



KI verstehen statt KI glauben

*eine Orientierung im
KI-Zeitalter*

MARKUS
BEGEROW

About me



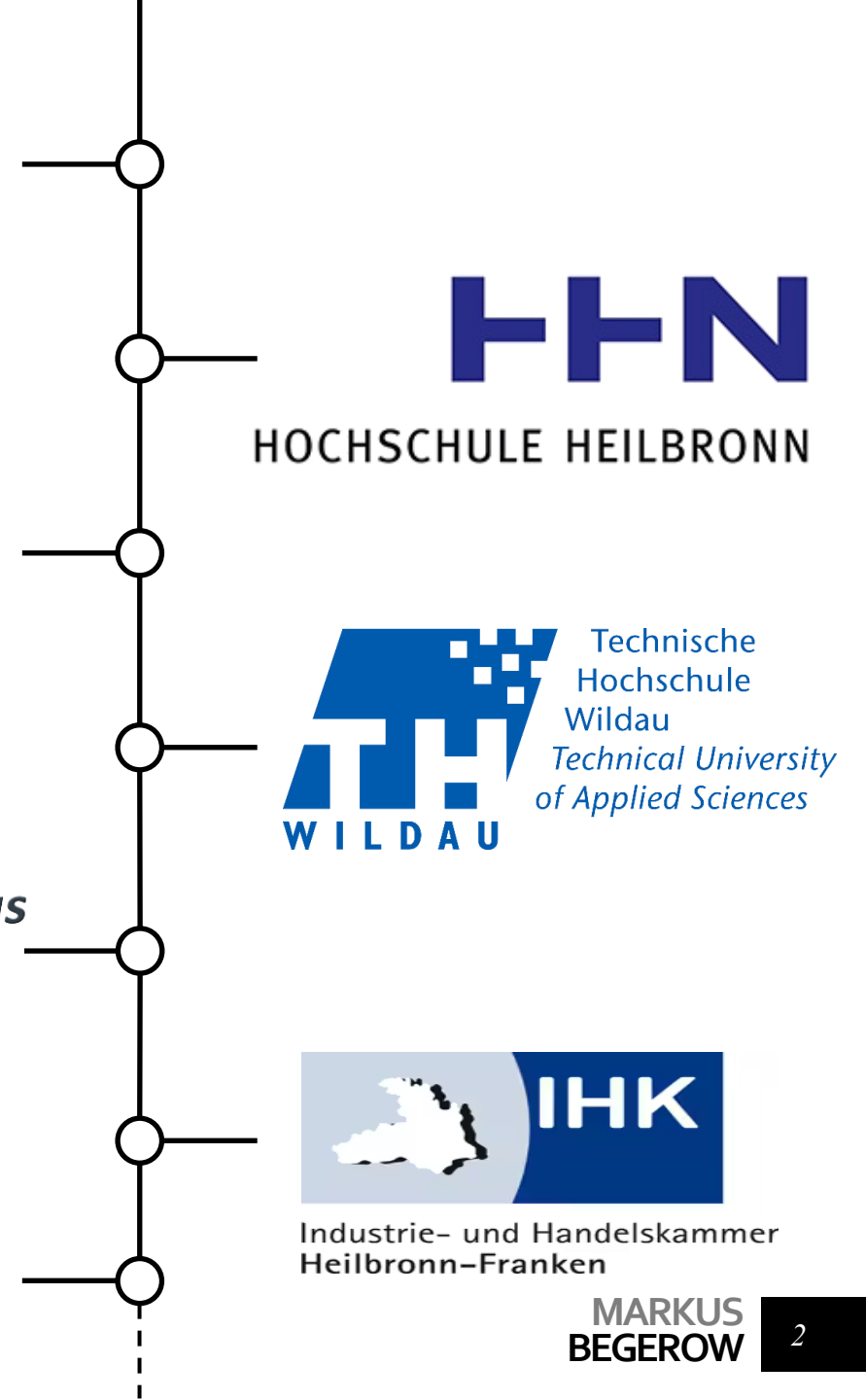
#gerneperDu



**DATENBANKEN
VERSTEHEN**
für Anfänger und Profis



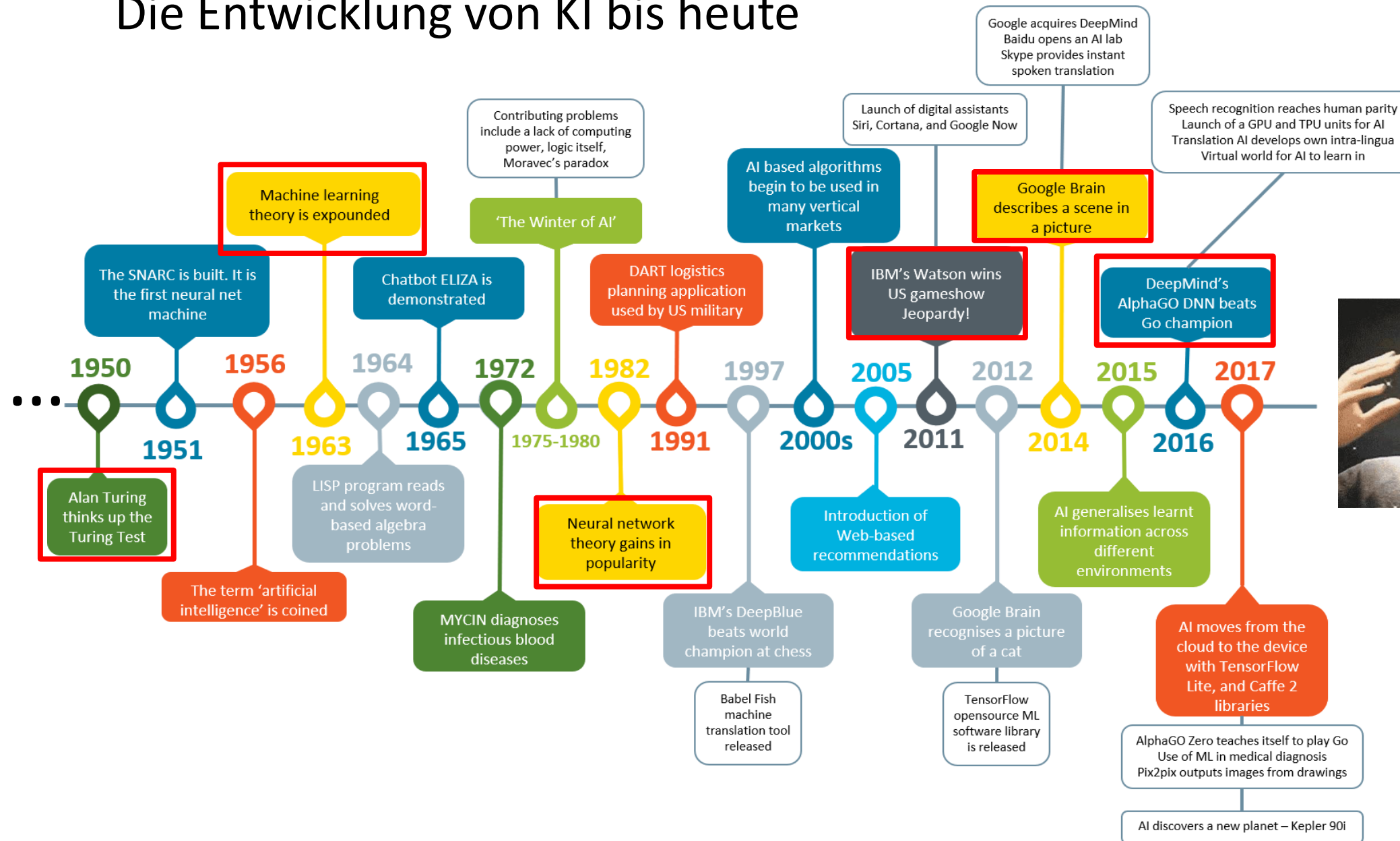
Data & AI Campus
Your next level in Data & Analytics





SCAN MICH 😊

Die Entwicklung von KI bis heute



big data
Suchbegriff

machine learning
Suchbegriff

artificial intelligen...
Suchbegriff

+ Vergleich hinzufügen

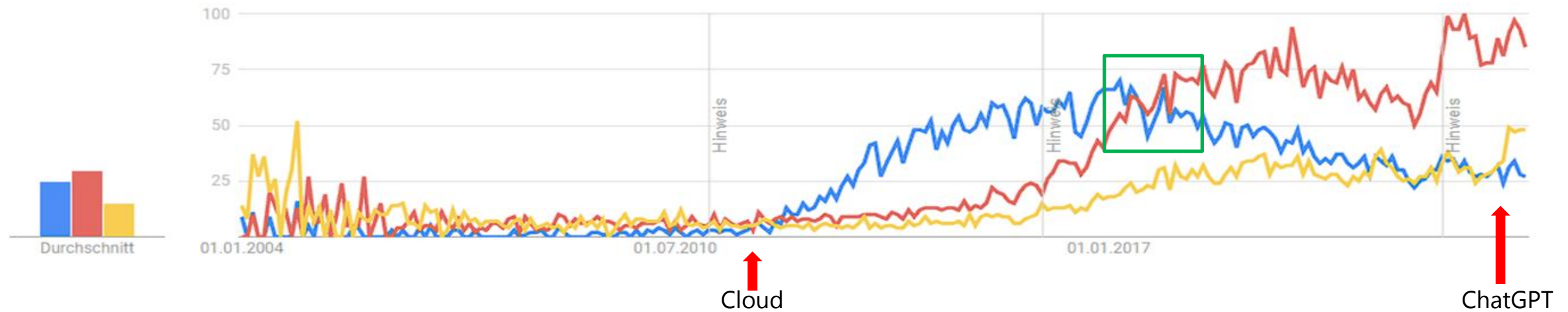
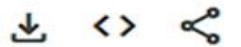
Deutschland ▼

2004 - heute ▼

Alle Kategorien ▼

Websuche ▼

Interesse im zeitlichen Verlauf ?



Wo stehen wir heute?



Source: [Gartner](#)

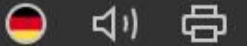


Markus Begerow ✓ • Sie
Advisor for Data, AI & Blockchain | Speaker · Author · Mentor

Thanks for sharing. Okay and 60% of the projects will be successful or what?
From 0 to 60% is a good start, I think 😊

Artificial intelligence: Vibe coding service Replit deletes production database

According to a Replit user, the service has deleted its production database, made false statements about it and ignored instructions. The manufacturer responds.

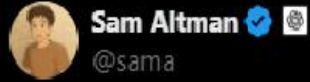


(Image: Shutterstock/Usa-Pyon)

Jul 25, 2025 at 10:23 am CEST 4 min. read Developer

By [Maika Möbus](#)

Source: [Heise](#)



Peter Steinberger is joining OpenAI to drive the next generation of agents. He is a genius with a lot of amazing ideas about smart agents interacting with each other to do very useful things for people. We expect this will quickly become core to our mission.

OpenClaw will live in a foundation as an open source project that we will continue to support. The future is going to be exciting and it's important to us to support open source as part of our mission.

[Post übersetzen](#)

10:39 nachm. · 15. Feb. 2026 · **16,2 Mio.** Mal angezeigt

4.899

8.822

46.299

Relevant ▾

OpenClaw

> What People Say

BUSINESS INSIDER

OpenClaw: Meta-Managerin verliert plötzlich die Kontrolle und erlebt einen KI-Albtraum

Henry Chandonnet

Di., 24. Februar 2026 um 12:50 PM MEZ



In diesem Artikel:

BTZI -6,25 % ☆



Meta's Summer Yue bezeichnete Ihre OpenClaw-Horrorgeschichte als „Anfängerfehler“. - Copyright: Tayfun Coskun/Anadolu Agency via Getty Images

MARKUS
BEGEROW

7

Source: [Forbes](#)

AI (artificial intelligence)

Josh Taylor Technology reporter

Mon 2 Feb 2026 06.39 CET

Explainer

What is Moltbook? The strange new social media site for AI bots

A bit like Reddit for artificial intelligence, Moltbook allows AI agents - bots built by humans - to post and interact with each other. People are allowed as observers only



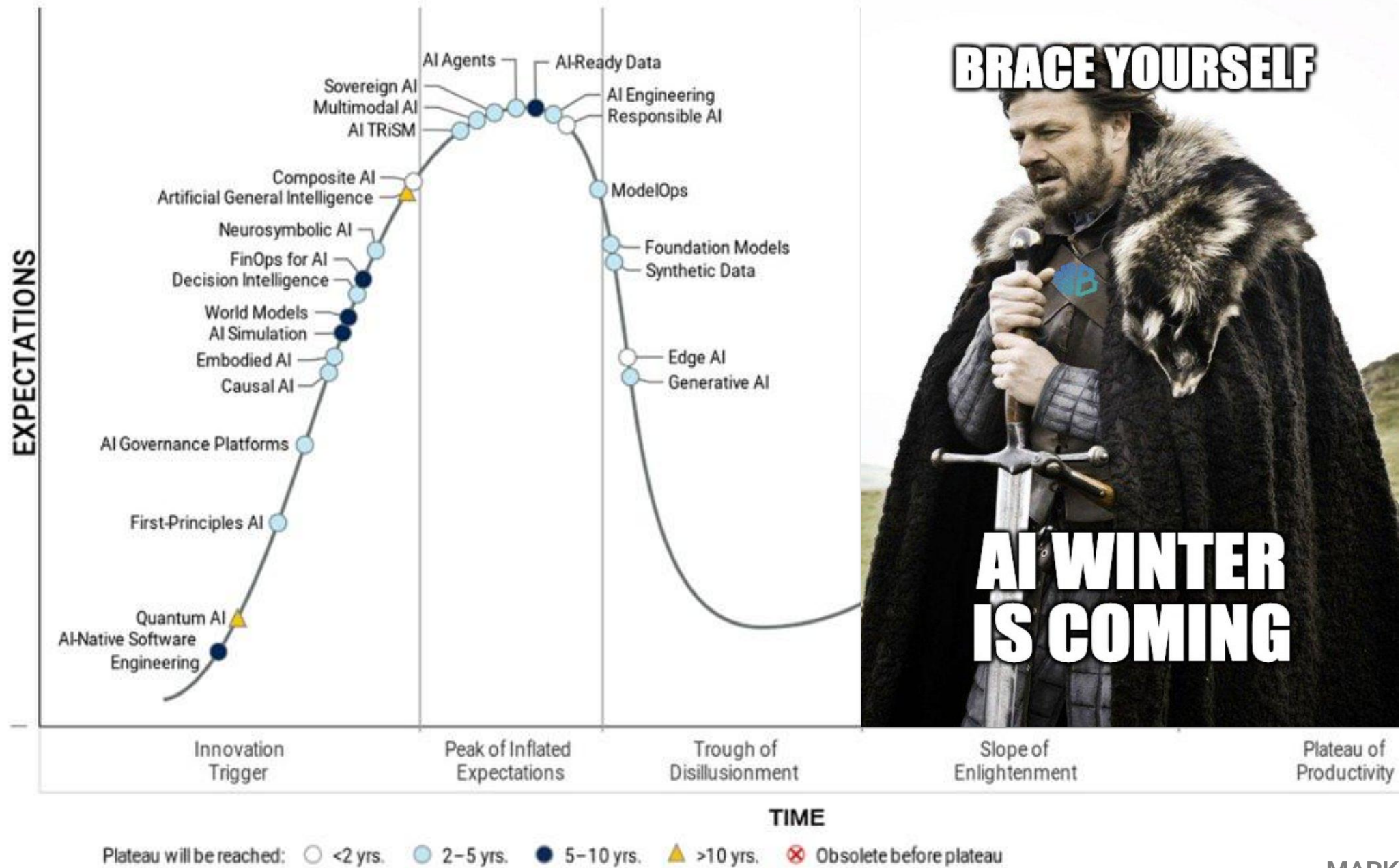
KYLE MACNEILL BUSINESS FEB 18, 2026 6:00 AM

The Rise of RentAHuman, the Marketplace Where Bots Put People to Work

WIRED spoke with the Zoomer founders of a platform where AI agents hire humans to do real-world tasks. Their pitch: "People would love to have a clanker as their boss."



Source: [Forbes](#)



The AI bubble will burst for firms that can't get beyond demos and I I Me

News Analysis
Feb 16, 2026 • 4 mins

Analysts warn that too many companies are ‘chasing the shiny object’ with the basics of success.



Credit: Bernd von Darl

The AI bubble isn't just hype — it's real and could create many corporate casualties if or when it bursts. The companies that will succeed will be the ones solving real-world problems and engaging clients, according to tech industry execs and analysts.

Elo Scores by Company - Top 9

Top Ranked Model by Company in the Chatbot Arena - Last 6 Months



Source: LMArena.ai; Created by Peter Gostev (<https://www.linkedin.com/in/peter-gostev/>)

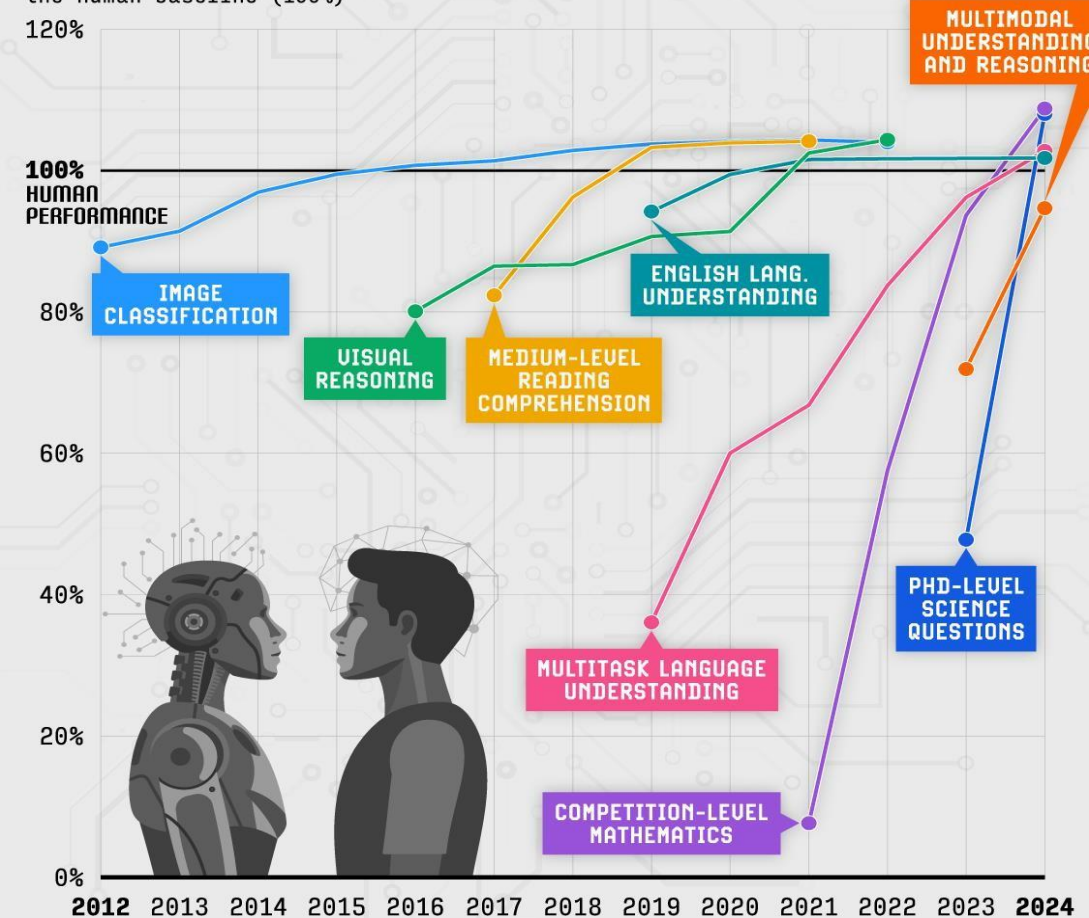
Source: [Computerworld](https://www.computerworld.com)



KI wird den Menschen in allen Bereichen, die wir trainieren und testen können, übertreffen oder hat dies bereits getan.

AI VS. HUMAN PERFORMANCE IN TECHNICAL TASKS

Performance relative to the human baseline (100%)



VISUAL CAPITALIST

Source: Stanford University, 2025 AI Index Report



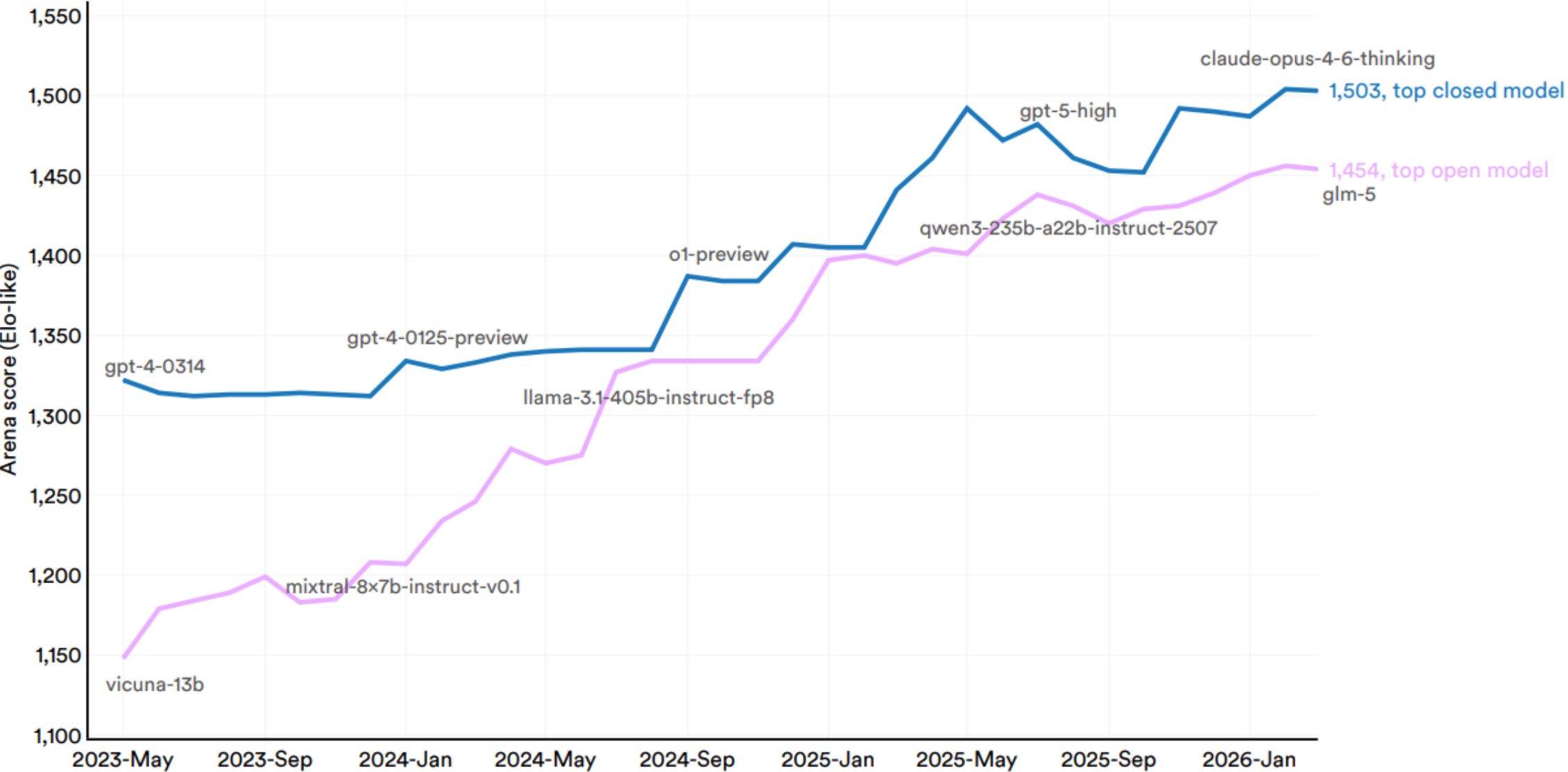
Source: [Stanford University](https://hai.stanford.edu/)

Top 5 Takeaways

1. Exponentielle AI-Entwicklung ohne Plateau
2. USA vs. China: AI-Wettbewerb auf Augenhöhe
3. „Jagged Frontier“: leistungstark, aber unzuverlässig
4. Produktivität steigt, Arbeitsmarkt verschiebt sich
5. Governance & Responsible AI hinken hinterher

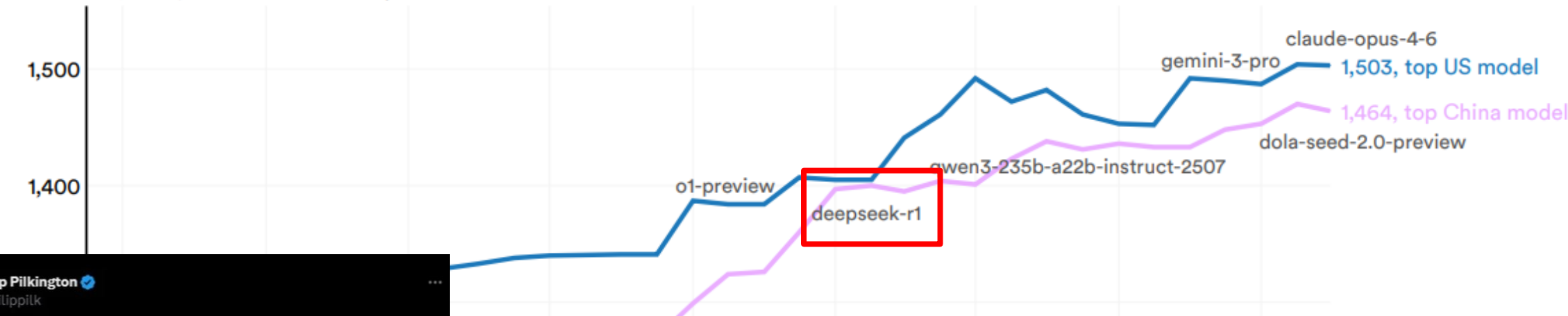
Performance of top closed vs. open models on the Arena

Source: Arena, 2026 | Chart: 2026 AI Index report



Performance of top United States vs. Chinese models on the Arena

Source: Arena, 2026 | Chart: 2026 AI Index report



Philip Pilkington @philippilk

Will be interesting to see if this guy and his buddies end up blowing up the NASDAQ bubble. NVIDIA is something like 14% of the NASDAQ market cap right now. 🗨️

Post übersetzen

Liang Wenfeng, DeepSeek AI CEO.



FORTUNE SUBSCRIBE NOW SIGN IN

How DeepSeek erased Silicon Valley's AI lead and wiped \$1 trillion from U.S. markets

BY NICHOLAS GORDON
March 30, 2025 at 8:00 PM EDT

2024-May 2024-Sep 2025-Jan 2025-May 2025-Sep 2026-Jan

Zum Glück wird massiv in Sicherheit...

Das Thema „Sicherheit“ bekommt ca. 1% der Ressourcen in der KI-Forschung

☰

🔍

FINANCIAL TIMES

👤 My Account

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

FT Digital Edition Portfolio myFT

OpenAI Added

OpenAI slashes AI model safety testing time

Testers have raised concerns that its technology is being rushed out without sufficient safeguards

✕

f

in

📶

Share

🔖

Save



© FT montage/Getty Images

Cristina Criddle in San Francisco

Published 2 HOURS AGO

💬 6 🖨️

OpenAI has slashed the time and resources it spends on testing the safety of its powerful artificial intelligence models, raising concerns that its technology is

Follow the topics in this article

US companies

✓ Added

Tech start-ups

✓ Added

Artificial intelligence

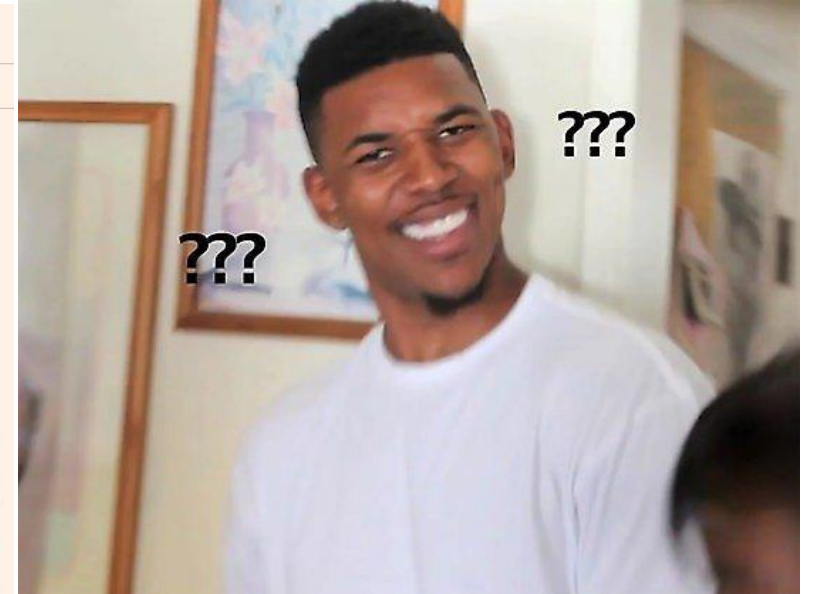
✓ Added

Technology

✓ Added

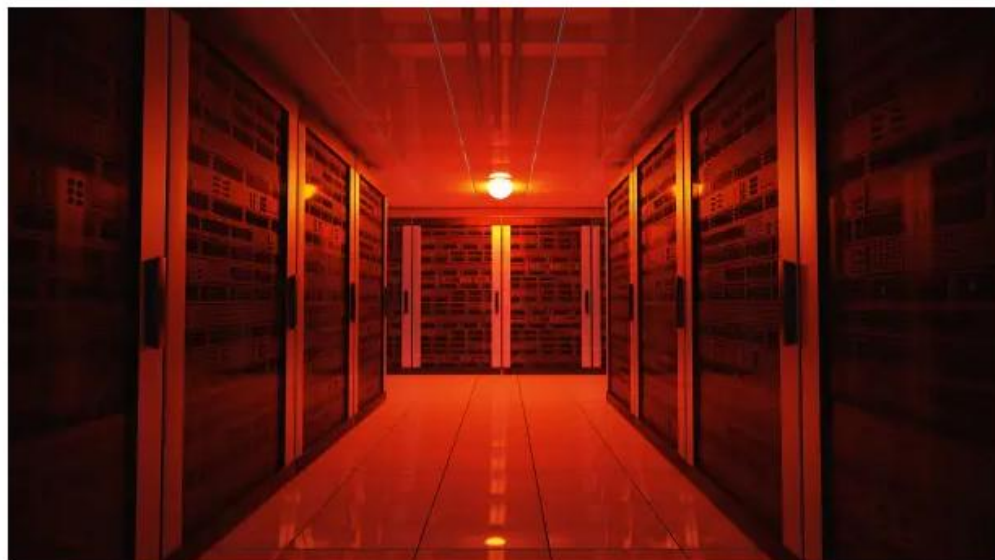
OpenAI

✓ Added



Das passiert, wenn der KI-Betreiber die Sicherheit vernachlässigt

Verträge, Rechnungen und weitere sensible Daten erreichten uns via E-Mail. Die Quelle: eine österreichische KI-Firma, die demnach bei der Sicherheit schlampete.



Notfall im Rechenzentrum (Bild: vchal/Shutterstock.com)

07.10.2025, 15:43 Uhr Lesezeit: 6 Min. | Security

Von Jürgen Schmidt

Source: [Heise](#)



Markus Begerow ✓ • Sie
Strategic Advisor for Data & AI & Blockchain • Speaker • Author • Mentor
5 Std. •

Vercel just got breached? This is getting really interesting...

They're selling internal DB + employee accounts + GitHub/NPM tokens for \$2M on BreachForums.

looks like someone got early access to **Anthropic** Mythos?

VERIFIED Vercel Database Access Key & Source Code -19 Apr 2026
by ShinyHunters - Sunday April 19, 2026 at 02:02 AM



[Admin] ShinyHunters
Administrator
Posts: 48
Threads: 42
Joined: May 2023
Reputation: 1,905
Warning Level: 0%

2 minutes ago (This post was last modified: Less than 1 minute ago by ShinyHunters)

Hello **Breachforums** Community.

Greetings All.

Today I am selling Access Key/ Source Code/ Database From **Vercel** Company

https://f.top4top.io/p_376062kuk0.png

Vercel Cloud

Vercel is an American cloud computing company that provides a platform for instant web application development, hosting, and deployment. The company is widely known as the creator and maintainer of Next.js, one of the most popular React-based web development frameworks.

We have verified access keys for a potential global supply chain attack.

We're selling this access. Are you interested in buying it?

This is just from Linear as proof, but the access I'm about to give you includes multiple employee accounts with access to several internal deployments, API keys (including some GitHub tokens and some NPM tokens).

Give me a quote if you're interested. This could be the largest supply chain attack ever if done right. Vercel owns **Next.js**, **Turbo.js**, and the entire **@vercel** sphere. 6 million weekly downloads for Next.js alone. You send one update with a payload, and it will hit every developer on the planet who runs an installation or updates a package.

Greetings All.

April 19

Today I am selling Access Key/ Source Code/ Database From **Vercel** Company

Vercel Cloud

Vercel is an American cloud computing company that provides a platform for instant web application development, hosting, and deployment. The company is widely known as the creator and maintainer of Next.js, one of the most popular React-based web development frameworks.

We have verified access keys for a potential global supply chain attack.

We're selling this access. Are you interested in buying it?

This is just from Linear as proof, but the access I'm about to give you includes multiple employee accounts with access to several internal deployments, API keys (including some GitHub tokens and some NPM tokens).

Give me a quote if you're interested. This could be the largest supply chain attack ever if done right.

Vercel owns **Next.js**, **Turbo.js**, and the entire **@vercel** sphere. 6 million weekly downloads for Next.js alone. You send one update with a payload, and it will hit every developer on the planet who runs an installation or updates a package.

data internal user member system

id	name	displayname	email	active	admin	guard	timezone	createdat	updatedat	lasttime
1	Markus Begerow	Markus Begerow	markus@begerow.com	active	admin	guard	UTC	2025-04-19 15:43	2025-04-19 15:43	2025-04-19 15:43

Price: \$2M USD

Contact: shiny@bepress.com

Telegram: [@shinybepress](#)

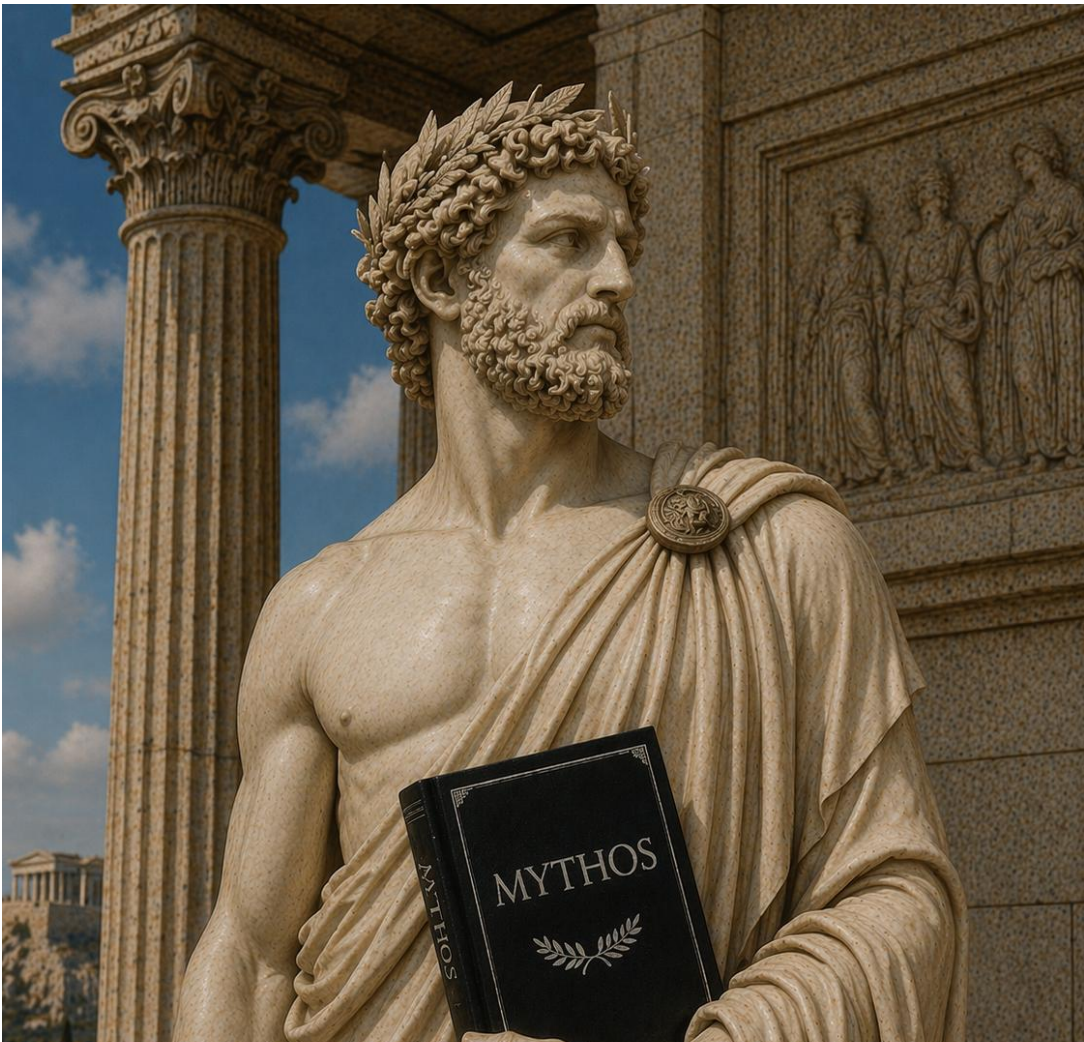
Email: shiny@bepress.com

Middleware: Required for purchase.

Updated: 19 Apr 2026

<https://breachforums.at/thread-VERIFIED-Verce-Database-Access-Key-Source-Code-19-Apr-2026>

Source: [LinkedIn](#)



KI-Modelle entwickeln sich schneller, als wir „Benchmark“ sagen können!

Evaluation		Claude family		Other models	
		Claude Mythos Preview	Claude Opus 4.6	GPT-5.4	Gemini 3.1 Pro
GPQA Diamond		94.5%	91.3%	92.8%	94.3%
MMMLU		92.7%	91.1%	—	92.6%–93.6%
USAMO		97.6%	42.3%	95.2%	74.4%
GraphWalks BFS 256K-1M		80.0%	38.7%	21.4%	—
HLE	no tools	56.8%	40.0%	39.8%	44.4%
	with tools	64.7%	53.1%	52.1%	51.4%
CharXiv Reasoning	no tools	86.1%	61.5%	–	–
	with tools	93.2%	78.9%	–	–
OSWorld		79.6%	72.7%	75.0%	

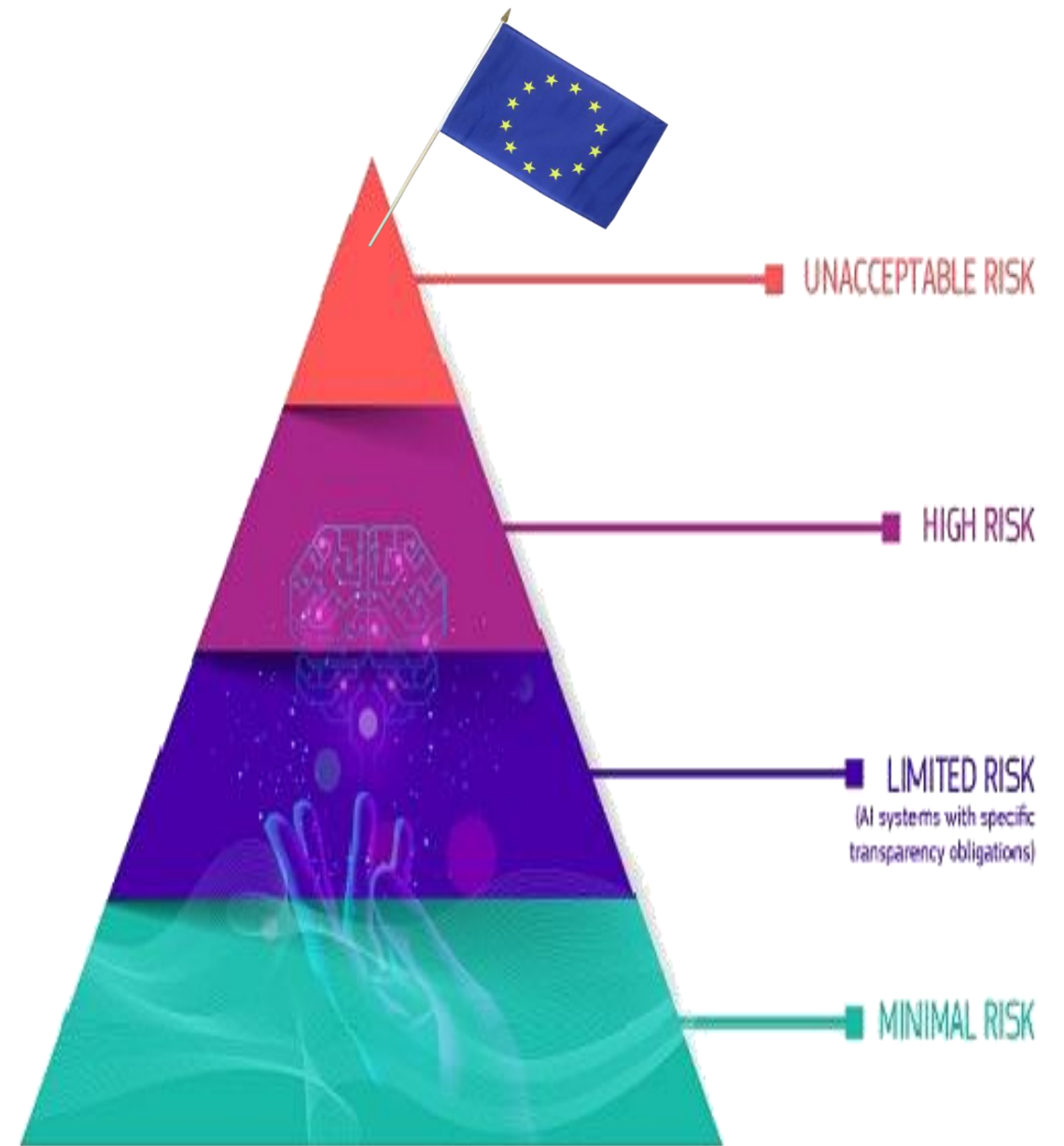
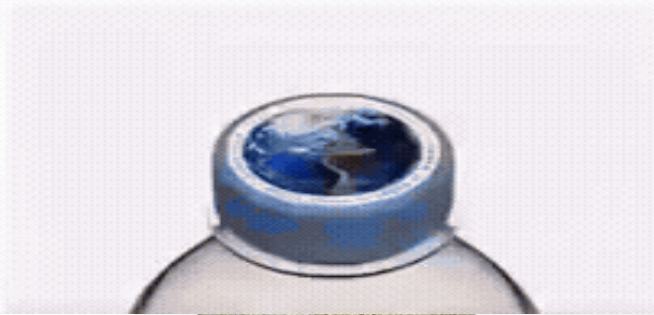

CHINA:




USA:




EU:

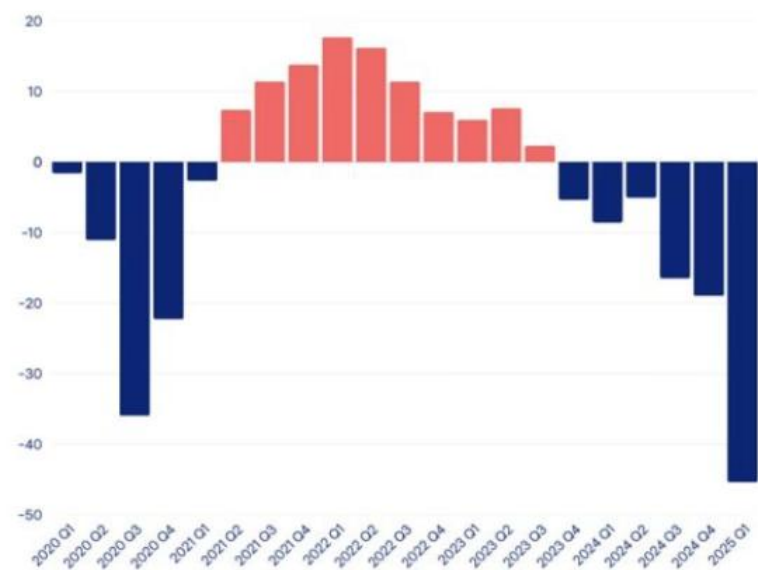


Demografischer Wandel & Nachwuchsprobleme

Handelsblatt

KI verdrängt Berufseinsteiger

Anteil an Einstiegsjobs auf dem Tiefpunkt



Stellenanzeigen auf Stepstone.de, die sich an Berufseinsteiger*innen richten
Veränderung zum 5-Jahres-Durchschnitt in Prozent

Source: [Handelsblatt](#)

Boomer werden Rentner

Zahl der Babyboomer in Deutschland ...

- ... unter dem gesetzlichen Renteneintrittsalter
- ... über dem gesetzlichen Renteneintrittsalter

2022	16.396.100	3.090.800
2023	15.453.900	4.065.100
2024	14.442.800	4.929.700
2025	13.196.500	6.014.200
2026	12.115.200	6.920.400
2027	10.993.800	7.853.300
2028	9.899.000	8.746.800
2029	8.778.000	9.656.000
2030	7.639.500	10.570.600
2031	6.284.200	11.688.900
2032	4.963.800	12.757.700
2033	3.655.200	13.799.600
2034	2.389.900	14.781.700
2035	1.163.700	15.705.400
2036	0	16.545.500
2037	0	16.198.900
2038	0	15.824.400
2039	0	15.421.500
2040	0	14.986.400

Babyboomer: in Deutschland lebende Personen der Geburtsjahrgänge 1954 bis 1969;
ab 2023: Prognose

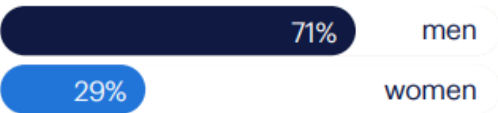
Quellen: Statistisches Bundesamt, Institut der deutschen Wirtschaft
© 2024 IW Medien / iwd

iwd

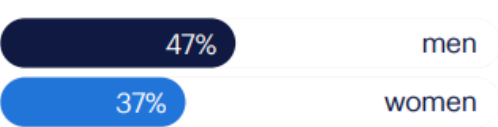
Source: [IWD](#)

men dominate AI usage in the workplace

percentage of men and women reporting having AI skills



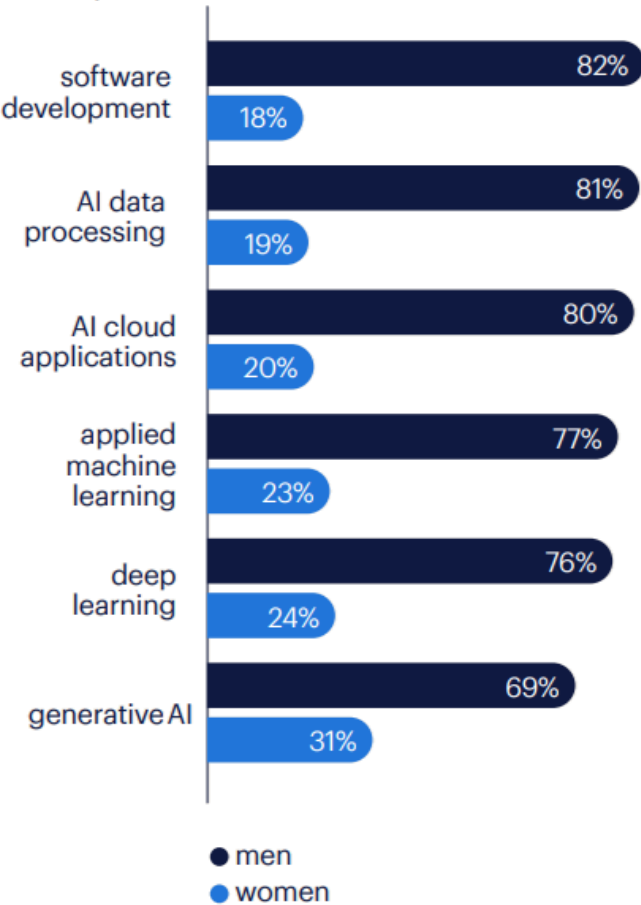
percentage of men and women that have used AI to problem-solve at work



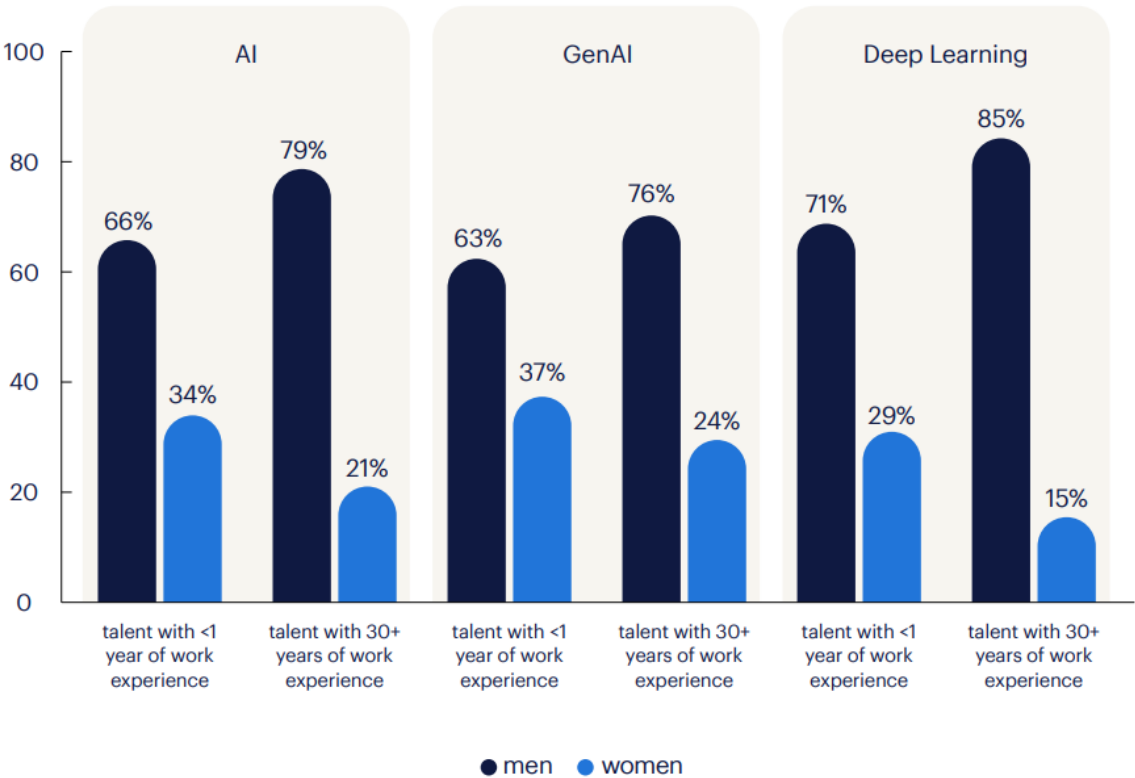
percentage of men and women provided with AI access by their employer



women are severely underrepresented in specialist AI skills



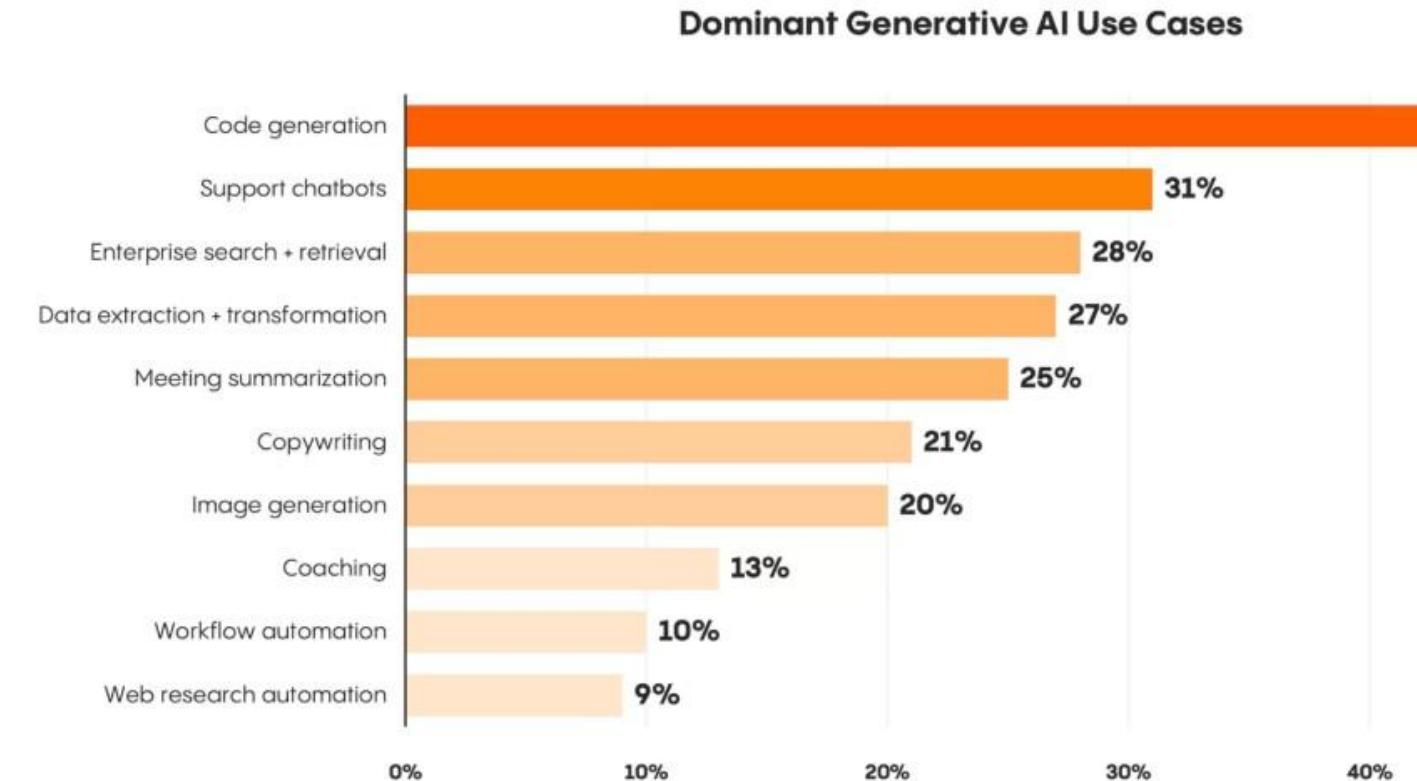
AI skills by gender breakdown across experience levels



Source: [Randstad](#)

KI-Nutzung in Unternehmen

Wie zu erwarten, stehen Code-Generierung, Kundenservice und Analyseaufgaben klar im Vordergrund.

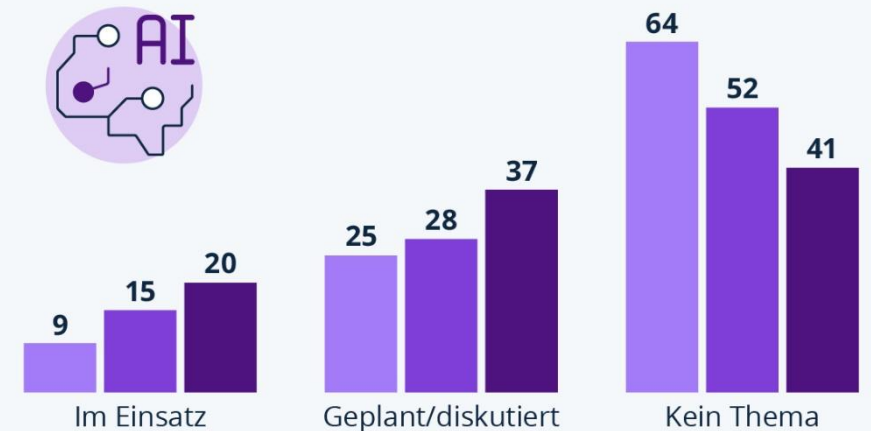


© 2024 Menlo Ventures

Jedes 5. Unternehmen in Deutschland setzt KI ein

Anteil der Unternehmen, bei denen künstliche Intelligenz im Einsatz/geplant/kein Thema ist (in %) **endlich**

■ 2022 ■ 2023 ■ 2024

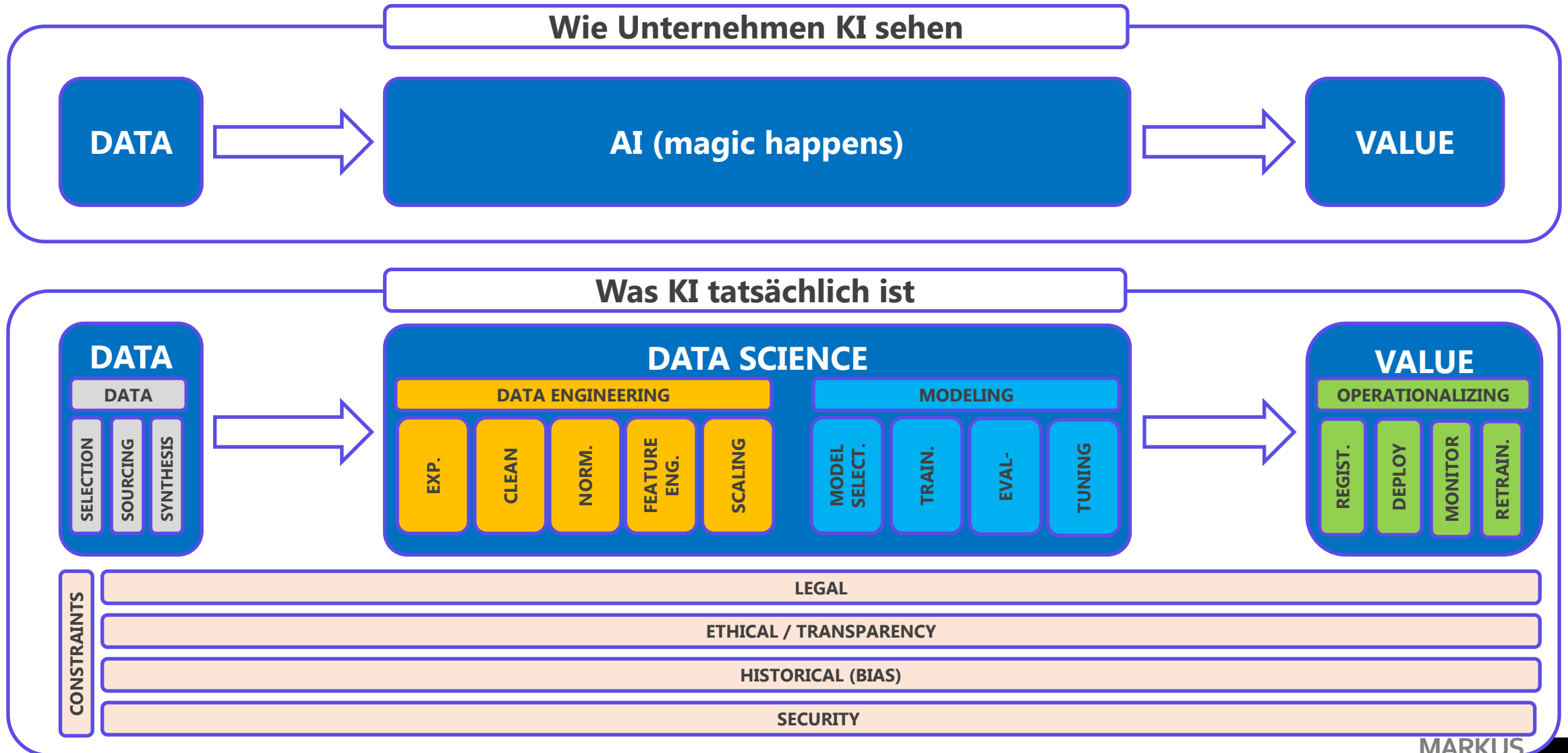


Basis: jew. rund 600 Unternehmen ab 20 Mitarbeiter:innen in Deutschland
Quelle: Bitkom Research

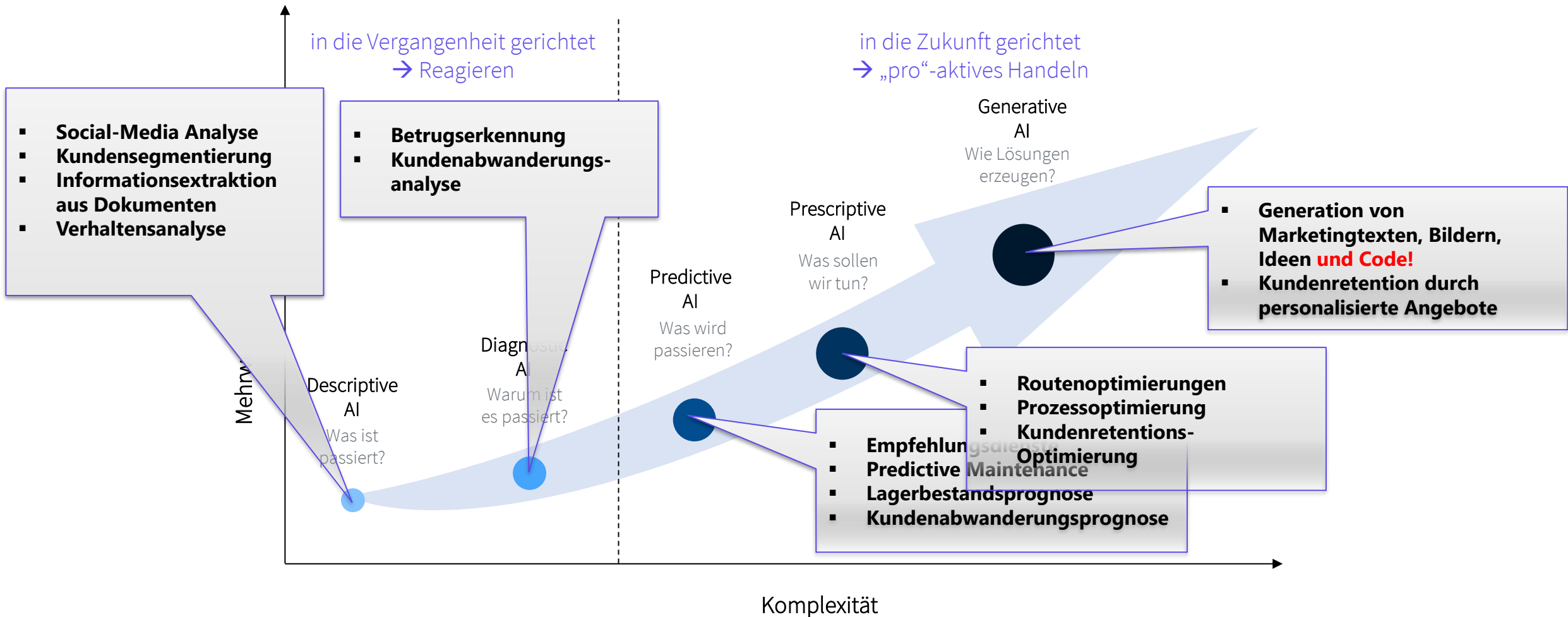


statista

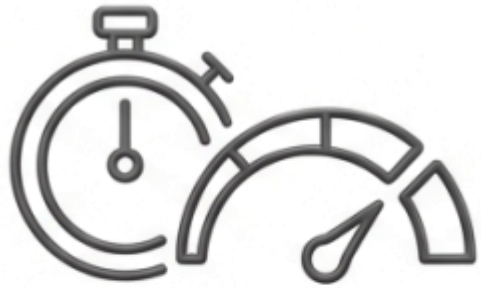
Wahrnehmung von Künstlicher Intelligenz



Anwendungsfälle für KI und Data Science in Unternehmen



Das Innovations-Dilemma: **Beschleunigung ohne Kontrollverlust.**



Der Zwang

Unternehmen müssen innovieren, um wettbewerbsfähig zu bleiben.



Das Risiko

Jeder Mitarbeiter, der unkontrolliert Firmendaten in öffentliche KI-Modelle kopiert, öffnet eine Tür für Datenabfluss.

**„Verbote
funktionieren
nicht -
Steuerung ist
die Lösung.“**

Die Realität am IT-Radar vorbei: Die unsichtbare Gefahr der Schatten-KI.



- ⚠️ **Status quo:** Die Fachbereiche handeln eigenständig und setzen Tools wie ChatGPT, DeepL & vergleichbare Dienste bereits produktiv ein
- ⚠️ **IP-Gefährdung:** Geschäftskritisches Know-how und vertrauliche Informationen verlassen den kontrollierten Unternehmenskontext.
- ⚠️ **Steuerungsdefizit im Management:** Die Unternehmensleitung trägt das Haftungs- und Reputationsrisiko.

KI ist keine Tech-Frage mehr - es ist eine Haftungsfrage!

- **Compliance-Falle:** Unkontrollierter KI-Einsatz ist kein Kavaliersdelikt.
- **EU AI Act:** Die Geschäftsführung haftet für nicht-konforme KI-Anwendungen.
- **DSGVO/GDPR:** Personenbezogene Daten in unsicheren Drittstaat-Clouds können Datenschutzverstöße darstellen.

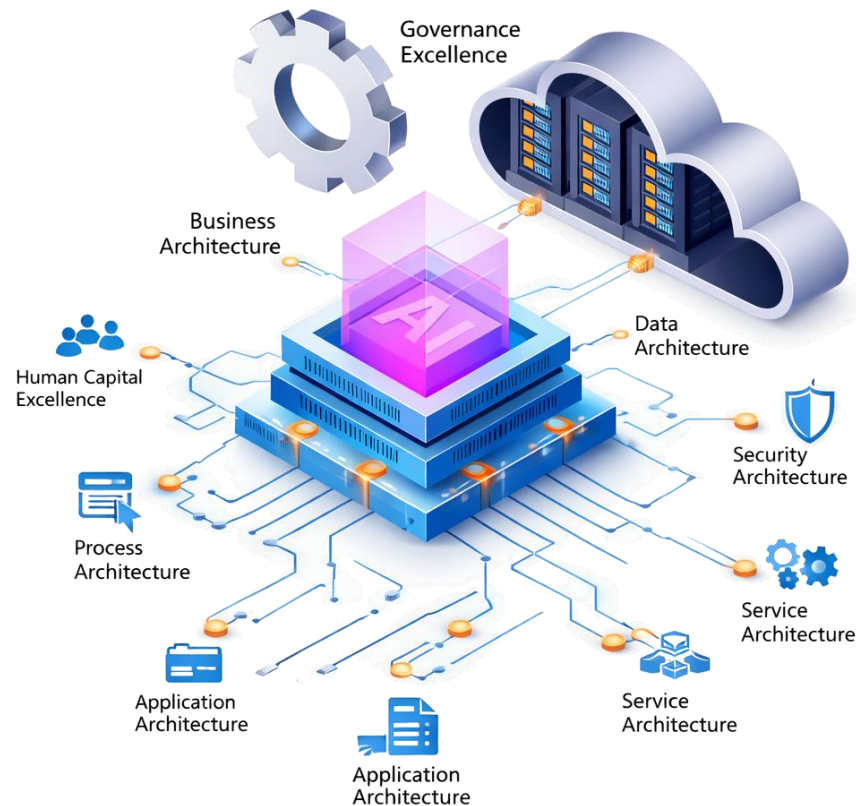


Compliance darf kein Hindernis sein, sondern muss das automatisierte Fundament bilden.

Strukturen schaffen - Systemarchitekturen aufbauen

Anwendung:

Applikationen werden gezielt über ein differenziertes Rollen- und Berechtigungskonzept bereitgestellt.



Speicherung:

Einsatz unterschiedlicher Datenbanktechnologien mit sicherer, kontrollierter Datenhaltung.

Infrastructure-as-Code: Isolierung einzelner Ökosysteme und Kundenbereiche durch automatisierte, versionierte Infrastruktur.

Governance by Design: Sicherheit ist kein Feature, sondern das Fundament für Vertrauen

Granulares Rollenkonzept:

„Nicht jeder darf alles.“

Der Bearbeiter sieht andere Daten als die Sachgebietsleiterin.



Privacy Filters:

Automatische Anonymisierung bzw. Maskierung personenbezogener Daten (PII), bevor sie die Unternehmensgrenzen verlassen.

Audit-Sicherheit:

Vollständige Nachvollziehbarkeit aller KI-Entscheidungen (Data Lineage) im Einklang mit den Anforderungen des EU AI Act.

Out-of-the-Box:

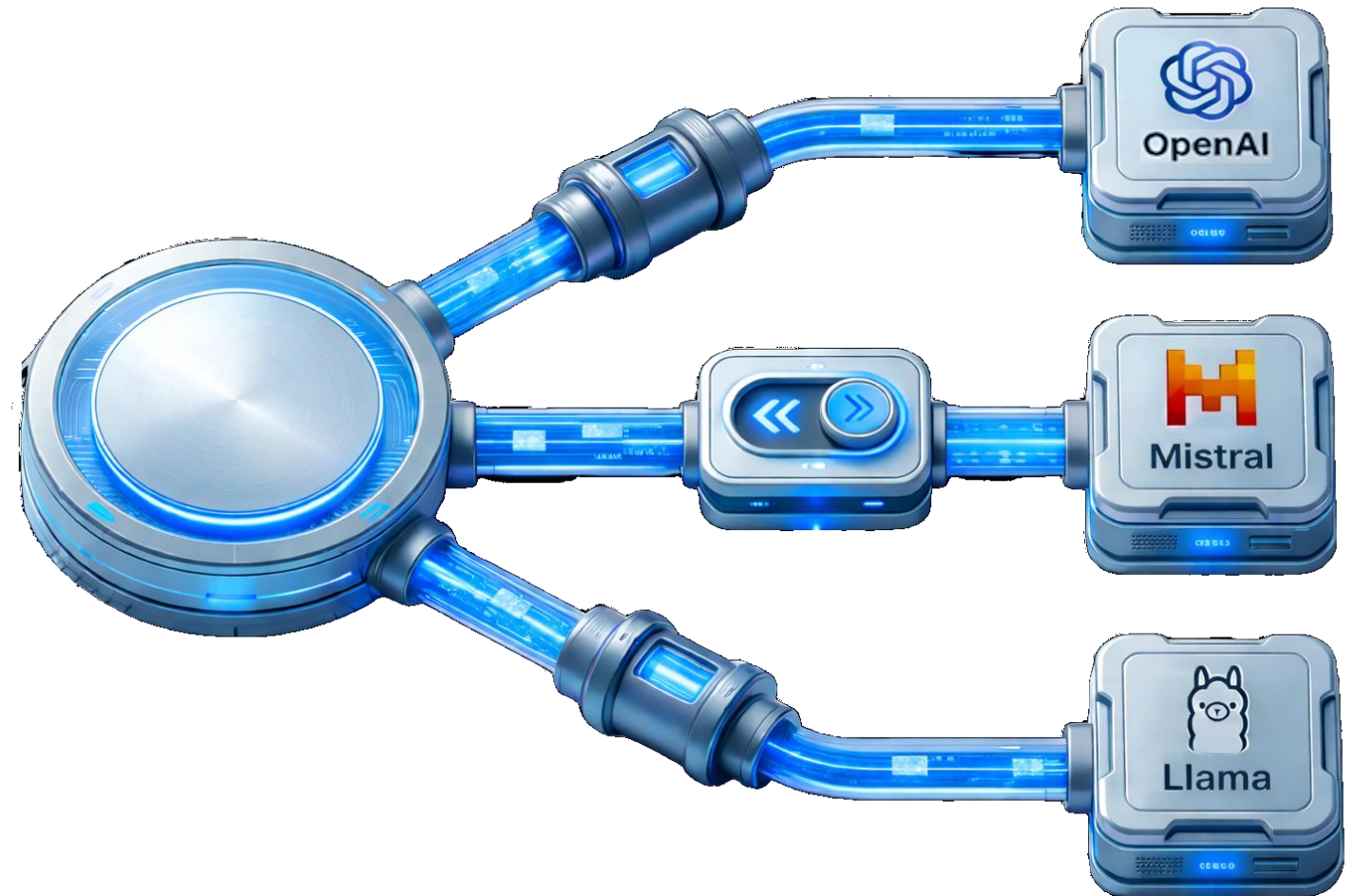
DSGVO-konforme Nutzung ohne komplexe Zusatzkonfiguration.

Strategische Unabhängigkeit durch Modell-Agnostik

Kein Vendor Lock-in

Heute führt OpenAI, morgen vielleicht Mistral oder Llama.

Eine **gute Architektur** erlaubt Ihnen, die **KI-Modelle** im Hintergrund **zu wechseln**, ohne Ihre Infrastruktur umzubauen.



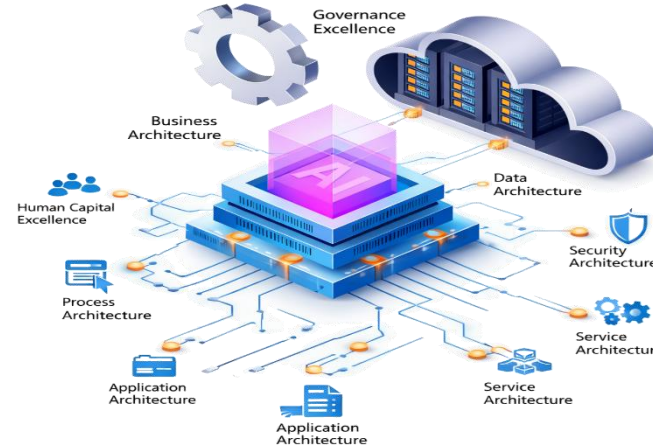
3 Punkte für den späteren Heimweg...



Kontrolle über Daten

- Daten verlassen nicht das Unternehmen
- Retention & Logs selbst definierbar
- Keine Vendor-Policy-Abhängigkeit

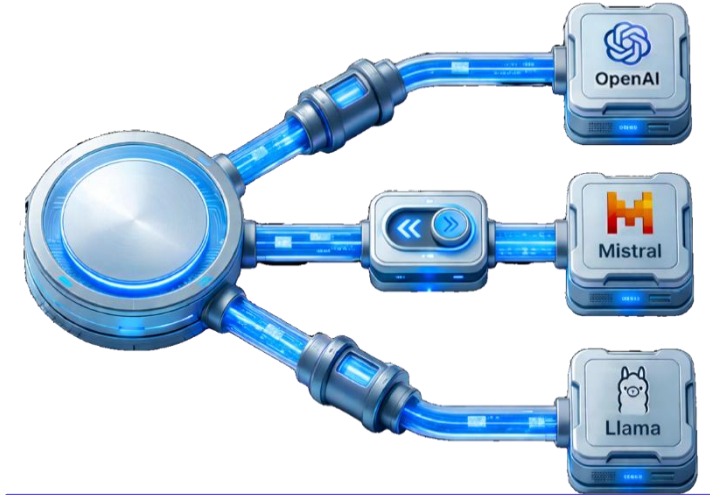
💡 **Souveränität ist Architektur, kein Feature!**



Produktionsreife durch Nachvollziehbarkeit

- Vollständige Inference-Logs
- Versionierte Modelle & Prompts
- Nachweis genutzter Datenquellen

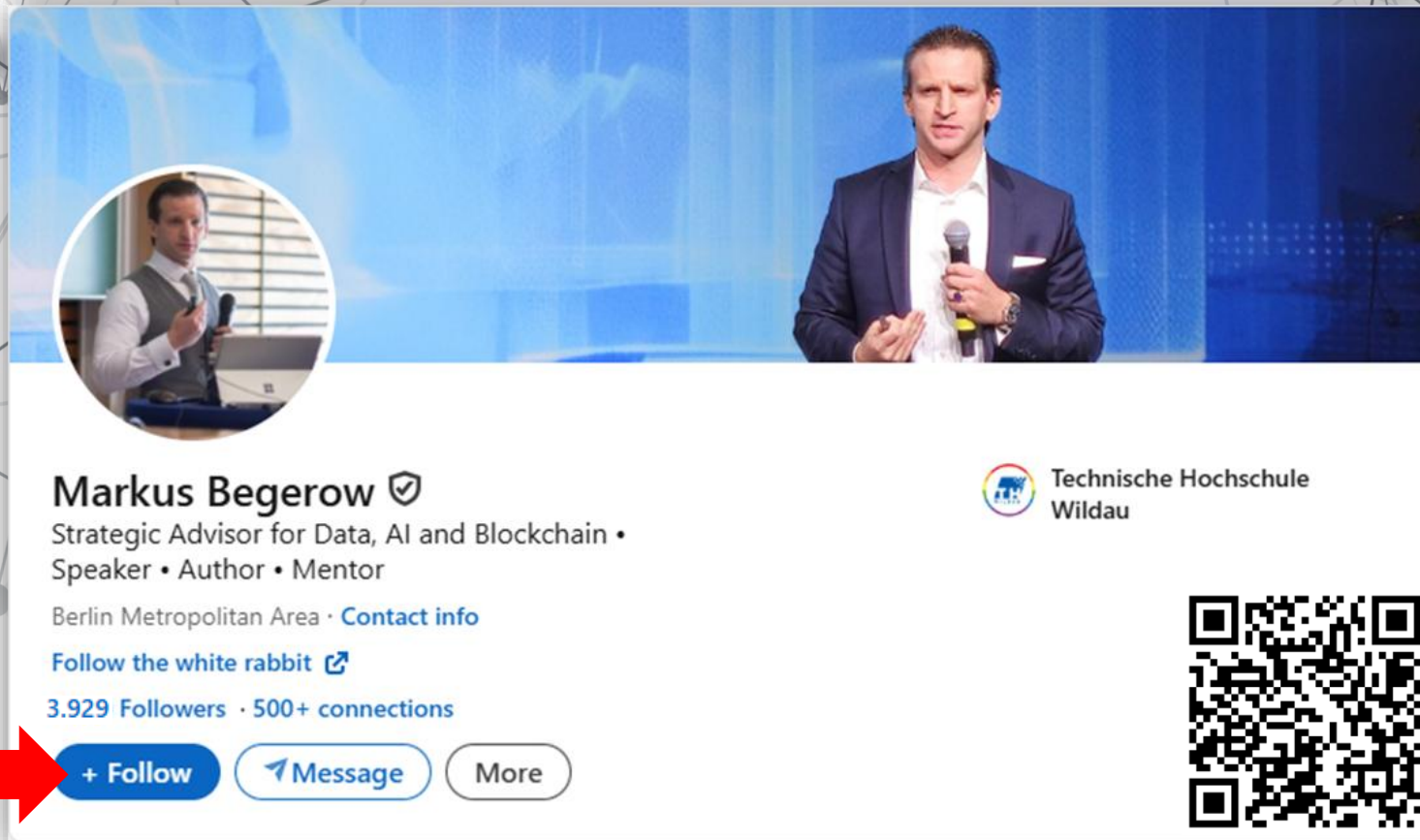
💡 **Was nicht prüfbar ist, ist nicht enterprisefähig!!**



Infrastruktur statt Mietlösung

- Keine API-Abhängigkeit
- Kosten langfristig planbar
- Modellwahl frei

💡 **AI ist Infrastruktur - nicht nur ein Service!!!**



Markus Begerow ✓
Strategic Advisor for Data, AI and Blockchain •
Speaker • Author • Mentor
Berlin Metropolitan Area · [Contact info](#)
[Follow the white rabbit](#) ↗
3.929 Followers · 500+ connections

[+ Follow](#) [Message](#) [More](#)

Technische Hochschule Wildau



THANK YOU!

Slides, Sources, Tools:
markus-begerow.de



📱 [@markusbegerow](#)

✉ mail@markus-begerow.de

🌐 linkedin.com/in/markusbegerow