2025: The YEAR of the AGENTS

RESEARCH NET.AI

Arunava (Ron) Majumdar
Founder, CEO

May 29th, 2025
in collaboration with

aitp Chicago Chapter Association of Information Technology Professionals

Abstract

The year started with an optimistic comment by Nvidia CEO Jensen Huang at the CES trade show in Las Vegas, that AI Agents will take off in 2025. Six months down the road, indeed the prophecy has now become a reality. Several agentic systems are now available to exploit the trend and automate processes. Join the session to learn about AI agents, competing agentic platforms and their strengths and the emergence of standards around agents. Learn why AI Agents will play a critical role in augmenting decision making in the future. Investigate how applications may be built with these agentic interactions.

RESEARCH NET.AI

Research Net is dedicated to accelerating research and development through the automation platform. It is a collaboration between multiple universities and research institute to bring academic research to life.

Multiple packages are available for the startup community and product developers to bring their ideas to life in a cost-effective manner.

Research Net works closely with Open Development Platform to harden Open-Source products and provide a plan to implement in production. Join the platform to build your own products at light speed.

Arunava (Ron) Majumdar

arunava@researchnet.ai

FOUNDER, CEO
Research Net.ai,
Open Development Platform,
Panthers Sports Inc.,
Chicago Panthers LLC.
Former Head, IBM Center for Advanced Studies (USA)

https://arunava.com

https://www.linkedin.com/in/arunava-majumdar/

Arunava (Ron) Majumdar is the Founder, CEO of Open Development Platform, providing an Open Source environment catered to Academics, Researchers and Professionals for co-development and free exchange of ideas. He is also the Founder, CEO of Research Net.AI Inc. where confidential products may be developed using the automation and agentic platform in a hyper-accelerated timeline.

He is the former Head of IBM Center for Advanced Studies (CAS) US and the coordinator for CAS India, CAS Australia and CAS Africa. He was the Principal Solution Architect with more than 28 years of software design, architecture and development leading the IBM Application Modernization portfolio for Signature Telecommunication Accounts.

Ron spearheaded in numerous Academic Research initiatives with top universities (NC State, Northwestern, University of Chicago, etc.) across multiple industries. He has led teams and provided Architecture Solutions, Design, Development and Deployment of 50+ Projects with 40+ Fortune 500. His focus areas are Integration, Artificial Intelligence and Pattern Engineering and holds several patents in these fields. He is involved with automated deployment strategies to the Cloud and Kubernetes environments.

Ron is in the leadership board for IBM Open Innovation Community (OIC) Chicago Chapter, Chicago Chapter Leader for AI Camp, Host of Future Tech SIG at AITP Chicago and the Leader for the Developer Advocacy program in Chicago with AI Alliance and a mentor at the Polsky Center. He is the Founder of IBM Services Asset Community and Chicago Panthers (sports).

Titles: • Founder, IBM Services Asset Community • Founder, Open Development Platform • Lead, IBM Asset Strategy • Member, IBM Academy of Technology • Host, Future Tech SIG, AITP Chicago • President, Chicago Emerging Leaders • Board, IdeazShack Innovation Center • Chapter Lead, AI Camp • Founder, Chicago Panthers • Life Member, Poet's Foundation • Content Creator and Editor, Open Development, Developerworks TV • Mentor, Polsky Center, University of Chicago • Lead, Developer Advocacy in Chicago, AI Alliance

What are Agents ?

IBM

An artificial intelligence (AI) agent refers to a system or program that is capable of autonomously performing tasks on behalf of a user or another system by designing its workflow and utilizing available tools.

Google

AI agents are software systems that use AI to pursue goals and complete tasks on behalf of users. They show reasoning, planning, and memory and have a level of autonomy to make decisions, learn, and adapt.

WIKIPEDIA

In artificial intelligence, an intelligent agent is an entity that perceives its environment, takes actions autonomously to achieve goals, and may improve its performance through machine learning or by acquiring knowledge.

Definition

An AI Agent is a software entity that is aware of its environment and can interact with it to automate tasks using AI models, has the ability to invoke tools and can either take a decision or produce a desired output.

Bots, Assistants, Agents

	AI agent	AI assistant	Bot
Purpose	Autonomously and proactively perform tasks	Assisting users with tasks	Automating simple tasks or conversations
Capabilities	Can perform complex, multi-step actions; learns and adapts; can make decisions independently	Responds to requests or prompts; provides information and completes simple tasks; can recommend actions but the user makes decisions	Follows pre-defined rules; limited learning; basic interactions
Interaction	Proactive; goal-oriented	Reactive; responds to user requests	Reactive; responds to triggers or commands

Source: https://cloud.google.com/discover/what-are-ai-agents#what-is-the-difference-between-ai-agents-ai-assistants-and-bots

Rise of AI Agents

Alan Turing's Turing Test (1950): Could a machine think like a human? That's what Turing set out to determine (Turing, 1950)

1950

1956

Dartmouth Conference (1956): AI was officially born, with researchers aiming to build systems that could replicate human intelligence.

ELIZA (1966): The first chatbot! Joseph Weizenbaum's ELIZA mimicked human conversation using simple pattern matching (Weizenbaum, 1966).

1966

1970-80

The Rise of Rule-Based AI Expert Systems Dominate (1970s-80s): These programs used rules and logic to solve problems (e.g., MYCIN, a medical diagnosis system).
PROLOG (1972): A programming language designed for logic-based AI development.
Reinforcement Learning Breakthrough (1988): Sutton and Barto developed temporal difference learning, a key reinforcement learning method (Sutton & Barto, 1988).

Intelligent Agents Take Shape
Rise of Intelligent Agents: AI systems began operating with a degree of autonomy, processing information and making simple decisions.
Early Virtual Assistants: Basic AI-driven assistants started to appear, laying the foundation for today's AI-powered chatbots.

1990s

2000s

Machine Learning Takes Over The ML Boom: AI agents started leveraging statistical machine learning models for better decision-making.
Advancements in NLP: AI agents became more conversational and useful in real-world applications.
IBM Watson (2006): This AI made headlines when it crushed human contestants on *Jeopardy!* (IBM Watson).

Deep Learning Changes Everything
AlexNet (2012): Deep Convolutional Neural Network for classification of images based on the paper.
AlphaGO (2016): Google DeepMind's deep reinforcement learning program beat world champion Lee Sedol.
Attention Network (2017): Attention is All You Need paper.

2010s

2020s

OpenAI GPT-3 (2020): AI agents gained serious conversational abilities with OpenAI's language model (Brown et al., 2020).

2021

DALL-E (2021): Text-to-image model.

LangChain (2022): Open-Source project by Harrison Chase, while working at machine learning startup Robust Intelligence to build simple agents.

2022

ImageBind (2023): Multi-modal model paper.

2023

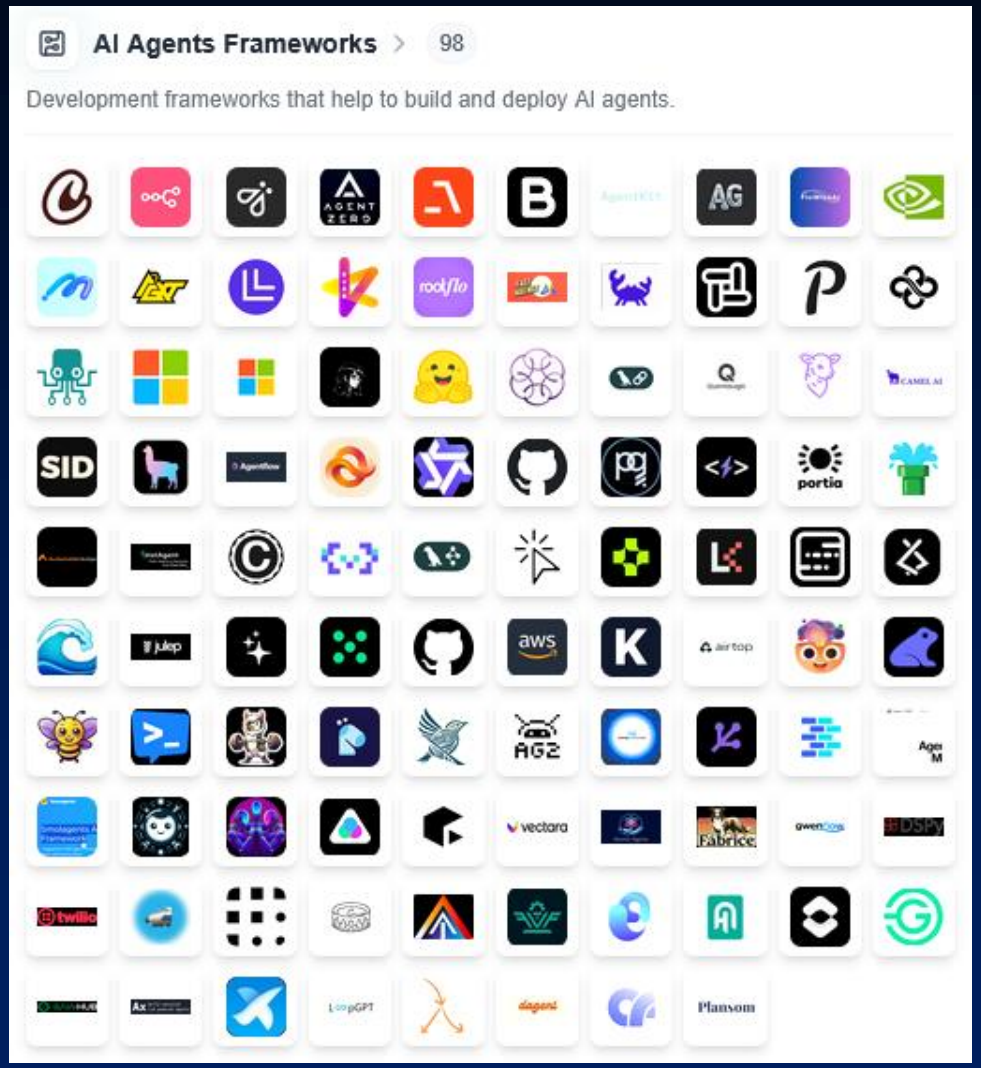
Devin AI (2024): AI software developer tool created by startup Cognition Labs.

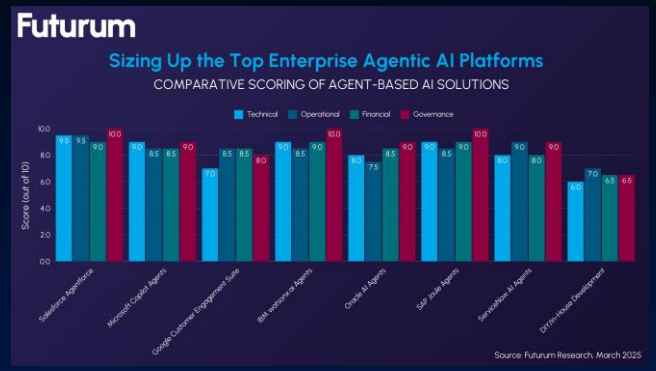
2024

2025

Source: https://www.wwt.com/blog/the-evolution-of-ai-agents-from-simple-programs-to-agentic-ai

State of the Art AI Agents





Source: https://futurumgroup.com/press-release/rise-of-agentic-ai-leading-solutions-transforming-enterprise-workflows-in-2025/

Source: https://www.techarena.ai/content/vast-data-launches-ai-operating-system

Source: https://aiagentsdirectory.com/landscape

Key Findings

SS&C Blue Prism AI Trends. Respondent base: 1,650 online interviews with Senior Management DMs at General Manager level or above in organizations with 250+ employees. Regions surveyed: Americas (300 interviews), Europe (1,100 interviews), and APAC (250 interviews). Fieldwork dates: 11-30 Dec, 2024.

29%

of organizations are already leveraging agentic AI

What are your organization's plans for adopting the latest leading-edge AI?

- **29%** - We have already implemented this
- **44%** - We are currently implementing this
- **18%** - We are planning implementation
- **5%** - We are considering options
- **3%** - We are exploring feasibility
- **1%** - We are not considering this

94%

view process orchestration as key to successful AI deployment

Process orchestration capabilities are key to the successful deployment of the latest leading-edge AI, because managing processes end-to-end is essential to achieving the best results.

- **94%** - Agree
- **4%** - Disagree
- **3%** - Not sure

88%

of global organizations are measuring the value derived from adopting AI

84%

of business leaders recognize AI's potential to disrupt traditional ways of working

80%

believe that by AI releasing knowledge workers, it will deliver high benefits

78%

of organizations don't always trust agentic AI

How would you describe the level of trust you have in the ability of agentic AI to make the right decisions and carry out work autonomously? I would trust agentic AI's work...

- **78%** - Mostly/sometimes/rarely/never/not sure
- **22%** - Always

69%

of AI projects don't make it into live, operational business use

- **31%** - The majority of our latest leading-edge AI projects make it into live, operational business use

Source: https://files.blueprism.com/downloads/gated/white-papers/kl-0245-AI-Survey-Main.pdf

LangChain

https://www.langchain.com/

The Agent Stack

ORCHESTRATION:
Build agents with LangGraph

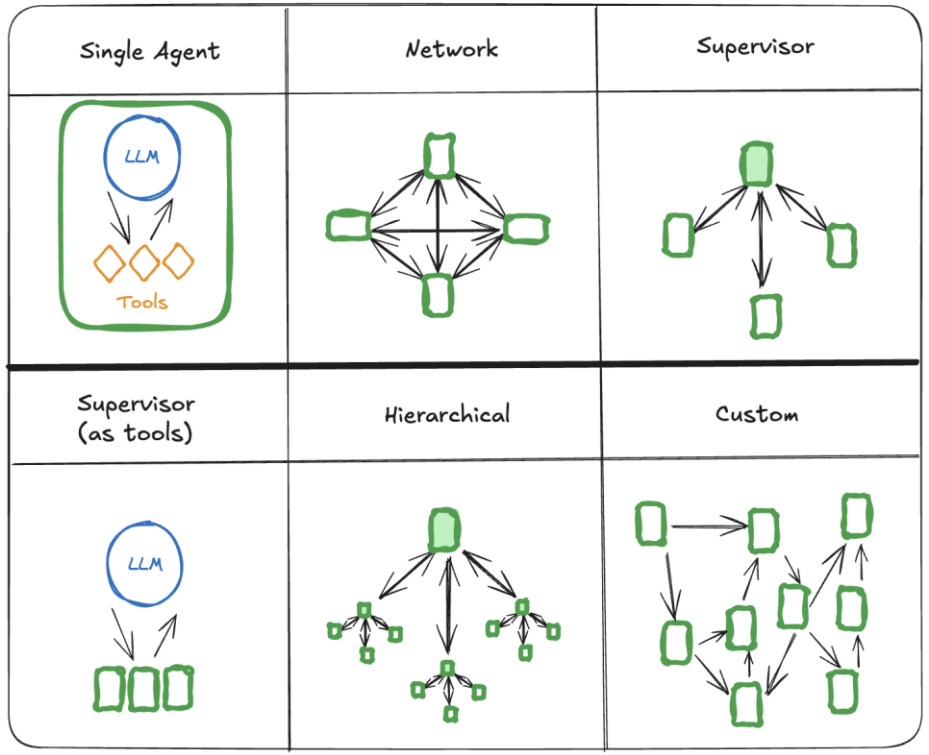
Controllable agent orchestration with built-in persistence to handle conversational history, memory, and agent-to-agent collaboration.

INTEGRATIONS:
Integrate components with LangChain

EVALS & OBSERVABILITY:
Gain visibility with LangSmith

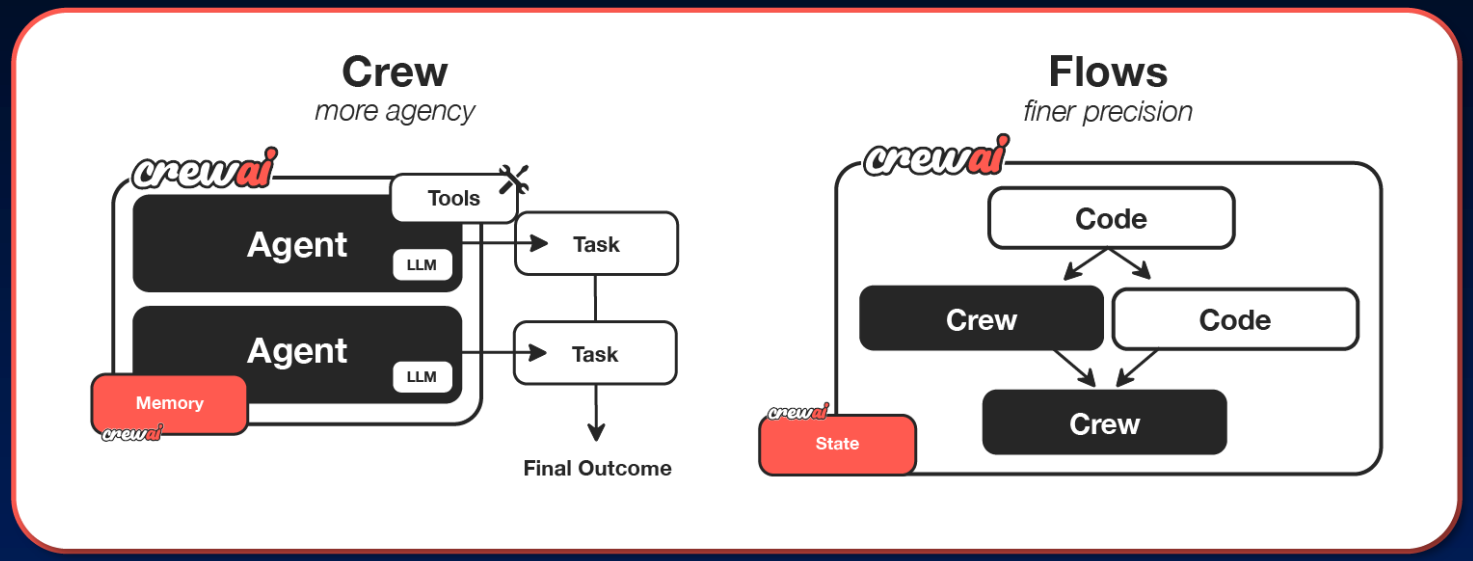
DEPLOYMENT:
Deploy & manage with LangGraph Platform

```
from langgraph.channels import LastValue,
EphemeralValue
from langgraph.pregel import Pregel,
NodeBuilder

node1 = (
    NodeBuilder().subscribe_only("a")
    .do(lambda x: x + x)
    .write_to("b")
)

node2 = (
    NodeBuilder().subscribe_only("b")
    .do(lambda x: x + x)
    .write_to("c")
)


app = Pregel(
    nodes={"node1": node1, "node2": node2},
    channels={
        "a": EphemeralValue(str),
        "b": LastValue(str),
        "c": EphemeralValue(str),
    },
    input_channels=["a"],
    output_channels=["b", "c"],
)

app.invoke({"a": "foo"})
```



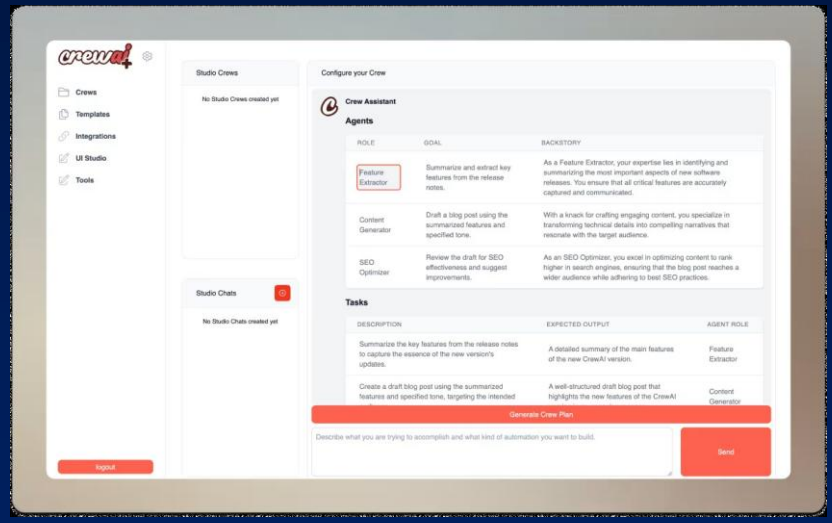
Features Supported:
Graph, Streaming, Human-in-the-Loop, Breakpoints, Time Travel, MCP

https://www.crewai.com/




```
# src/my_project/crew.py
from crewai import Agent, Crew, Process, Task
from crewai.project import CrewBase, agent, crew, task
from crewai_tools import SerperDevTool
from crewai.agents.agent_builder.base_agent import BaseAgent
from typing import List

@CrewBase
class LatestAiDevelopmentCrew():
```

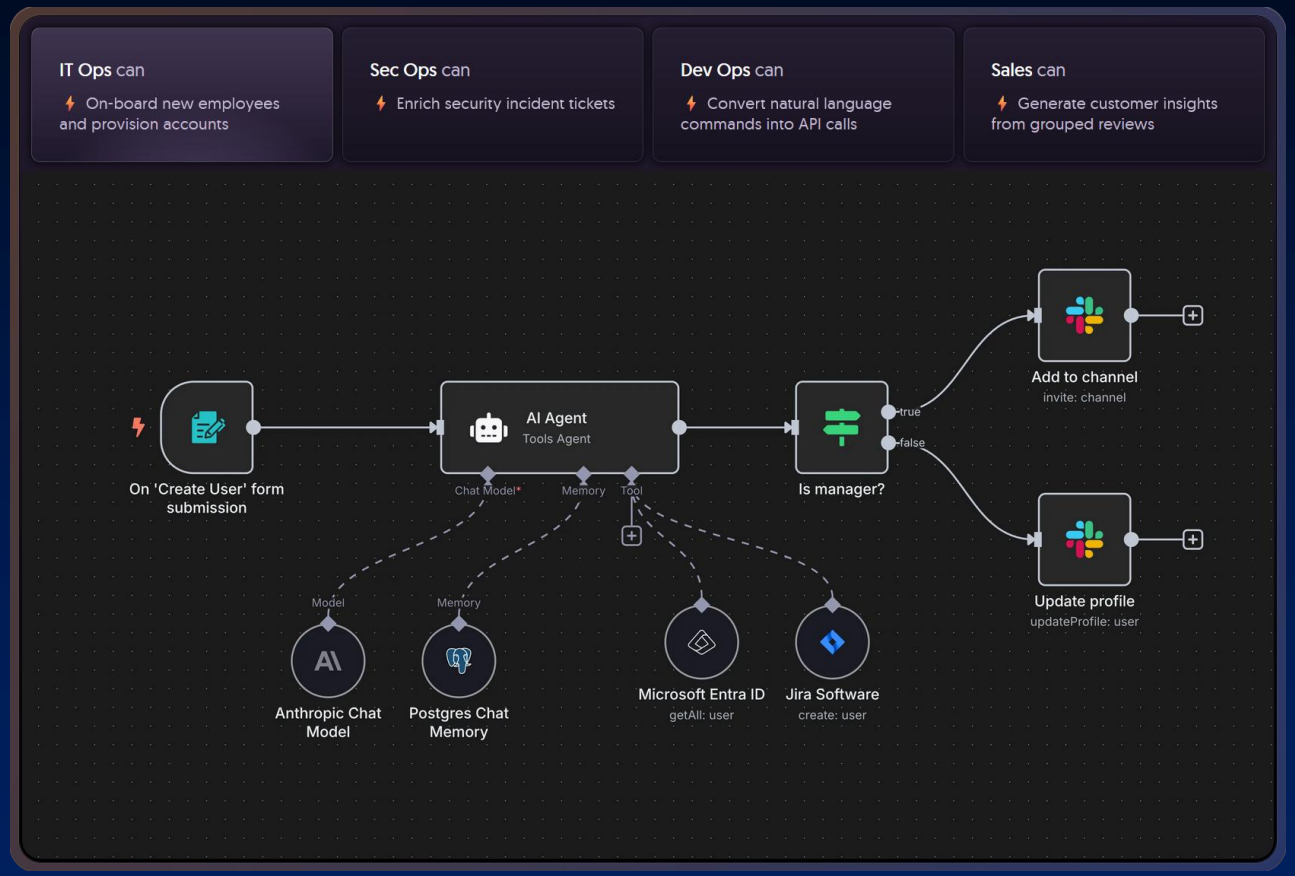
...

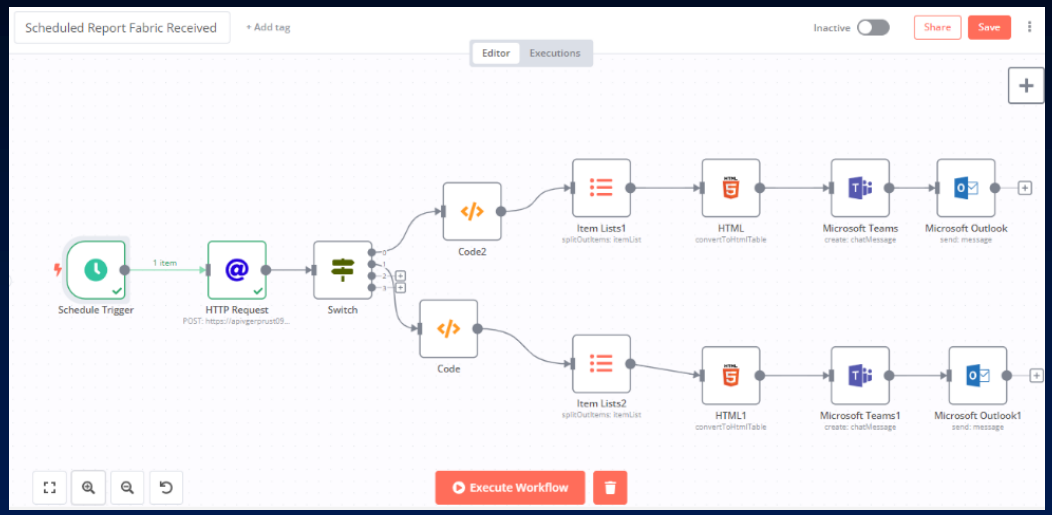


Features Supported:
Multi-Agent Collaboration, Sequential, Hierarchical, Asynchronous, Memory

n8n

https://n8n.io/



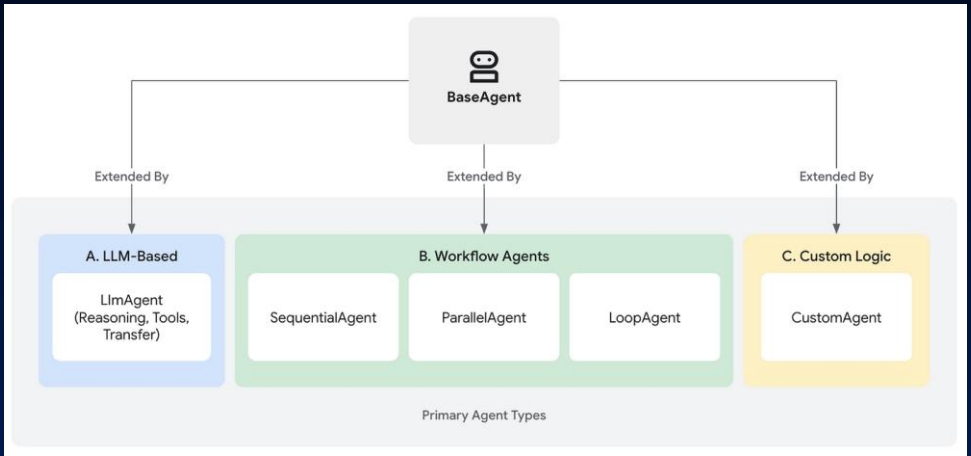



```
  subscribers_to_notify = []
    for item in items[0]["json"]["low_stock_items"]:
        if item["stock"] > 0:
            for subscriber in
items[0]["json"]["subscribers"]:
                if subscriber["product_id"] == item["id"]:
                    subscribers_to_notify.append({
                        "product_name": item["name"],
                        "email": subscriber["email"]
                    })
    output = {
        "subscribers_to_notify": subscribers_to_notify
    }
```

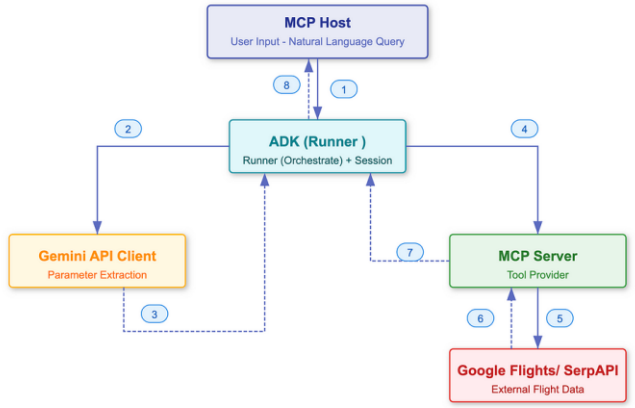
Features Supported:
Multi-Agent Collaboration, Sequential, Hierarchical, Asynchronous, Memory, No-Code

Agent Development Kit

https://google.github.io/adk-docs/



ADK (Agent Development Kit) + MCP (Model Context Protocol) with Gemini 2.5 Pro LLM



Flexible Orchestration

Define workflows using workflow agents (`Sequential` , `Parallel` , `Loop`) for predictable pipelines, or leverage LLM-driven dynamic routing (`LlmAgent` transfer) for adaptive behavior.

Learn about agents

Multi-Agent Architecture

Build modular and scalable applications by composing multiple specialized agents in a hierarchy. Enable complex coordination and delegation.

Explore multi-agent systems

Rich Tool Ecosystem

Equip agents with diverse capabilities: use pre-built tools (Search, Code Exec), create custom functions, integrate 3rd-party libraries (LangChain, CrewAI), or even use other agents as tools.

Browse tools

Deployment Ready

Containerize and deploy your agents anywhere – run locally, scale with Vertex AI Agent Engine, or integrate into custom infrastructure using Cloud Run or Docker.

Deploy agents

Built-in Evaluation

Systematically assess agent performance by evaluating both the final response quality and the step-by-step execution trajectory against predefined test cases.

Evaluate agents

Building Safe and Secure Agents

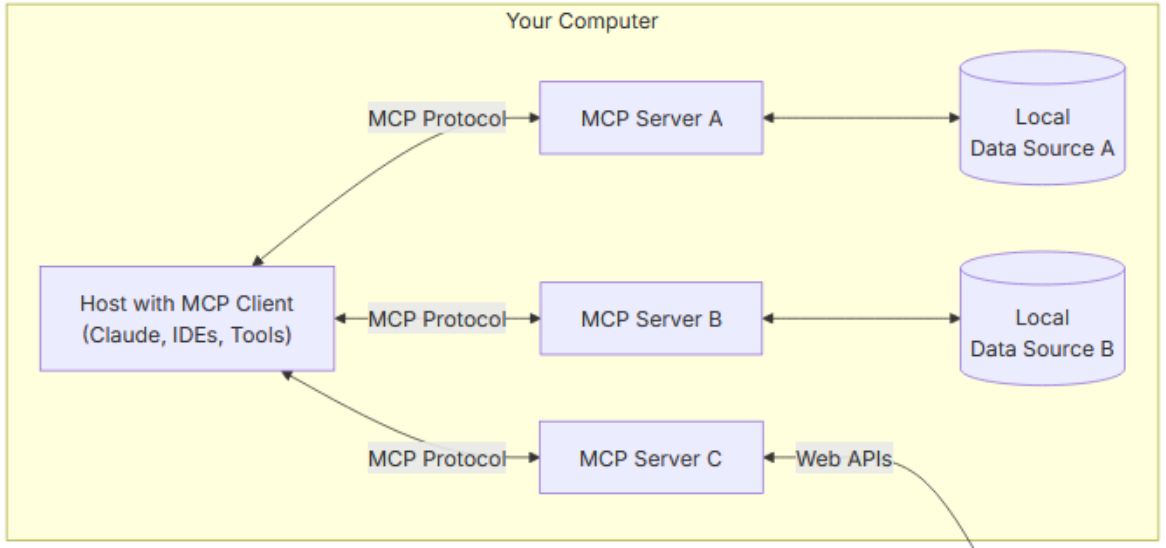
Learn how to building powerful and trustworthy agents by implementing security and safety patterns and best practices into your agent's design.

Safety and Security

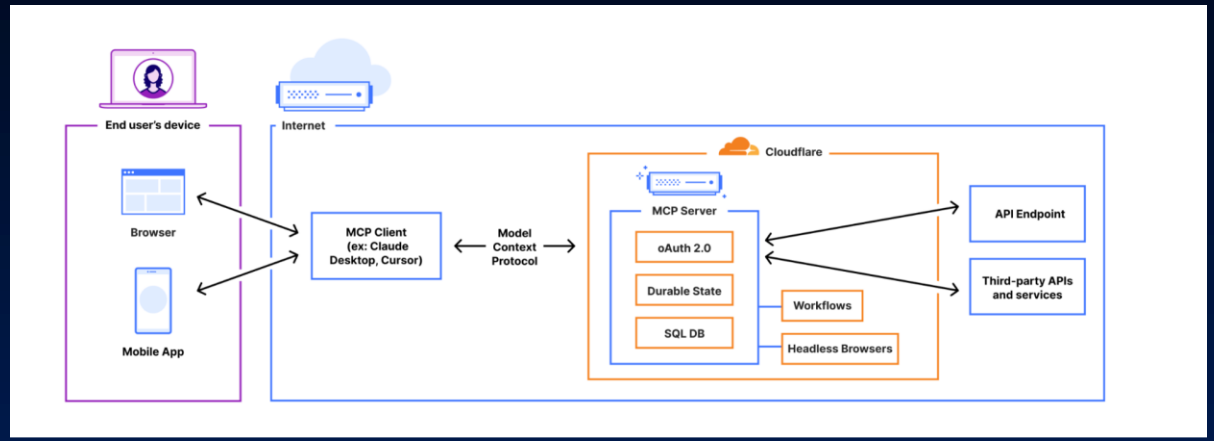
Features Supported:
Multi-Agent Collaboration, Sequential, Parallel, Loop, MCP, A2A

Model Context Protocol

https://www.anthropic.com/news/model-context-protocol



- **MCP Hosts**: Programs like Claude Desktop, IDEs, or AI tools that want to access data through MCP
- **MCP Clients**: Protocol clients that maintain 1:1 connections with servers
- **MCP Servers**: Lightweight programs that each expose specific capabilities through the standardized Model Context Protocol
- **Local Data Sources**: Your computer's files, databases, and services that MCP servers can securely access
- **Remote Services**: External systems available over the internet (e.g., through APIs) that MCP servers can connect to



Source: https://humanloop.com/blog/mcp

Features Supported:
Multi-Agent Collaboration, Integration

The Agentic Spectrum

1 RPA

- Unattended automation
- Attended automation

2 RPA and BPM

- Attended and unattended automation
- Orchestration
- Generative AI

3 RPA, BPM and Agents

- Attended and unattended automation
- Orchestration
- Specific agents
- AI-powered agents

4 RPA, BPM, Agents and an Agent Builder

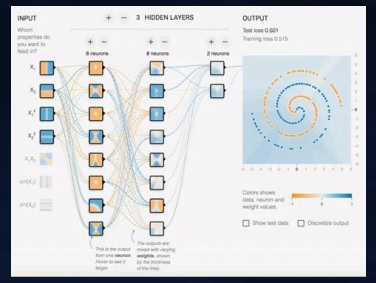
- Semi-agentic automation
- Non-AI automation
- Gen AI-enabled automation

5 RPA, BPM and an Agent Builder for Semi-Agentic and Fully Agentic Automation

- Automation
- Orchestration
- Third-party agents
- Semi-agentic building
- Fully-agentic building

Source: https://files.blueprism.com/downloads/gated/white-papers/mr_0417_Path-To-Agentic-AI.pdf

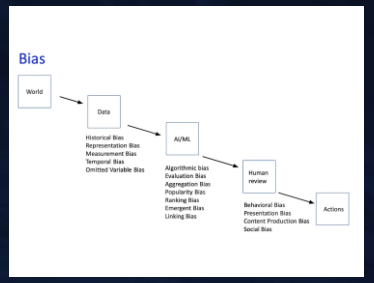
Pillars for Responsible AI



Explainability

Visibility in Decision Making

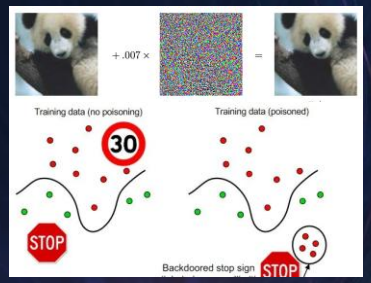
Contextualization in the decision-making process. How was the decision taken, what were the feature sets used to come to the inference, what are the models used, what data was used in the training set for the model.



Fairness

Unbiased Decision Making

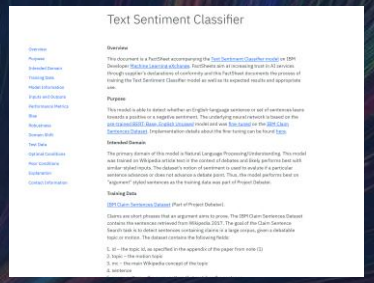
Bias against views such as age, gender, race, or socioeconomic status must be eliminated. Fairness models should check for Demographic Parity, Equalized Odds, Individual Fairness, Counterfactual Fairness and Casual Reasoning.



Robustness

Defend against Attacks

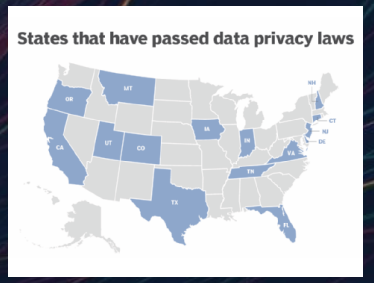
AI models are subject to adversarial attacks to produce wrong inferences. Robust AI must handle exceptional conditions, such as data poisoning or malicious attacks, without causing unintentional harm.



Transparency

AI Factsheet Publication

Transparency reinforces trust. The AI process must be disclosed, including what data is being collected, how it will be used and stored, and who will have access to it.



Privacy

Protect Personal Information

AI Systems must de-identify and obfuscate data that has personal information before training the model. The system must also comply with various data and privacy laws and export regulations around the world.

Attack Surface for Generative AI

Prompt Injection

Prompt injection attacks aim to elicit an unintended response from LLM-based tools.
Direct: Hackers control the user input and feed the malicious prompt directly to the LLM.
Indirect: hackers hide their payloads in the data the LLM consumes, such as by planting prompts on web pages the LLM might read.

Infection

Attack the Supply Chain of LLM. Surgical editing of the LLM to spread false information. Impersonation to upload the LLM to a popular Model Hub under a known Open Source contributor.

Evasion

Evasion attack is designed in such a way that when the network is fed an adversarial noise (a carefully perturbed input) that looks and feels the same as its untampered copy to a human, completely throws off the classifier.

Poisoning

LLMs are dependent on the training dataset and if the data is not carefully analyzed before training, it may cause serious problems for the LLM output. One study done on RAG poisoning showed that an Attack Success Rate of 97% can be achieved by 0.0002% of poisoned text based on the poisoned question.

Prompt Leakage

Extraction of information may be achieved by carefully crafted targeted questions. If the model training set contains PI or SPI it may be retrieved by this method. The information can then be used for AI Generated Phishing attacks using emails, chatbots, Deep Fake audio, etc.

Denial of Service

Overwhelm the services with questions to stop processing of legitimate interactions. This targets features in the LLM like the Attention Mechanism, Memory Constraints, Output Generation Algorithms to send a barrage of complex queries exploit specific vulnerabilities and bottlenecks of the target model.

Other Risks in Generative AI

Hallucination

Hallucination in a foundation model (FM) refers to the generation of content that deviates from factual reality or includes fabricated in-formation. This a feature of LLMs rather than a bug and can be mitigated using Knowledge Injection using methods like Retrieval Augmented Generation (RAG).

Retrieval Augmented Generation

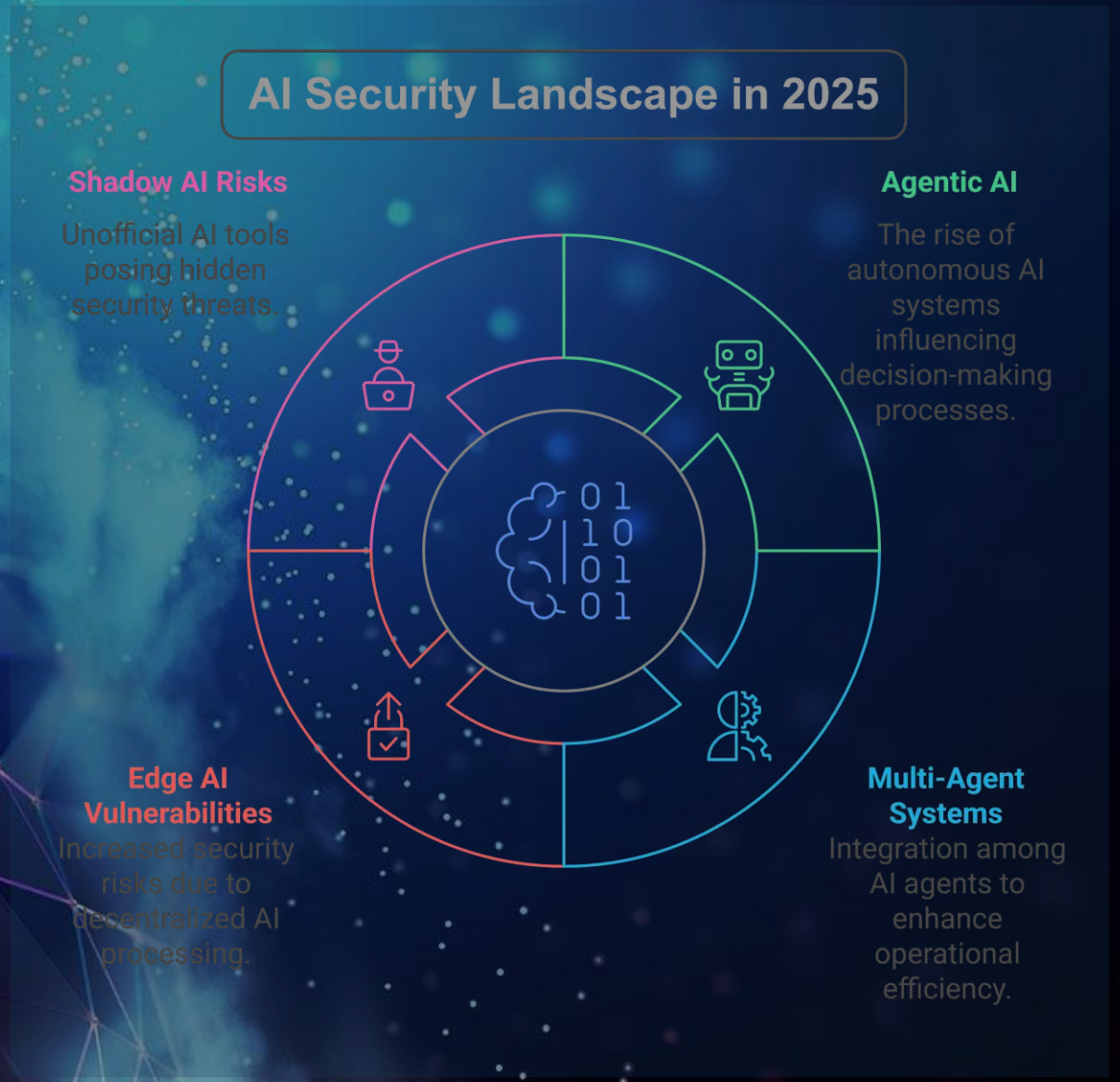
Data Drift

Data Drift refers to the phenomenon where the distribution of input data used to train a machine learning model changes over time, leading to degradation in the model's performance on new data. Create a profile for the input data model, continually monitor production data and create profile and find statistical divergence.

Model Drift

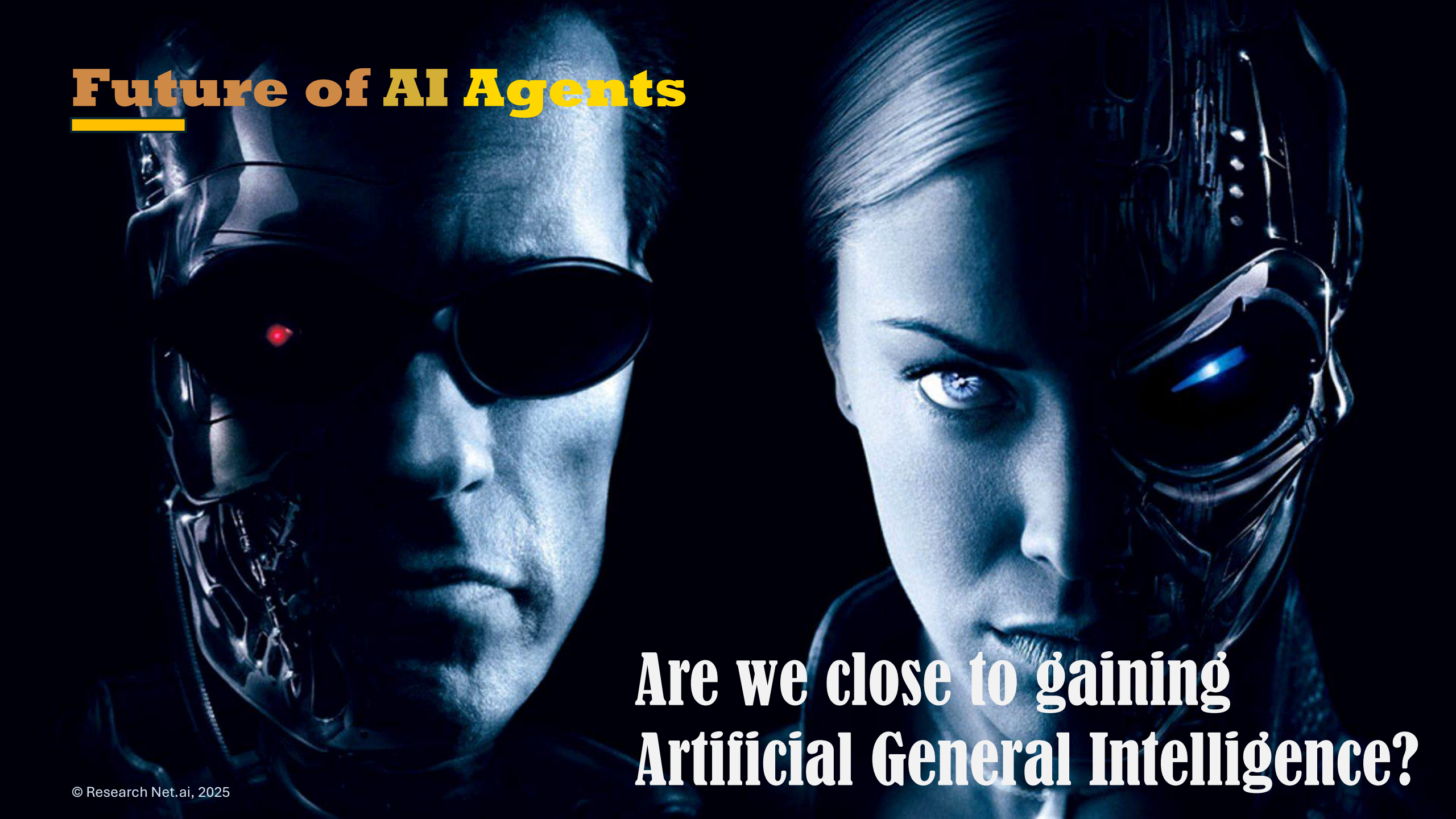
Also known as Concept Drift, occurs when there is a shift between the input variables and the target variable, at which point the algorithm begins to provide incorrect answers because the definitions are no longer valid. The shift in independent variables can take effect over a variety of time periods.

Extending the Risks based on AI Agent Deployments

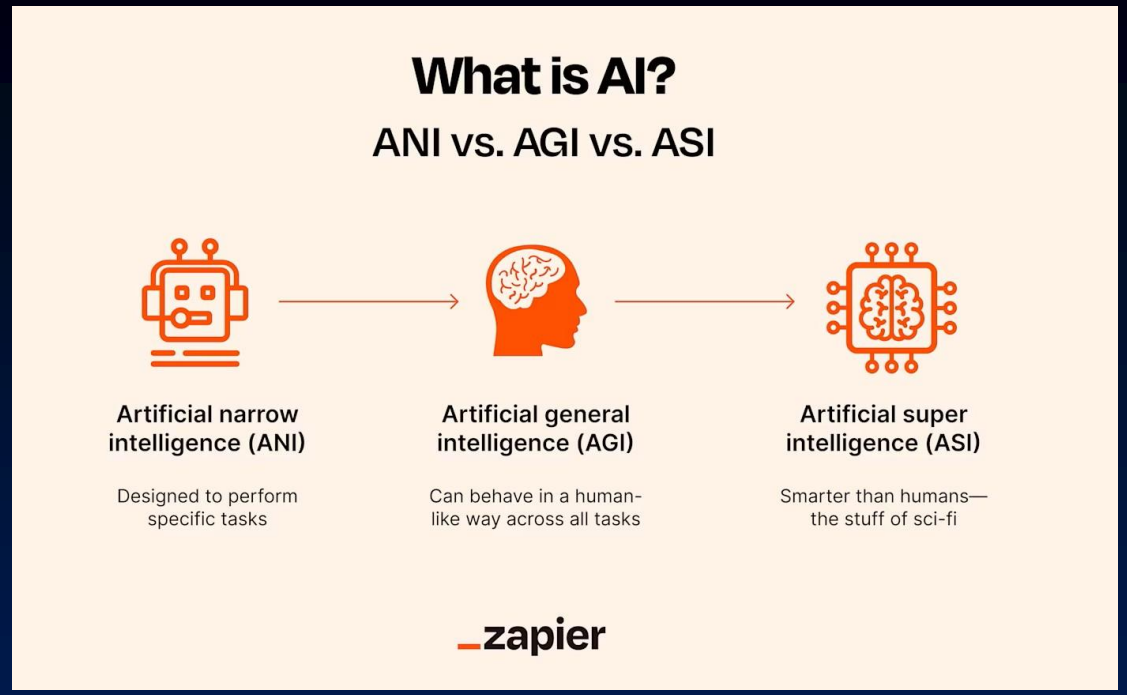


Source: https://becomingahacker.org/the-ai-security-landscape-in-2025-4add2123e045

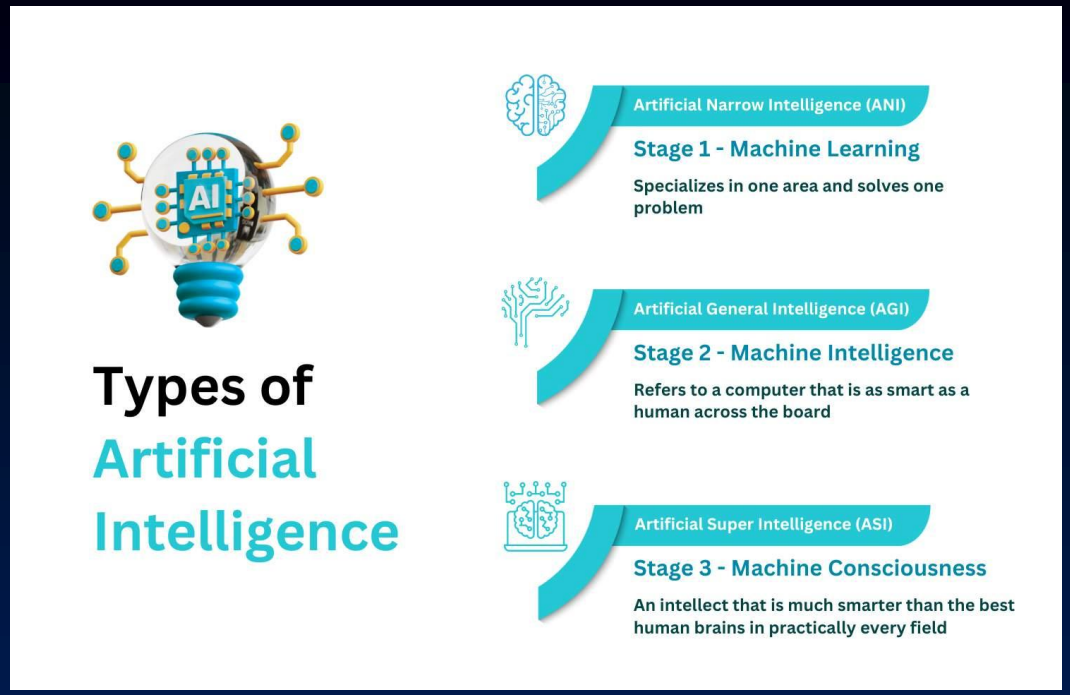
Future of AI Agents



Are we close to gaining Artificial General Intelligence?



Source: https://zapier.com/blog/artificial-general-intelligence/



Source: https://zapier.com/blog/artificial-general-intelligence/

Google leaders see AGI arriving around 2030

May 21, 2025

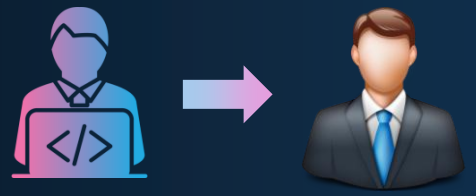
Source: https://www.axios.com/2025/05/21/google-sergey-brin-demis-hassabis-agi-2030

Let's leave it at that…


Thank You
Shukria
Dhanyavadagalu
Asante
Maake
Kiitos
köszönöm
Vinaka
감사합니다
Kam Sah Hammida
Manana
Dankon
Matondo
Terima Kasih
Dank Je
Dankscheen
спасибо
Mauruuru
Biyan
Diolch i Chi
Taiku
Tack
Blagodaram
Ngiyabonga
Dziekuje
Chokrane
Grazie
Arigato
Juspaxar
Mochchakkeram
Gracias
Tingki
Paldies
नन்றி
Bedankt
Dakujem
धन्यवाद
cảm ơn bạn
Grazas
Gratias Tibi
Ua Tsaug Rau Koj
Obrigado
Dĕkuji
Nirringrazzjak
Di Ou Mèsi
Kia Ora
Kop Khun Khap
ありがとう
Suksama
Hvala
Welalin
Djiere Dieuf
Rahmat
Matur Nuwun
谢谢
хвала
Danke
Merci
Go Raibh Maith Agat
Eskerrik Asko
Misaotra
Salamat
ขอบคุณ
Najis Tuke

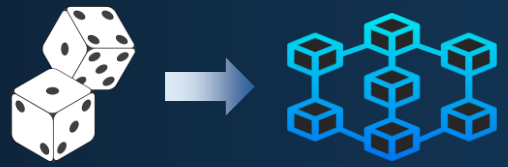
RESEARCHNET.AI

BRIDGING THE GAP BETWEEN ARTIFICIAL INTELLIGENCE AND COMPLEX BUSINESS PROCESSES



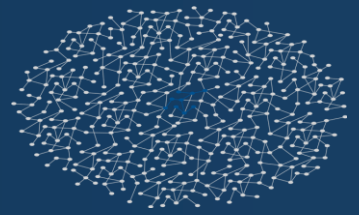
Focus on building business applications rather than generating code for the developer.

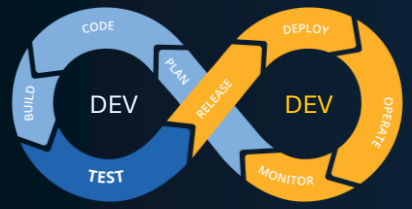
Provide generation and integration with complex business processes for essential operations of the business.



Moving from probabilistic code generation to deterministic artifact generation based on tested models.

Complex data structures are mapped with AI powered models for ERP systems.



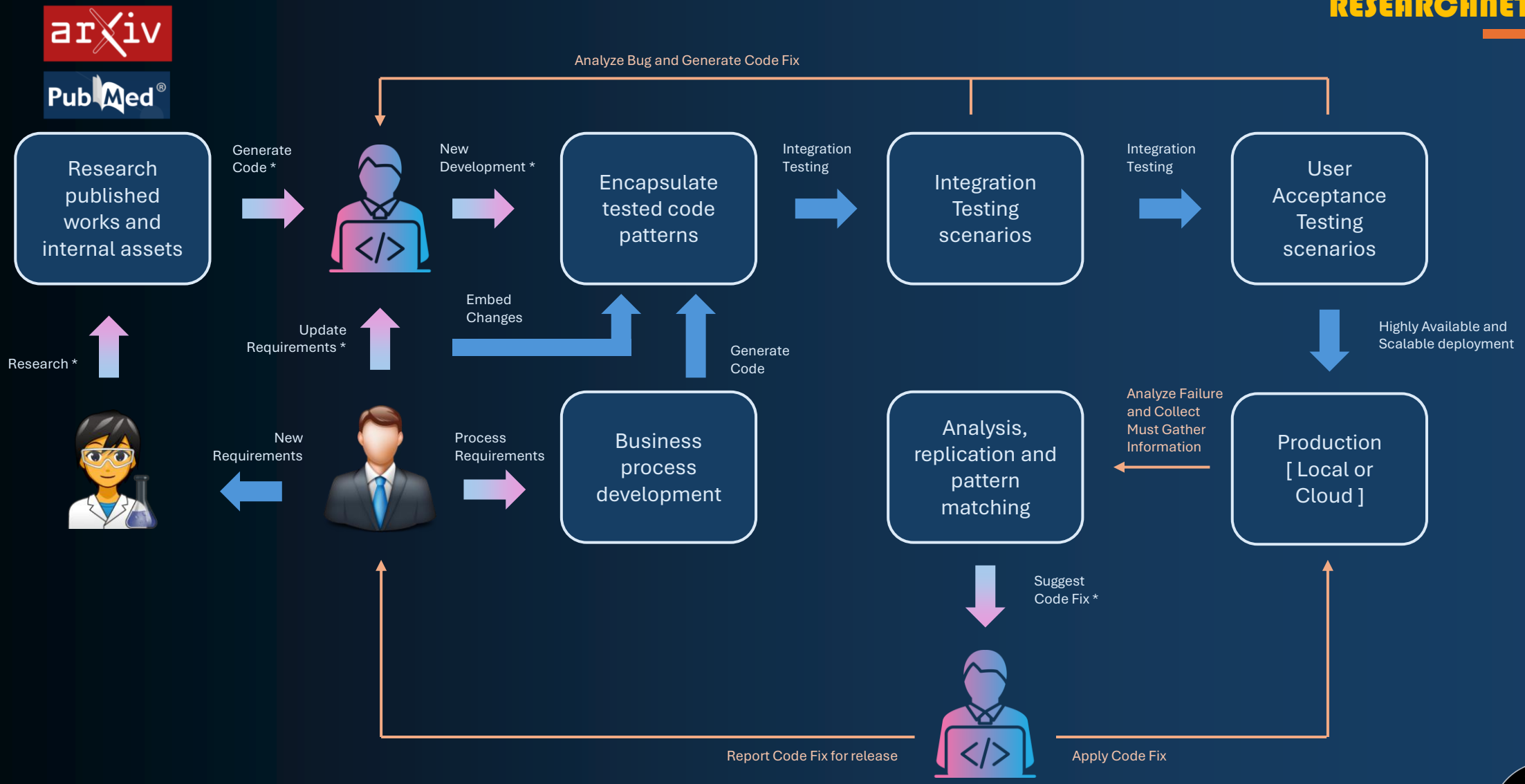


Support for the complete development lifecycle through patterns and plugins.

Requirements change over time and the regeneration of artifacts is achieved by preserving custom changes in delegate functions.

Connect with Researchers and Scientists around the world for collaborations on new research and products.

RESEARCHNET.AI



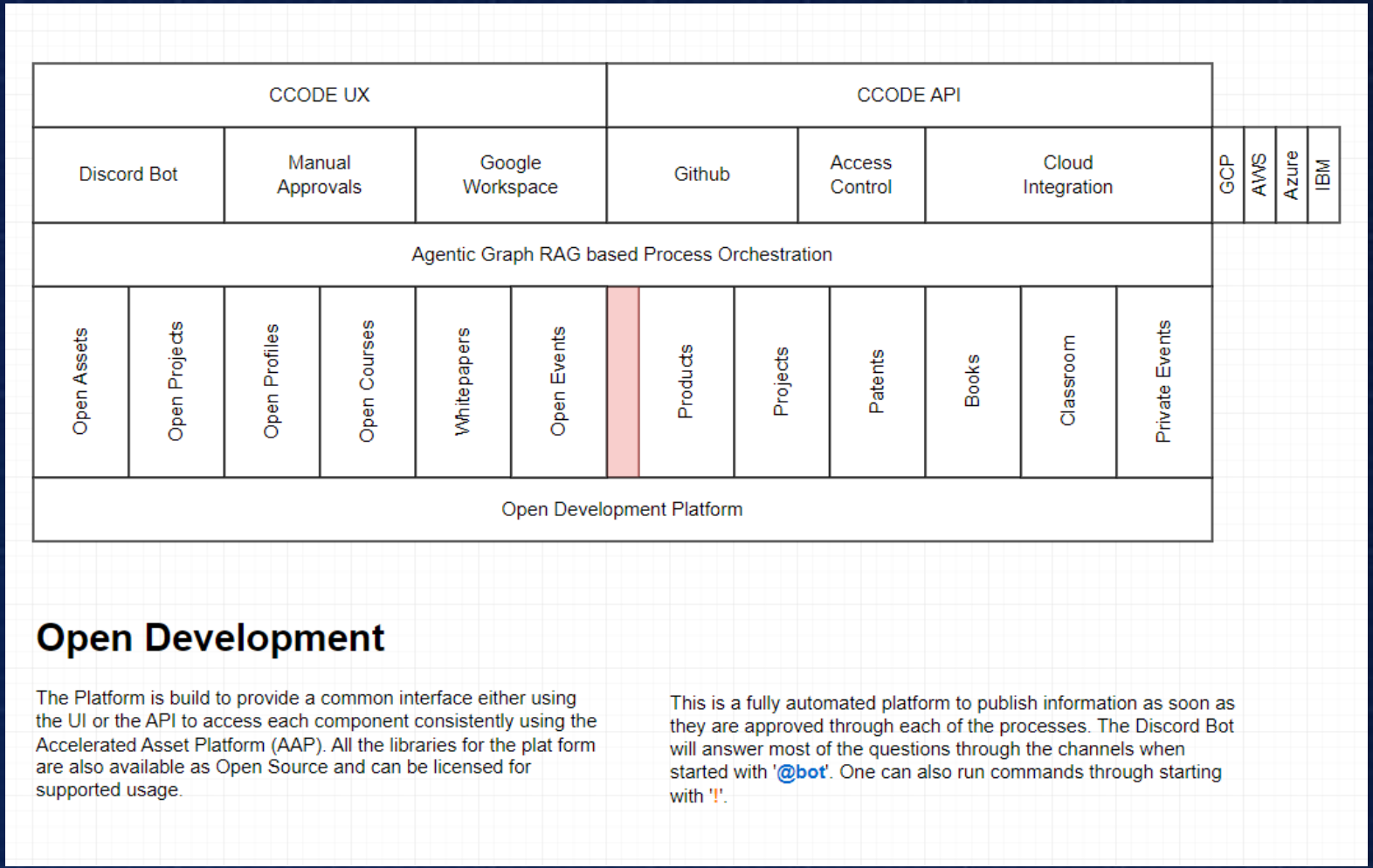
[*] Chat Interface

Open Development Platform

RESEARCH COLLABORATION AT SCALE

Collaborate on Open Source and Confidential Research on a Single Plane:

- Work with students and faculty on Open Project initiatives with Capstone projects
- Develop assets and publish academic papers for the work
- Participate in Open Events – hackathons, meetups, executive panels, etc.
- Work on Confidential projects, develop and submit patents
- Academic courses in collaboration with universities
- Earn Micro-credentials as digital badges for the contributions



Open Development

The Platform is build to provide a common interface either using the UI or the API to access each component consistently using the Accelerated Asset Platform (AAP). All the libraries for the plat form are also available as Open Source and can be licensed for supported usage.

This is a fully automated platform to publish information as soon as they are approved through each of the processes. The Discord Bot will answer most of the questions through the channels when started with '@bot'. One can also run commands through starting with '!'.