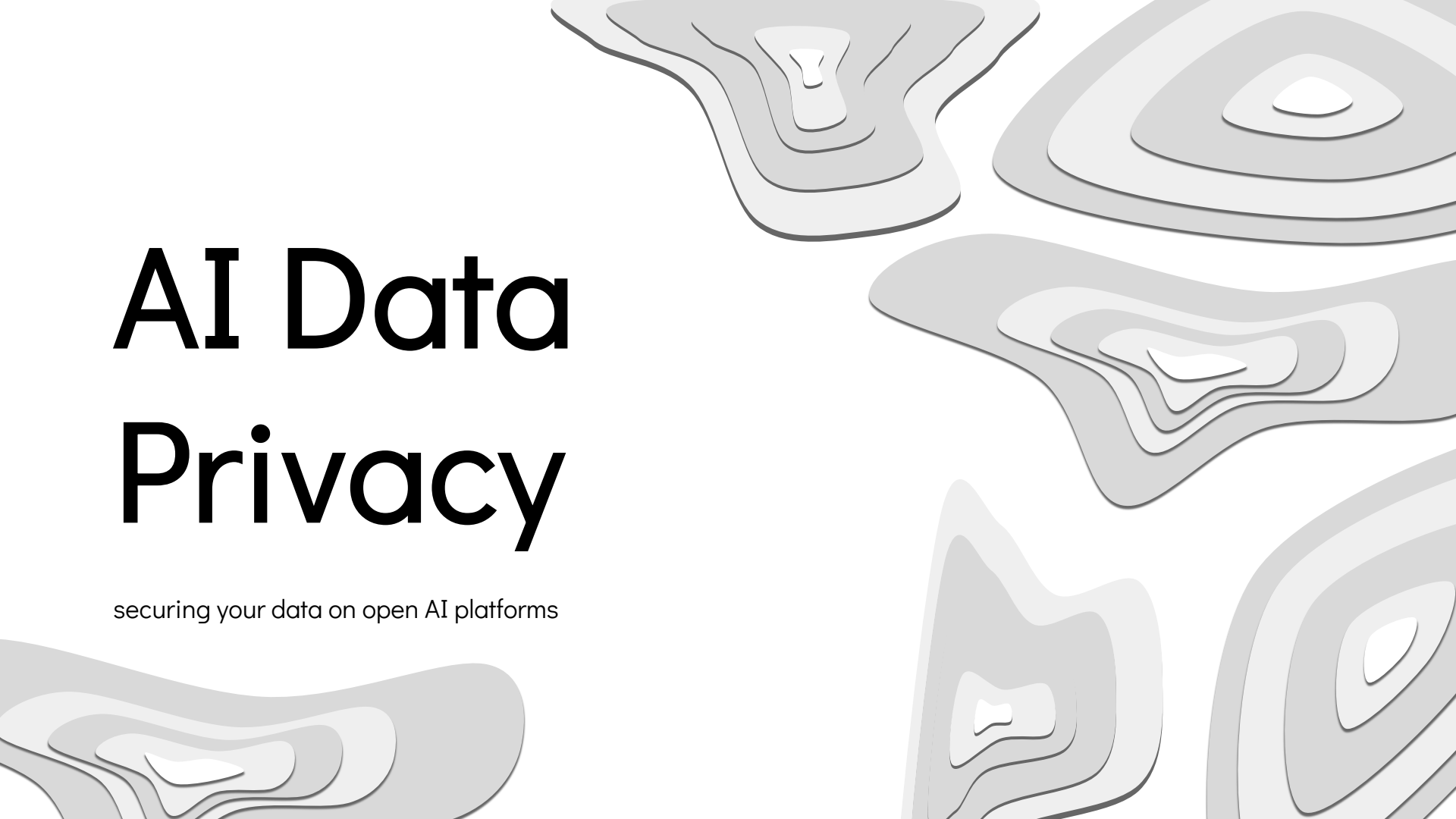


AI Data Privacy

securing your data on open AI platforms





AI Data Privacy

The landscape of AI data privacy constantly evolves due to technological advancements, new regulations, and changing consumer expectations, requiring continual adaptation and vigilance from businesses.

This presentation is focused on running LLMs in production environment.



Lwin Maung

[linkedin.com/in/lmaung](https://www.linkedin.com/in/lmaung)





Min Maung

[linkedin.com/in/minmaung](https://www.linkedin.com/in/minmaung)





TLDR;

Should I (or my organization) use publicly available products such as OpenAI? If so, how?

OK. No... Maybe... Sure... Why not?

Session Breakdown



Understanding AI

Technology behind AI and what does that mean?

Solutions


How can I protect the components?

(AI) Data Privacy

What components of AI need to protected?

Discussion, Q & A

Open discussion and questions and answers

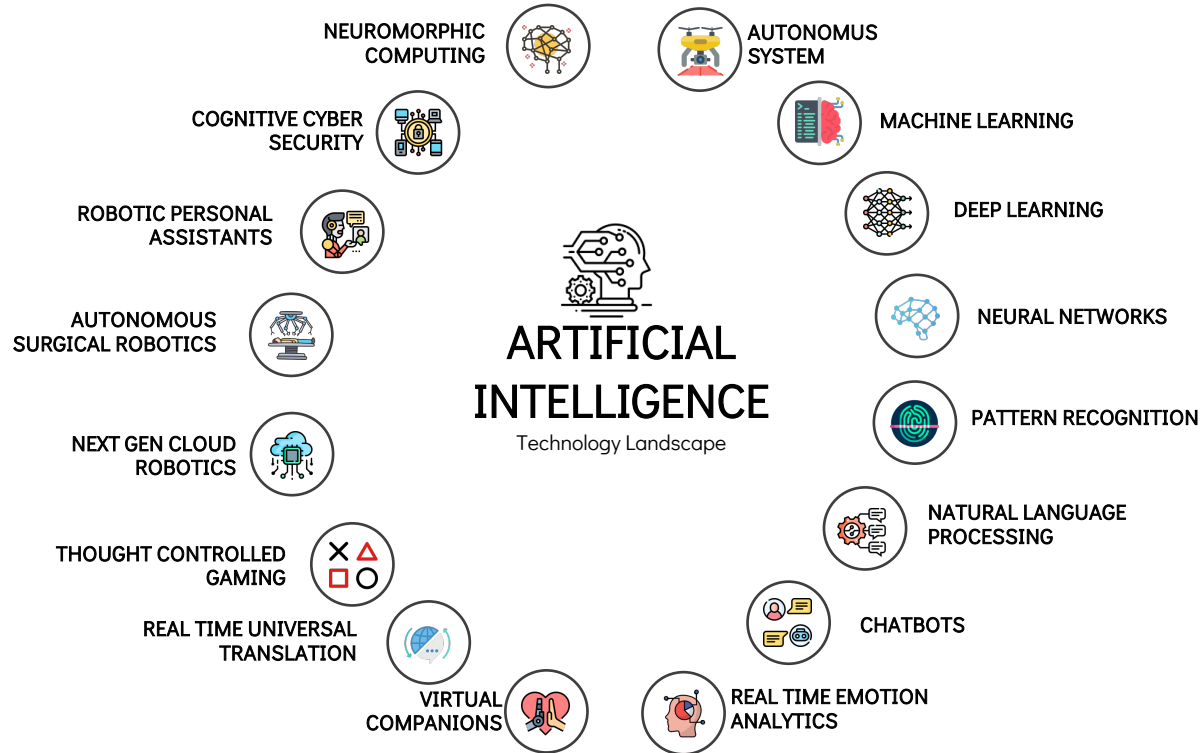




Understanding AI

.

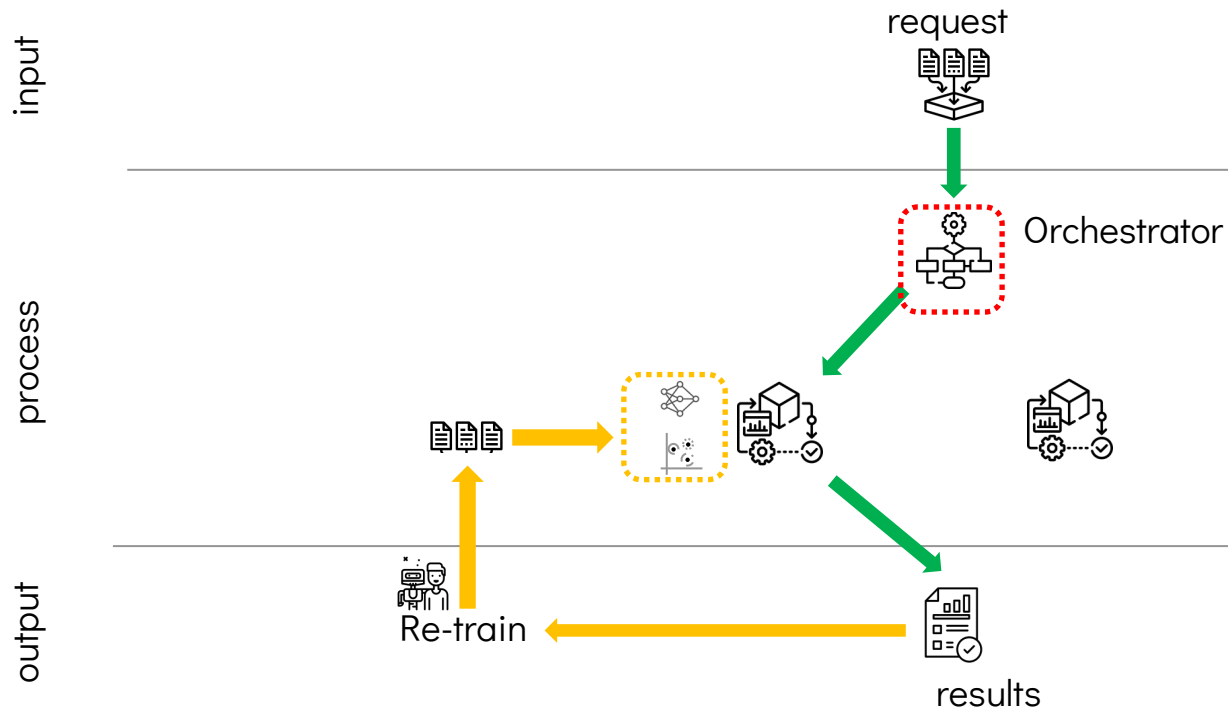
What is AI?



Who owns AI (and data)?



Data/Processing Flow



Mistakes were made

What data of ChatGPT was leaked?

The data that was leaked from ChatGPT due to a bug in the AI's source code included sensitive user data.

1. Chat Histories: A bug in ChatGPT's source code resulted in a breach of sensitive data, where unauthorized actors were able to view users' chat history due to a vulnerability in the Redis memory database used by OpenAI.
2. Users' Personal and Payment Information: The incident also exposed personal and payment data of approximately 1.2% of active ChatGPT Plus subscribers on a specific date (March 20th). This included:
 1. Names
 2. Email addresses
 3. Payment addresses
 4. Credit card types
 5. The last four digits of credit card numbers
 6. Potentially, the first message of a newly-created conversation if both users were active around the same time
3. Samsung's Confidential Data: Separate from the system vulnerability, Samsung employees reportedly shared confidential company information with ChatGPT. This included:
 1. Source code from a faulty semiconductor database
 2. Confidential code for a defective equipment issue
 3. An entire meeting transcript for the chatbot to create meeting minutes

[Home](#) > [News](#) > [Security](#)

Microsoft AI Employee Accidentally Leaks 38TB of Data

A software repository on GitHub dedicated to supplying open-source code and AI models for image recognition was left open to manipulation by bad actors thanks to an insecure URL.

Data leak reveals auto giant and others harvesting user data to train AI models

Van Mossel, the biggest auto dealer in Benelux, and other companies used the services of an obscure data analytics company to train AI models, which leaked their client data to anyone on the internet.

On February 1st, our research team uncovered a concerning misconfiguration on systems belonging to Rawdamental, a data collection and analysis company, that caused a leak of personal data.



(AI) Data Privacy

.

Privacy of my...

Intellectual Property



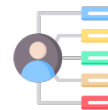
models
weights
vectors
orchestrations
machine (specs)

Data and Assets



training data
training assets
live data
raw data
user data

Client/User Privacy



CPRA
GDPR

DATA STEWARD / CDO



Breaking down tools

Intellectual Property



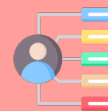
models
weights
vectors
orchestrations
machine (specs)

Data and Assets



training data
training assets
live data
raw data
user data

Client/User Privacy



CPRA
GDPR

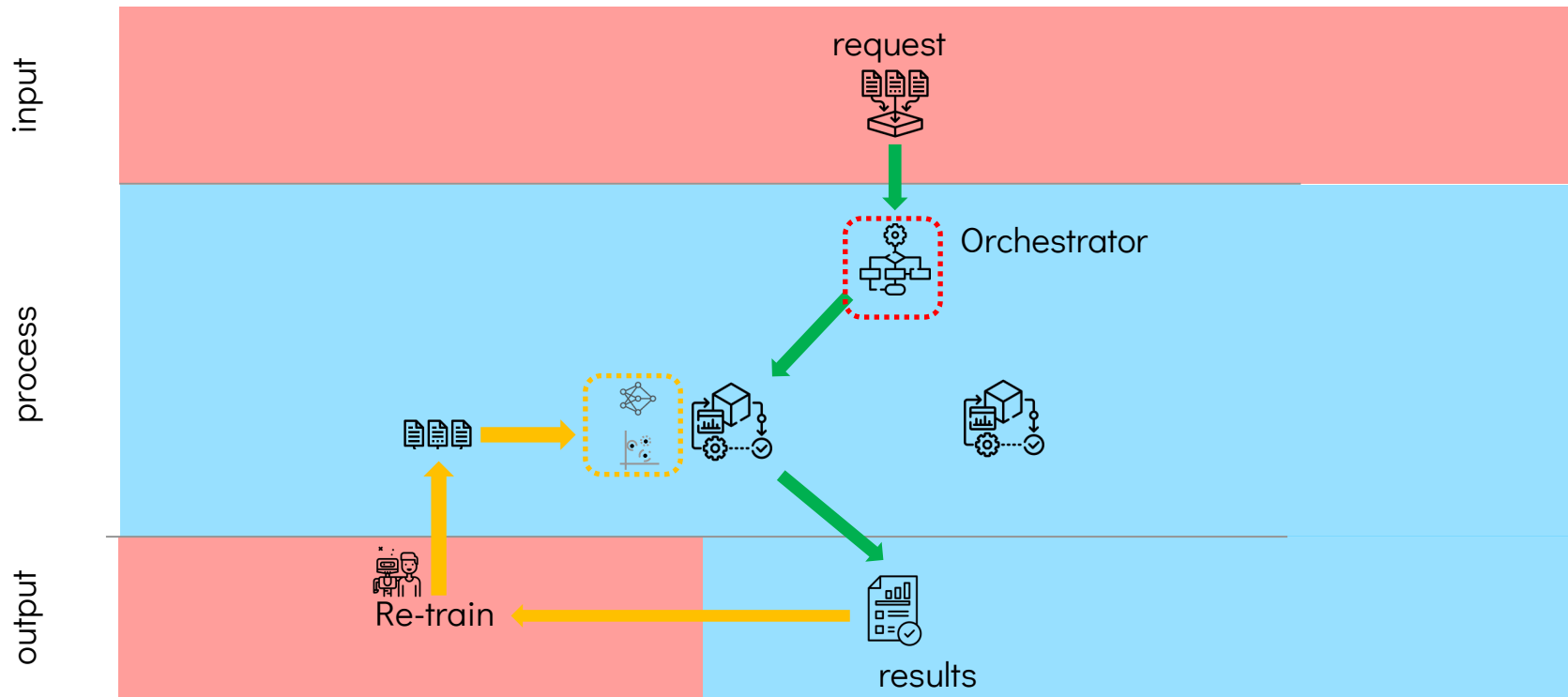


EULA, My Machine, My Code, My Vectors



Traditional network and data protection tools – APIM
Lineage and Metadata governance tools – Purview

Looking for mistakes



Privacy Options



Policy based security and access controls



New security, privacy, and processes for AI related workloads + Policy based controls





Solutions

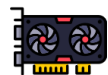
Hardware Choices

Model Training, Data Scrubbing, Data
Management

Choices to Make

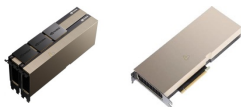


my hardware
my AI



\$\$\$\$

Meta - Llama 3: 70B



Nvidia A100 80GB
\$35,000

Nvidia H100 80GB
\$45,000

I AM MICROSOFT



your hardware
my AI



\$\$\$

Meta - Llama 3: 70B

Azure A100 v4 Series**

\$27.197 / hour

~\$19,853 / month

** Dedicated 8x A100

I WANT TO BE LIKE MICROSOFT



your hardware
your AI, private resource



\$\$

OpenAI GPT 4.x

Training: \$102 per hour
Hosting: \$5 per hour
Input Tokens: \$0.03 per 1K tokens
Response Tokens: \$0.06 per 1K tokens

I NEED AI NOW. I MUST BE AHEAD OF
EVERYONE ELSE!



your hardware
your AI, our EULA



\$

OpenAI GPT 4.x

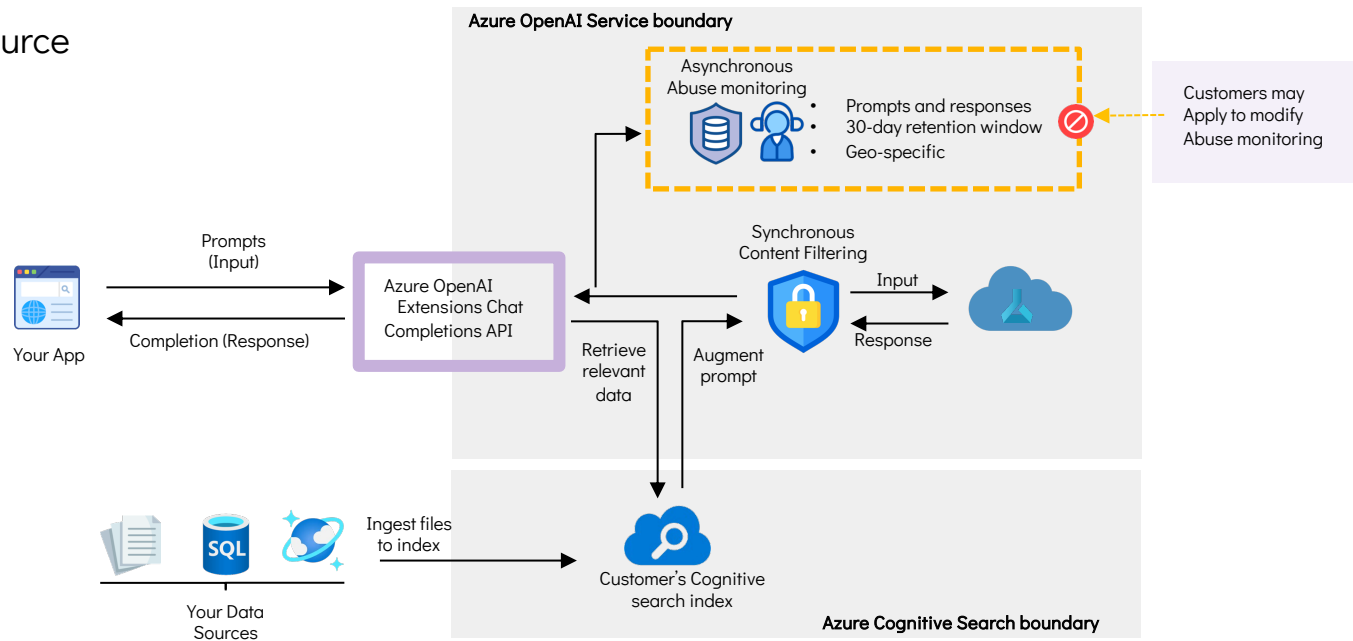
GPT4 Enterprise
\$60/user/month
Min: 150 users @ 12 months

\$9,000 / month

input: \$5.00 / 1M tokens
output: \$15 / 1M tokens

EVERYONE IS TALKING ABOUT AI.
I NEED TO BE IN THE GAME!

Privacy on cloud-based AI models



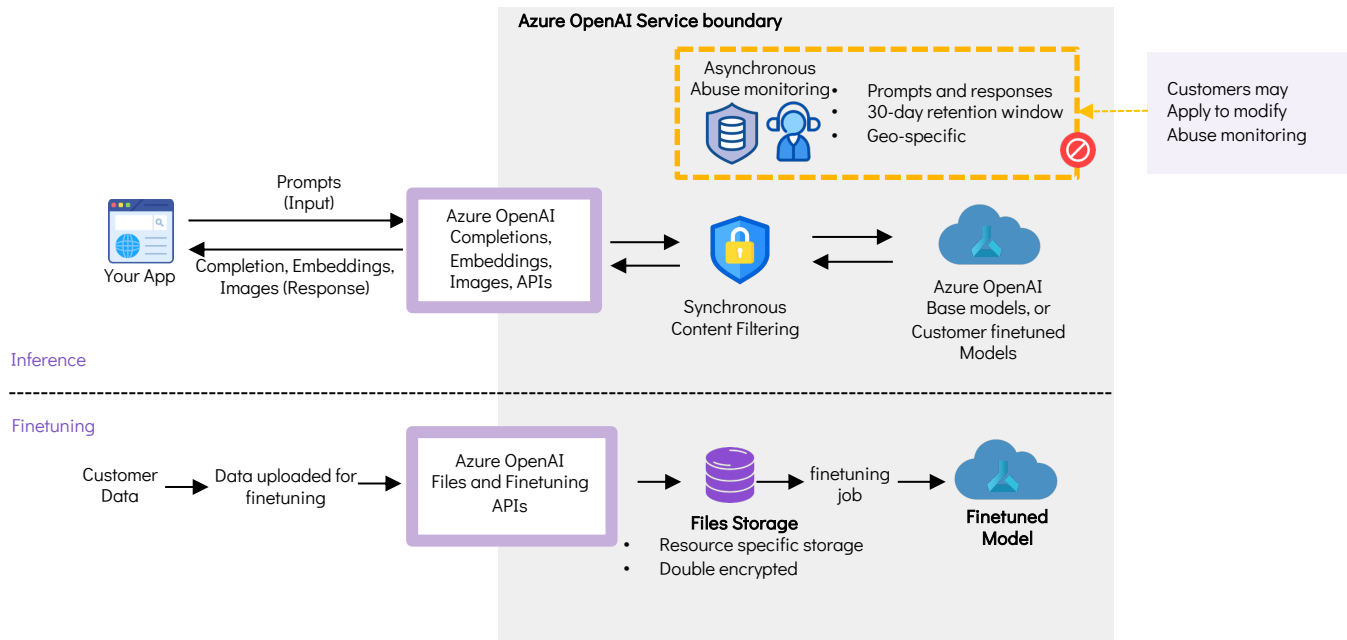
Privacy on cloud-based AI models



your hardware
your AI, private resource



Azure OpenAI | Data flows for inference and training

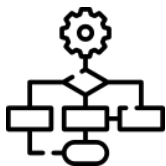


What else can I do?

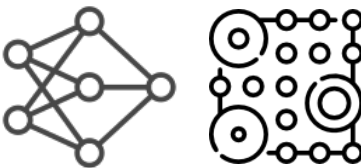
What can I do to make my model forget things that I accidentally trained it with?




Re-train
a new model



  **LangChain**



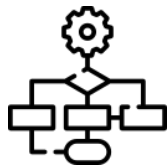
 **Chroma**


Weaviate

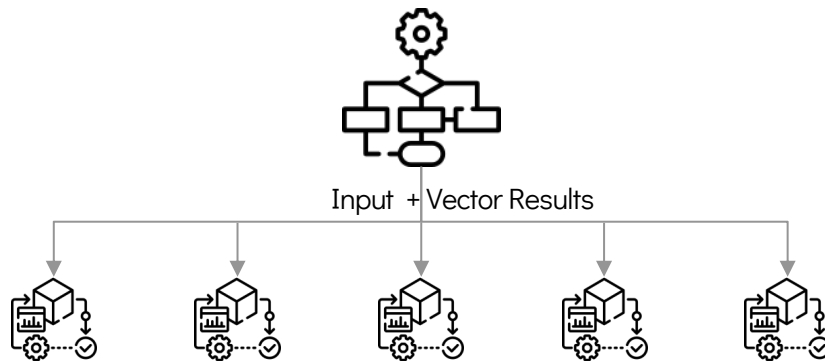


Data & Bias Removal

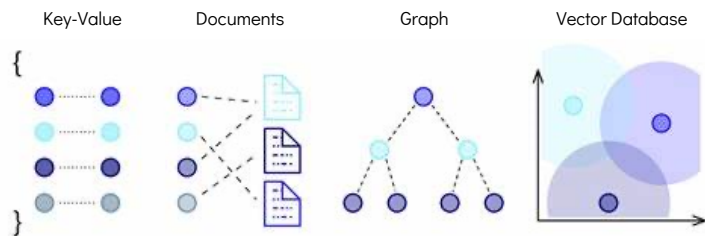
AI Orchestrator



AI Orchestrator helps developers build, observe, and deploy context-aware, reasoning applications with large language models (LLMs).



Vector DB vs Traditional DB



DATA TYPE	TRADITIONAL DATABASES	VECTOR DATABASES
Text (Short, Structured)	✓	
Numbers	✓	✓
Dates/Time	✓	
Images		✓
Audio Files		✓
Videos		✓
Text (Long, Unstructured)		✓

Vector DB

Query: 

Result: [ 0.212,  0.381]



Quick Show and Tell



The background features several abstract, organic, gray shapes that resemble liquid droplets or cells. These shapes are distributed across the frame, with some containing white, irregular voids. The overall aesthetic is clean and modern, with a focus on fluid, non-geometric forms.

Q & A

.



AI Data Privacy

The landscape of AI data privacy constantly evolves due to technological advancements, new regulations, and changing consumer expectations, requiring continual adaptation and vigilance from businesses.

Thank you for attending our session.

We hope to see you at our
LLM session tomorrow at 3 PM.