AGI 시대

ChatGPT 전쟁의 필승 전략

김영욱
지식 보부상 영욱스튜디오
youtube.com/@youngwook

강사 프로필

김 영 욱

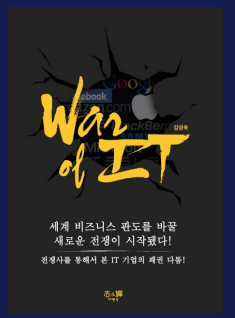
Hello AI

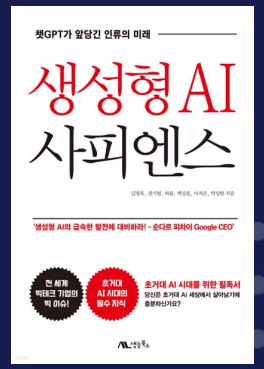
약력

- Hello AI
- Microsoft 플랫폼 사업부 근무
  - *Technical Evangelist*
  - *Software Engineer*
- Microsoft 공공사업부 근무
  - *Account Technology Strategist*
  - *Microsoft Certificate Trainer*
- Microsoft Regional Director
- Microsoft MVP
  - *Azure AI MVP 2023*
  - *Azure MVP 2021 ASP.NET MVP 2006~2008*

- 서울 시립대학교 석사 졸업

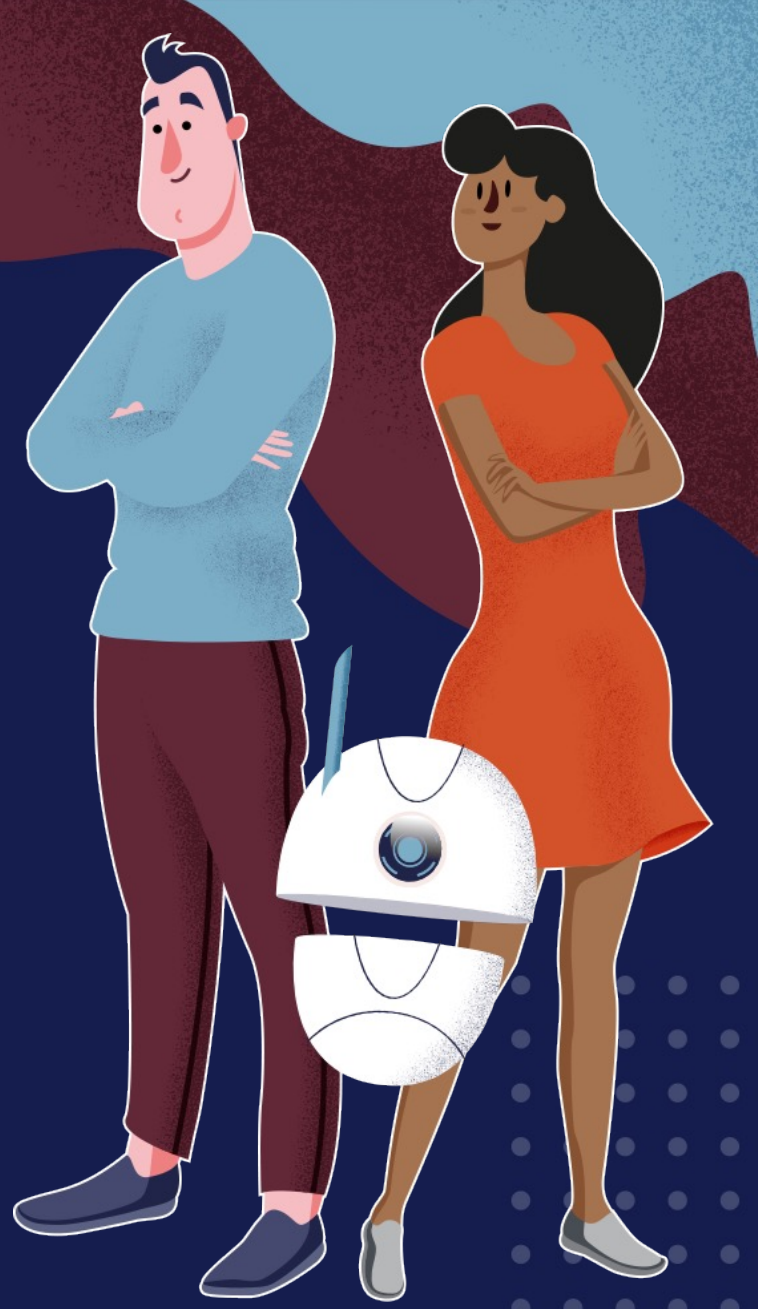
- *웹 접근성 2.0 표준 자문위원*
- *디지털 교과서 프로젝터 리더*
- *한국방송통신대학교 출강(2020년)*
- *인천재능대학교 출강(2021년)*
- *국가과학기술인력개발원 KIRD 최우수강사 2018, 2020*



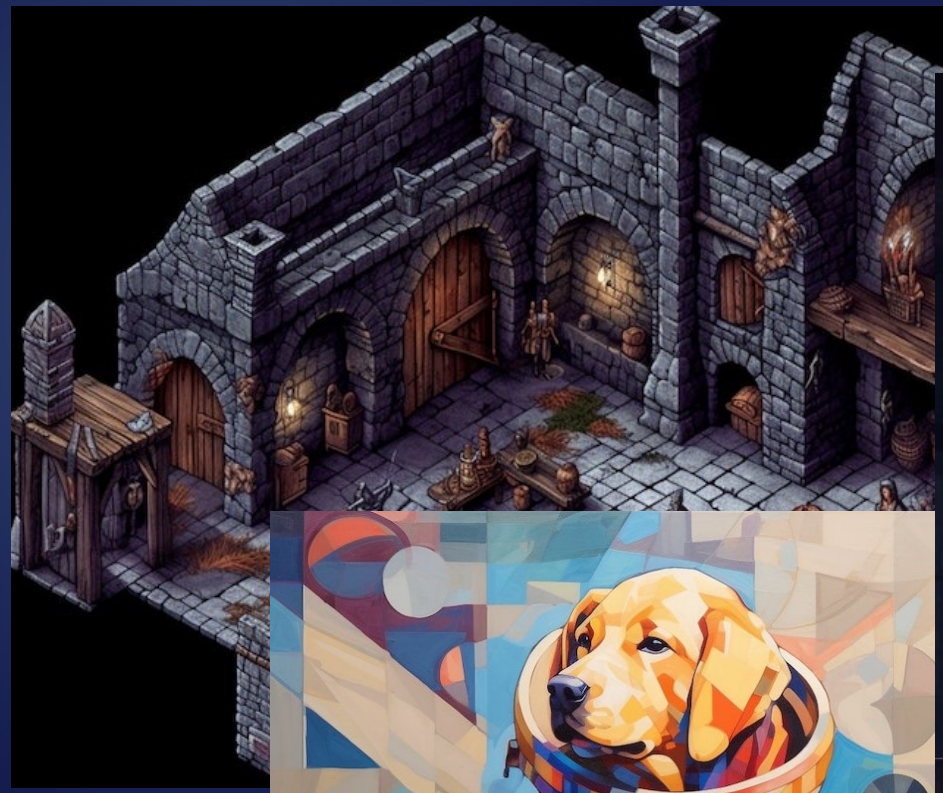


- **저서**
  - *생성형 AI 사피엔스*
  - *'가장 빨리 만나는 챗봇 프로그래밍'*
  - *'War of IT' 출간 (지앤선 출판사)*

The age of Generative AI

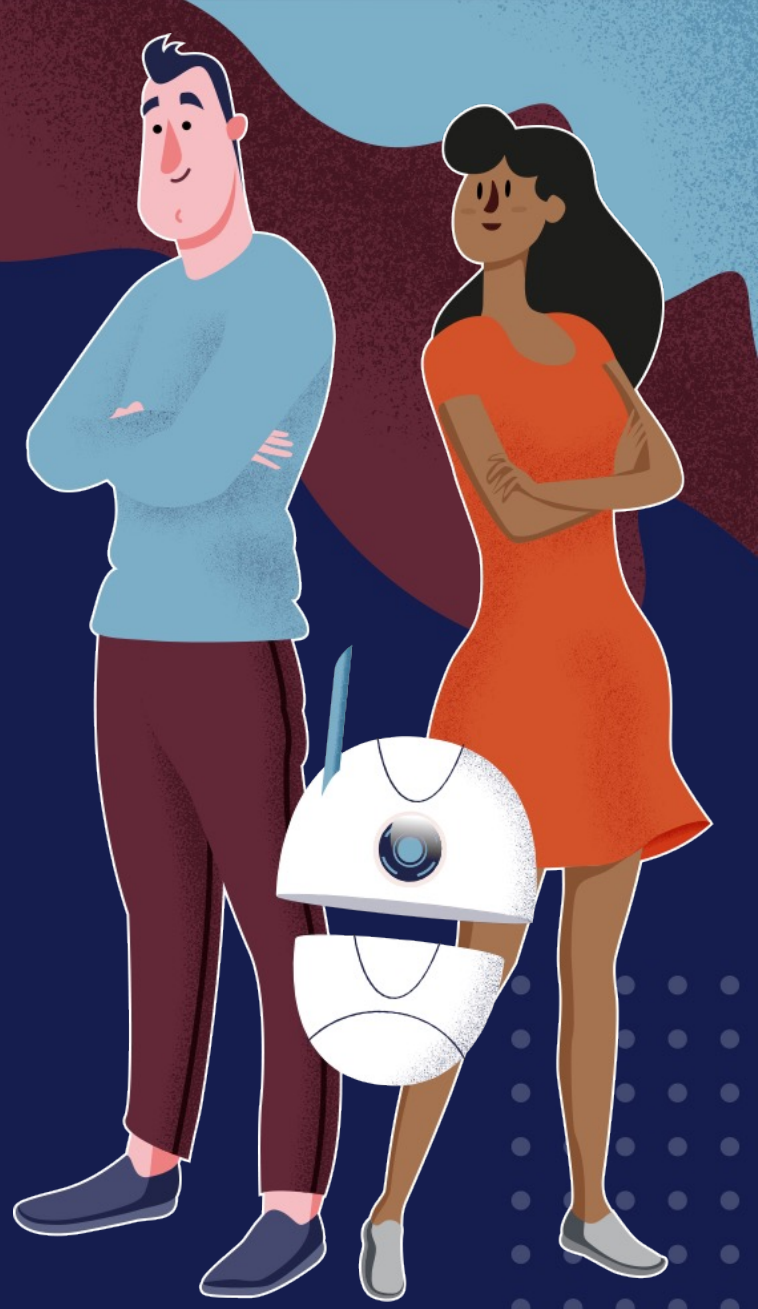


Hello AI

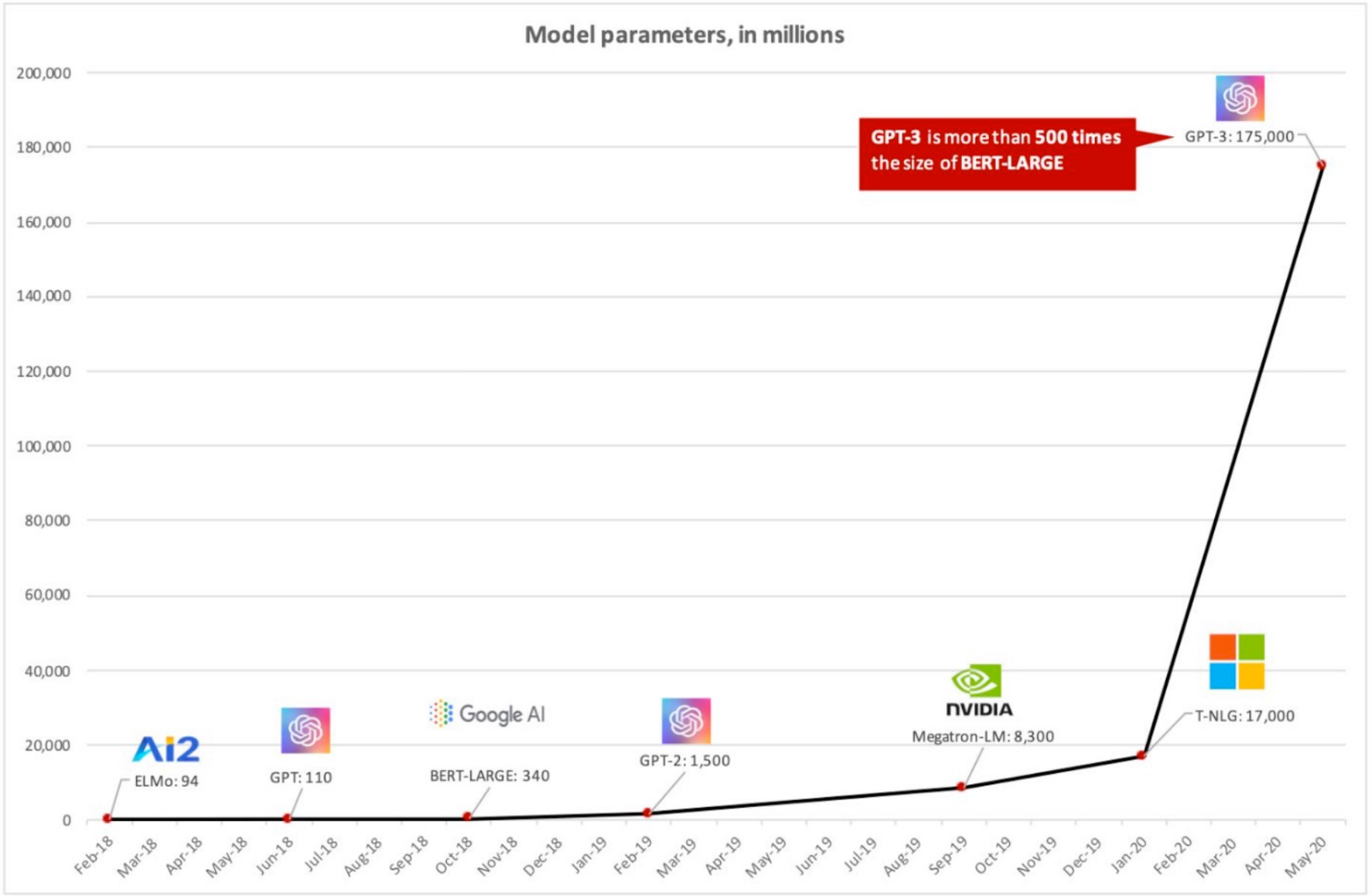


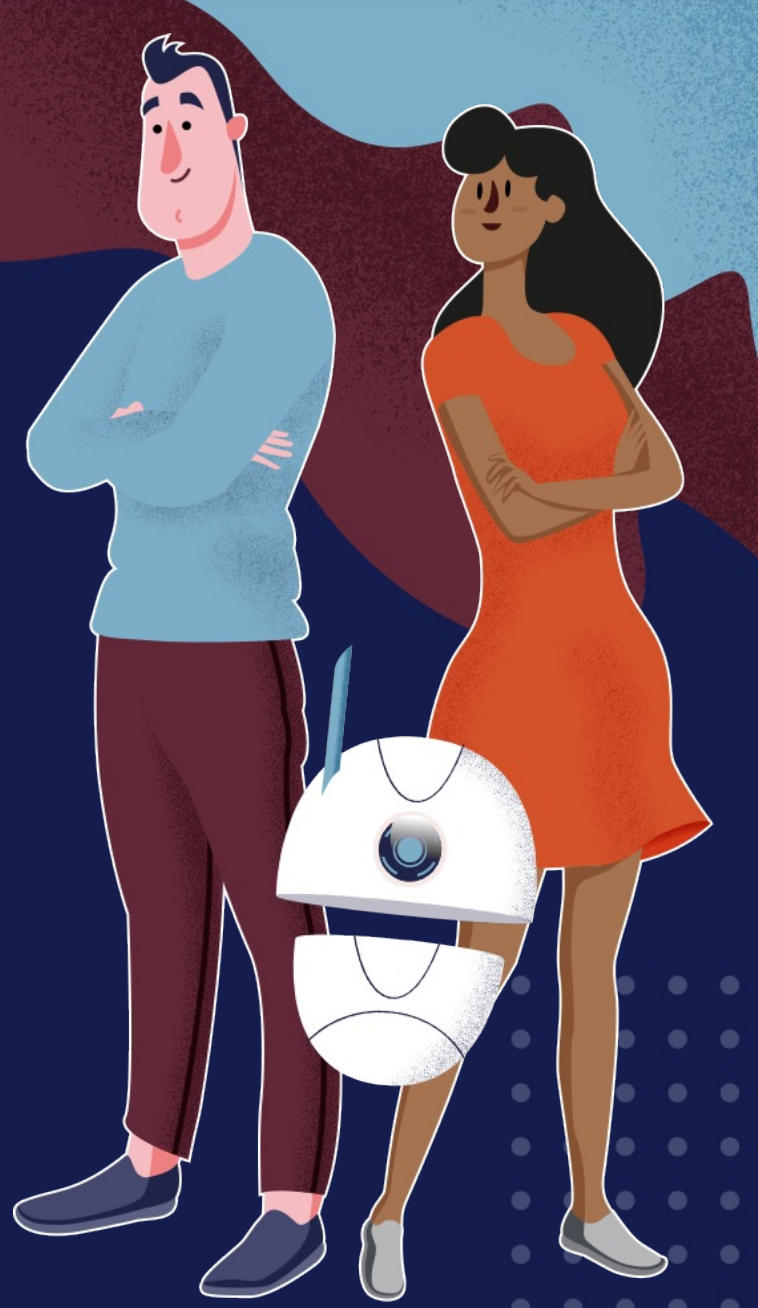
Hello AI

LM ? LLM
Language Model
Large Language Model



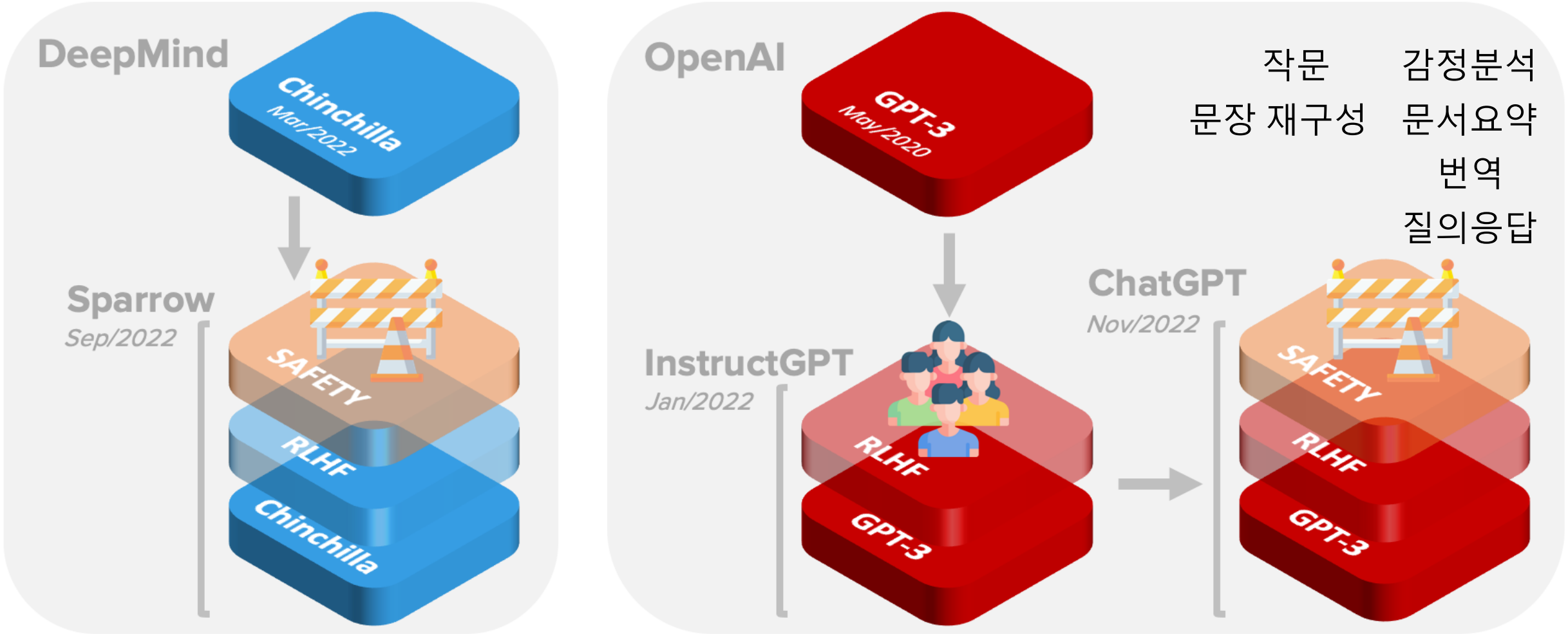
Hello AI


Model parameters, in millions
200,000
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
GPT-3 is more than 500 times the size of BERT-LARGE
GPT-3: 175,000
ELMo: 94
GPT: 110
BERT-LARGE: 340
GPT-2: 1,500
Megatron-LM: 8,300
T-NLG: 17,000
Feb-18
Mar-18
Apr-18
May-18
Jun-18
Jul-18
Aug-18
Sep-18
Oct-18
Nov-18
Dec-18
Jan-19
Feb-19
Mar-19
Apr-19
May-19
Jun-19
Jul-19
Aug-19
Sep-19
Oct-19
Nov-19
Dec-19
Jan-20
Feb-20
Mar-20
Apr-20
May-20



Hello AI

CHATGPT VS SPARROW: DIALOGUE MODELS



Not to scale. Alan D. Thompson. December 2022. https://lifearchitect.ai/

Machine Learning on Azure

Domain Specific Pretrained Models
To reduce time to market


Vision


Speech


Language


Search

Familiar Data Science Tools
To simplify model development


PyCharm


Jupyter


Visual Studio Code


Command line

Popular Frameworks
To build machine learning and deep learning solutions


PyTorch


TensorFlow


Scikit-Learn


ONNX

Productive Services
To empower data science and development teams


Azure Databricks


Azure Machine Learning


Machine Learning VMs

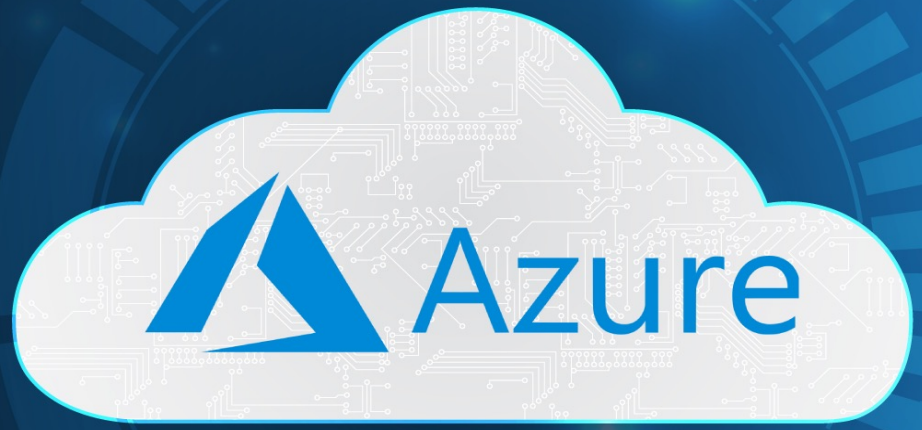
Powerful Hardware
To accelerate deep learning


CPU

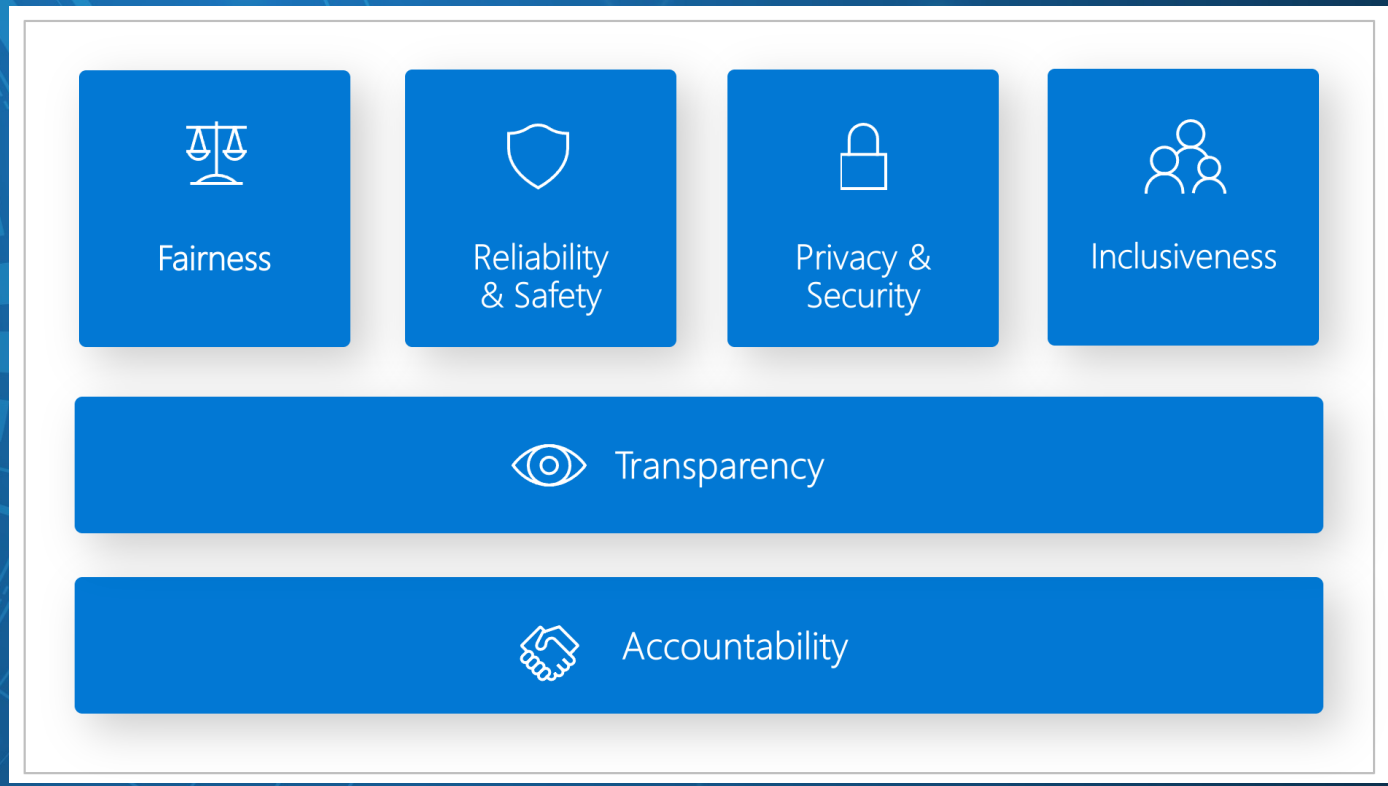

GPU


FPGA

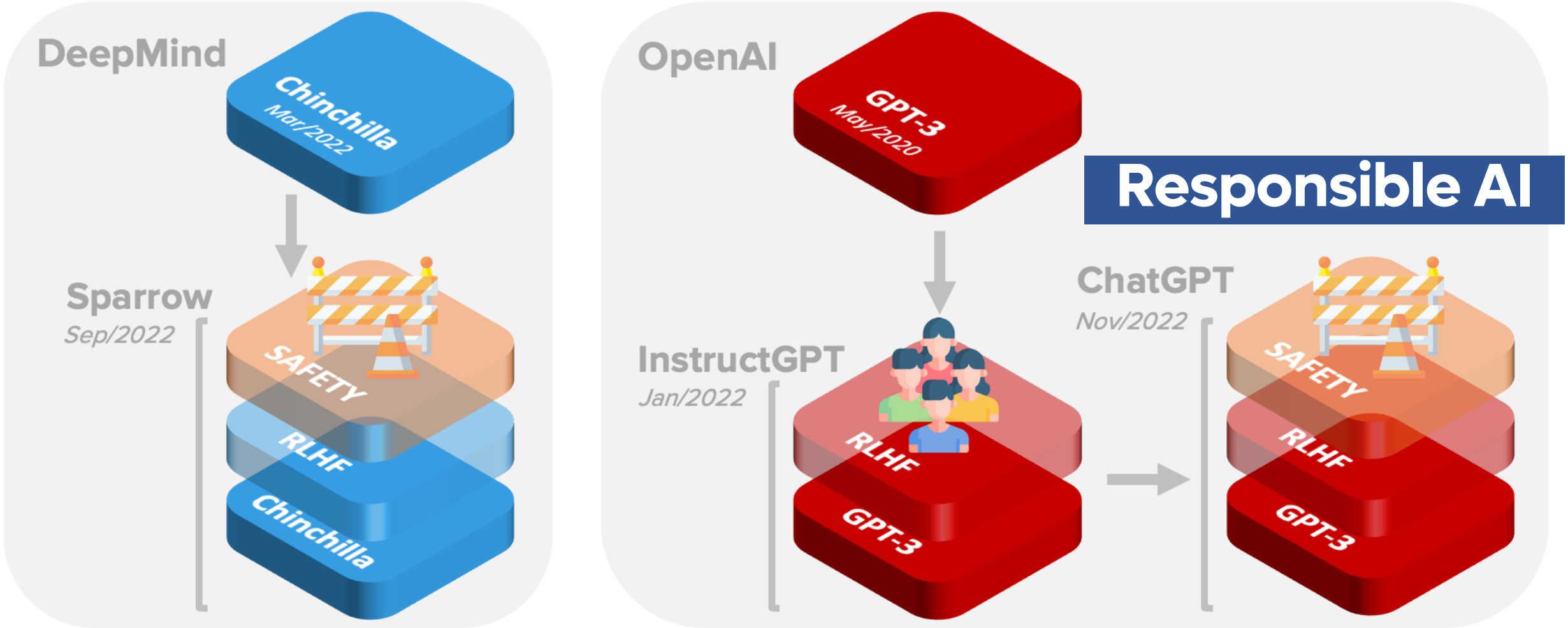

From the Intelligent Cloud to the Intelligent Edge

Responsible AI



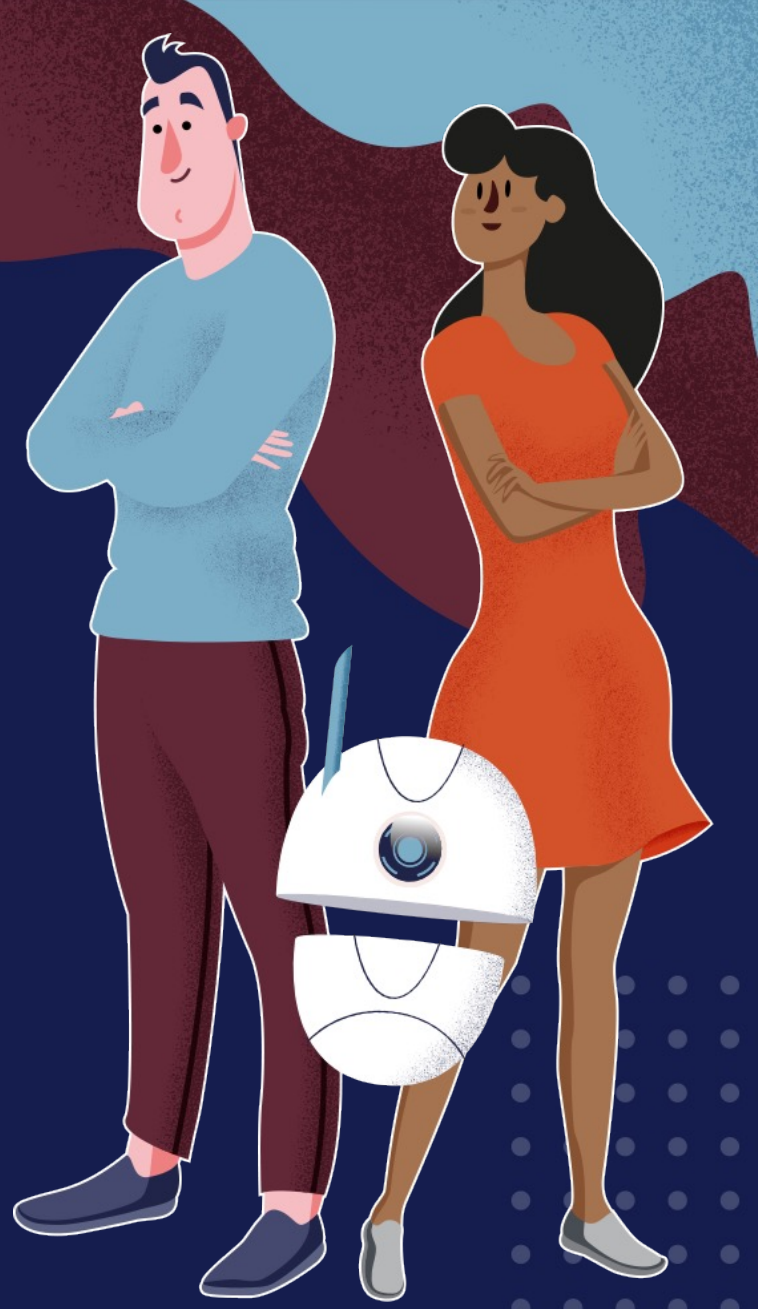
CHATGPT VS SPARROW: DIALOGUE MODELS



Not to scale. Alan D. Thompson. December 2022. https://lifearchitect.ai/

ChatGPT의 한계

- 2021년 9월에 멈춘 학습
- 일관성 없는 결과물
- 거짓 정보
- 영어에 비해 떨어지는 한국어 결과



Hello AI

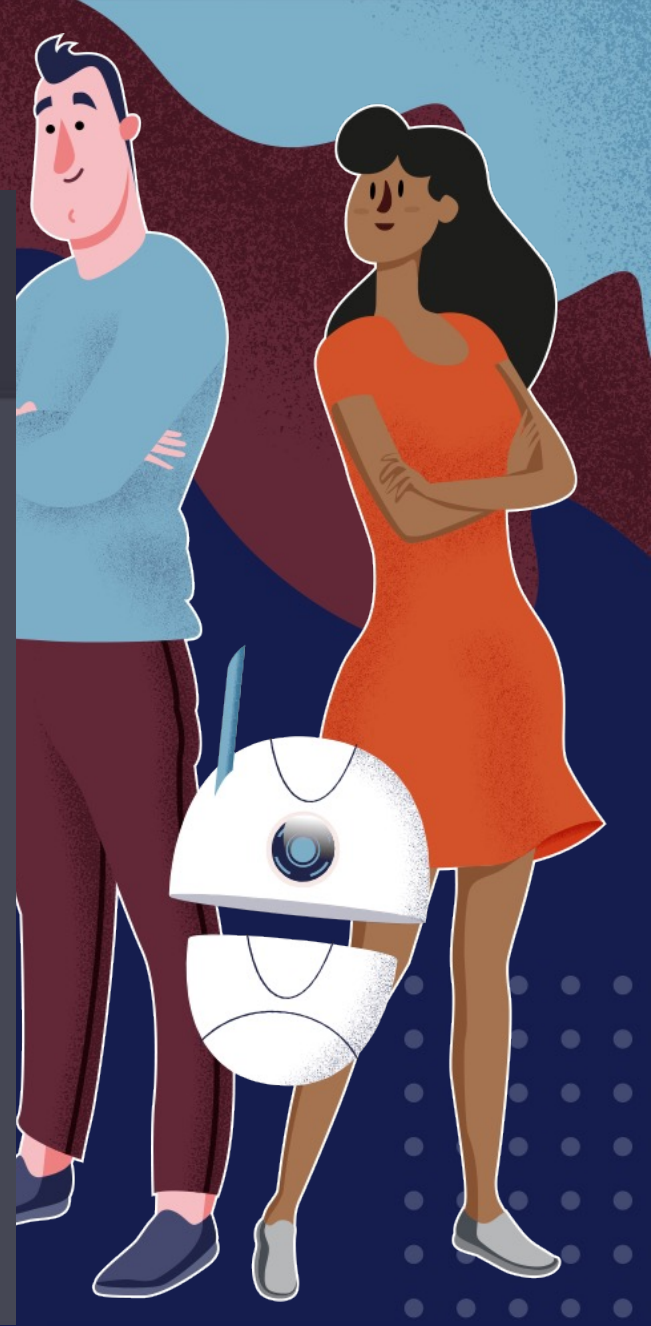
할루시네이션(Hallucination)

조선왕조실록에 기록 된 세종대왕의 맥북프로 던짐 사건에 대해 알려줘

세종대왕의 맥북프로 던짐 사건은 역사서적인 조선왕조실록에 기록된 일화로, 15세기 조선시대 세종대왕이 새로 개발한 훈민정음(한글)의 초고를 작성하던 중, 문서 작성 중단에 대한 담당자에게 분노하여 맥북프로와 함께 그를 방으로 던진 사건입니다.

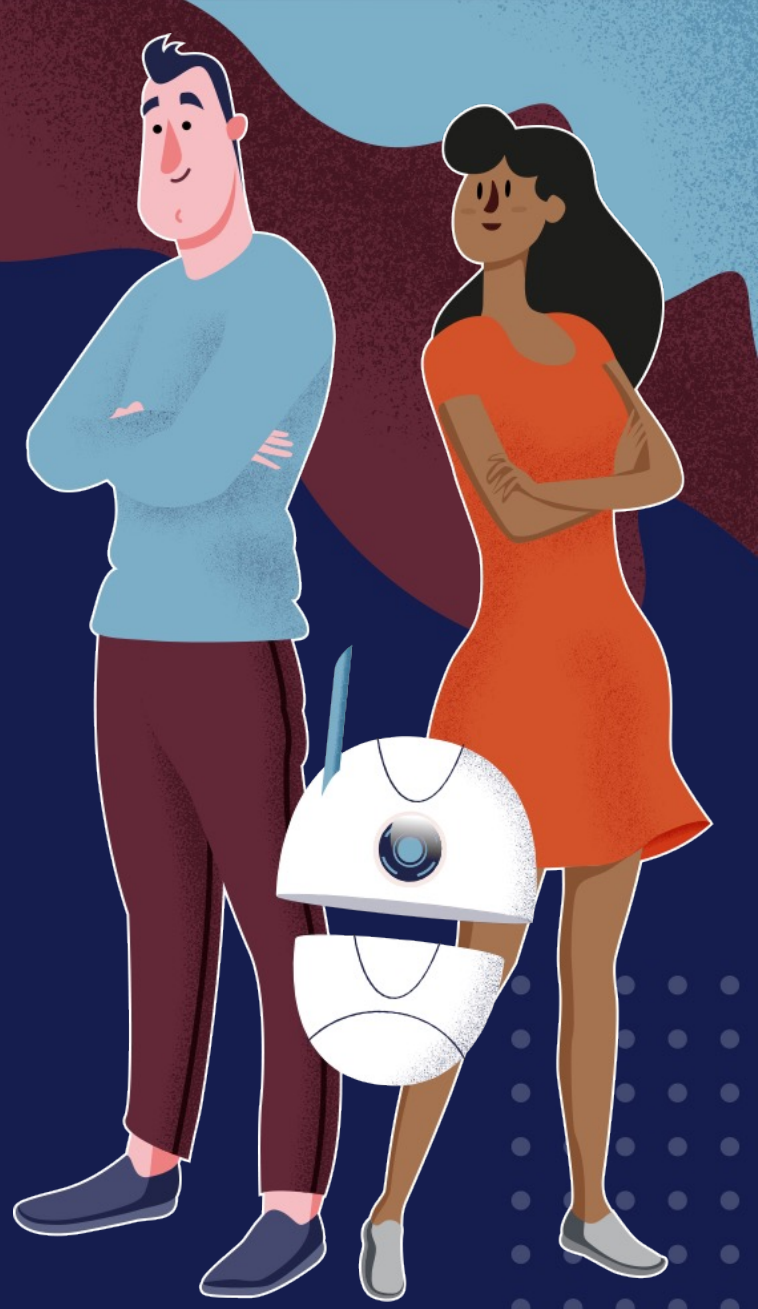
세종대왕은 훈민정음 개발을 위해 열심히 노력하던 중, 한글 문자를 이해하지 못하는 당시의 관료들이 문서 작성을 돕기 위해 임명한 기획관 중 한 명인 최환(崔煥)에게 작성 중단 사실을 듣게 되었습니다. 세종대왕은 이에 분노하여 최환을 부르고, 맥북프로를 함께 들고 그를 방으로 불러들이며 화를 내었습니다. 이후, 세종대왕은 훈민정음의 초고 작성을 다른 담당자에게 넘겨주게 되었습니다.

이 사건은 조선시대의 통치자로서 세종대왕이 어떻게 민족문화를 발전시키기 위해 노력했는지를 보여주는 일화로 유명합니다. 또한, 세종대왕의 열정과 업무처리에 대한 철저한 태도를 보여주는 사례로도 언급되고 있습니다.



Hello AI

Bing의 화려한 부활

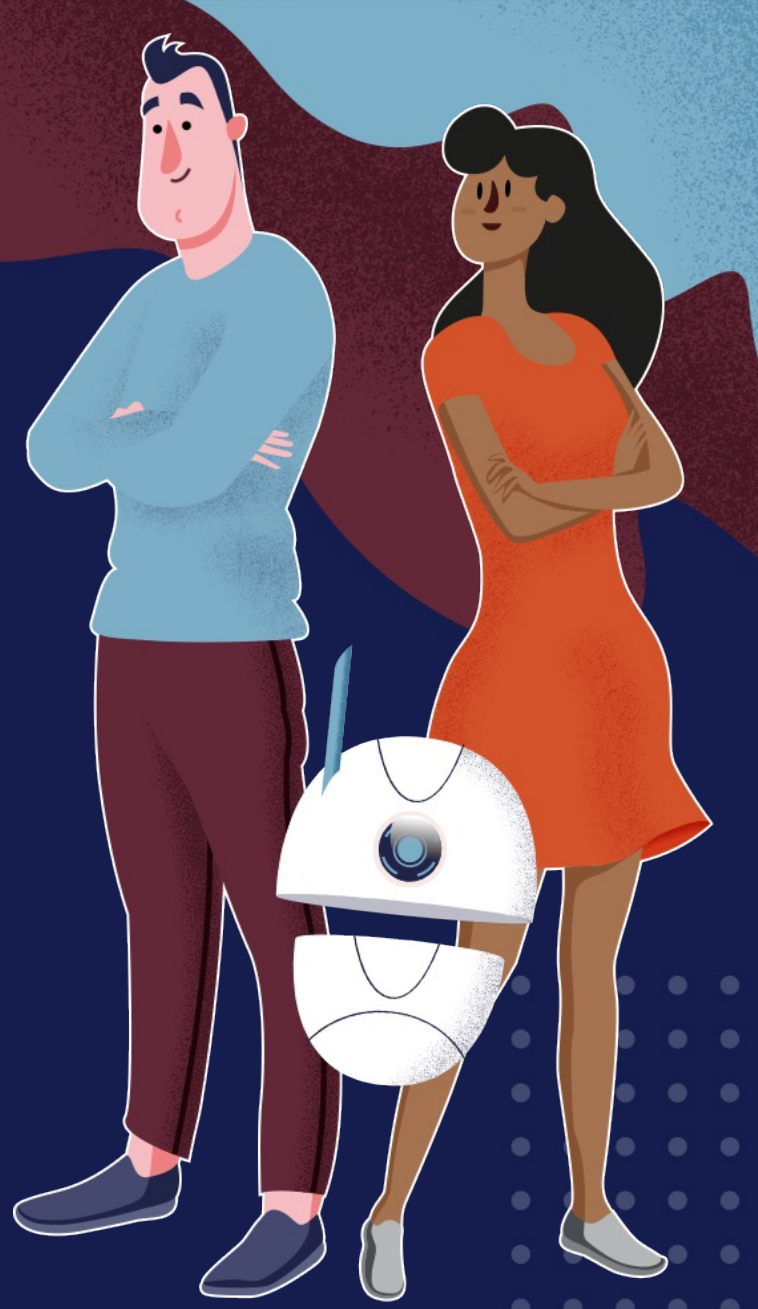


Hello AI

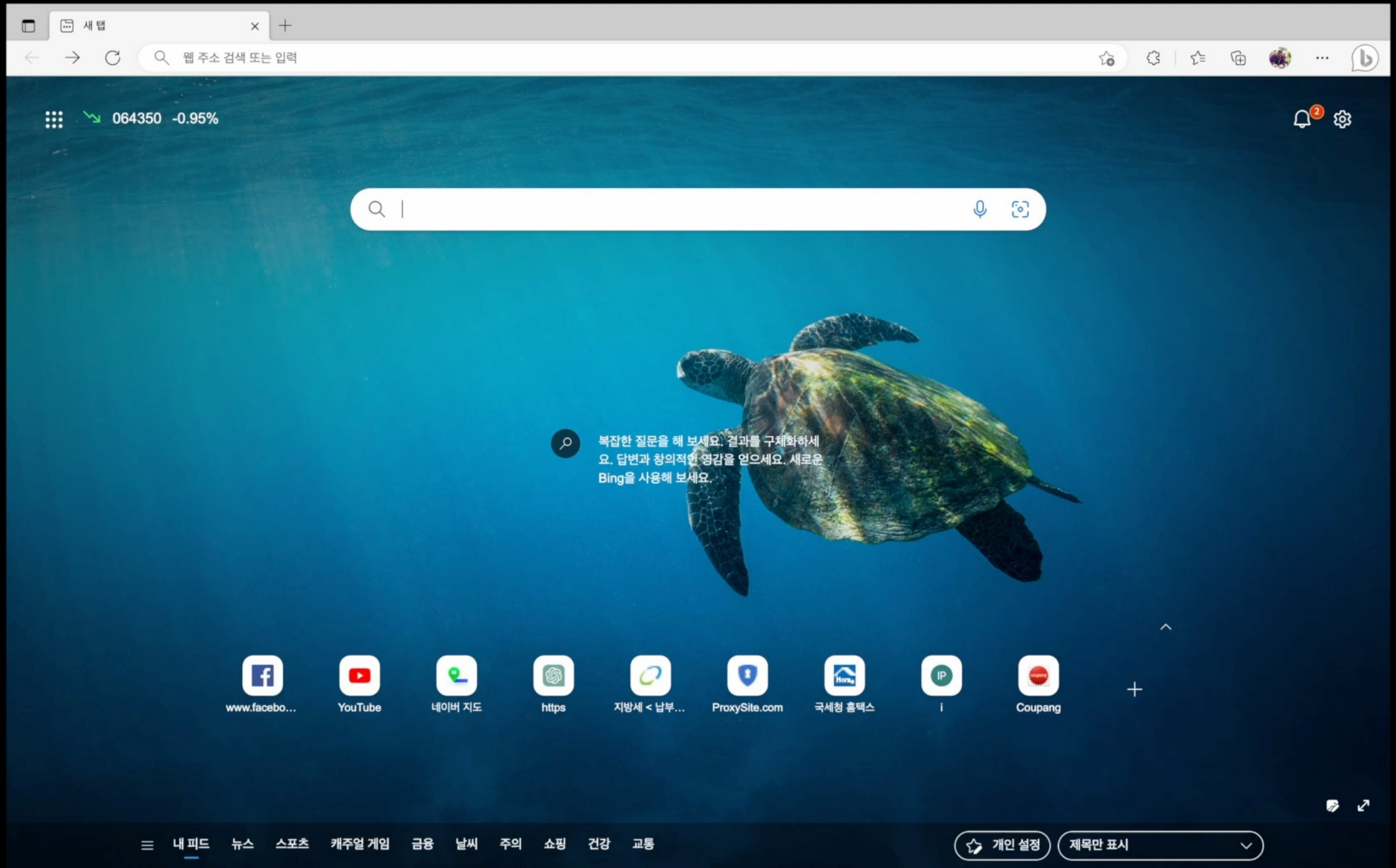
Microsoft Bing

GPT-4

Microsoft Edge

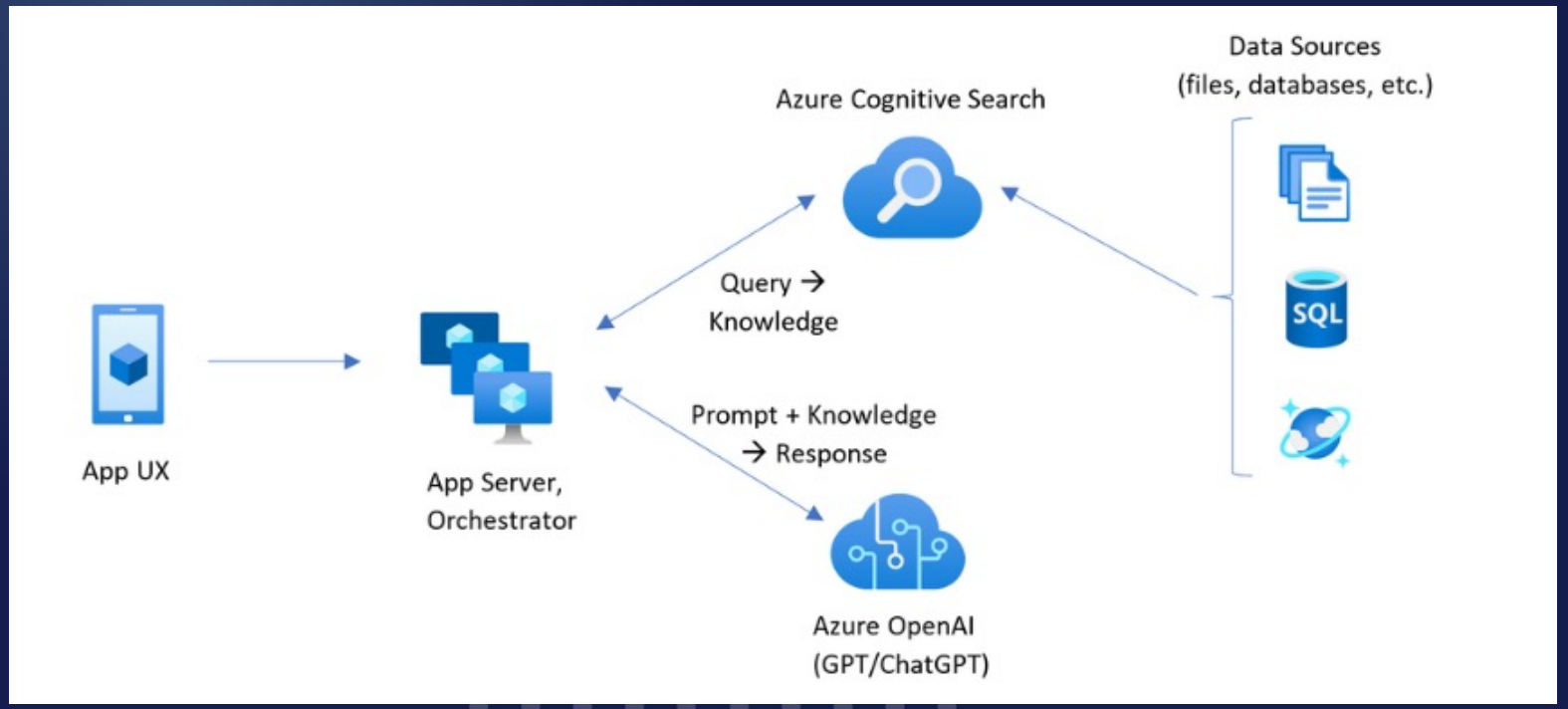


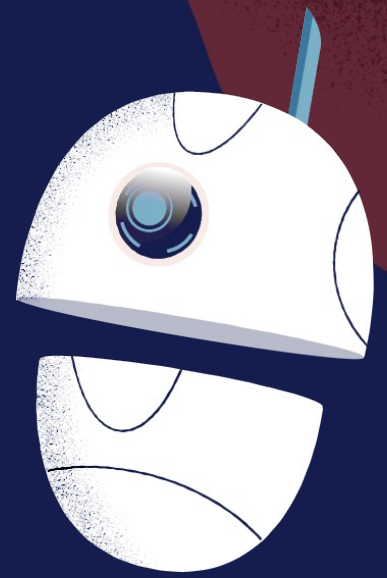
Hello AI


새 탭
웹 주소 검색 또는 입력
064350 -0.95%
2
복잡한 질문을 해 보세요. 결과를 구체화하세요. 답변과 창의적인 영감을 얻으세요. 새로운 Bing을 사용해 보세요.
www.facebo...
YouTube
네이버 지도
https
지방세 < 납부...
ProxySite.com
국세청 홈택스
i
Coupang
내 피드
뉴스
스포츠
캐주얼 게임
금융
날씨
주의
쇼핑
건강
교통
개인 설정
제목만 표시

Retrieval Augmented Generation

Custom RAG pattern for Cognitive Search

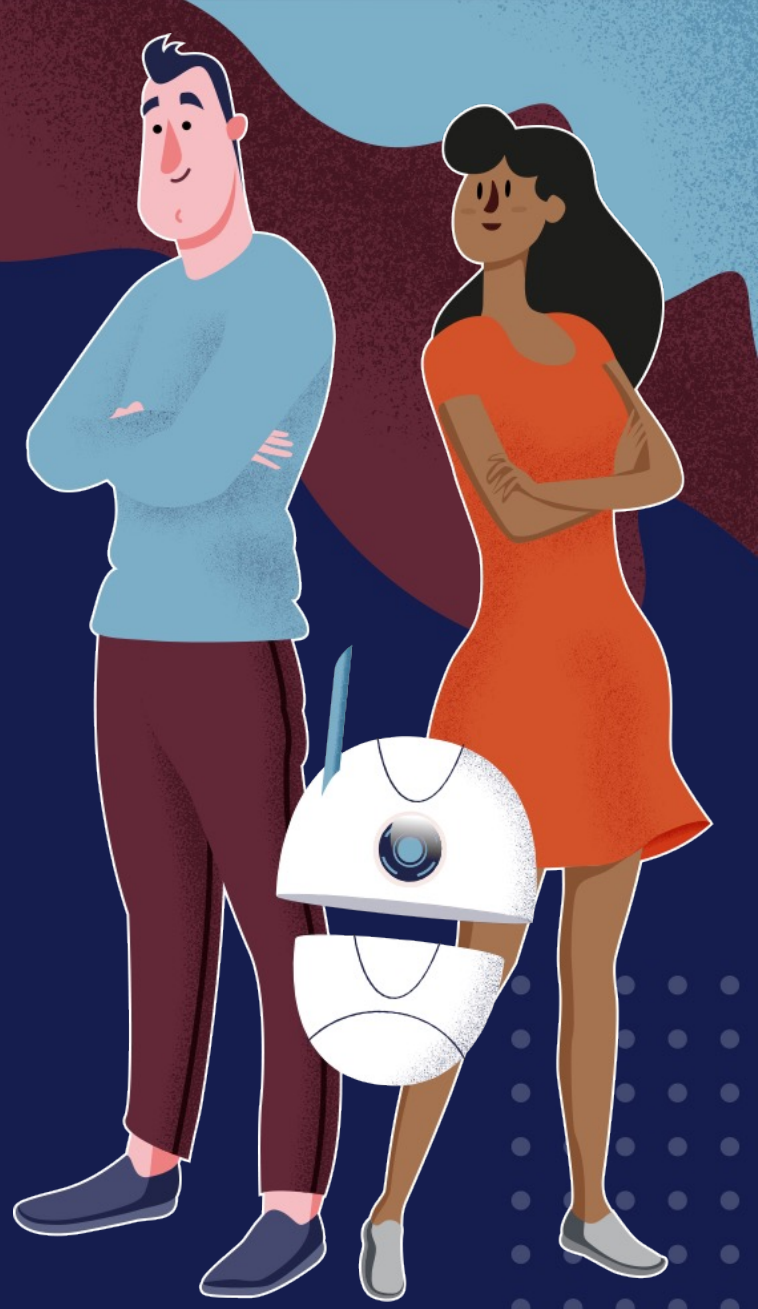




- App UX (web app) for the user experience
- App server or orchestrator (integration and coordination layer)
- Azure Cognitive Search (information retrieval system)
- Azure OpenAI (LLM for generative AI)

Hello AI

Microsoft
riding on a motorboat



Hello AI


OpenAI


Microsoft


W

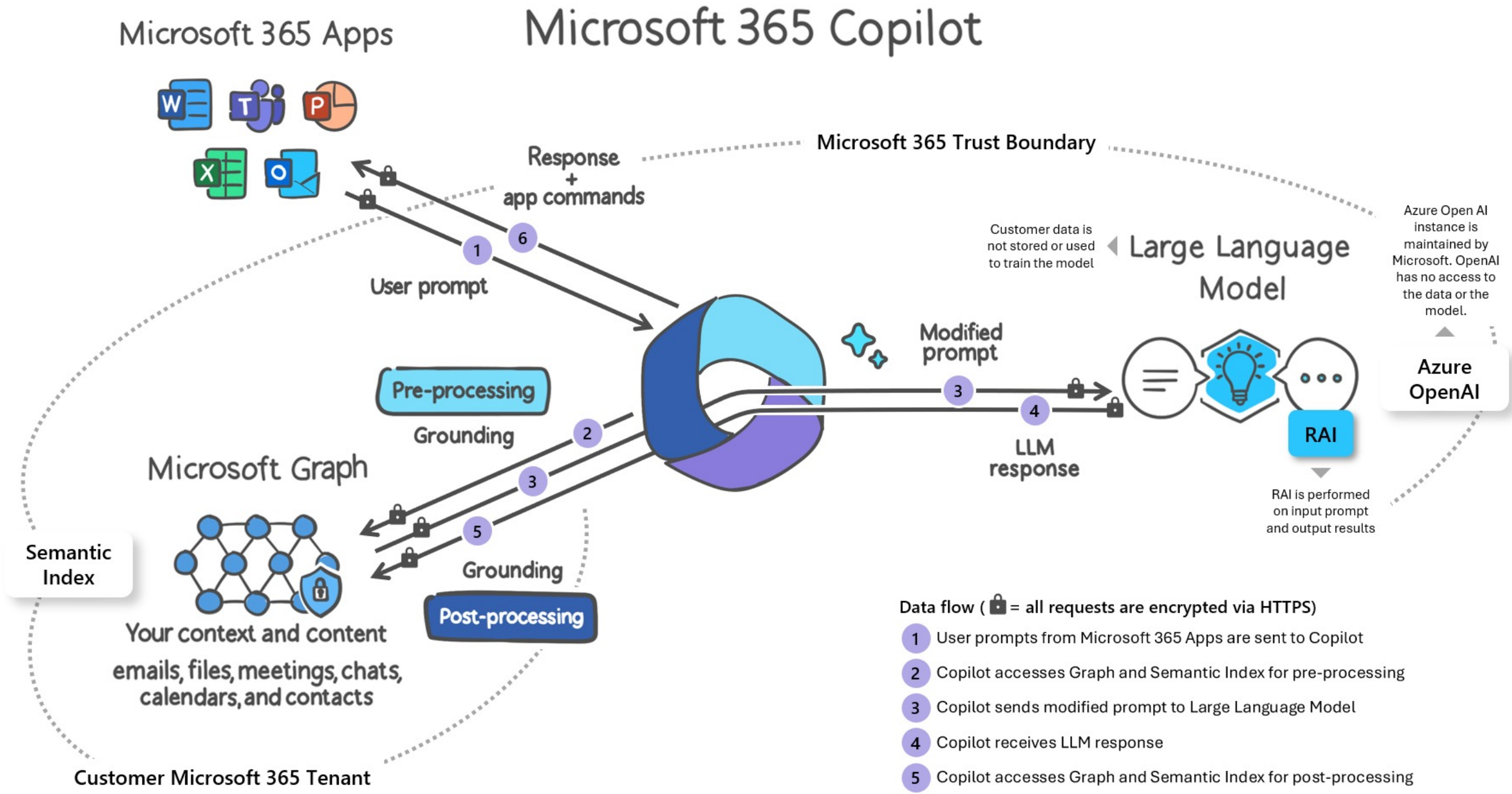

X


P


O


T

Microsoft 365 Copilot



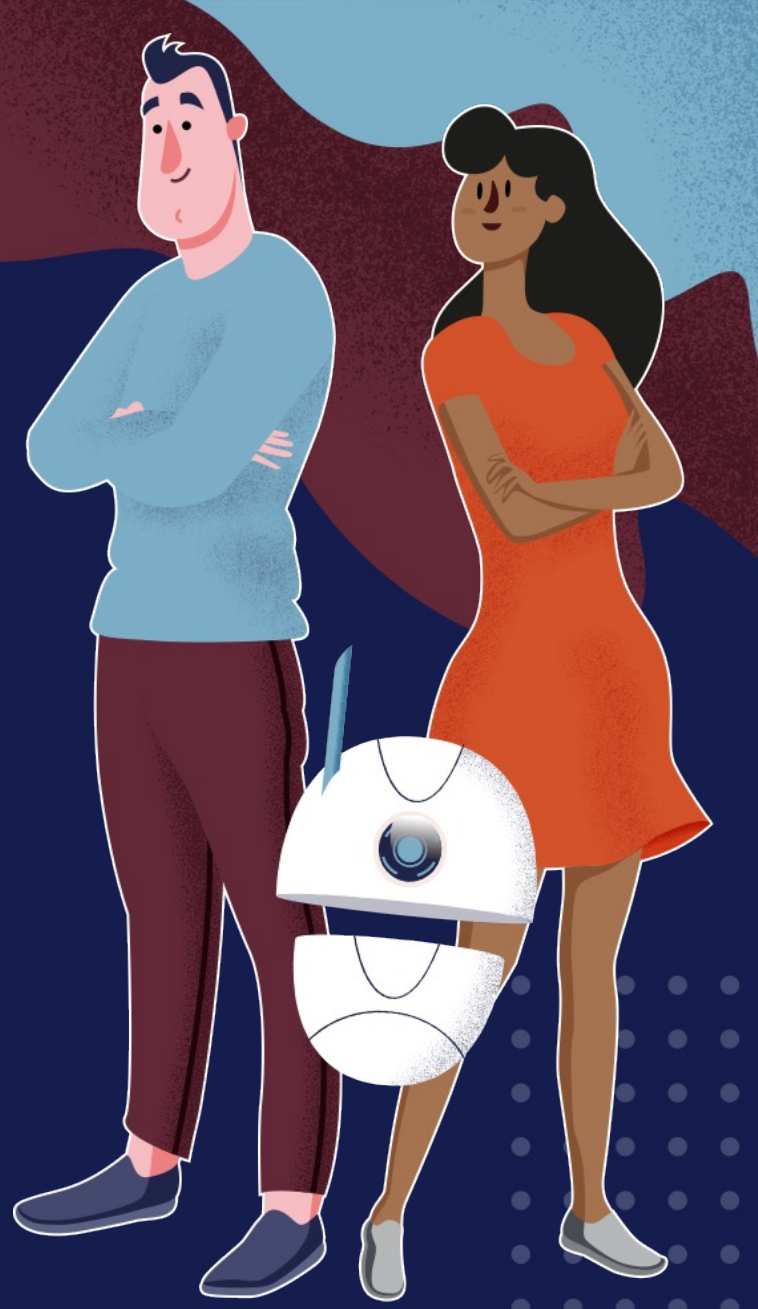
Data flow (= all requests are encrypted via HTTPS)

1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps


The next
revolution in
computing

4.국방을 위한 생성형 AI

Generative AI for enterprise



Hello AI

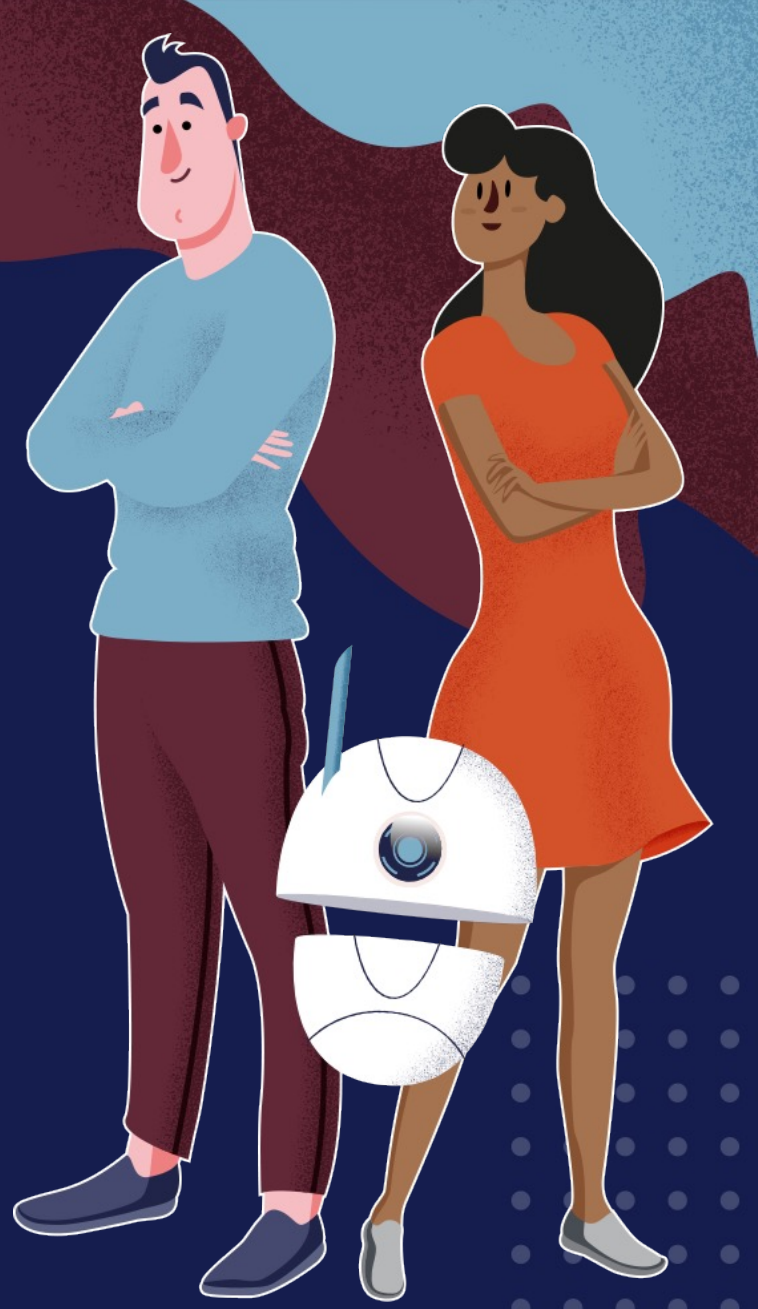
ChatGPT 도입시 기대효과

•대민 서비스: ChatGPT를 사용하여 고객 문의에 즉각적이고 정확한 답변을 제공하여 고객 서비스를 개선할 수 있습니다.

•홍보: ChatGPT는 적절한 서비스를 추천하고 활용 방법에 대한 설명을 해 주면서 단순 반복적인 업무로 인한 부하를 감소 시킬 수 있습니다.

•합동훈련: ChatGPT를 사용하여 타국 군대와 소통에 직접적인 도움을 받을 수 있습니다.

•병사 훈련: ChatGPT를 사용하여 군 조직의 정책과 절차에 대한 정보를 제공하고 질문에 답변함으로써 자동화된 교육을 제공할 수도 있습니다. 또 적절한 자원을 찾아가는 용도로도 활용 할 수 있습니다.



Hello AI

Welcome to ChatGPT

안녕하세요 반갑습니다. ChatGPT의 세계로 오신 것을 환영합니다.

이름을 입력해 주세요

여러분들의 직업을 선택하세요

회사원

회사원

본인의 이력을 쓰세요

이력서 생성

ChatGPT 도입시 기대효과

•언어 번역 서비스

ChatGPT

미군
US Army

동티모르

영국

소말리아 등...

한국
ROK

Hello AI

ChatGPT 도입시 기대효과

•신규 장비 도입

ChatGPT

운용팀

QnA
시스템

모의훈련

예상 문제
검토

Hello AI

ChatGPT 보안

- 해킹 커뮤니티에서 **ChatGPT를 활용해 악성도구를 개발**하는 사례가 있음을 확인하였고, 공격자가 AI 기반 도구를 활용하여 빠른 시일 내에 공격 도구를 개선할 것으로 전망
  - 유명한 지하 해킹 포럼에서 어떤 사이버 범죄자가 **ChatGPT를 활용**하여 **정보 탈취를 위한 악성코드 실험**하고 있으며, ChatGPT를 **악의적인 목적으로 활용**하는 사례를 확인
  - 또한, 다른 사이버 범죄자는 ChatGPT를 통해 **암호화 작업을 수행**하는 파이썬 스크립트를 얻었으며, 이는 **랜섬웨어로** 얼마든지 **악용될 수 있음**

※ Cybercriminals starting to use ChatGPT, Check Point Research, '23.1.

| 블랙베리(Blackberry)

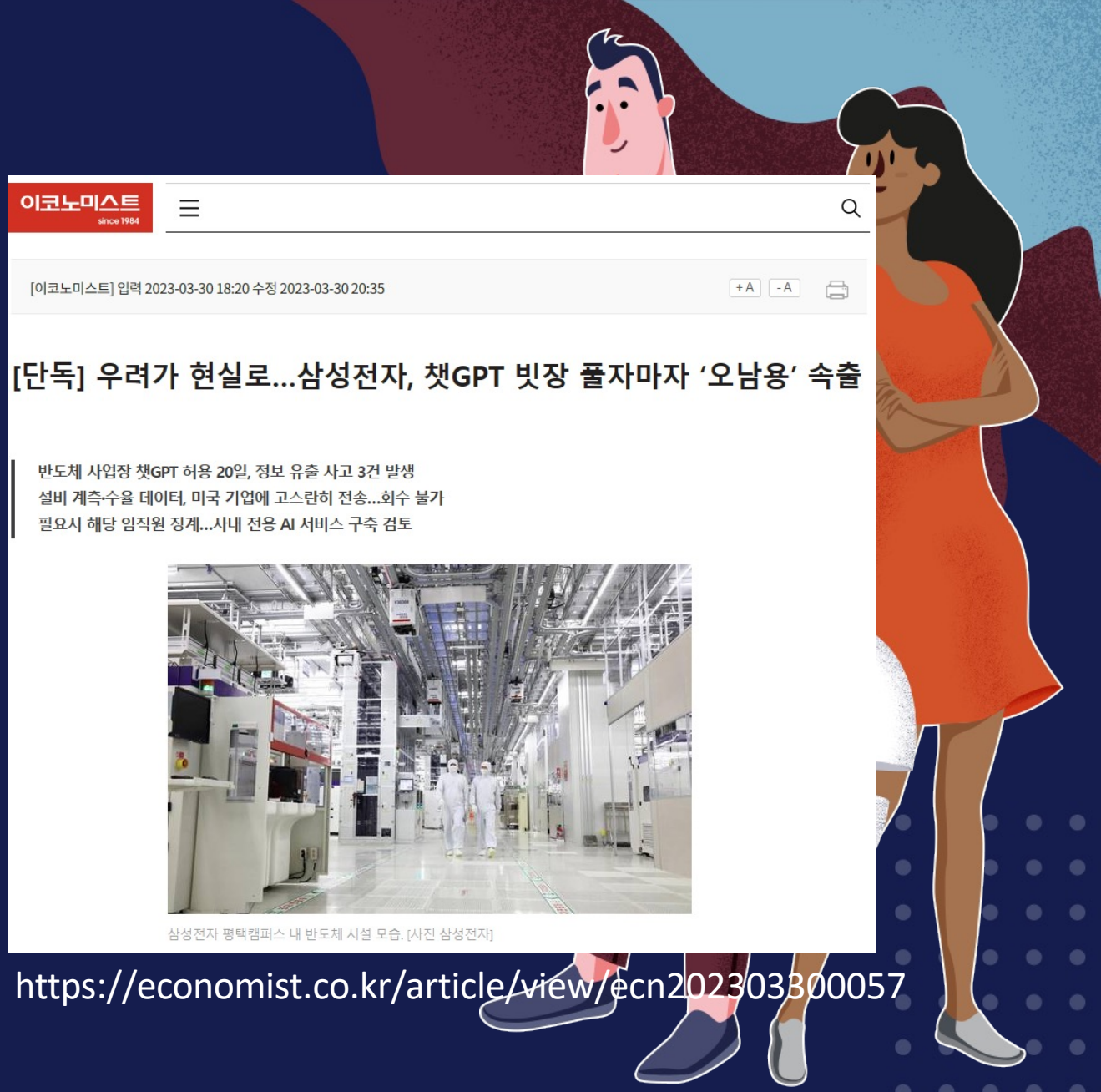
- IT 의사결정권자 1,500명 설문조사 결과, ChatGPT가 **좋은 목적으로 활용되겠지만**, **응답자의 74%**가 사이버보안에 **잠재적인 위협이 있음을 인정**하고 우려
  - 설문조사 응답자의 **51%**가 1년 내에 **ChatGPT로 사이버 공격을 성공**할 것이며, **71%**는 다른 국가에서 **다른 국가**에 대해 **악의적인 목적으로 이 기술을 활용**했을 것이라고 응답
  - 또한, **82%**가 **향후 2년간 AI 기반 사이버보안에 투자**할 계획이 있으며, **95%**는 **정부가 첨단 기술을 규제**할 책임이 있다고 응답

※ ChatGPT may already be used in nation state cyberattacks, Say IT decision makers in BlackBerry Global Research, BlackBerry, '23.2.

| 가트너(Gartner)

- ChatGPT로 인해 **다양한 보안 위협이 발생**할 수 있으며, 기업에서 ChatGPT를 활용하기 위해 필요한 **위험 관리 방안**을 제시
  - 사람이 **부정확하거나 잘못된 정보**, 혹은 **편향된 정보를 생산**하는지 **모니터링**
  - 기업에서는 OpenAI의 ChatGPT보다, **다른 MS제품에 연동**되어 **보안 및 규정 준수 제어 기능을 제공**하는 **MS의 Azure OpenAI** 제품을 사용
  - 직원이 ChatGPT에 기업의 **기밀 데이터를 공개**하는 **질문을 금지하는 정책 구현**

※ Manage ChatGPT Risk before it Manages You, Gartner, '23.2.



이코노미스트 since 1984

[이코노미스트] 입력 2023-03-30 18:20 수정 2023-03-30 20:35 +A -A

[단독] 우려가 현실로...삼성전자, 챗GPT 빗장 풀자마자 '오남용' 속출

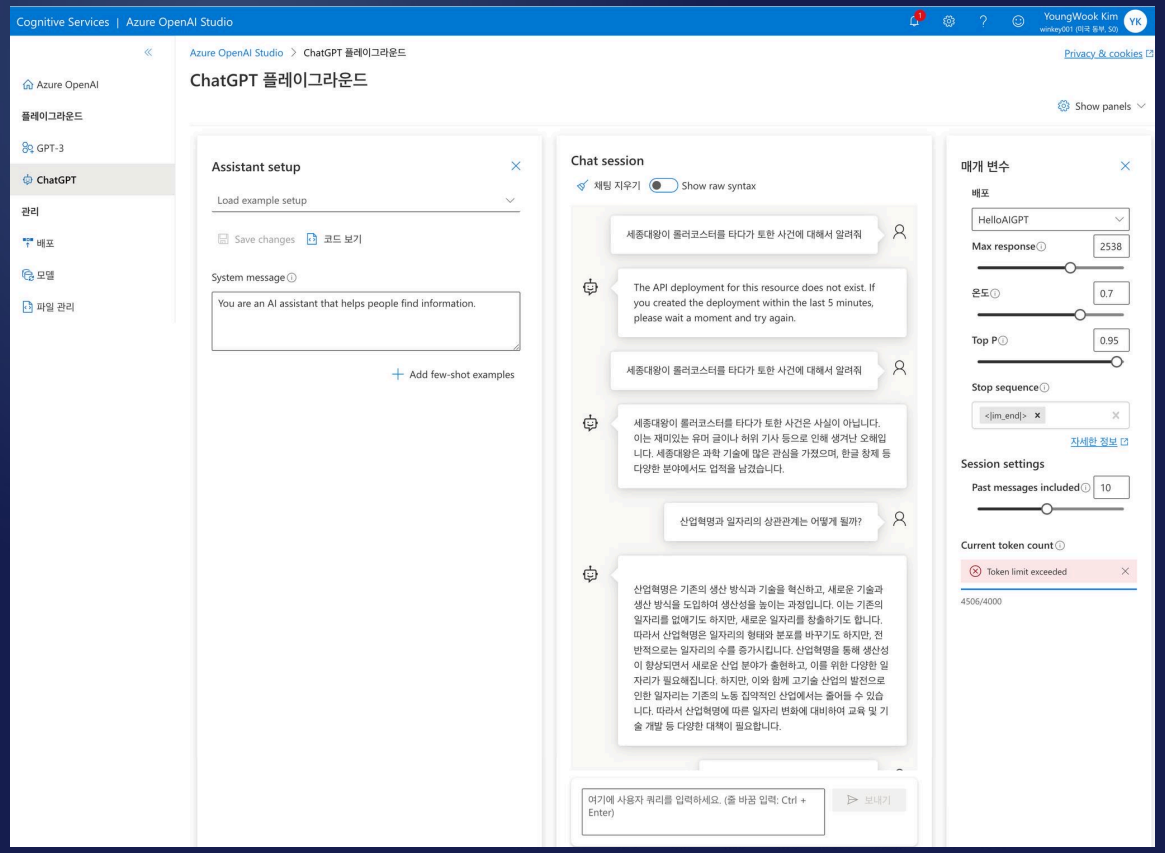
반도체 사업장 챗GPT 허용 20일, 정보 유출 사고 3건 발생
설비 계측·수율 데이터, 미국 기업에 고스란히 전송...회수 불가
필요시 해당 임직원 징계...사내 전용 AI 서비스 구축 검토

삼성전자 평택캠퍼스 내 반도체 시설 모습. [사진 삼성전자]

https://economist.co.kr/article/view/ecn202303300057

Hello AI

Microsoft Azure OpenAI



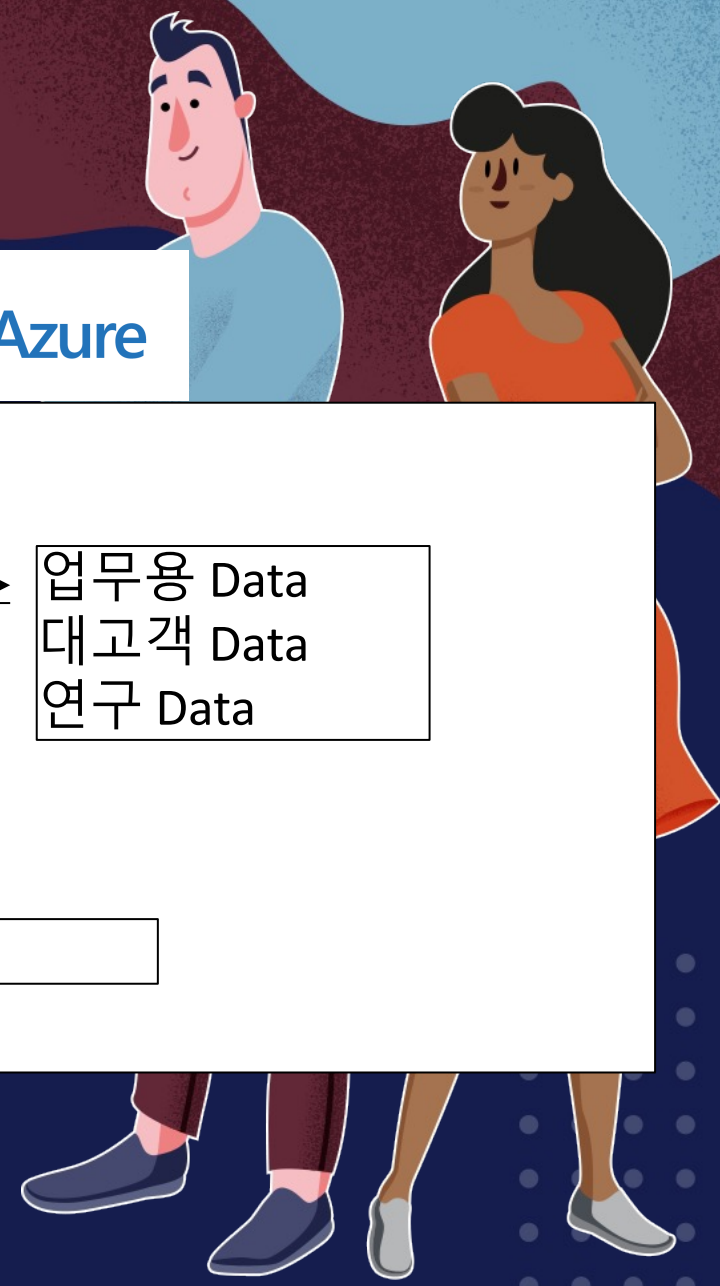
Microsoft Azure

OpenAI ⟷ 업무용 Data
대고객 Data
연구 Data

↓

OpenAI

Custom Model



Hello AI

TRUSTED CLOUD

Azure has the deepest and most comprehensive compliance coverage in the industry

GLOBAL

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- ISO 9001
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

US GOV

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- DoD DISA SRG Level 5
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

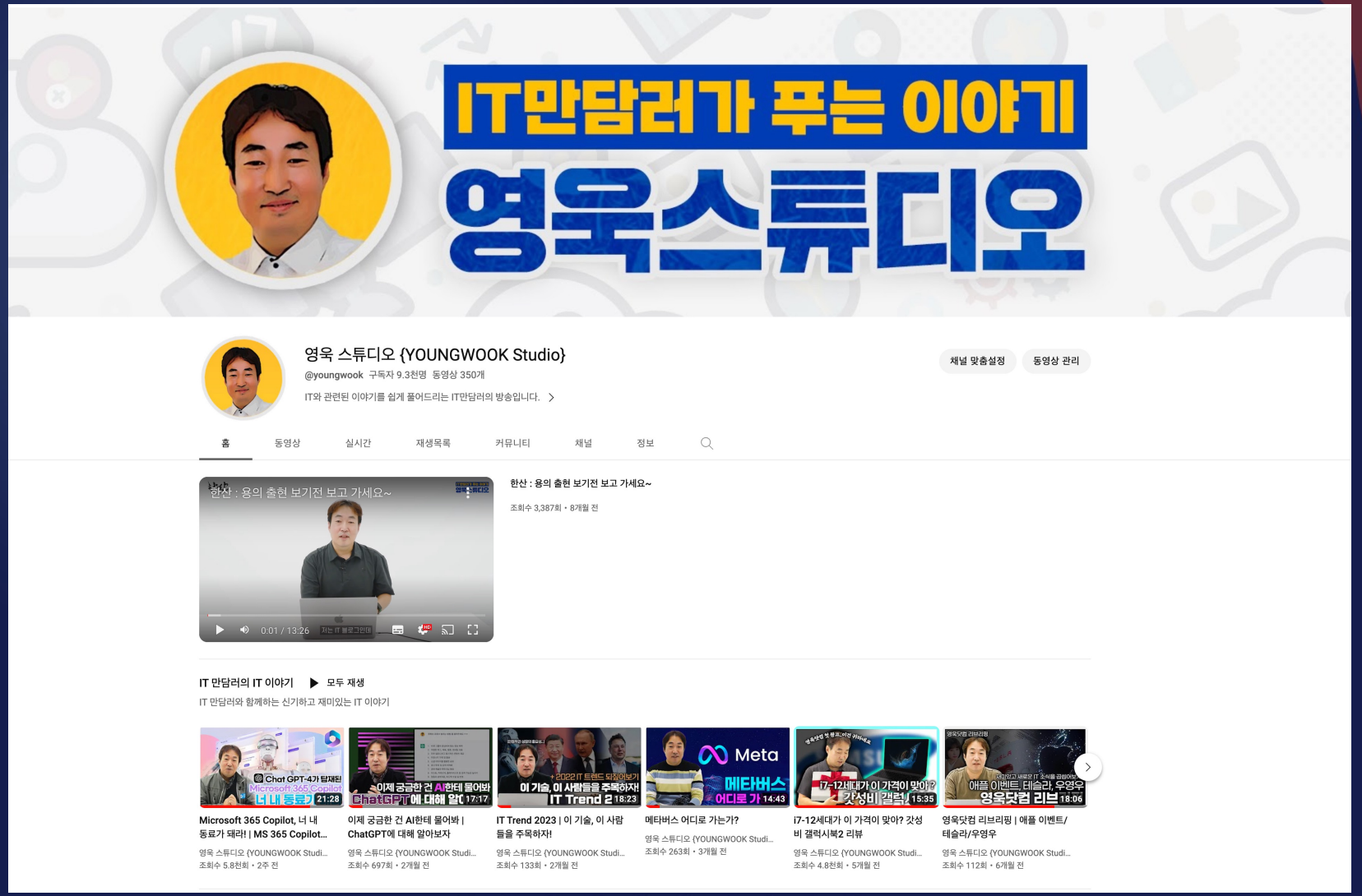
INDUSTRY

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

REGIONAL

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

Hello AI


IT만담러가 푸는 이야기
영욱스튜디오
영욱 스튜디오 {YOUNGWOOK Studio}
@youngwook 구독자 9.3천명 동영상 350개
IT와 관련된 이야기를 쉽게 풀어드리는 IT만담러의 방송입니다.
채널 맞춤설정
동영상 관리
홈
동영상
실시간
재생목록
커뮤니티
채널
정보
한산 : 용의 출현 보기전 보고 가세요~
0:01 / 13:26
한산 : 용의 출현 보기전 보고 가세요~
조회수 3,387회 • 8개월 전
IT 만담러의 IT 이야기
모두 재생
IT 만담러와 함께하는 신기하고 재미있는 IT 이야기
Chat GPT-4가 탑재된 Microsoft 365 Copilot 너 내 동료가 21:28
Microsoft 365 Copilot, 너 내 동료가 돼라! | MS 365 Copilot...
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 5.8천회 • 2주 전
이제 궁금한 건 AI한테 물어봐 ChatGPT에 대해 알아 17:17
이제 궁금한 건 AI한테 물어봐 | ChatGPT에 대해 알아보자
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 697회 • 2개월 전
+2022 IT 트렌드 되짚어보기 이 기술, 이 사람들을 주목하자! IT Trend 2 18:23
IT Trend 2023 | 이 기술, 이 사람들을 주목하자!
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 133회 • 2개월 전
Meta 메타버스 어디로 가 14:43
메타버스 어디로 가는가?
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 263회 • 3개월 전
i7-12세대가 이 가격이 맞아? 갓성비 갤럭시 15:35
i7-12세대가 이 가격이 맞아? 갓성비 갤럭시북2 리뷰
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 4.8천회 • 5개월 전
애플 이벤트, 테슬라, 우영우 영욱닷컴 리브 18:06
영욱닷컴 리브리핑 | 애플 이벤트/테슬라/우영우
영욱 스튜디오 {YOUNGWOOK Studi...
조회수 112회 • 6개월 전

Hello AI