

Künstliche Intelligenz

Wie sieht KI in der Unternehmenspraxis aus?

XIBIX Solutions

Zertifizierungen



TISAX®
Label für "Information with Very High Protection Needs" gültig bis 2026-12-13 mit Scope-ID: SNXVM

TISAX® ist eine eingetragene Marke der ENX Association.



ISO 27001
Informationssicherheits-Management





ISO 9001
Qualitätsmanagement





BSFZ Forschungszulage
Bescheinigte Forschung & Entwicklung im Sinne des FZulG – 2026





ISO 14001 im Aufbau
Umweltmanagement

2014
Foundation

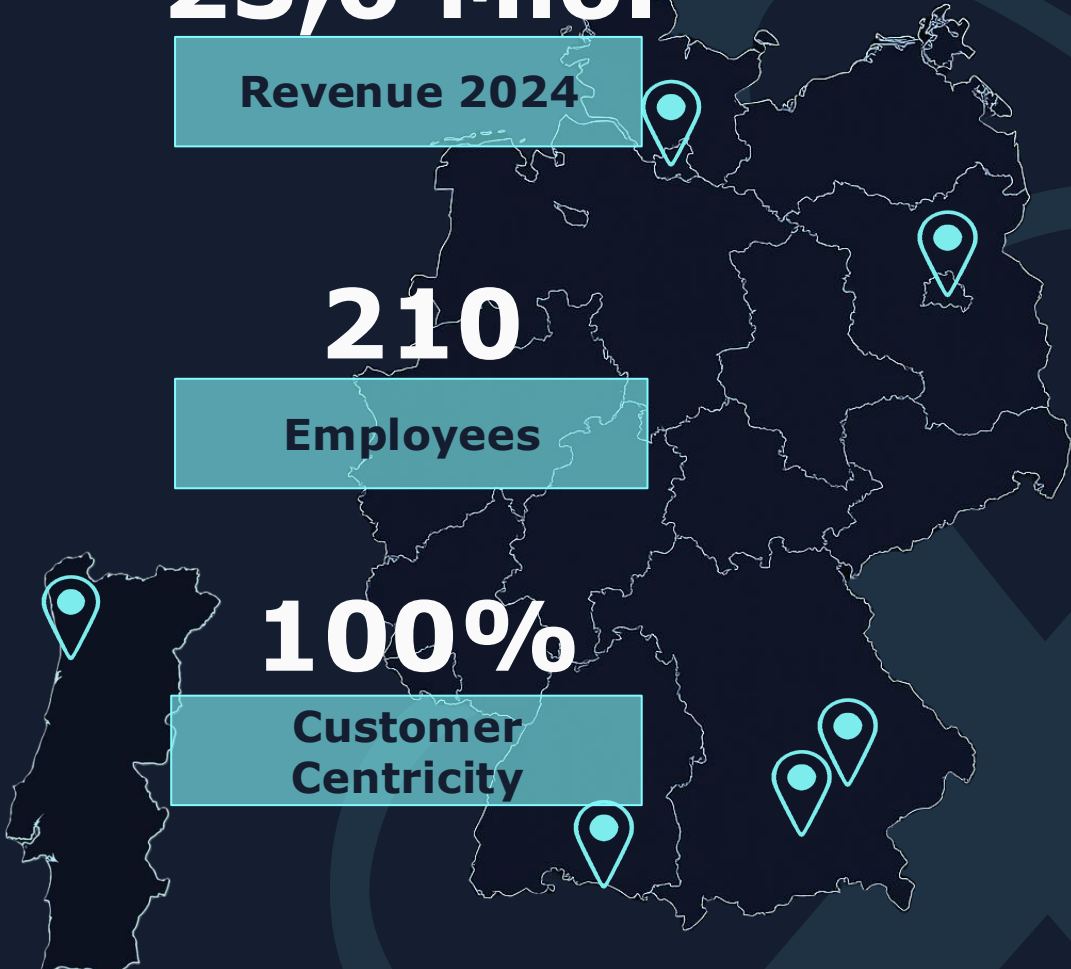
6
Locations

33%
Women's Quota

23,6 Mio.
Revenue 2024

210
Employees

100%
Customer Centricity



XIBIX Portugal

XIBIX Solutions

Zertifizierungen

**TISAX®**
Label für "Information with Very High Protection Needs" gültig bis 2026-12-13 mit Scope-ID: SNXVM

TISAX® ist eine eingetragene Marke der ENX Association.

**ISO 27001**
Informationssicherheits-Management



**ISO 9001**
Qualitätsmanagement



**BSFZ Forschungszulage**
Bescheinigte Forschung & Entwicklung im Sinne des FZulG – 2026



**ISO 14001** im Aufbau
Umweltmanagement

2014
Foundation

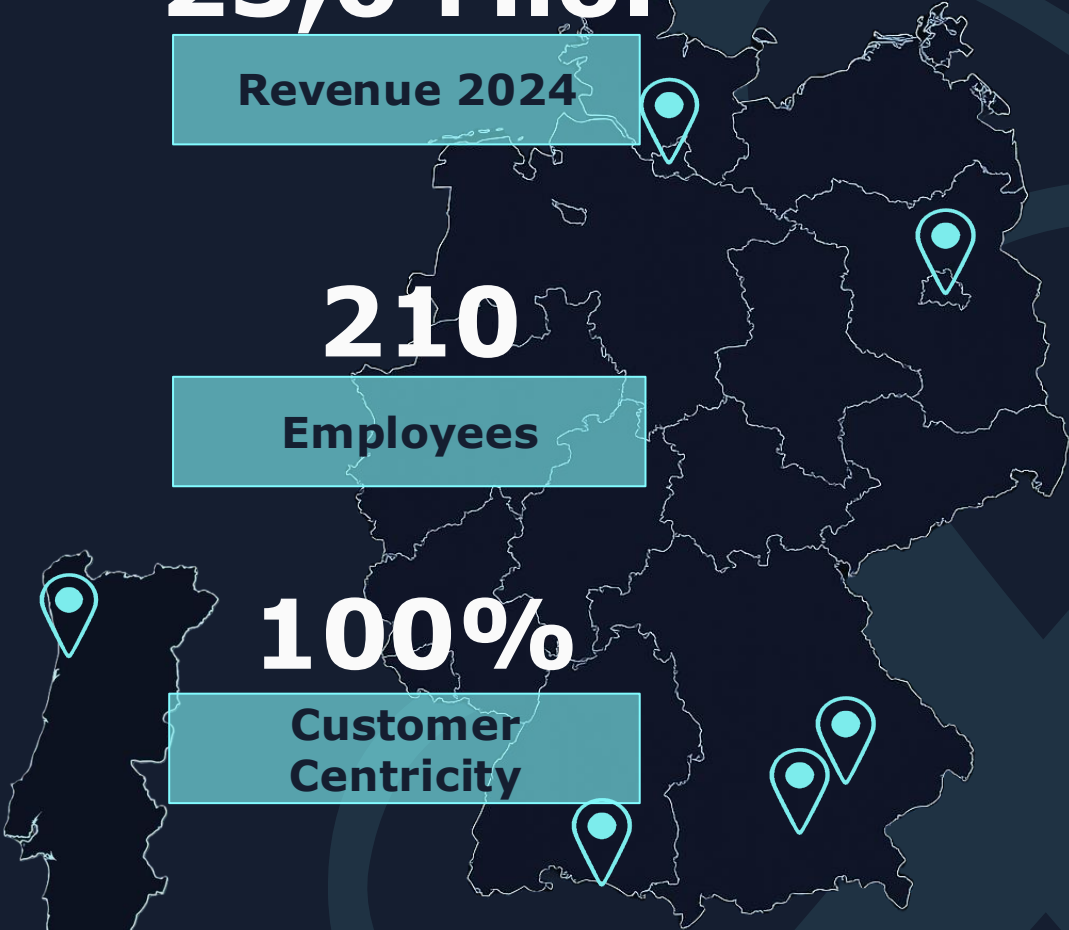
6
Locations

33%
Women's Quota

23,6 Mio.
Revenue 2024

210
Employees

100%
Customer Centricity



XIBIX Portugal



Wie sieht KI in der Unternehmenspraxis aus?

Jeder spricht über KI, doch viele setzen den Einsatz von KI-Anwendungen mit echter KI-Kompetenz gleich.



AI GATEWAY

Eine Schnittstelle. Jedes LLM. Volle Kontrolle.

Multi-Provider-Routing

Auto-Tier AI

PII-Schutz

Enterprise-Governance

3-Stufen-Cache

KI in Unternehmen zu verwalten ist unübersichtlich



Mehrere KI-Anbieter, keine einheitliche API

Jedes Team integriert Azure, AWS oder Google separat: Code-Duplikate und Wartungsaufwand.



Unkontrollierte KI-Ausgaben pro Team

Ohne zentrale Budgetkontrolle explodieren die Kosten unbemerkt.



Verstreute API-Keys, kein Audit-Trail

Niemand weiß, wer wann welches Modell mit welchen Daten genutzt hat.



Node-Middleware kostet 30–80 ms

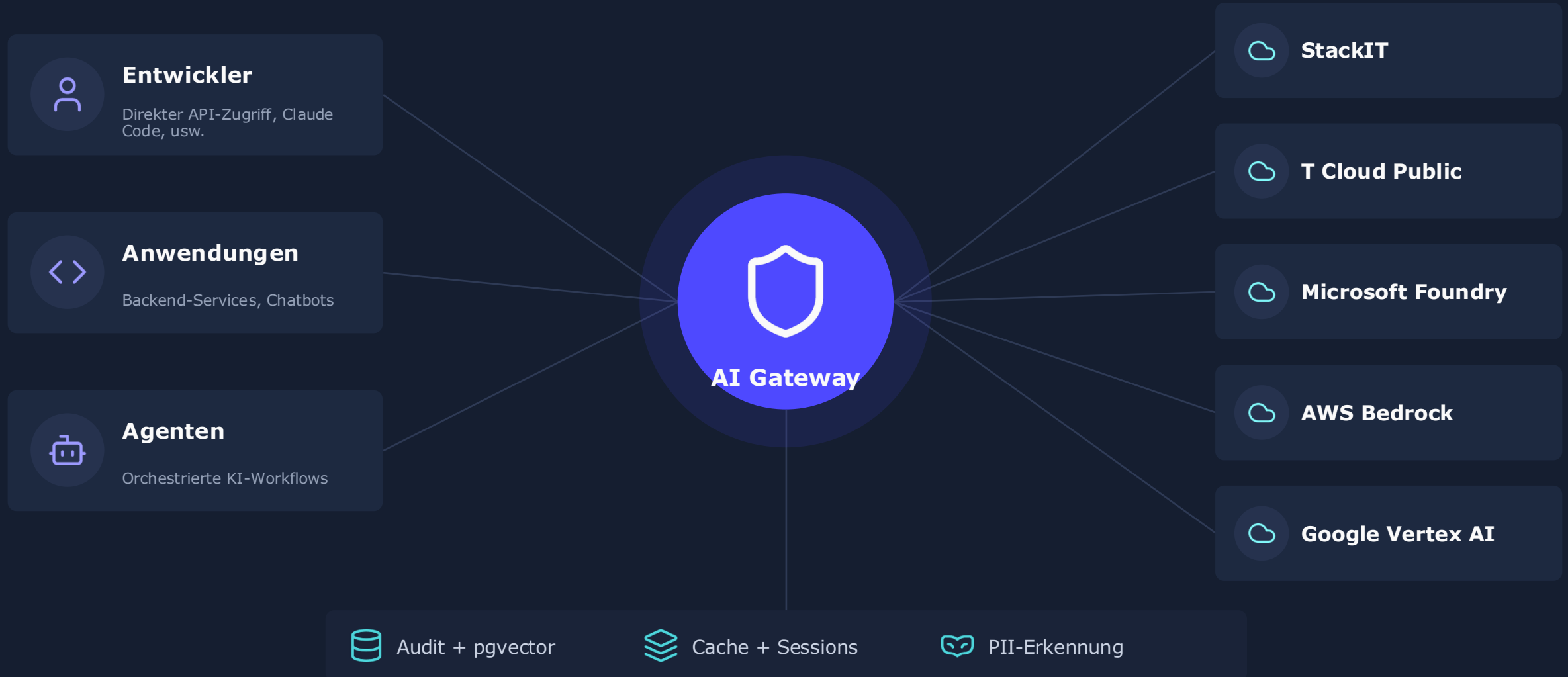
Zusätzliche Latenz durch selbstgebaute Zwischenschichten.



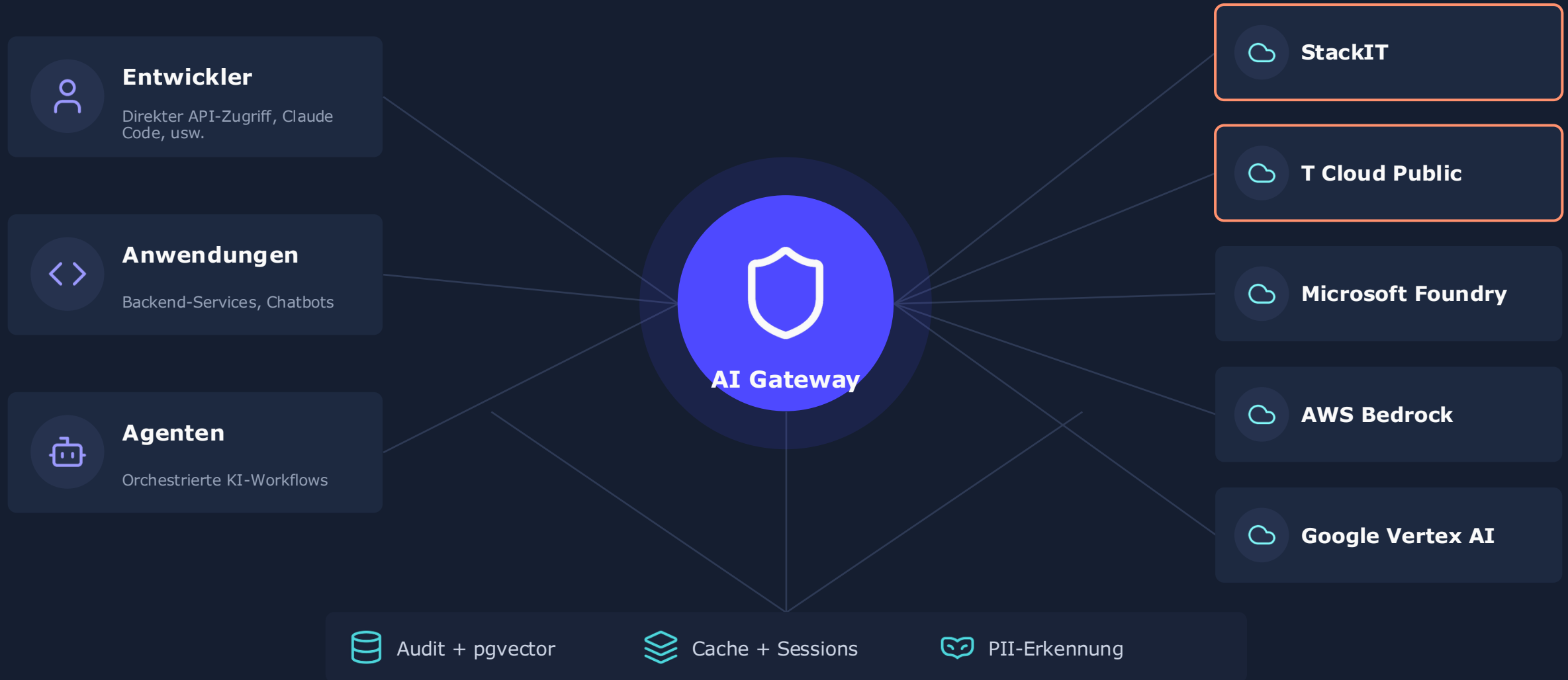
Keine Datenhoheit, keine DSGVO-Konformität

Sensible Daten verlassen unkontrolliert die Unternehmensgrenzen.

Eine zentrale Plattform für die gesamte KI-Infrastruktur



Eine zentrale Plattform für die gesamte KI-Infrastruktur



Intelligentes Routing per 15-Dimensionen-Analyse

< 1 ms lokale Bewertung · automatische Weiterleitung an das passende Modell

EINGEHENDER PROMPT

„Analysiere die geopolitischen Auswirkungen aktueller KI-Regulierung in der EU im Vergleich zu den USA. Berücksichtige wirtschaftliche Effekte, Innovationsgeschwindigkeit und Wettbewerbsdynamik.“

COMPLEXITY ENGINE

token_count

question_density

technical_depth

reasoning_required

context_length

code_present

math_complexity

multi_step

Komplexitäts-Score

0.74

von 1.0

● Simple (0.0 – 0.35)

Q&A, Zusammenfassungen, Klassifikation

Haiku · GPT-4.1 nano · Open Source Model

● Medium (0.35 – 0.65)

Reasoning, Coding, Analyse

Sonnet · GPT-4o-mini · Open Source Model

● Complex (0.65 – 1.0)

Deep Research, komplexes Reasoning

Opus · GPT-5 · Open Source Model

Guardrails: PII-Schutz & Prompt-Security-Engine

Presidio PII-Anonymisierung · 150+ Sicherheitsregeln · Angriffskategorien · Threat-Scoring

VOR DER ANONYMISIERUNG

Bitte helfen Sie John Smith (**john.smith@firma.de**) bei der Analyse des Vertrags für unseren Kunden in der **Musterstrasse 1, Berlin**.
Telefon **+49 151 0000000** bleibt vertraulich.

NACH PRESIDIO ANONYMIZER

Bitte helfen Sie **[PERSON]** (**[EMAIL]**) bei der Analyse des Vertrags für unseren Kunden in **[ORT]**. Telefon **[TELEFON]** bleibt vertraulich.

✓ **DSGVO-konform · PII erreicht nie den Modell-Anbieter**

Unicode-Verschleierung · Homoglyphen · Base64/Hex werden vor der Prüfung dekodiert

PROMPT SECURITY ENGINE

Injection

Jailbreak

System-Prompt-Leak

RolePlay

Threat Score

0.82

0.4 flag

0.7 block

ANFRAGE BLOCKIERT

Score 0.82 überschreitet Schwellenwert 0.7 · Treffer: Injection (×2),
Jailbreak (×1)

Wiederholungs-Sperre

3× gleiches Angriffsmuster in 24 h → automatisch 72 h gesperrt

Enterprise-Governance: Kosten, Zugriff & Nachvollziehbarkeit

VIRTUELLE SCHLÜSSEL-TYPEN

- Personal Key**
5 Anfr./Min · 20 EUR/Monat
- Group Key**
50 Anfr./Min · 500 EUR/Monat
- Service Key**
unbegrenzt · kein Limit

BUDGETÜBERWACHUNG

alice@firma.de

12,40 / 20,00 EUR

Engineering-Team

440 / 500 EUR

⚠ Limit fast erreicht

Budgets werden automatisch durchgesetzt, nicht nur beobachtet – live pro Nutzer, Team oder Projekt.

FLEXIBLE AUTHENTIFIZIERUNG

- Lokale Konten

E-Mail + Passwort
- Azure Entra ID

OIDC-SSO
- Google Workspace

OIDC-SSO

Jeder OIDC-Provider über config.toml · parallel nutzbar

AUDIT-LOG · APPEND-ONLY · CSV-EXPORT · VOLLSTÄNDIGE HISTORIE

ZEIT	NUTZER	MODELL	PROVIDER	KOSTEN	LATENZ
14:23:01	alice@firma.de	gpt-4o	Azure	0,0124 EUR	312 ms
14:23:04	bob@firma.de	claude-3-5-sonnet	Bedrock	0,0467 EUR	448 ms
14:23:07	svc-pipeline	gpt-4o-mini	Azure	0,0009 EUR	198 ms

Warum das AI Gateway in der Unternehmenspraxis den Unterschied macht



Kontrolle

Ein Endpunkt für alle Modelle und Anbieter.



Sicherheit

PII-Schutz und Prompt-Firewall serienmäßig.



Geschwindigkeit

Kein Python-/Node-Overhead.



Compliance

DSGVO-konform per Design.



Kosteneffizienz

Auto-Routing und harte Budgetgrenzen.

Ein Endpunkt. Jedes LLM. Volle Kontrolle.

KONTAKT

Vielen Dank für Ihre Aufmerksamkeit

Sprechen wir darüber, wie das AI Gateway in Ihrem Unternehmen den Unterschied macht.

Dr. Fabrizio Palmas

HEAD OF BUSINESS DEVELOPMENT



+49 89 7167 221-0



www.xibix.de



fabrizio.palmas@xibix.de



Networking made easy,
scan my **LinkedIn**

