



AI and Data Synergy: Transforming the Business Landscape

Dr Michael Mavroforakis,
CTO, InTTrust

*InTTrust-IBM Executive Event, 'AIOps, Automation, Data Security - solving the puzzle'
02.11.23 @ Semiramis Hotel*

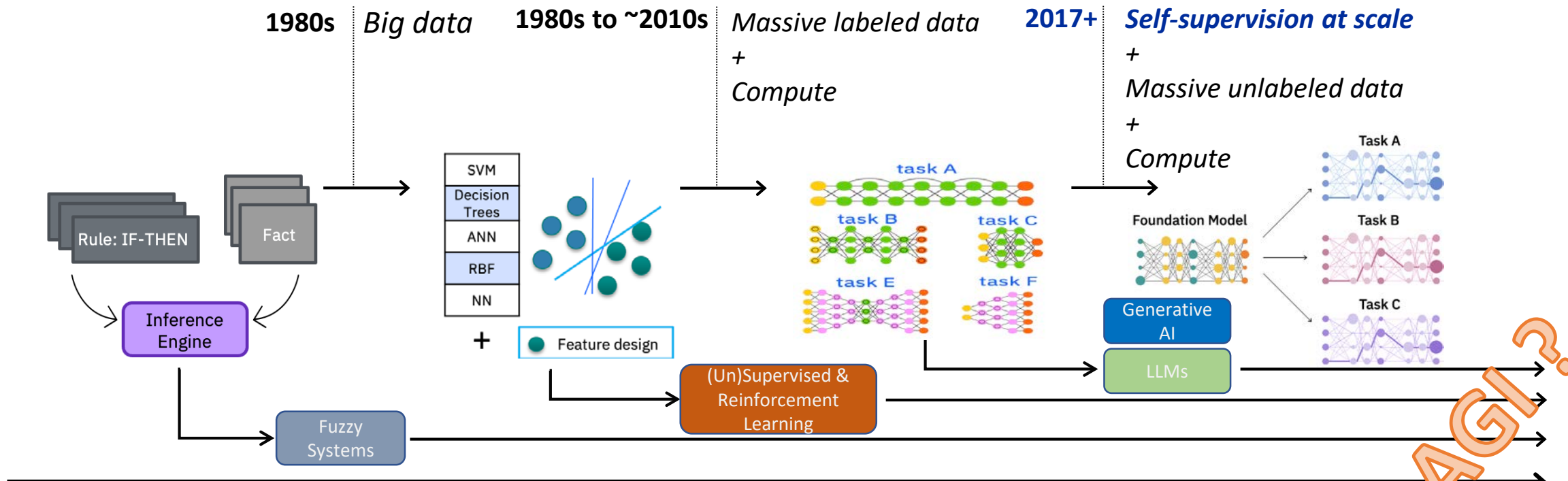


Overview



- From Data to AI
 - Evolution and adoption of AI
- From AI to new Data
 - Generative AI: GANs – Transformers – LLMs
- How AI transforms business
- AI Risks & Concerns
- AI application: Water Underground
- AI integrated platform: **watsonx**
- Conclusions

From Data to AI



AGI?

Expert systems

- Rule engines

Machine Learning

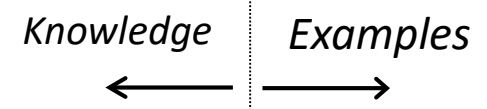
- ML algorithms
- Task-specific decision boundaries

Deep learning

- Network architectures
- Task-specific decision boundaries + feature representations

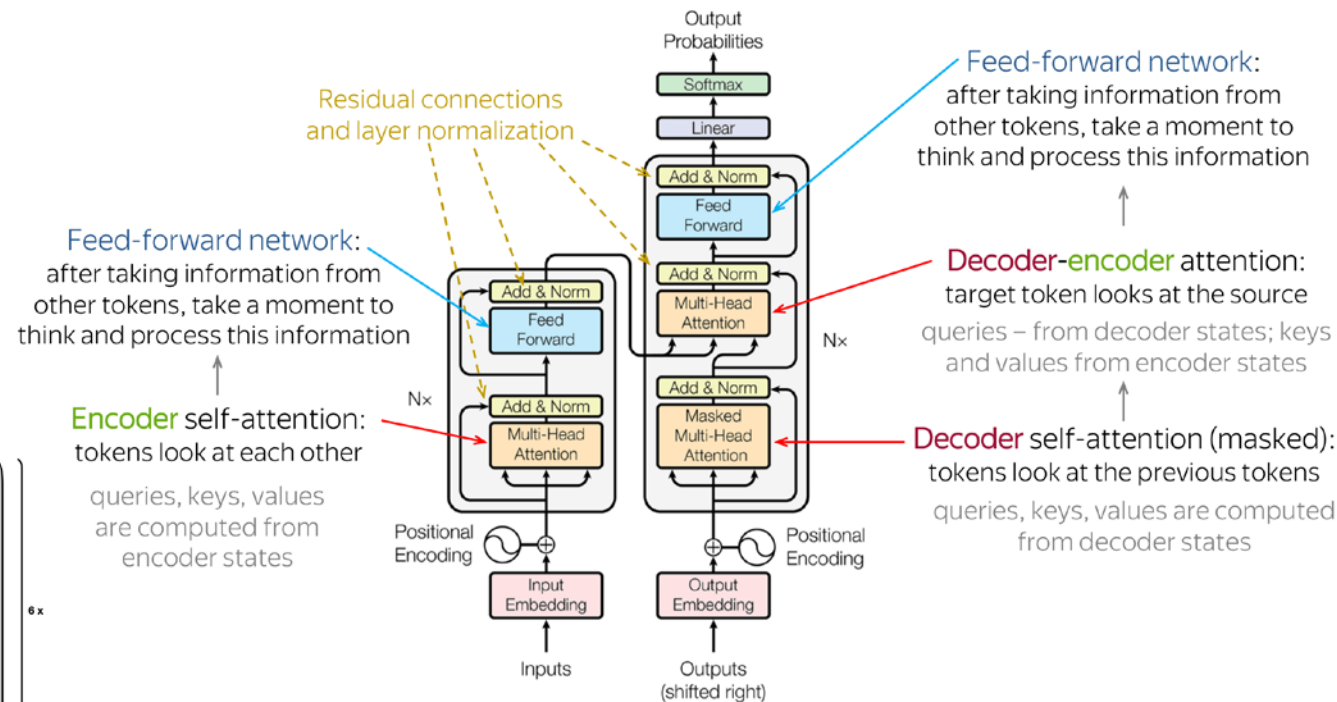
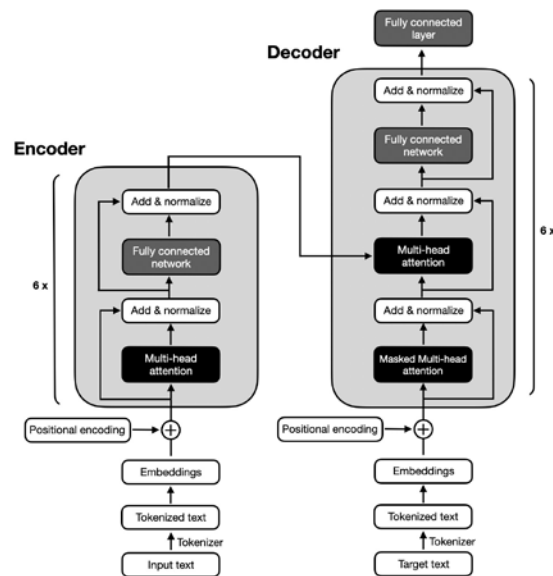
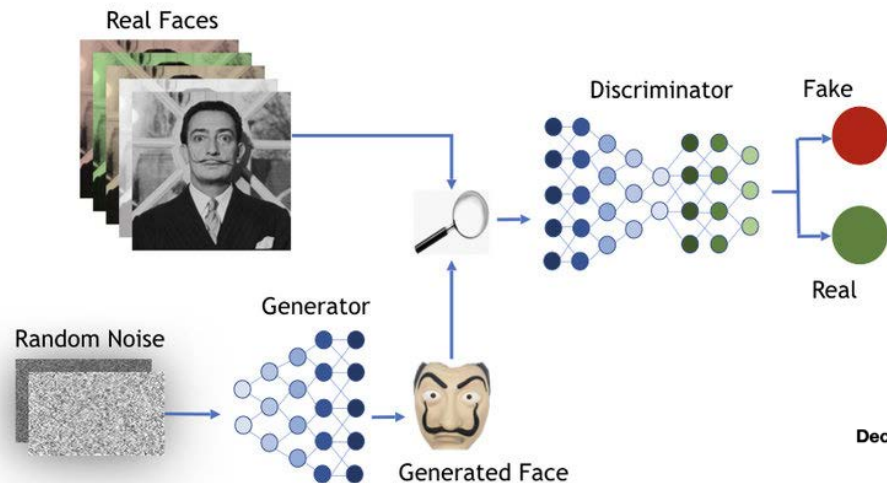
Foundation models

- Base model
- Adaptable decision boundaries and feature representations



From AI to *new* Data – *Generative AI*

Generative Adversarial Networks (GANs) – Encoders – Decoders – Transformers



Feed-forward network: after taking information from other tokens, take a moment to think and process this information

Encoder self-attention: tokens look at each other queries, keys, values are computed from encoder states

Feed-forward network: after taking information from other tokens, take a moment to think and process this information

Decoder-encoder attention: target token looks at the source queries – from decoder states; keys and values from encoder states

Decoder self-attention (masked): tokens look at the previous tokens queries, keys, values are computed from decoder states

GPT2 (2019) : 1.5 billion parameters
 GPT3 (2020): 175 billions ->-
 GPT4 (2023): 1.8 trillion ->- (13T tokens)

New (AI-Generated) Data examples



Encoders – Decoders – Transformers – Generative Adversarial Networks (GANs)
Generative AI and all that



Dall-e



StyleGAN

```
GPT-4
MM Write a program in Python to count and display the prime numbers up to 10000.
AI Certainly! Below is a Python program that calculates and displays all the prime numbers up to 10,000:

python Copy code
def is_prime(num):
    """Check if a number is prime."""
    if num < 2:
        return False
    for i in range(2, int(num**0.5) + 1):
        if num % i == 0:
            return False
    return True

def prime_numbers(limit):
    """Generate prime numbers up to a given limit."""
    for num in range(2, limit + 1):
        if is_prime(num):
            print(num, end=" ")

# Display prime numbers up to 10,000
prime_numbers(10000)

This program defines two functions:

1. 'is_prime(num)': This function checks whether a given number 'num' is prime. It returns 'True' if the number is prime and 'False' otherwise. For efficiency, it only checks divisibility up to the square root of the number.
2. 'prime_numbers(limit)': This function generates and prints all prime numbers up to a specified 'limit'. It calls the 'is_prime' function to determine whether each number in the range is prime.

When you run this program, it will display all prime numbers up to 10,000. Keep in mind that the output will be quite long, as there are 1,229 prime numbers between 2 and 10,000.
```

ChatGPT

```
GPT-4
MM Propose a strategy and implementation plan, writing a corresponding essay of about 300 words, of a steel parts European manufacturing industry to mitigate the ESG risk in two years time.
AI Title: Streamlining ESG Strategies in the European Steel Parts Manufacturing Sector

Introduction

As global emphasis on Environmental, Social, and Governance (ESG) standards continues to escalate, the European steel parts manufacturing industry must adapt swiftly. This essay outlines a concise strategy and two-year implementation plan to mitigate ESG risks, ensuring sustainability and fostering resilience.

Strategy and Implementation Plan

1. Environmental Enhancement:
Year 1: Initiate a transition towards renewable energy sources, focusing on solar and wind energy. Invest in energy-efficient machinery and optimize production processes to reduce waste. Implement a recycling program for scrap metal and promote the use of recycled materials in production.
Year 2: Continue the transition to renewable energy and evaluate the impact of energy-efficient initiatives. Further reduce waste and improve recycling rates, aiming for a circular economy model. Obtain environmental certifications to validate efforts and communicate achievements to stakeholders.

2. Social Responsibility:
Year 1: Enhance workplace safety through better training and upgraded safety equipment. Engage with local communities, initiating programs that focus on education and skill development. Establish clear labor standards for suppliers to ensure ethical practices.
Year 2: Monitor and assess the impact of safety improvements, adjusting strategies as necessary. Expand community engagement programs and evaluate their effectiveness. Strengthen supplier relationships, ensuring adherence to social responsibility standards.

3. Governance and Transparency:
Year 1: Strengthen the governance structure, ensuring diverse and skilled board representation. Implement ESG risk management frameworks and enhance transparency in ESG reporting, adopting recognized standards like GRI or SASB.
Year 2: Regularly review governance practices, ensuring alignment with best practices and stakeholder expectations. Continue to enhance ESG disclosure, providing clear and comprehensive reports on progress and performance.

Conclusion

By adopting a holistic approach to ESG risk mitigation, the European steel parts manufacturing industry can build a robust foundation for sustainable growth. The outlined two-year plan provides a strategic roadmap, aligning environmental initiatives, social responsibility, and governance excellence. Through diligent implementation and continuous improvement, the industry can secure its position as a leader in sustainable manufacturing, contributing to a more resilient and equitable future.
```


The speed, scope, and scale of generative AI impact is unprecedented

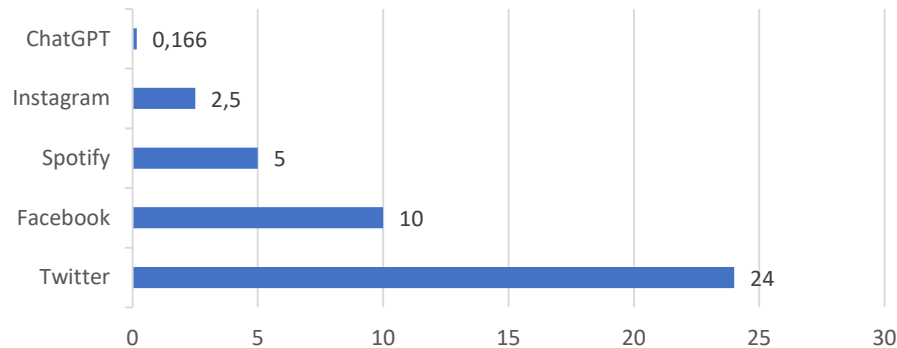


Massive grassroots adoption



1 M users within 1 week **100 M** users within 2 months

Months to reach 1 M



Broad-reaching and deep impact

*Generative AI could raise global GDP by **7%** within 10 years*

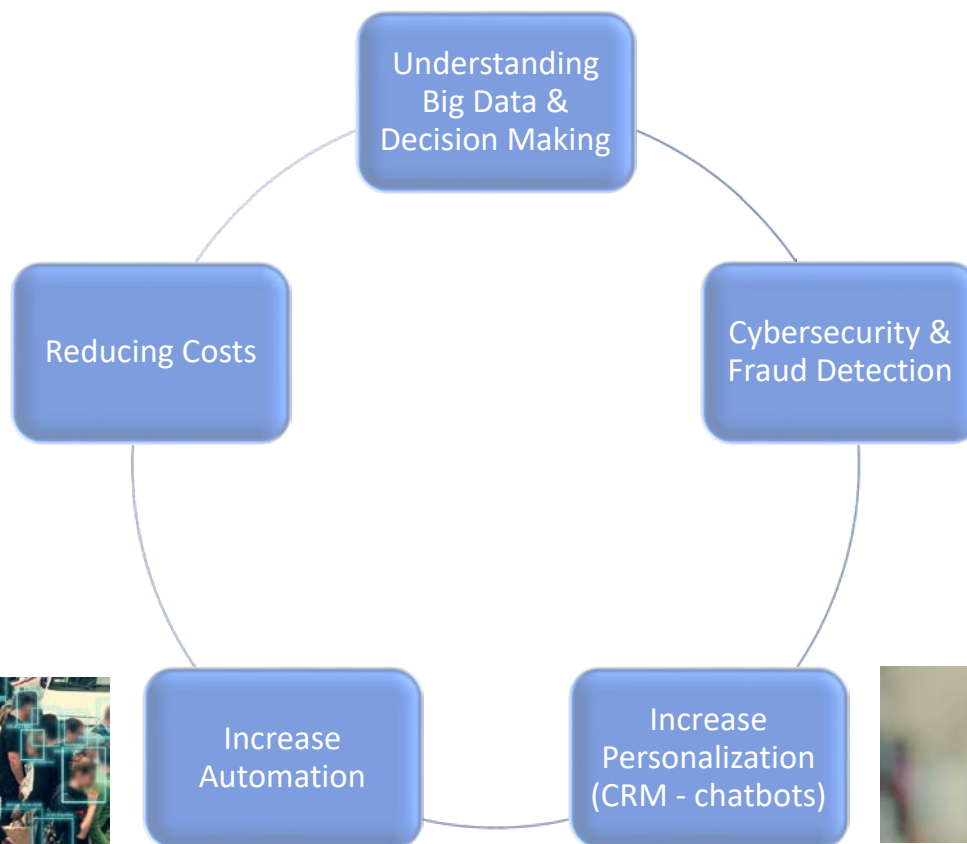
- Goldman Sachs

Generative AI has democratized AI and accelerated the largest commercial opportunity in today's economy, sized at USD 15.7 trillion of GDP by 2030.

□ IBV Tech-led disruptions are accelerating, driven by Generative AI

How AI Transforms Business

AI is *drastically* changing the way of doing Business



The most common *Generative AI* tasks implemented today



- **Retrieval-augmented generation**

- Based on documents or dynamic content, create a chatbot or question-answering feature.
- *Building a Q&A resource from a broad knowledge base, providing customer service assistance*

- **Summarization**

- Transform text with domain-specific content into personalized overviews that capture key points.
- *Conversation summaries, insurance coverage, meeting transcripts, contract information*

- **Content generation**

- Generate text content for a specific purpose.
- *Marketing campaigns, job descriptions, blog posts and articles, email drafting support*

- **Named entity recognition**

- Identify and extract essential information from unstructured text.
- *Audit acceleration, fact extraction, e.g., SEC 10K*

- **Insight extraction**

- Analyze existing unstructured text content to surface insights in specialized domain areas.
- *Medical diagnosis support, user research findings*

- **Classification**

- Read and classify written input with as few as zero examples.
- *Sorting of customer complaints, threat and vulnerability classification, sentiment analysis, customer segmentation*

AI Risks & Concerns



Generative AI related questions

- How was it trained?

- Garbage in → garbage out
- An enterprise cannot use a foundation model trained with Web crawl
- The training material needs to be huge and comprehensive but must also be **curated**

- Can it detect & minimize bias & hallucinations?

- How does the platform detect and correct **bias**?
- How can it prevent **hallucination** (providing random and untrue answers with absolute aplomb and convictions)?

- Is it transparent?

- Open vs black-box
- How to **audit** and **explain** the model, and the answers it generates?
- Does the model track **drift** and **bias**? And how does it address them?

Clients cannot just use *any* AI tools & services

- Does it support regulatory compliance?

- How do foundation models and their usage comply with **privacy** and government **regulations**?
- What are the guardrails?
- Who is **responsible** for an inadvertently exposed PII or a “wrong answer”?

- Is it safe?

- Who has control over the model, input data, and output data?
- How to **ensure** that confidential information is not given out?
- How is it monitored?
- What safety features and guardrails are in place?

- Can it be customized?

- Hybrid and multicloud?
- Can the model be **fine-tuned** with clients’ data?
- How can clients update, and **extend** the model to make it more suitable for their use cases?
- How to **integrate** with applications? What APIs are in place?

Elements of AI risk



Accountability



Accuracy




Fairness



Veracity



Regulatory Risk



Transparency



Drift




Trusted data



Energy consumption



Reputational Risk



Explainability



Adversarial Robustness



IP/PII leakage

...



Operational Risk

AI application: Water Underground



Incorporate:

Smart sensors – IoT –
Edge computing

Back-end processing,
ML/analytics,
short/long-term
predictions

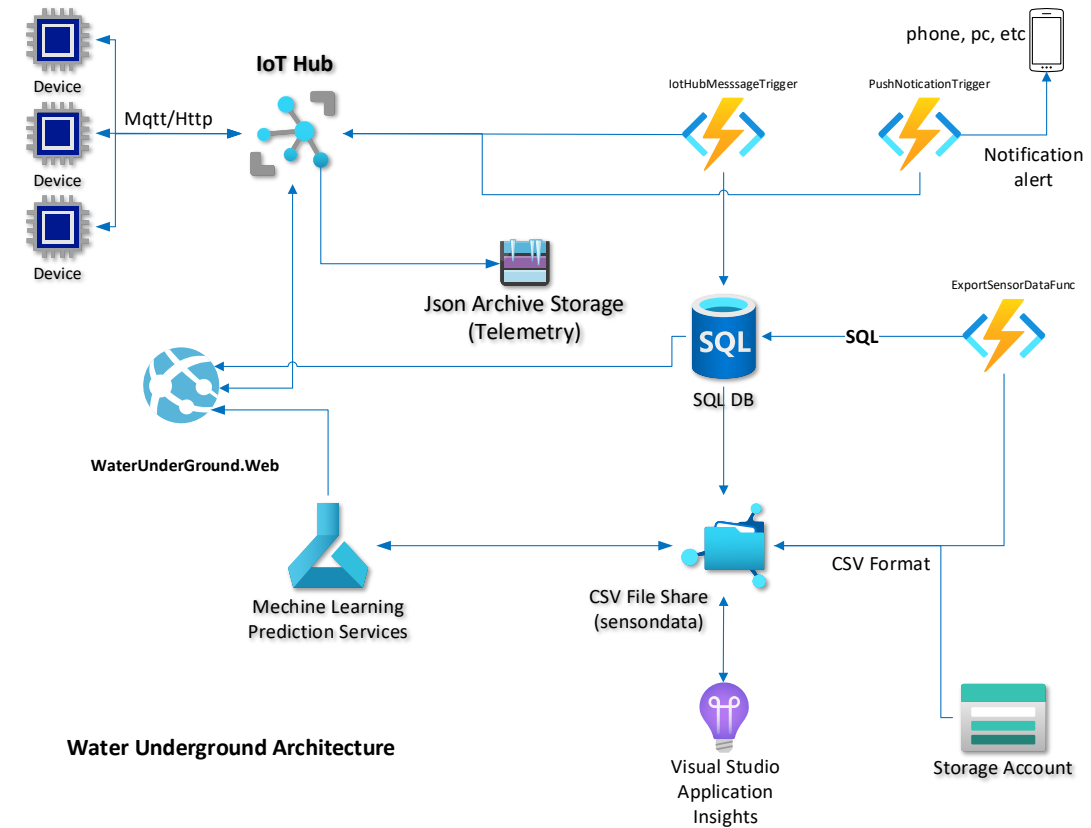
Aquifers' modeling

Cloud computing

Front-end application,
User Interface



Interconnected IoT devices for real-time monitoring of the underground waters' level and quality.

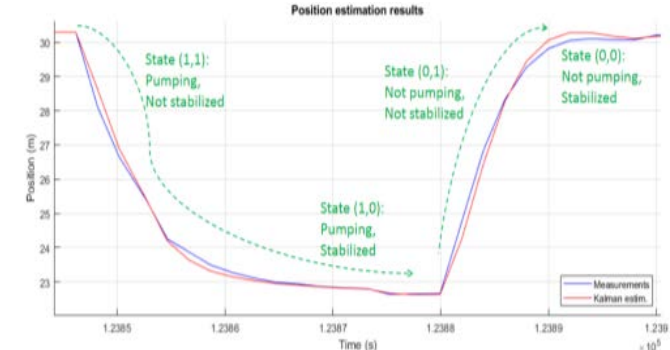
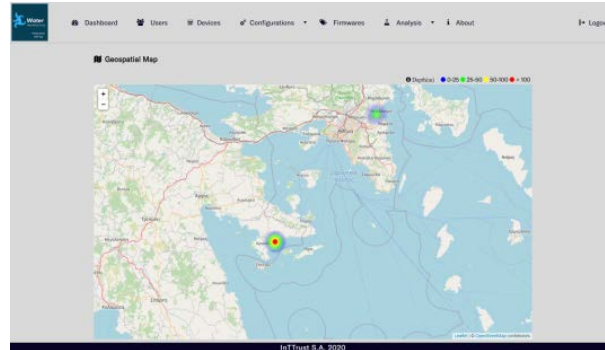


Water Underground Architecture

AI application: Water Underground



Map representation



Dashboard - Metrics

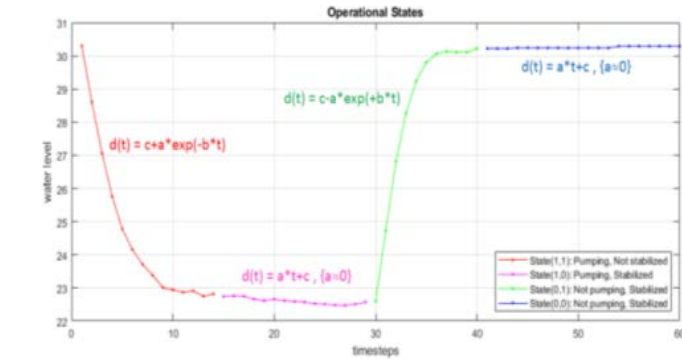
Depth

Prediction

Trends

Statistics

Quality

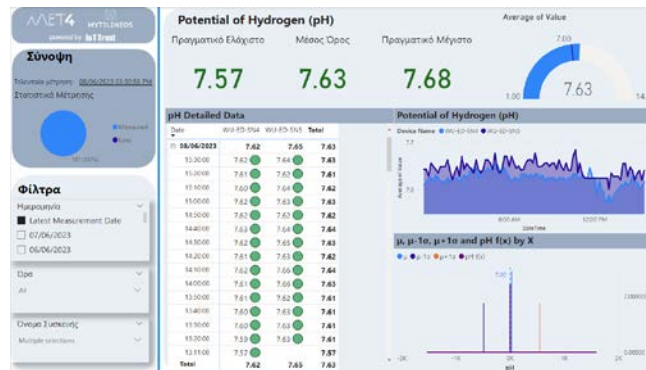


Time-Series Analysis

Water height/level graph

Water quality graph (pH,

TDS, ORP, EC, Temp)



Configuration

Application, System,

Device

Remote IoT Device

Updates

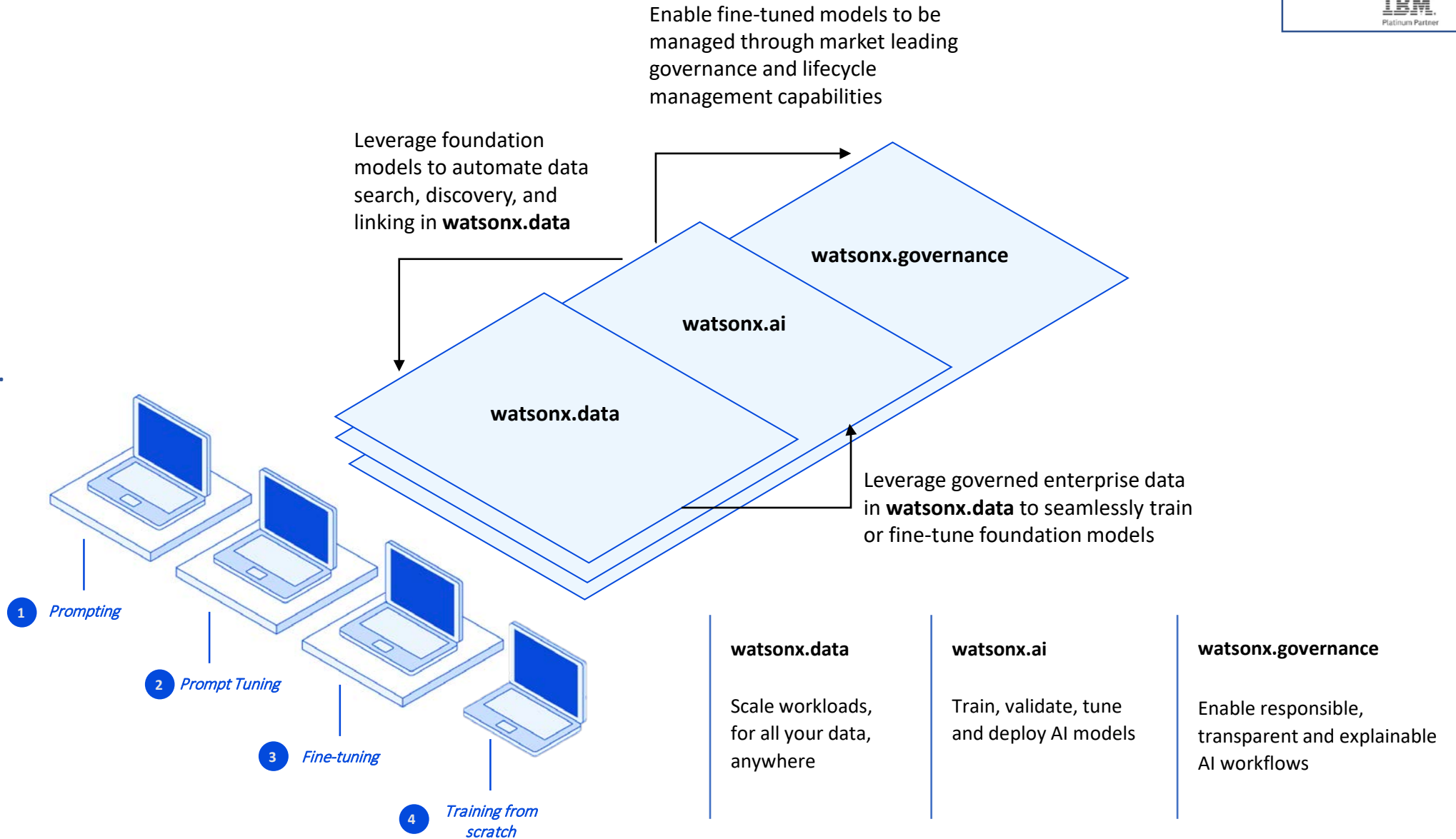
AI integrated platform



watsonx

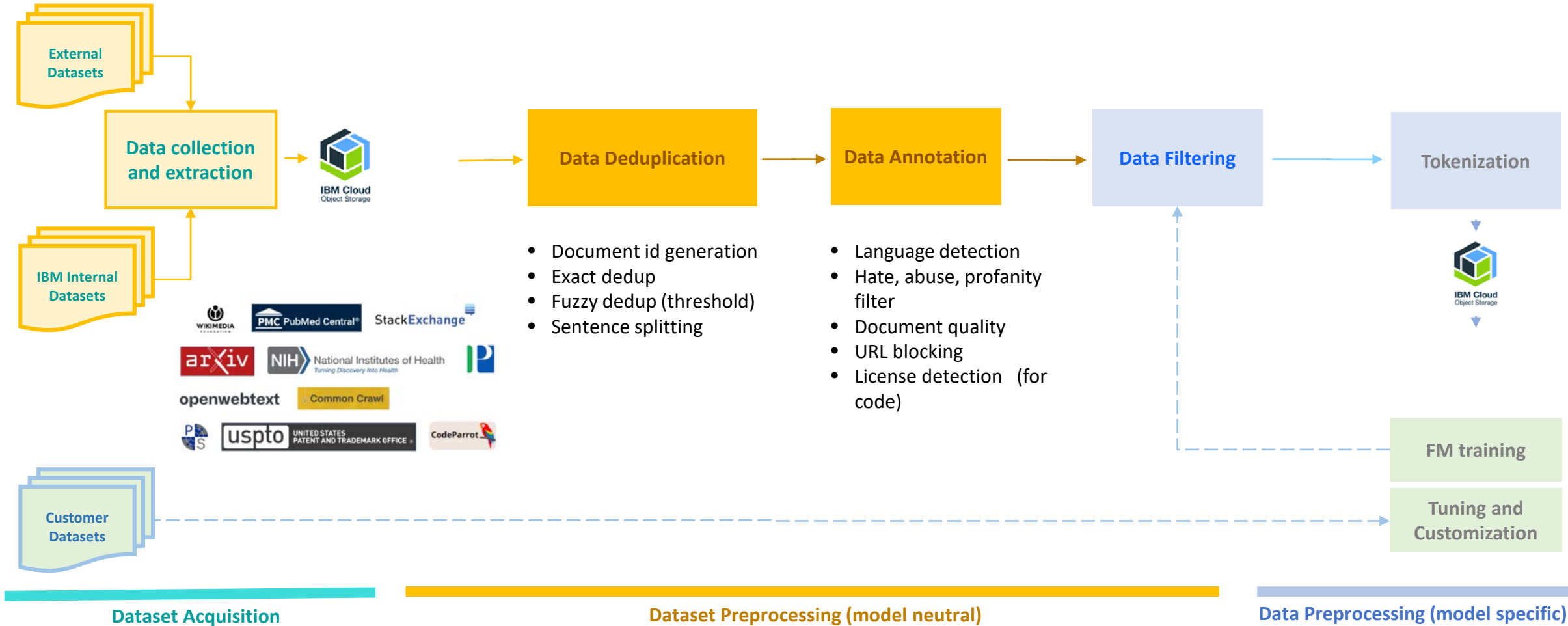
The platform for AI and data

Scale and accelerate the impact of AI with trusted data.

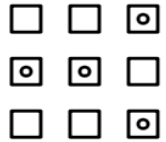


watsonx.data: curated IBM Data Pile

Enterprise-ready data acquisition, curation, provenance, and governance



- Generative AI capabilities



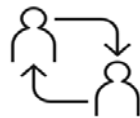
Foundation model library



Prompt Lab

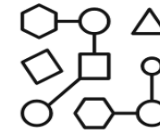


Tuning Studio*

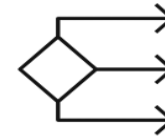


Team collaboration and data preparation

- Plus, a proven Studio for Machine Learning



ModelOps



Automated development



Decision optimization



NIST
National Institute of
Standards and Technology



European
Commission

NAIC
National Association of
Insurance Commissioners



watsonx.governance

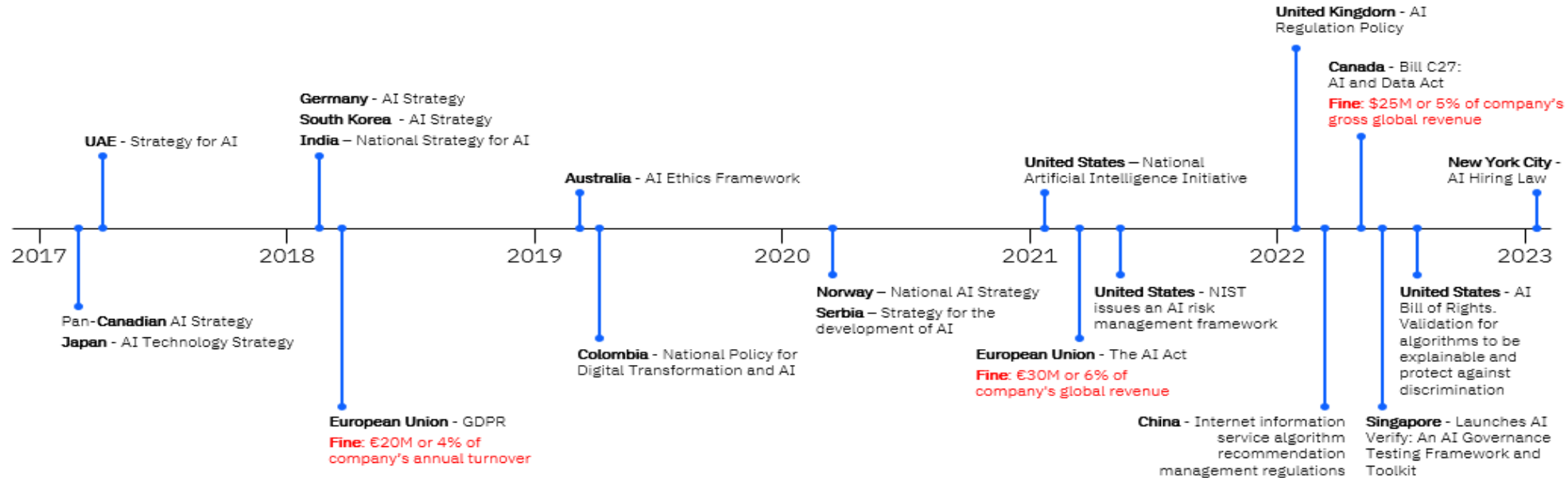
Adhere to regulatory compliance

Drive AI model explainability

- Automate the translation of AI regulations into enforceable standards and policies
- Track provenance, document model performance against KPIs
- Use dynamic dashboards and automated collaborative tools
- Document model facts using factsheets

Better meet growing AI and industry regulations

- Avoid costly fines and audits due to noncompliance and quickly respond to regulatory change
- Efficiently process large volumes of regulations and industry standards
- Ensure stakeholders need to be informed on regulatory compliance.



Conclusions

Artificial Intelligence (AI)

- is advancing exponentially, permeating and impacting all facets of life and business
- relies on *data* and generates *new data* (Generative AI)
- is readily available (*here and now*) and **transforms businesses**
- comes with Risks & Concerns (technical challenges, regulatory issues, need for expertise)
- InTTrust and IBM can assist businesses to take this journey at
maximum speed, effectiveness and safety



Thank you for your attention

