APDL

Association pour la Protection des Données au Luxembourg

MARKCOM EVENT

DPO FORUM

13 FEBRUARY 2025

APDL

Association pour la Protection des Données au Luxembourg

ETHICAL AI AND EVOLUTION

TUESDAY 13TH FEBRUARY 2025

MICHAEL HOFMANN – PRESIDENT APDL

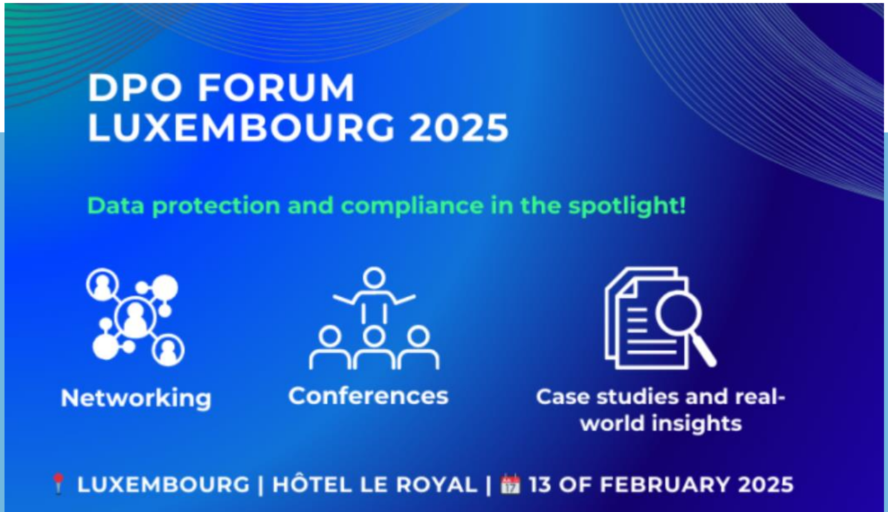
PROGRAM

MICHAEL HOFMANN

Ethical AI and Evolution

APDL
Association pour la Protection des Données au Luxembourg

MARKCOM EVENT



DPO FORUM
LUXEMBOURG 2025

Data protection and compliance in the spotlight!

Networking

Conferences

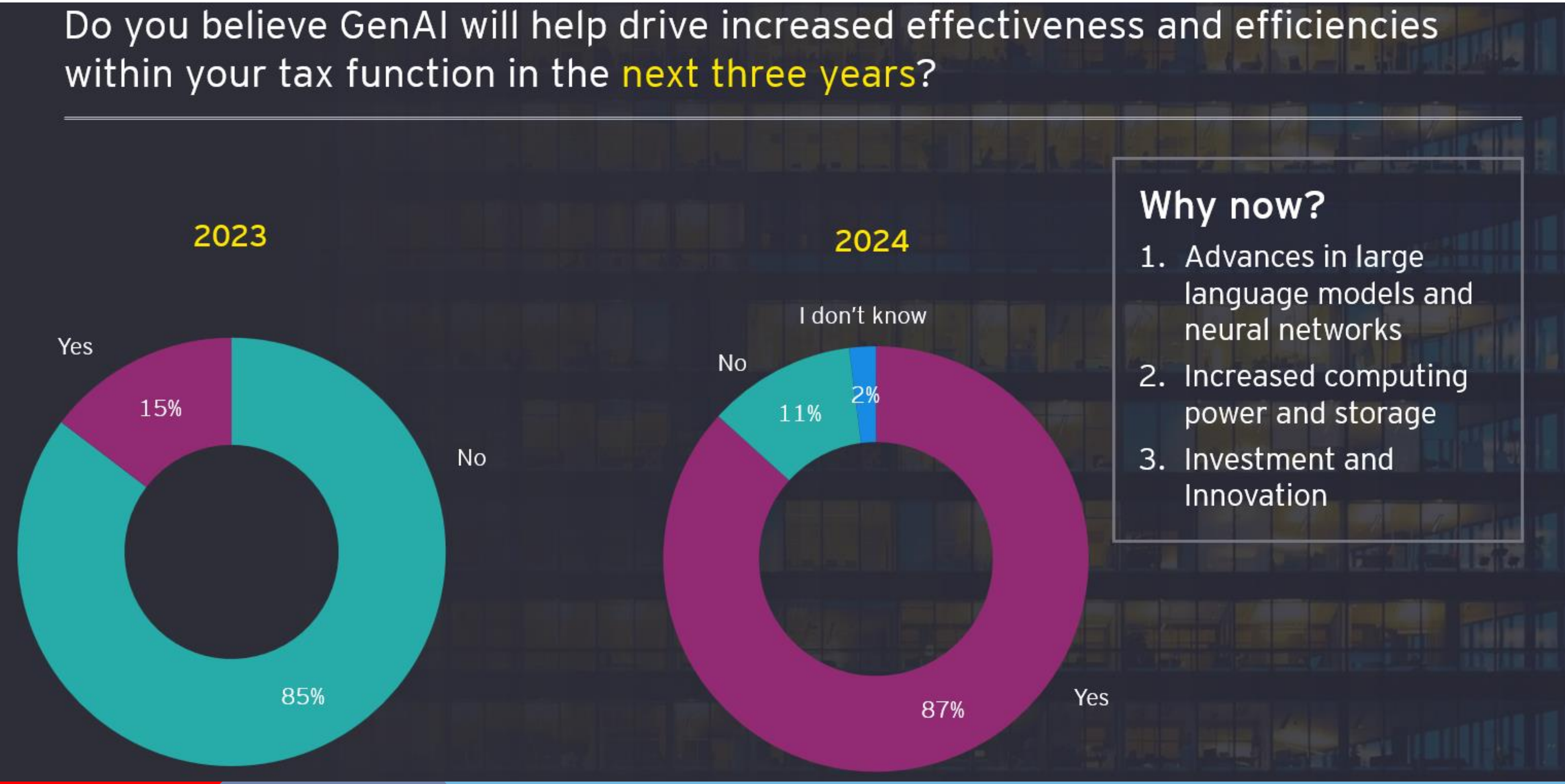
Case studies and real-world insights

📍 LUXEMBOURG | HÔTEL LE ROYAL | 📅 13 OF FEBRUARY 2025

1

KEY TRENDS: STATISTICS

EXAMPLE OF CHANGE IN OPINION


Do you believe GenAI will help drive increased effectiveness and efficiencies within your tax function in the next three years?

Why now?

1. Advances in large language models and neural networks
2. Increased computing power and storage
3. Investment and Innovation

2024 EY TAX AND FINANCE OPERATIONS SURVEY
CONDUCTED ANONYMOUSLY BY OXFORD ECONOMICS

- 1,600 LEADERS (WITH MAJORITY OF CFOS AND VP TAX)
- 32 COUNTRIES

2

KEY RISKS

RISKS, ETHICS AND CONTROLS

Trust, Transparency & Accuracy

- Accuracy of data inputs and output results
- Over reliance on given information without due diligence on sources.
- Transparency: explain-ability and trace-ability of outputs

Privacy, Surveillance & Security

- Data collection with unclear use; will your sensitive data be made open to the public via the next training round?
- What surveillance applications of GPT will society deem ethical?
- Privacy & Cybersecurity Concerns

Fairness & Bias

- Bias towards certain sub-groups due to public training data
- Bias in model can drive unfair outcomes in some business applications
- Toxicity in responses requires ongoing management

Legal Issues

- Potential Copyrights and IP infringement
- Liability of Use
- GDPR Compliance

Autonomy of Agentic AI

Training data and training method bias

Transparency of propriety models

START OF ACCELERATED AI RACE

Generative AI and Agentic AI :

- Agentic AI workflow design pattern: Reflection -> Tool use -> Planning tasks -> Multi Agent collaboration

key Features	Generative AI	Agentic AI
Decision-Making	Input dependent	Independent
Orientation	Output	Goal
Focus	Creativity	Autonomy
Key Applications	Content Creation	Autonomous Systems
Interaction	Content-Based	Environment
External Tools	No	Yes
Learning (real time adaptation)	No	Yes

- Ethical dilemma: AI bias, data privacy, data bias, method bias and empowerment

Agentic AI :

“an autonomous AI capable of decision making”

“Agentic” comes from “Agent” , an entity that perceives environment, process information and perform actions to achieve the targeted goal”

AI CYBER AND DATA PROTECTION THREATS

AI social engineering attacks

- AI algorithms for personalized phishing and contextualization
- Deepfakes
- Self improving, adaptive threats and agentic AI
- Dynamic targeting and automated spear phishing
- Multi-modal social engineering

AI Cyber defense

- Fight Agentic AI with Agentic AI
- Emerging agentic AI market and proliferation of multi agent systems
- Manage shadow AI used by staff
- AI security and Agentic AI awareness

Agentic AI :

“The age of decision making machines and enhanced human capabilities”

3

APDL
Association pour la Protection des Données au Luxembourg

CAN AI ENABLE THE DPO

BIOMETRICS AND UX'S

Use Case 1

APDL
Association pour la Protection des Données au Luxembourg

AI solutions have the power to create increased User Experience with improved security and …

From password to Multi Factor Authentications

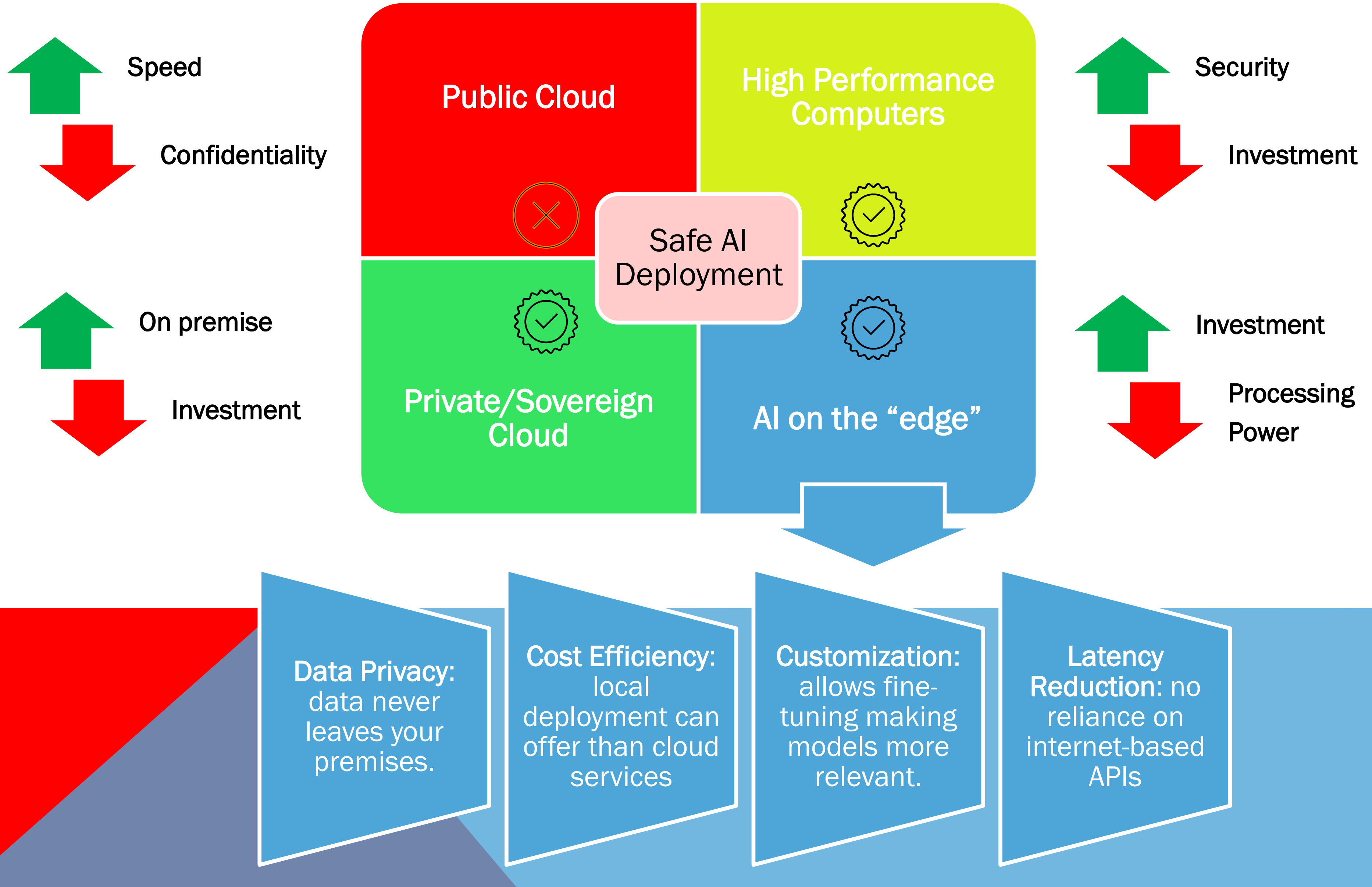
From parameter security to trusted third parties

From symmetric encryption to PKI

From end user complexity to increase UX

Advanced AI's is part of our business reality and creates always faster evolving needs for staying in business

PRAGMATIC ETHICAL AI DEPLOYMENT



Speed ↑

Confidentiality ↓

On premise ↑

Investment ↓

Public Cloud ✗

High Performance Computers ✓

Safe AI Deployment

Private/Sovereign Cloud ✓

AI on the “edge” ✓

Security ↑

Investment ↓

Investment ↑

Processing Power ↓

Data Privacy: data never leaves your premises.

Cost Efficiency: local deployment can offer than cloud services

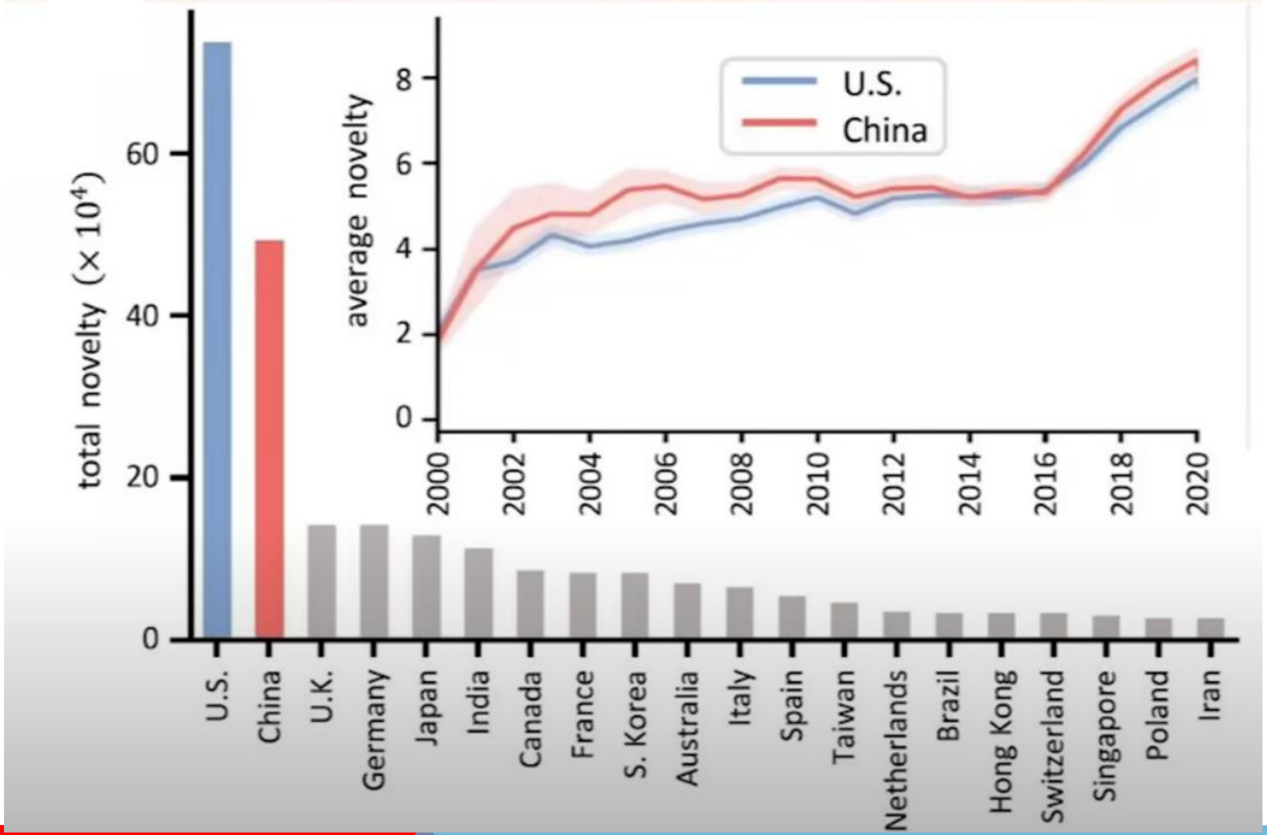
Customization: allows fine-tuning making models more relevant.

Latency Reduction: no reliance on internet-based APIs

4

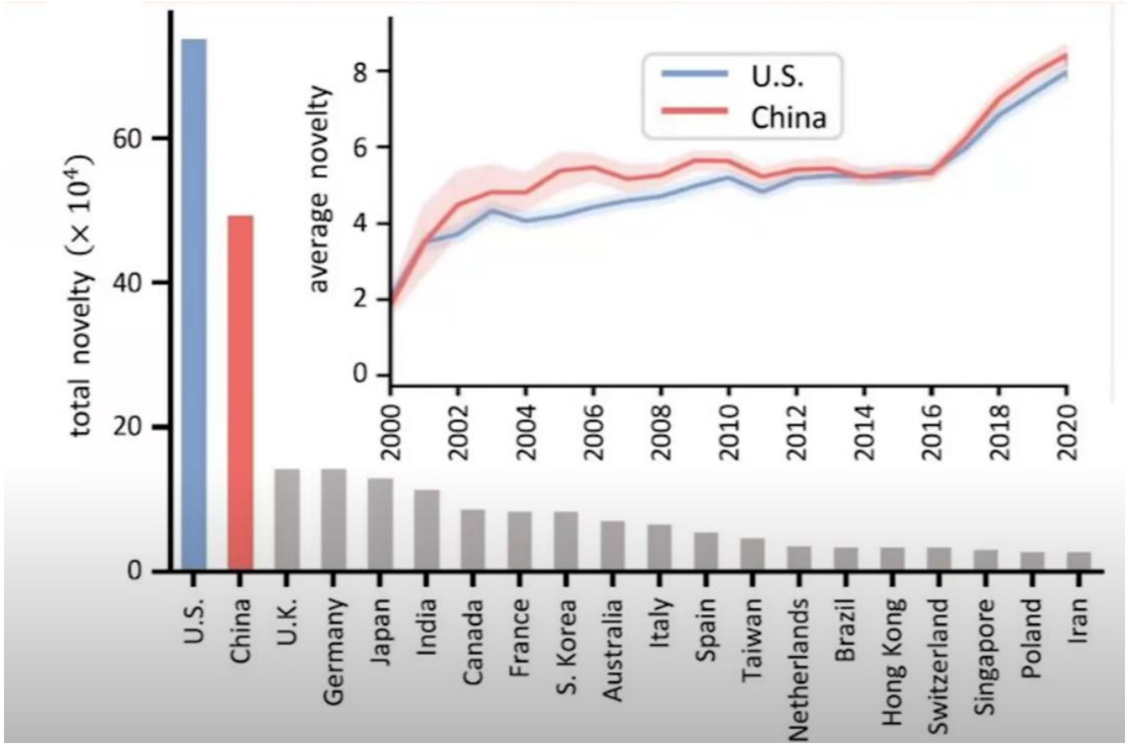
EVOLUTION

EVOLUTION



total novelty (× 10⁴)
0
20
40
60
U.S.
China
U.K.
Germany
Japan
India
Canada
France
S. Korea
Australia
Italy
Spain
Taiwan
Netherlands
Brazil
Hong Kong
Switzerland
Singapore
Poland
Iran
average novelty
0
2
4
6
8
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
U.S.
China

EVOLUTION



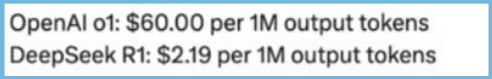
Open AI training: 5 billion USD

- Propriety model – Black Box
- Massive financing and data centers
- Most advanced chips
- Heavy energy costs

Stargate: 100 - 500 billion USD

Deepseek R1 evolutions

- Open source model
- AI training: 5 million USD
- Performance, Chain of Thought COT
- Cheaper, less power
- Transparency & Censorship


OpenAI o1: $60.00 per 1M output tokens
DeepSeek R1: $2.19 per 1M output tokens

US - CHINA AI BATTLE

Deepseek R1 zero is an open AI, developed in China with High Performance, Transparency and Minimal Cost

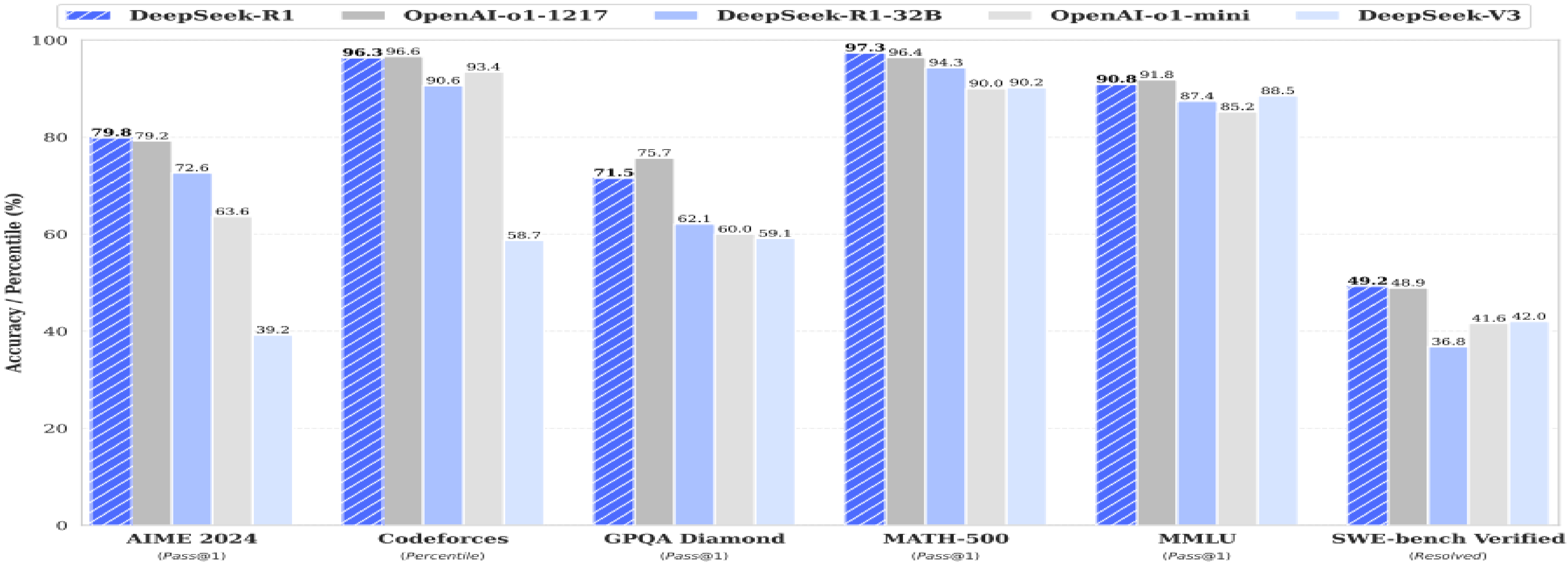
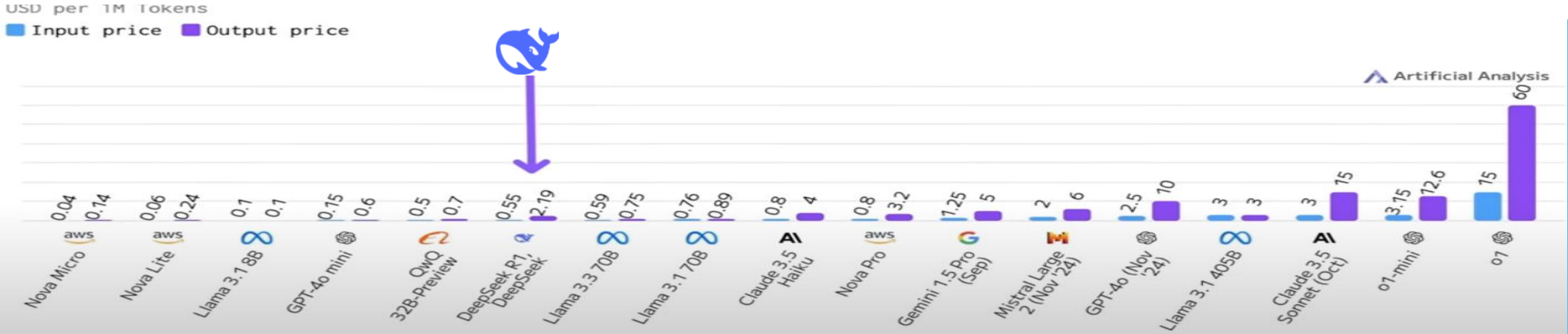


Figure 1 | Benchmark performance of DeepSeek-R1.

arXiv:2501.12948v1 [cs.CL] 22 Jan 2025



START OF ACCELERATED AI RACE

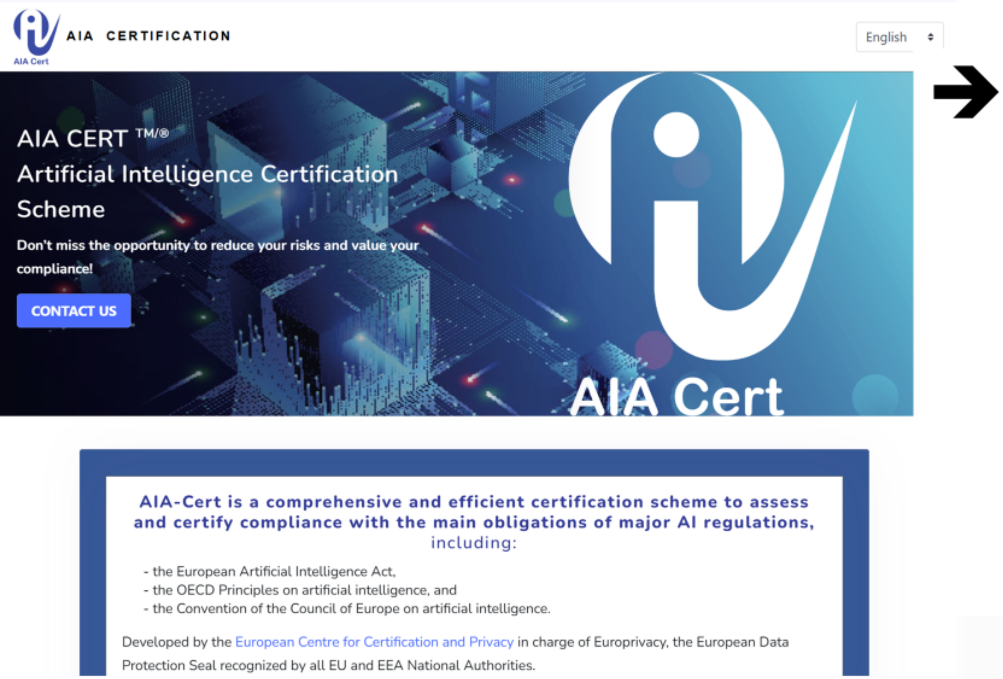
From transformer models to distilled models

- Increased efficiency: Transformer models with mixture of experts and reinforcement of learning and CPU load balancing (V1 to V3), R1 reasoning with reinforcement learning, supervised fine tuning and distilled models
- Example v3 with 2000 CPU vs LLama4 with 100.000 CPU
- Mixture of Expert (MoE) architecture

- New path of invention based on fast experimentation, prototyping and UX's with parallel build and collect data
- Speed vs responsibility: Exponential machine learning stresses slower areas of the organizations

BENEFIT OF CERTIFICATION GDPR & AI

AIA Cert



AIA CERT TM/®
Artificial Intelligence Certification Scheme

Don't miss the opportunity to reduce your risks and value your compliance!

AIA-Cert is a comprehensive and efficient certification scheme to assess and certify compliance with the main obligations of major AI regulations, including:

- the European Artificial Intelligence Act,
- the OECD Principles on artificial intelligence, and
- the Convention of the Council of Europe on artificial intelligence.

Developed by the European Centre for Certification and Privacy in charge of Europrivacy, the European Data Protection Seal recognized by all EU and EEA National Authorities.

→ Regulatory compliance with:

- EU AI Act
- OECD Principles
- CoE Framework Convention on AI

aiacert.com

APDL
Association pour la Protection des Données au Luxembourg

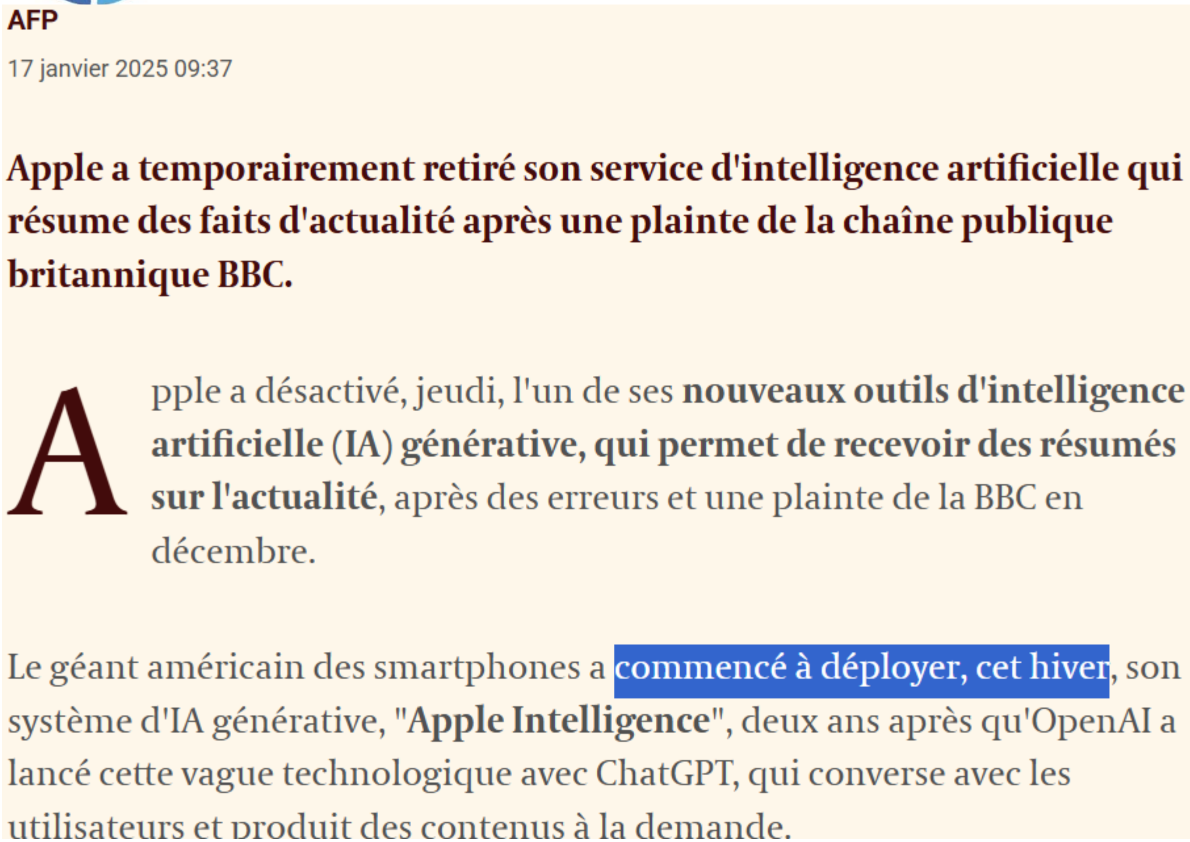
5

THANK YOU!

Association à but non lucratif créée par et pour les professionnels de la protection des données au Luxembourg

Rejoignez-nous sur www.apdl.lu

EXAMPLE OF NEWS



AFP

17 janvier 2025 09:37

Apple a temporairement retiré son service d'intelligence artificielle qui résume des faits d'actualité après une plainte de la chaîne publique britannique BBC.

Apple a désactivé, jeudi, l'un de ses **nouveaux outils d'intelligence artificielle** (IA) **générative, qui permet de recevoir des résumés sur l'actualité**, après des erreurs et une plainte de la BBC en décembre.

Le géant américain des smartphones a commencé à déployer, cet hiver, son système d'IA générative, "**Apple Intelligence**", deux ans après qu'OpenAI a lancé cette vague technologique avec ChatGPT, qui converse avec les utilisateurs et produit des contenus à la demande.

L'outil d'Apple Intelligence a inventé des informations en attribuant la source à la BBC. - ©EPA

<u>Essentials still are:</u>

- **Trust**
- **Risk**
- **Context**
- **The Trusted AI Solution Lifecycle ?**