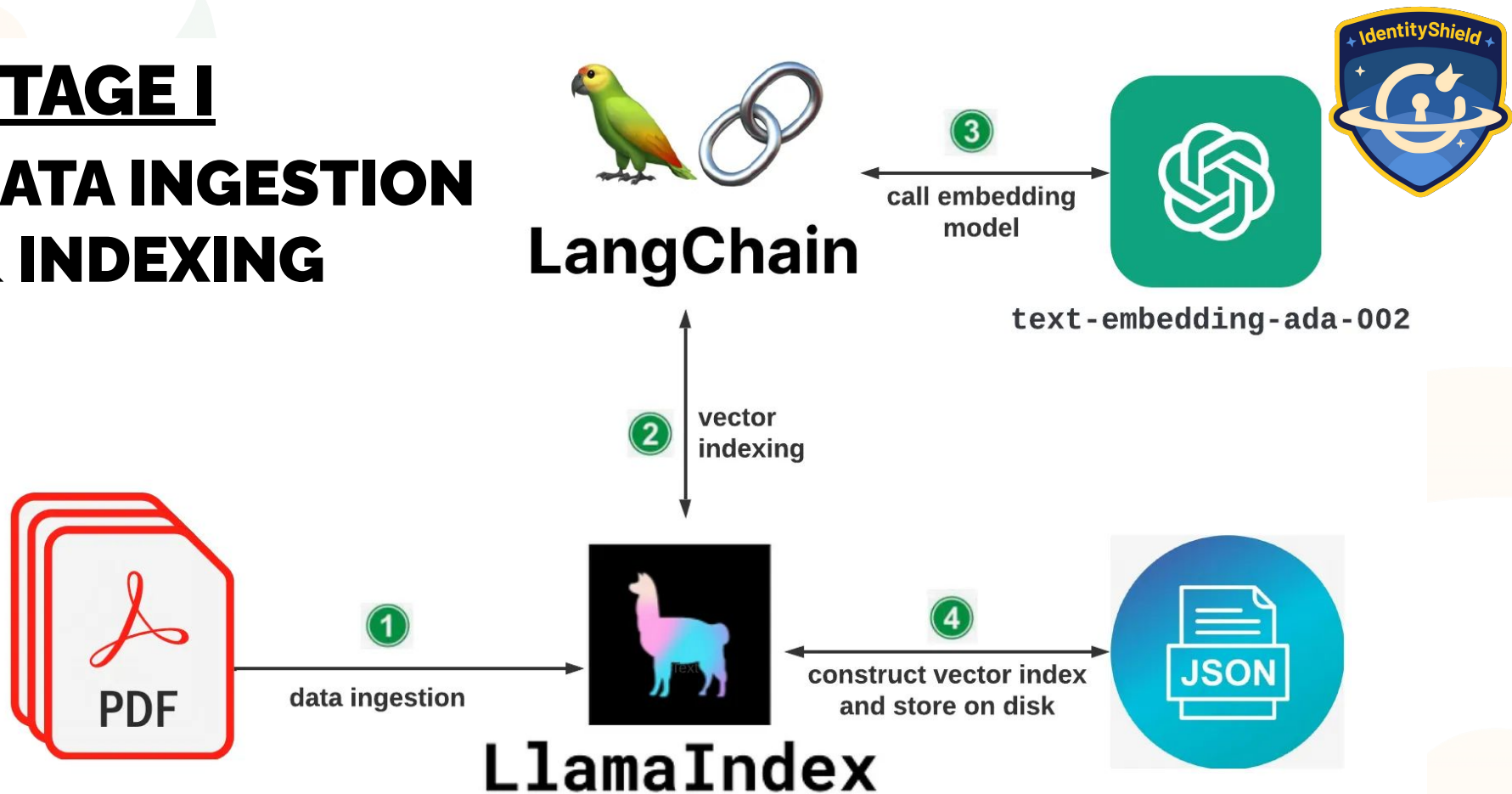


HOW DOES THIS WORK?



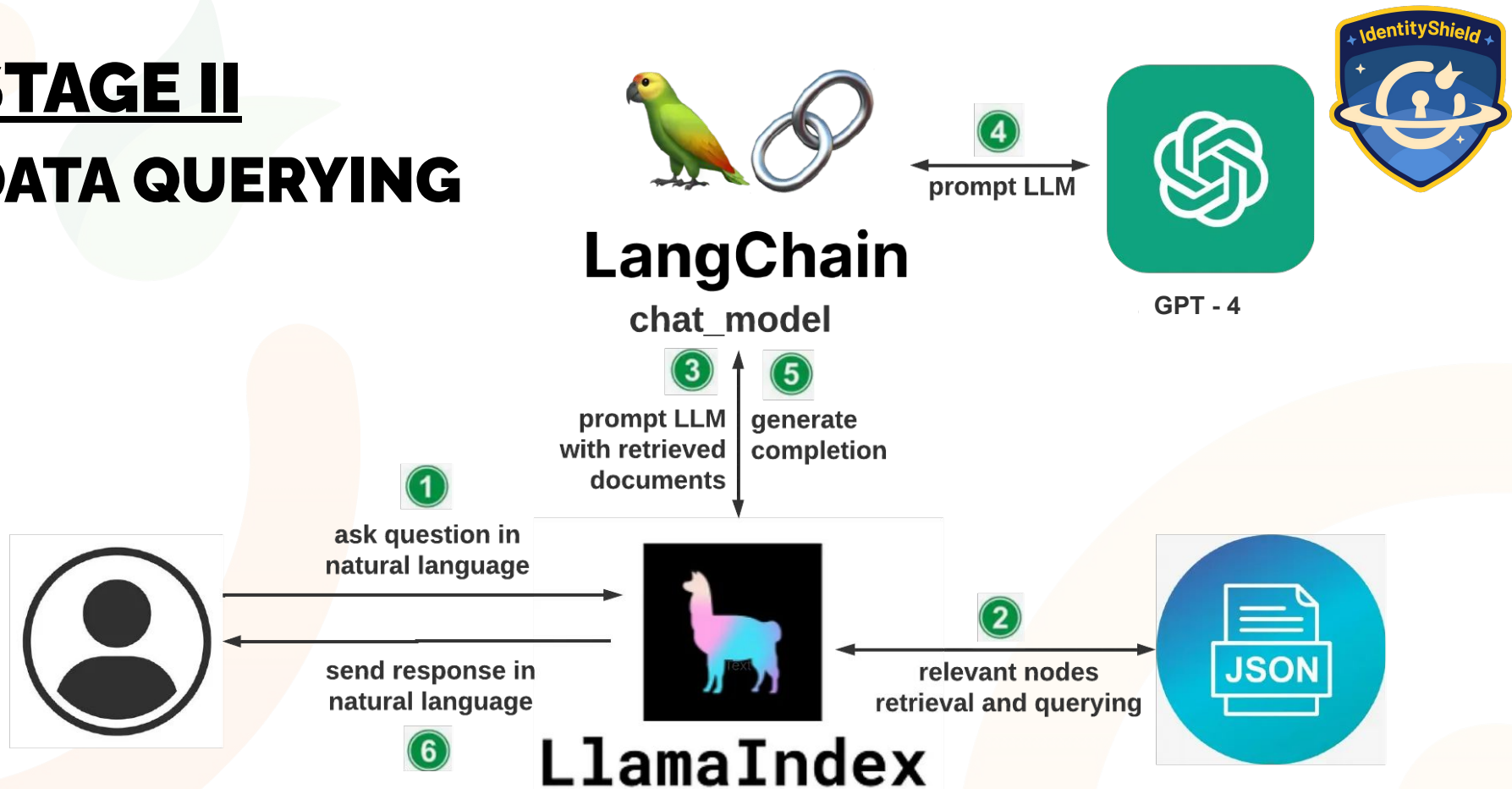
STAGE I

DATA INGESTION & INDEXING



STAGE II

DATA QUERYING





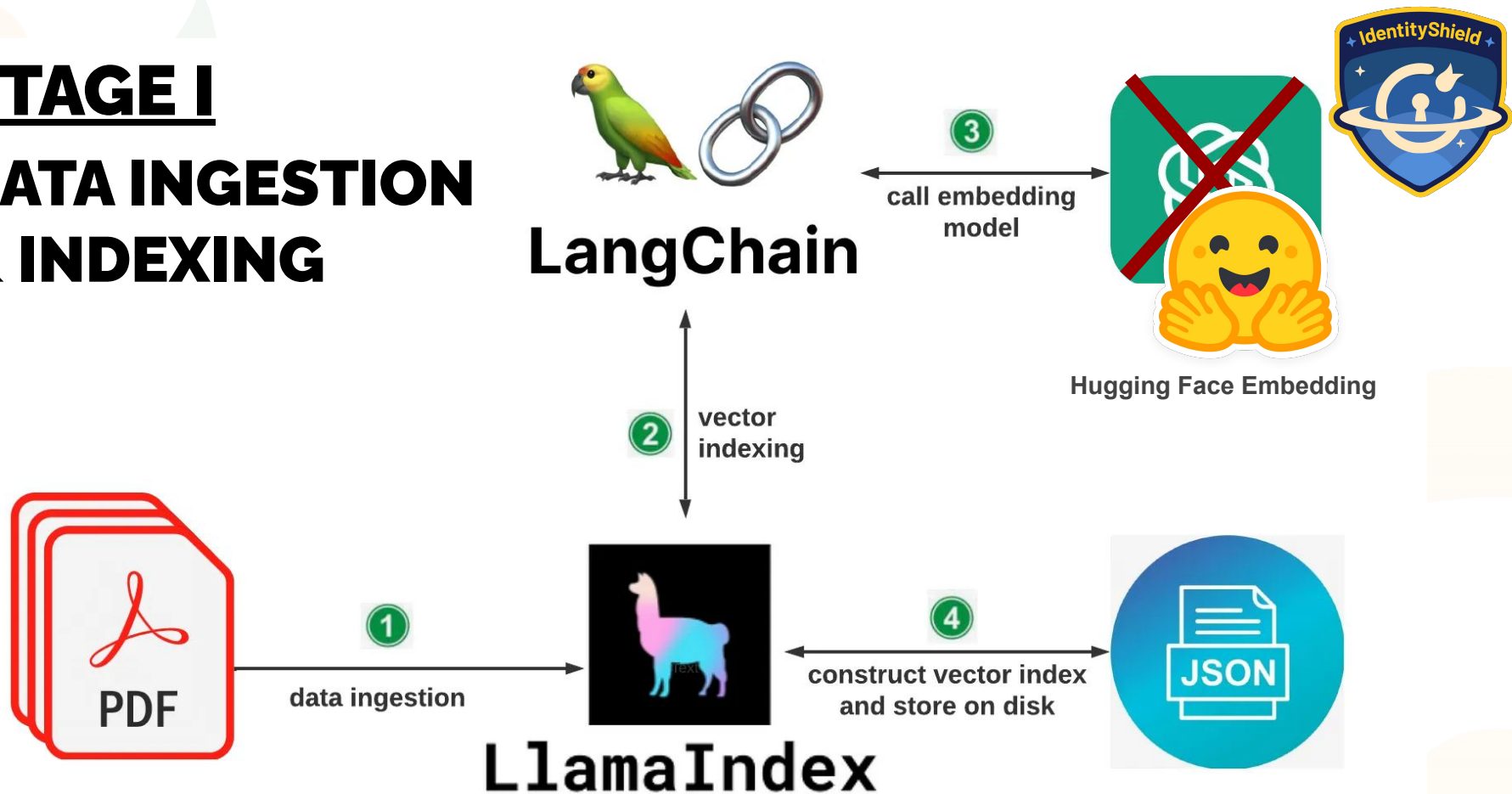
**WHOA!
HOLD IT**



**AREN'T WE USING OPENAI
CHATGPT IN THE BACKEND???**

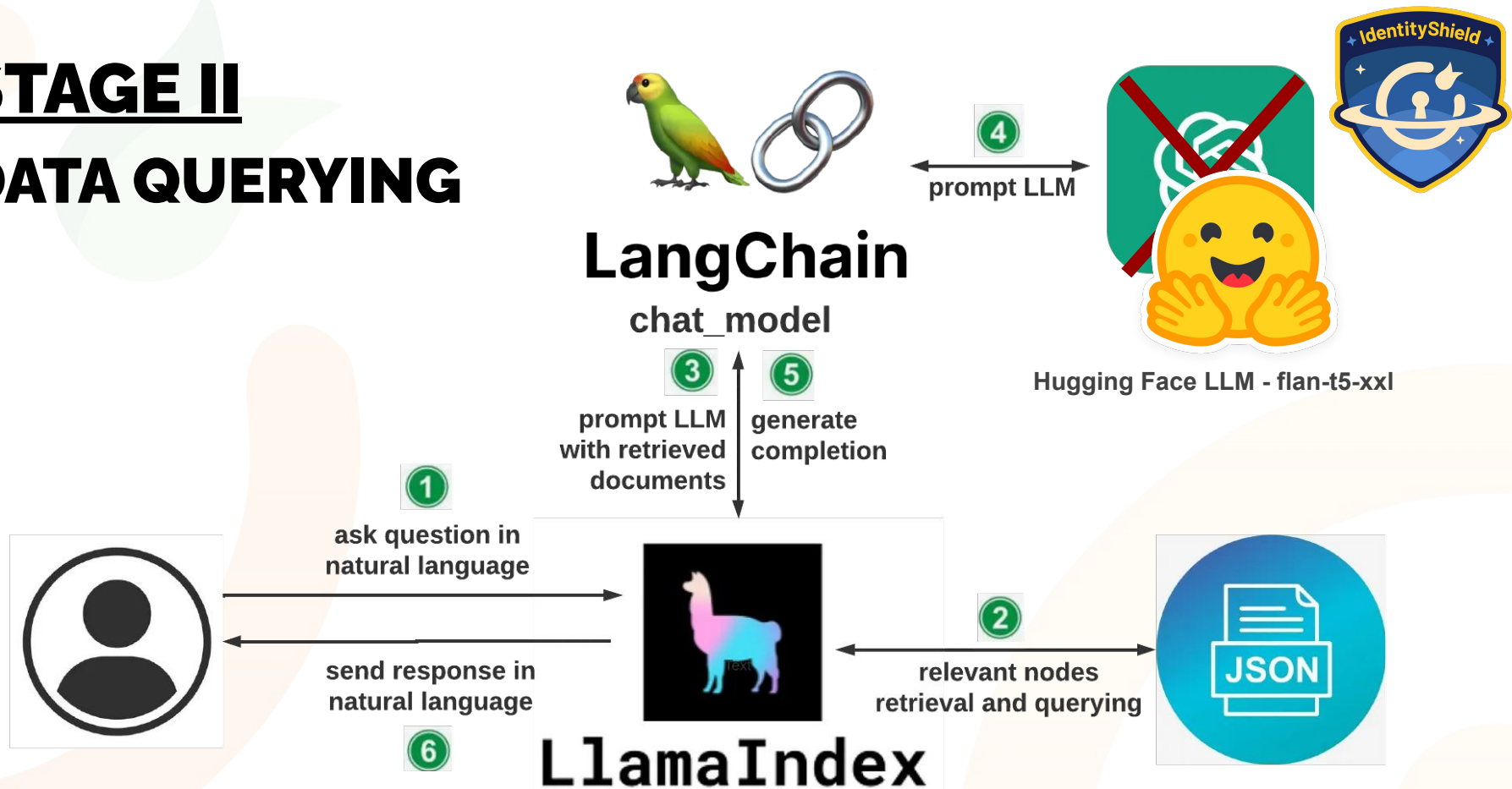
STAGE I

DATA INGESTION & INDEXING



STAGE II

DATA QUERYING





SUMMARY

- 1. BENEFITS AND DRAWBACKS OF CHATGPT**
- 2. HOW CAN WE LEVERAGE AI FOR BUSINESS**
- 3. HOW TO DEPLOY YOUR OWN CHATGPT SOLUTION**
- 4. OPTIONS AVAILABLE TODAY**
- 5. HOW DOES EACH SOLUTION WORK**
- 6. HOW DOES A PRIVATE GPT HELP WITH SECURITY**
- 7. TOOLS AND LIBRARIES AVAILABLE**



DO YOU HAVE ANY QUESTIONS?

✉ pratish@xecurify.com | www.miniorange.com

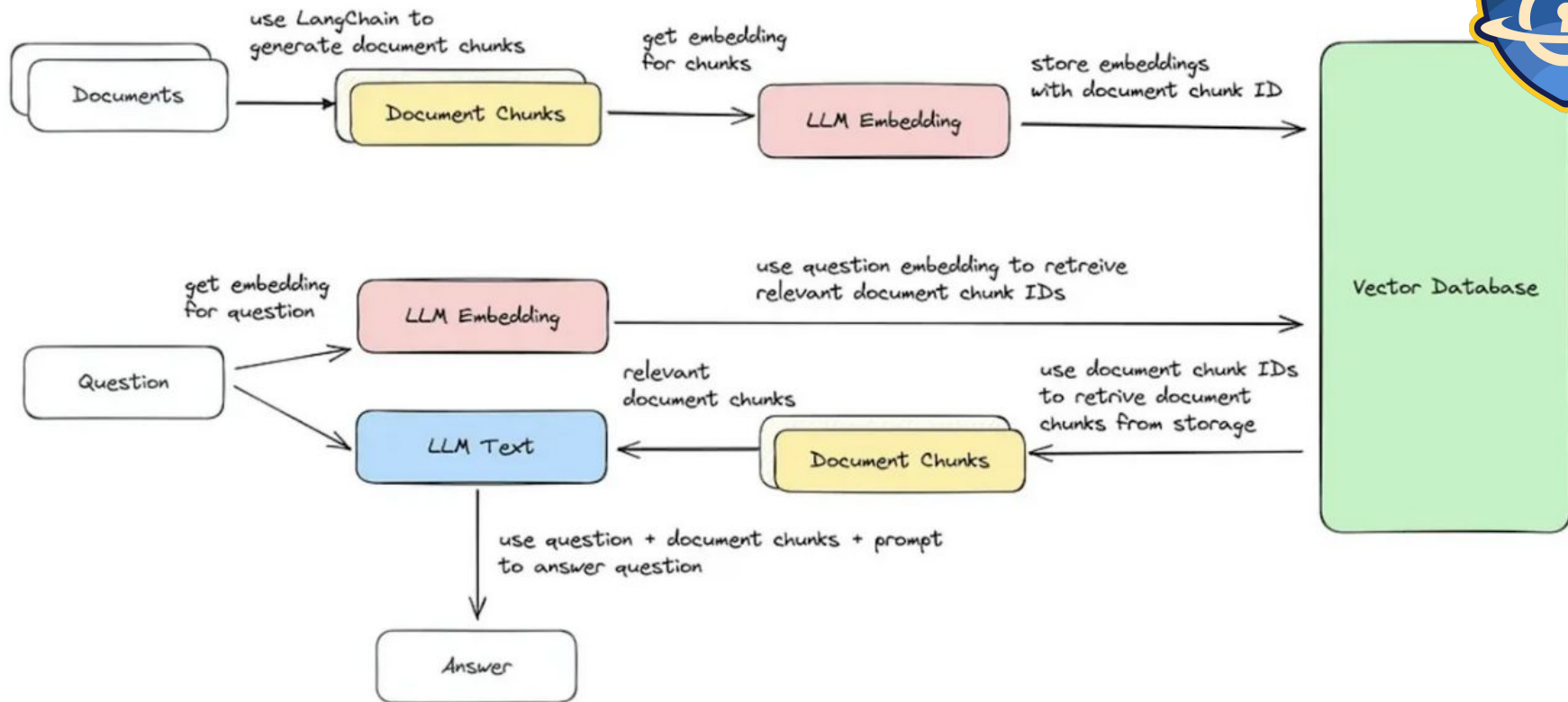
🔄 <https://github.com/frittlechasm>

🌐 <https://www.linkedin.com/in/pratish-ray/>

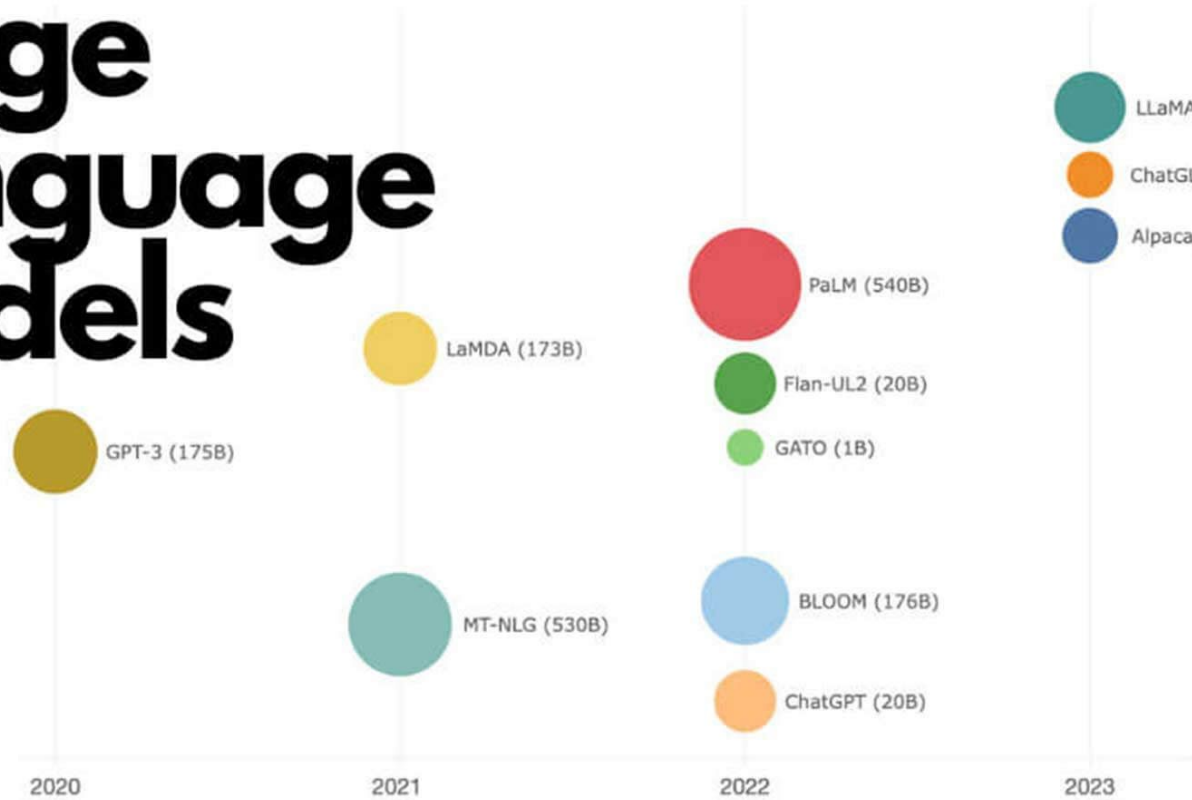
**THANK YOU
FOR BEING A
LOVELY AUDIENCE**

FEEDBACK





Top Large Language Models



- LLaMA (65B)
- ChatGLM (6B)
- Alpaca (7B)



Pros of Paid Service LLMs like OpenAI	Cons of Paid Service LLMs
High quality responses	Sensitive data can be exposed
Cost effective for low usage (1000-10000 requests per day)	Expensive for high usage (1M+ requests per day)
Minimal infrastructure setup	Prone to external service outages

Pros of Open-Source LLMs	Cons of Open-Source LLMs
Hosting on premises for sensitive data	Quality tends to be lower due to training limitations
Cost effective for high usage (1M+ requests per day)	Large initial costs – not ideal for low usage
Outages can be troubleshooted internally	Need to carefully consider infrastructure and scaling during setup



Key Factors to Look for in an LLM

PARAMETER SIZE



refers to the total number of learnable parameters in the AI model

CONTEXT WINDOW



refers to the number of tokens the model considers when predicting a specific token and the sequence of text

FOCUS AREA



refers to the specific domain or the subject of expertise of the model in which it is trained for providing solutions

CUSTOMIZATION



to choose and alter the model you see fit for your purpose

LICENSING



protects intellectual property rights, allows for commercialization, guarantees ethical usage, and supports customization

OFFERING



provides diverse ways to utilize your models