

ti&m x Finance Forum Zürich

Wer kontrolliert die Bank?

Souveränität für Technologie und Daten im Banking

David Furrer, Lead Consultant

Nico Kaiser, Lead Consultant

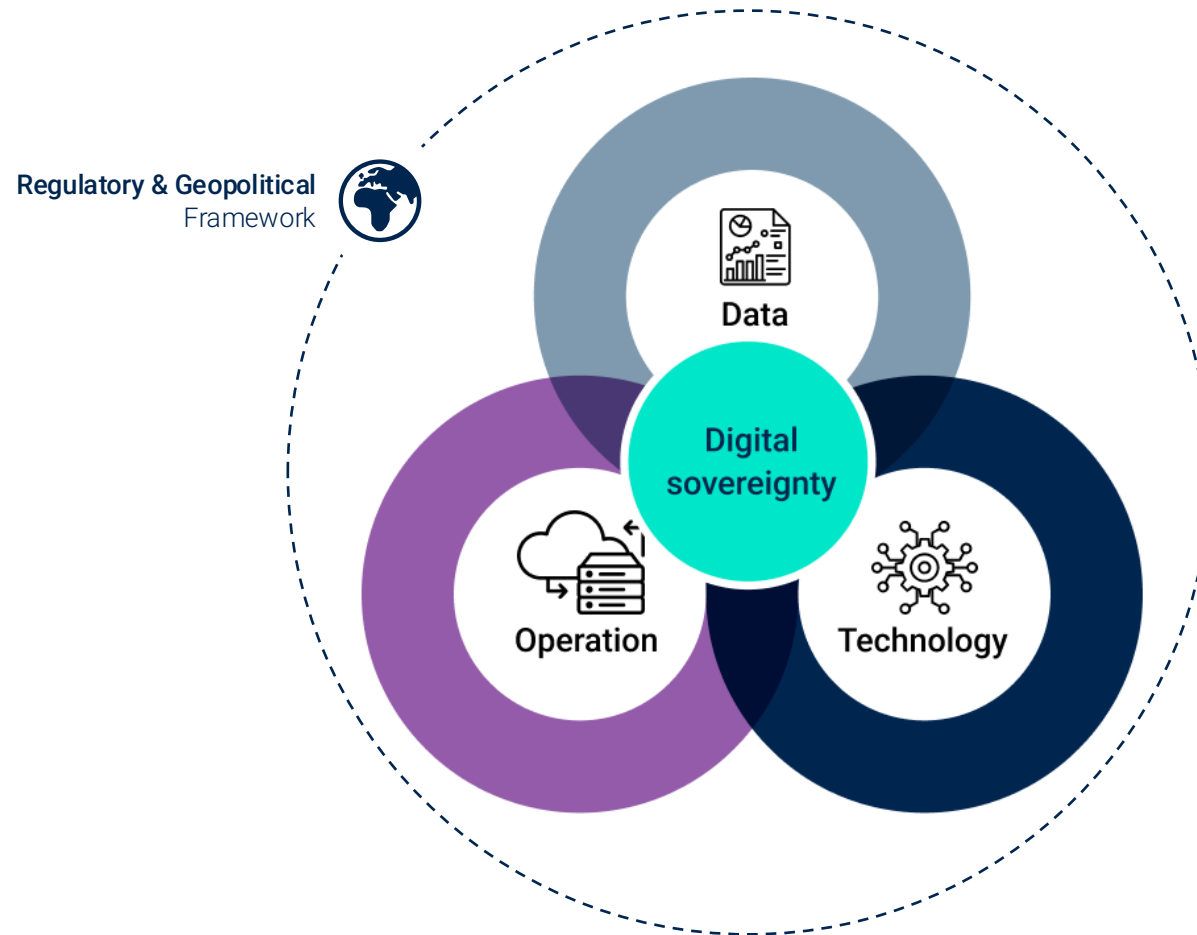
Zürich, 2026 V1.0

ti&m



Warum jetzt digitale Souveränität?

Thema und Begrifflichkeiten



Warum jetzt?

Zentrale Treiber machen digitale Souveränität 2026 zu einer strategischen Pflichtaufgabe



Verschärfte Regulatorik

U.a. verschärfen Regulatorien wie z.B. die Privatism-Resolution, Bundes-Leitlinien Souveränität und FINMA-Outsourcing Anforderungen an Verschlüsselung / Datenhaltung, Nachweis- und Exit-Pflichten



Abhängigkeiten kosten immer mehr

Preiserhöhungen, Lizenzmodell-Wechsel und Konzentrationsrisiken bei grossen Software-Anbietern (z.B. Broadcom/VMware, Salesforce) sowie Hyperscaler (AWS, MS Azure & GCP) treffen die TCO



Geopolitische Lage bringt erhöhte Risiken

US CLOUD Act, Sanktionsregime und Schweizer Souveränitätsdebatte stellen Datenstandorte und technologische Abhängigkeiten in Frage



KI bringt zusätzliche Herausforderungen

GenAI-Services lagern Daten, Modelle und Geschäftslogik an wenige Anbieter aus, manchmal intransparent / unbemerkt und schaffen neue Abhängigkeiten

Drei aktuelle Beispiele zeigen die verschärfte Risikolage

Exportkontrollen für Top-Technologien, auch für Europa

AI Model Export Controls: The Fable-Mythos Precedent

Executive Summary

On the evening of June 12, 2026, Anthropic received a letter from Commerce Secretary Howard W. Lutnick directing the company to immediately suspend access to its two most capable AI models — Claude Fable 5 and Claude Mythos 5 — for any foreign national, whether located inside or outside the United States. Because Anthropic serves hundreds of millions of users globally [1] and cannot screen for citizenship in real time, the only compliant response was a full global shutdown. The action marked the first time the U.S. government had used export control law to halt a commercial AI model already in broad public deployment [12].

The statutory mechanism was an "Is Informed" letter issued under the Export Control Reform Act of 2018 (ECRA), invoking the Commerce Department's Bureau of Industry and Security (BIS) authority over emerging and foundational technologies essential to national security [1][2]. The proximate trigger was a jailbreak technique demonstrated to government officials by Amazon researchers — a multi-step method for framing cybersecurity requests as defensive code review to bypass Fable 5's safety classifiers [3]. The deeper driver was a classified NSA red-team finding, subsequently briefed to Congress, that Mythos 5 had penetrated nearly all NSA classified systems in an authorized exercise within hours — a capability the government judged too dangerous to remain in unrestricted global access [4].

<https://labs.cloudsecurityalliance.org/research/ai-model-export-controls-fable-mythos-regulatory-precedent-v/> (12. Juni 2026)

Rechtliche Eingriffe betreffen kritische Services und Daten

Criminal Court: Microsoft's email block a wake-up call for digital sovereignty

Microsoft blocked the email account of Chief Prosecutor of the International Court of Justice after Trump's sanctions. Critics: "We urgently need alternatives."



The International Criminal Court in The Hague. (Image: ICC)

<https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html> (19. Mai 2025)

Ein Europäischer Datenstandort garantiert die Datensouveränität nicht zwingend



Quelle: Depositphotos

Unter Eid: Microsoft kann Schutz vor Cloud Act nicht garantieren

Microsoft schafft laut eigener Aussage eine souveräne Cloud für Europa, um die Datenschutzbedenken auf dem alten Kontinent zu adressieren. Ein Microsoft-Manager hat nun aber unter Eid bestätigt: Eine Garantie, dass keine Daten an US-Behörden weitergegeben werden, ist nicht möglich.

17. Juli 2025

<https://www.itmagazine.ch/artikel/85137/Unter-Eid-Microsoft-kann-Schutz-vor-Cloud-Act-nicht-garantieren.html> (17. Juli 2025)



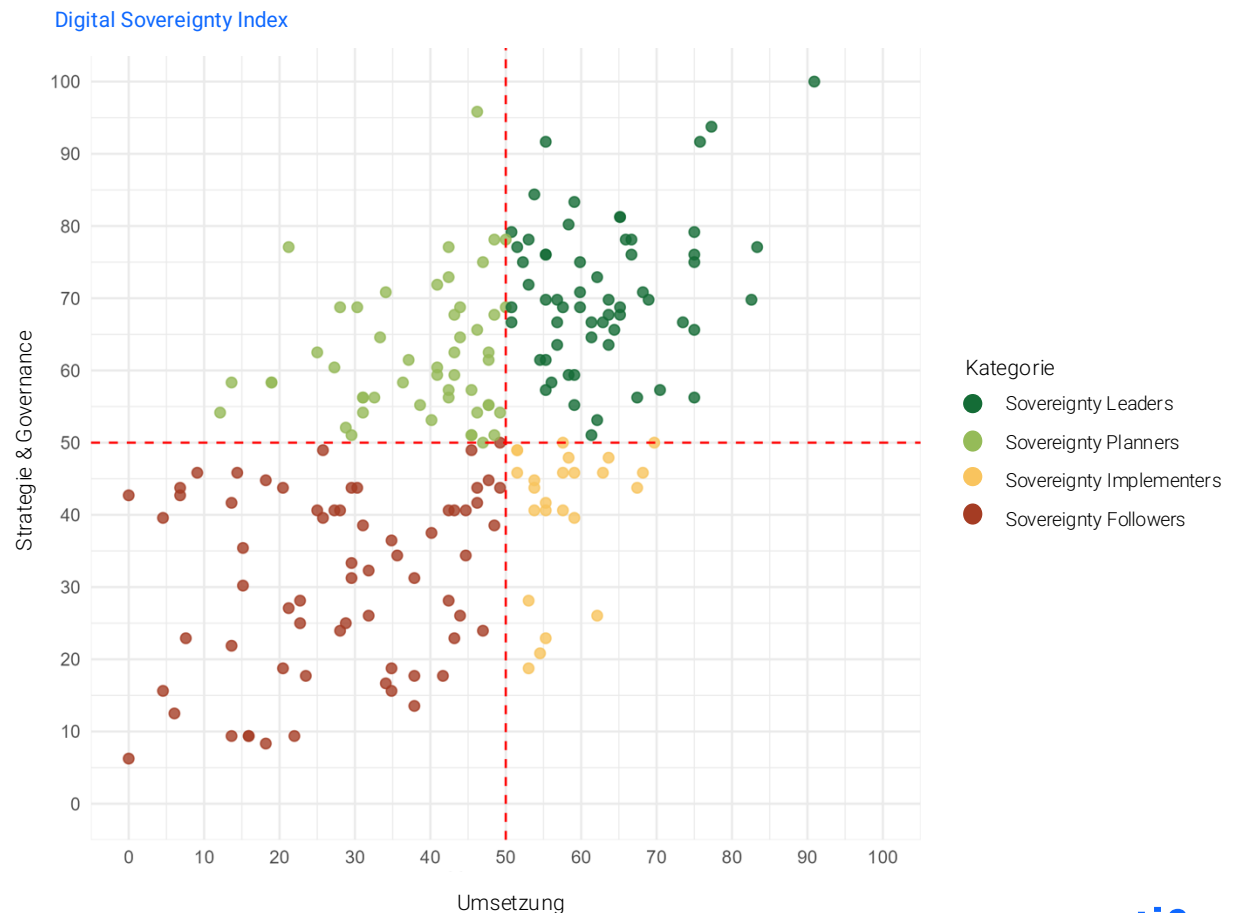
Digital Sovereignty Index Studie

Der Digital Sovereignty Index (DSI) gliedert Unternehmen nach Maturität in Strategie & Governance und in der Umsetzung

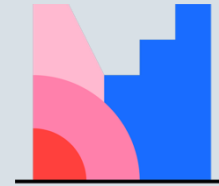
- 39 Single-Choice- und Multiple-Choice-Fragen
- Rund **230 Teilnehmer aus über 15 Branchen**, nach der Datenbereinigung wurden **200 Teilnehmer** für die Auswertung berücksichtigt.

Aufgrund der Resultate wurden folgende Archteypen identifiziert:

- **Sovereignty Leaders** (Strategie und Governance Framework vorhanden, digitale Souveränität durch verschiedene Massnahmen gestärkt)
- **Sovereignty Planners** (Strategy & Governance First)
- **Sovereignty Implementers** (Pragmatische Umsetzung von Digital Sovereignty Massnahmen, wenig strategische Planung / Struktur)
- **Sovereignty Followers** (Handlungsbedarf auf strategischer Ebene und Umsetzungsebene)



Digitale Souveränität Ziele, Risiken und Massnahmen

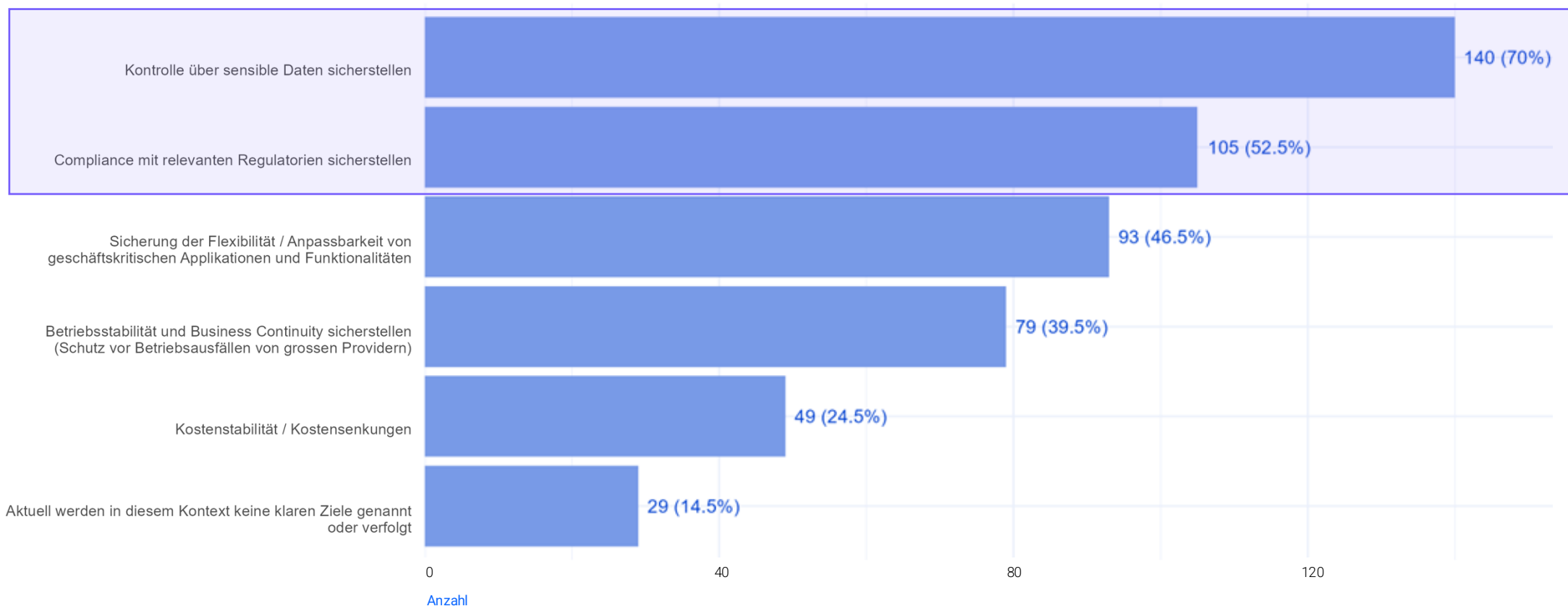


Mentimeter

QR-Code scannen

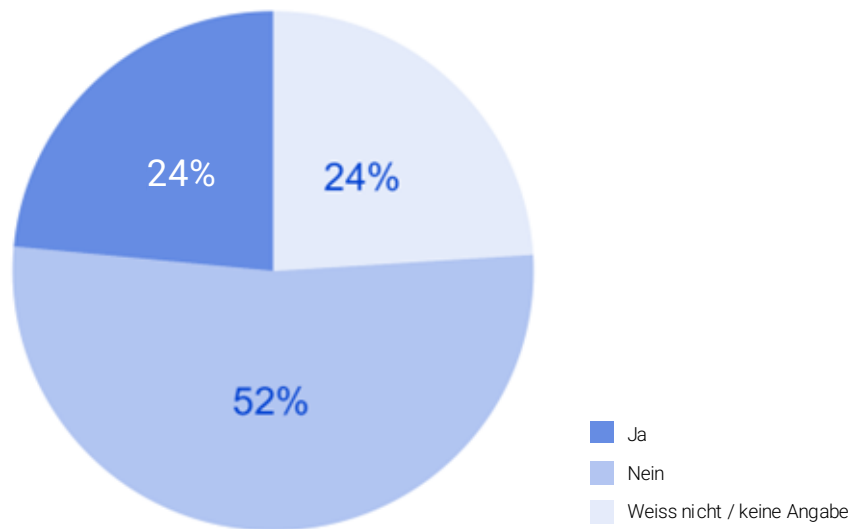


Kontrolle über sensible Daten ist mit Abstand das wichtigste Ziel

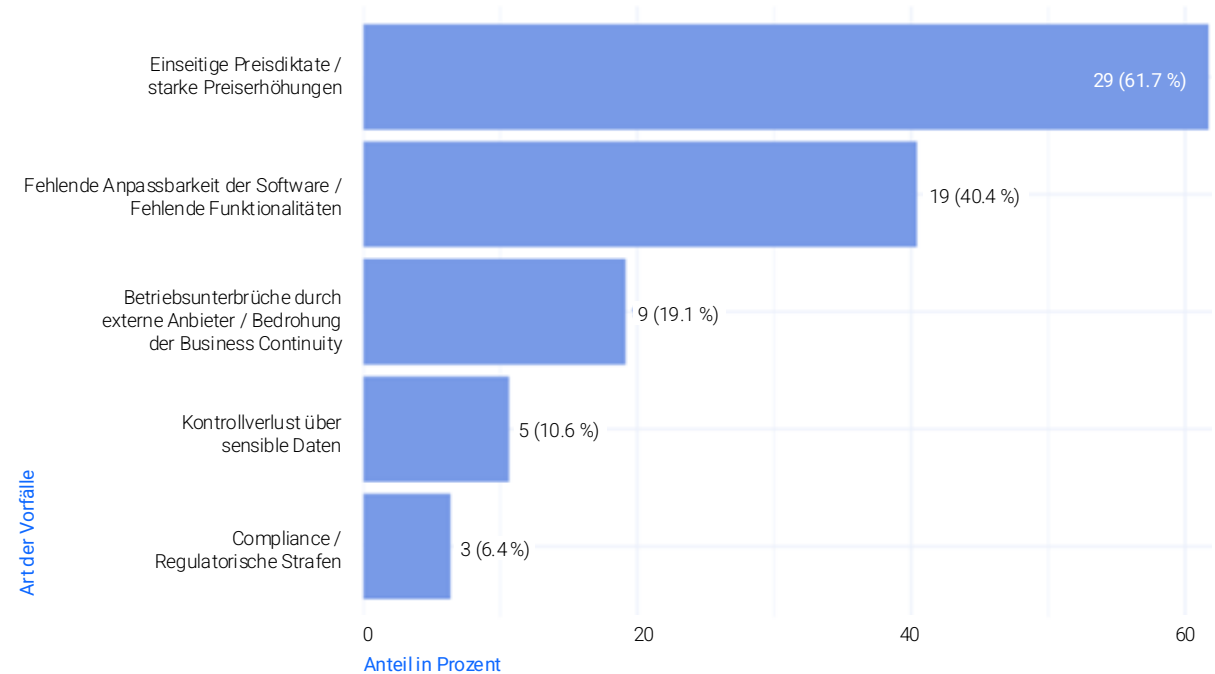


Das meistgenannte Risiko tritt selten ein – Preiserhöhungen dagegen häufig

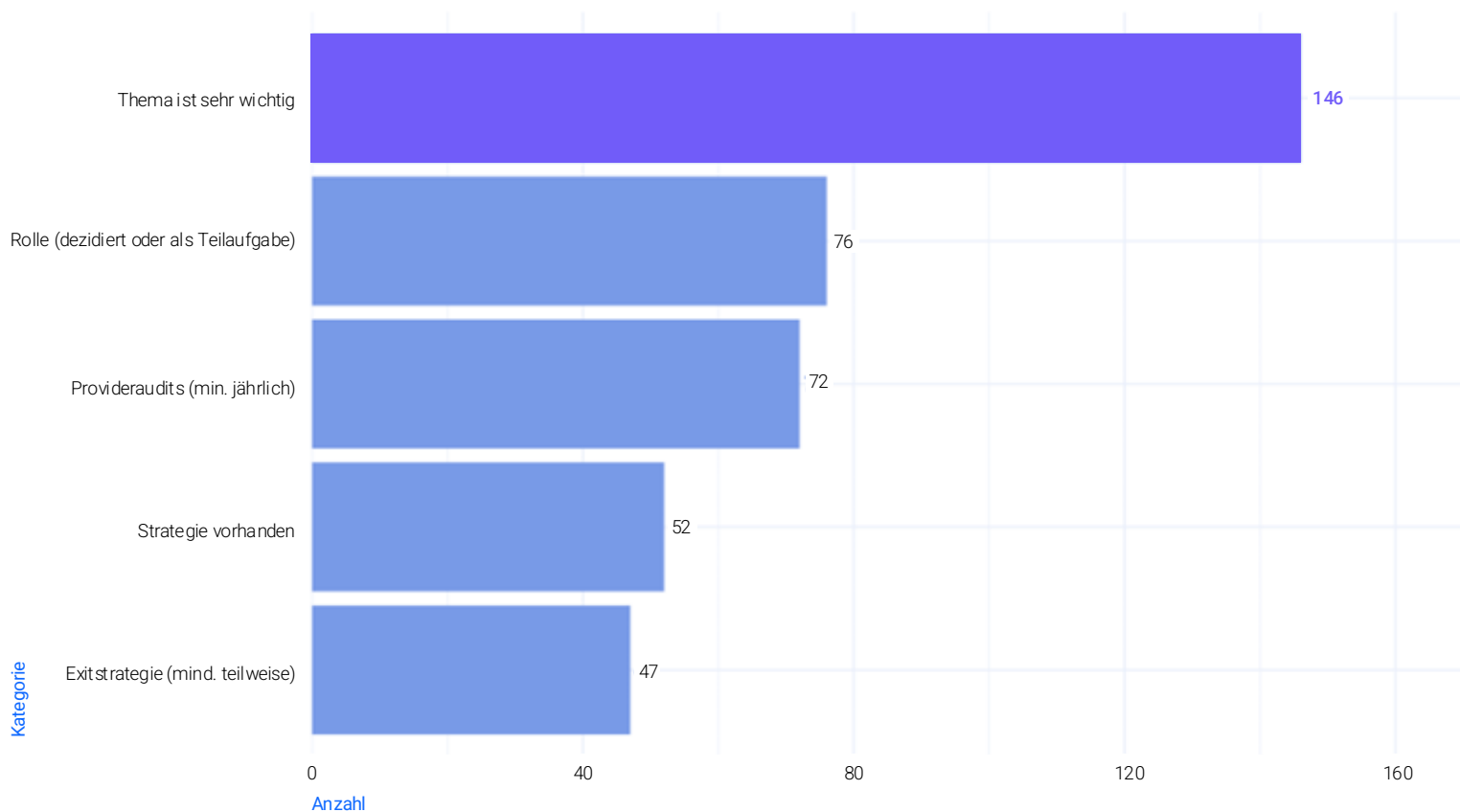
Kontrolle über sensible Daten ist das wichtigste Ziel und das grösste wahrgenommene Risiko – eingetreten ist es sehr selten. Einseitige Preisdiktate und starke Preiserhöhungen, die sich wegen hoher Abhängigkeit nicht abwenden lassen, kommen deutlich häufiger vor.



Unternehmen mit negativen Vorfällen aufgrund fehlender digitaler Souveränität / aufgrund starker Abhängigkeiten



Hohe Relevanz, geringe strategische Verankerung



73 %

halten digitale Souveränität für sehr oder eher wichtig (n=146)

35.6 %

davon haben eine Strategie für digitale Souveränität formuliert

32.2 %

davon haben (mindestens für gewisse kritische Services) Exit-Strategien formuliert

Wie können wir **gemeinsam** Ihre digitale Souveränität erhöhen?





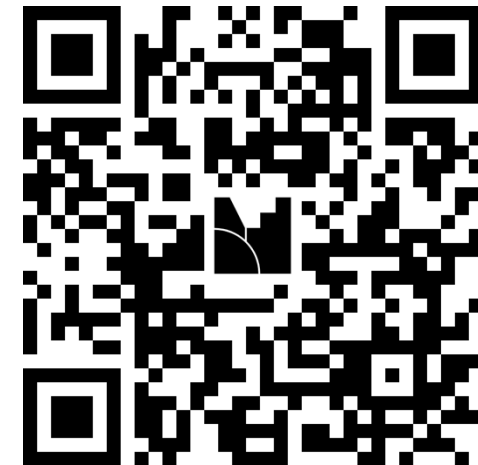
Digitale Souveränität im Kontext von BI-Lösungen

Digitale Souveränität BI-Lösungen



Mentimeter

QR-Code scannen



Platzhirsche schaffen starke Abhängigkeiten



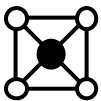
Cloud-only als Software-as-a-Service



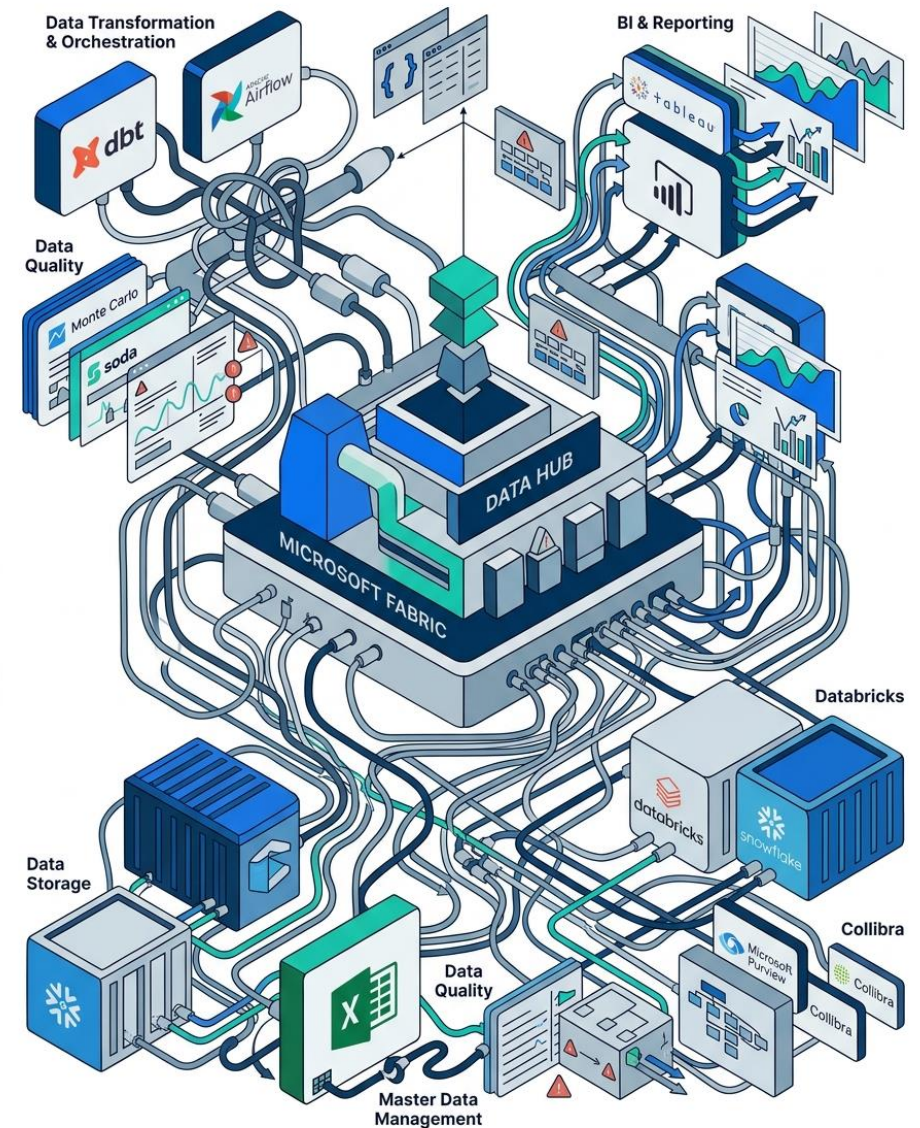
Amerikanische Marktdominanz



Proprietäre Technologieansätze



Weitreichende Ökosysteme mit enger Integration



Die Lösung

Nutzung von Open Source



Datenhoheit: freie Wahl des Hosting-Orts, kein Datenabfluss



Kein Lock-in: offene Standards & Schnittstellen, frei anpassbar



Transparenz: auditierbarer Code, nachvollziehbare Datenflüsse



Betriebsunabhängigkeit: durch Partner oder intern möglich

Datenvisualisierung



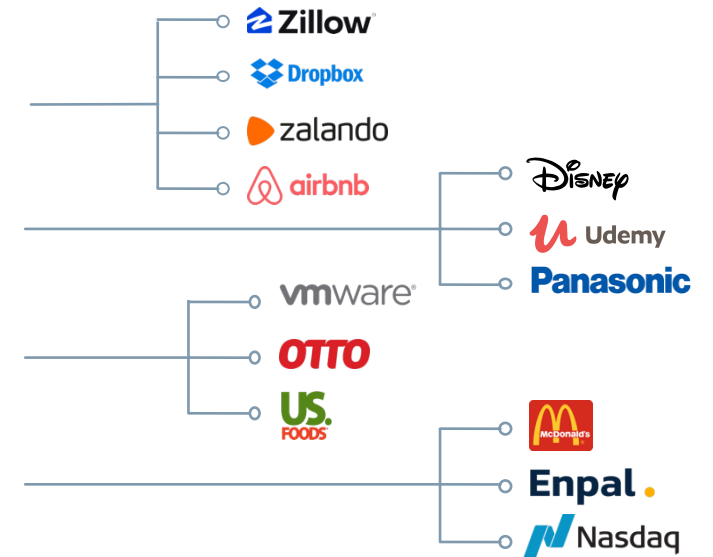
Datenqualität



Orchestrator



Datentransformation



Führende Organisationen setzen auf Open Source Technologien.

Query Engine



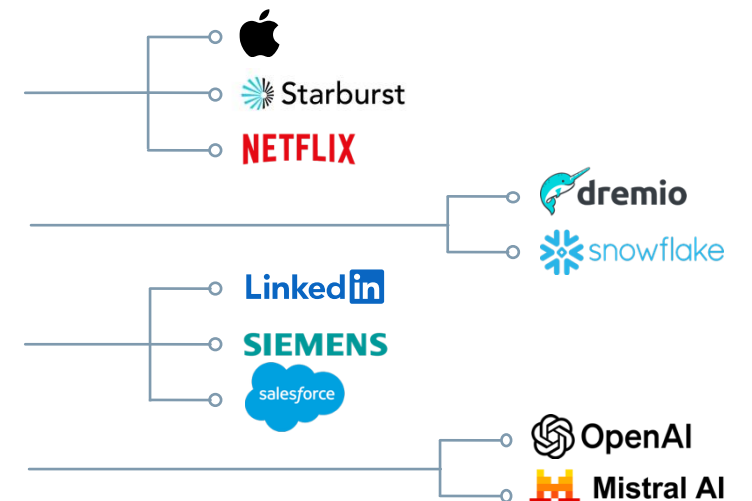
Metadatenkatalog



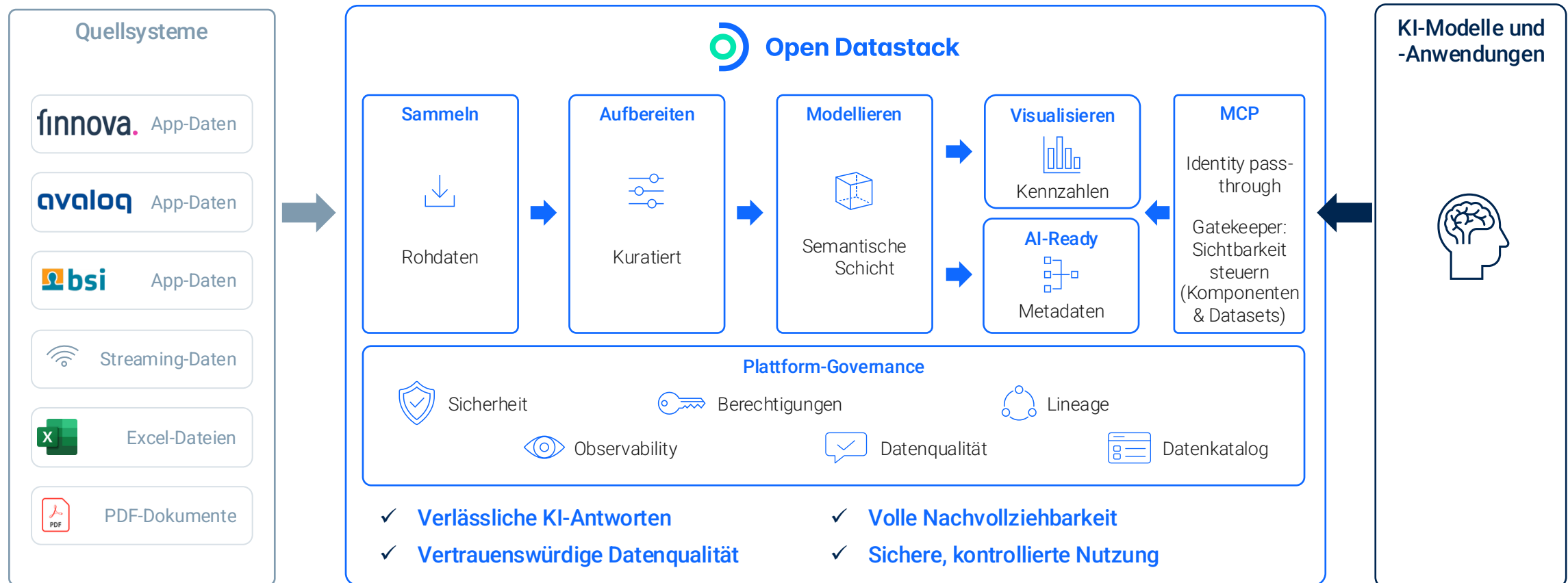
Tabellenformat



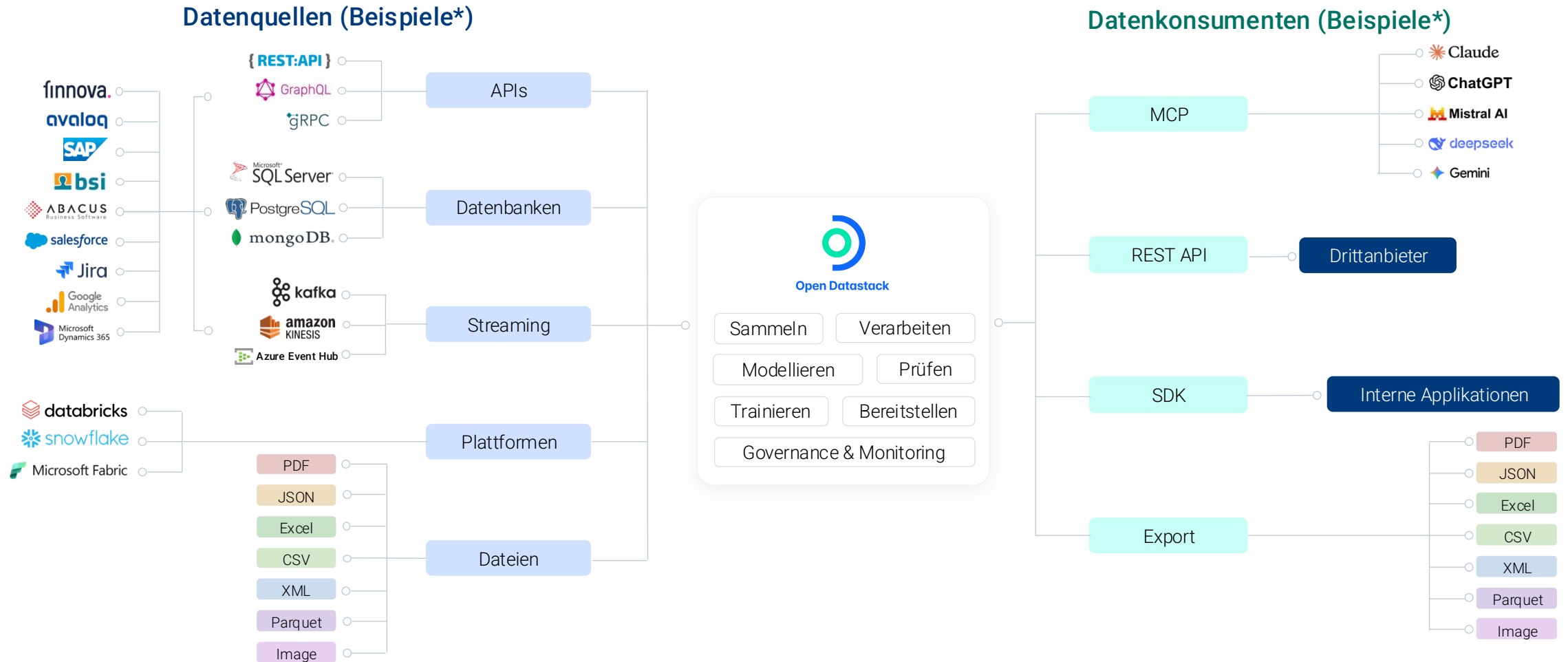
Authorisierung



Open Datastack integriert diese Open Source Technologien zu einer souveränen, AI-ready Daten- und Reportingplattform



Mit Open Datastack Silos aufbrechen und Erkenntnisse verfügbar machen, wo gearbeitet wird



Nutzen – Erkenntnisse in Workflows überführen, eine Plattform für die Kollaboration der relevanten Datenrollen

Überall verfügbar, immer informiert

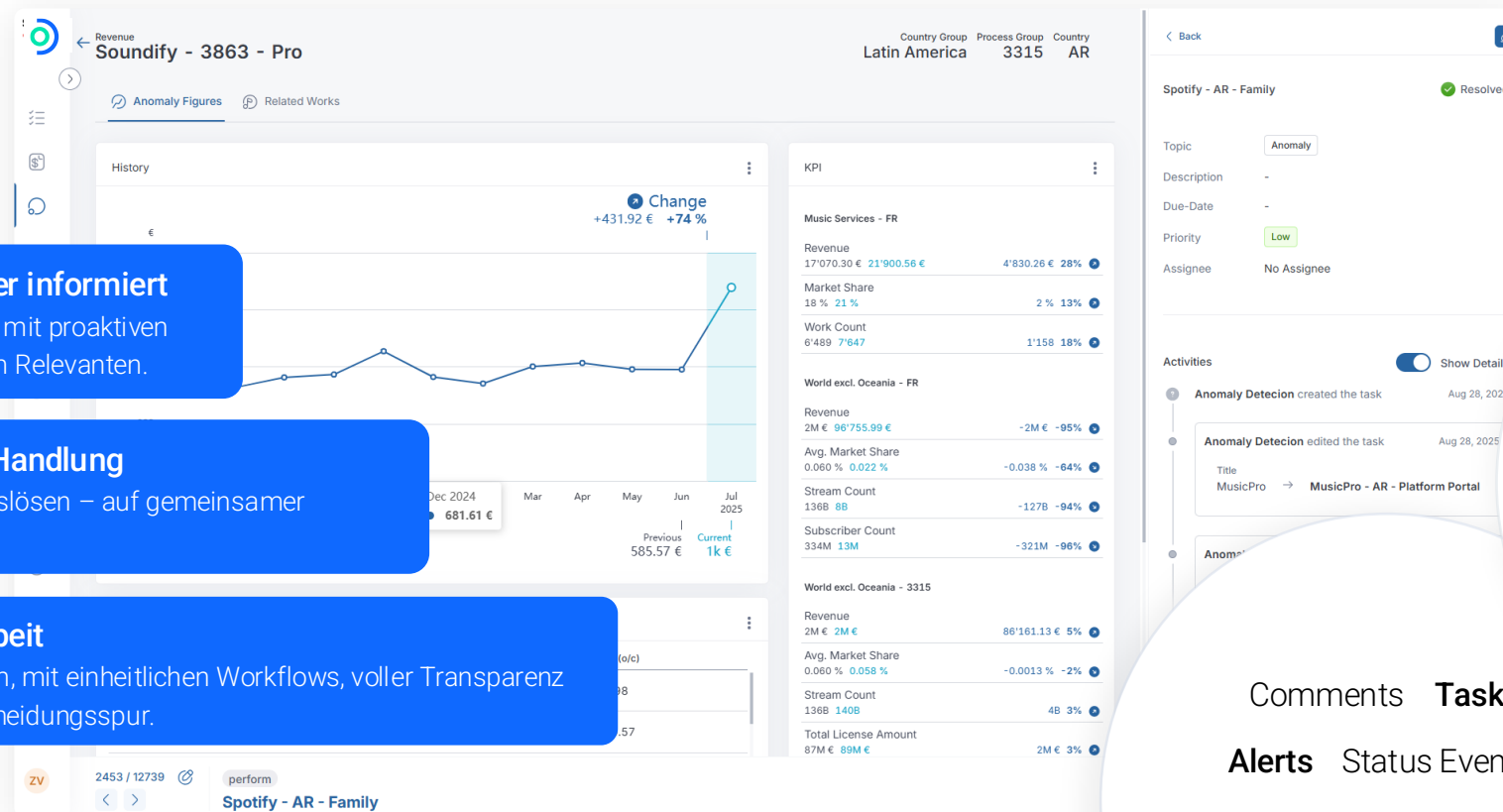
Responsive auf jedem Gerät, mit proaktiven Benachrichtigungen bei allem Relevanten.

Von den Rohdaten zur Handlung

Diskutieren und Prozesse auslösen – auf gemeinsamer Datengrundlage.

Nahtlose Zusammenarbeit

Alle Rollen auf einer Plattform, mit einheitlichen Workflows, voller Transparenz und nachvollziehbarer Entscheidungsspur.

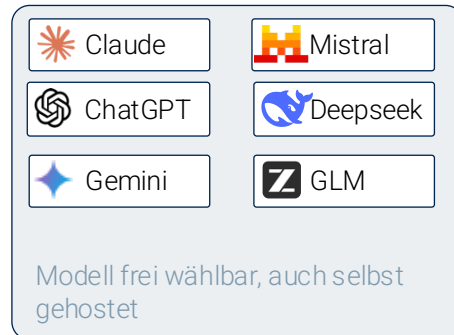


Comments Tasks
Alerts Status Events
Data Catalog Custom Charts
Theming

ODS Code Plus – Data Pipelines und Dashboards mit Best Practices von ti&m KI-gestützt entwickeln

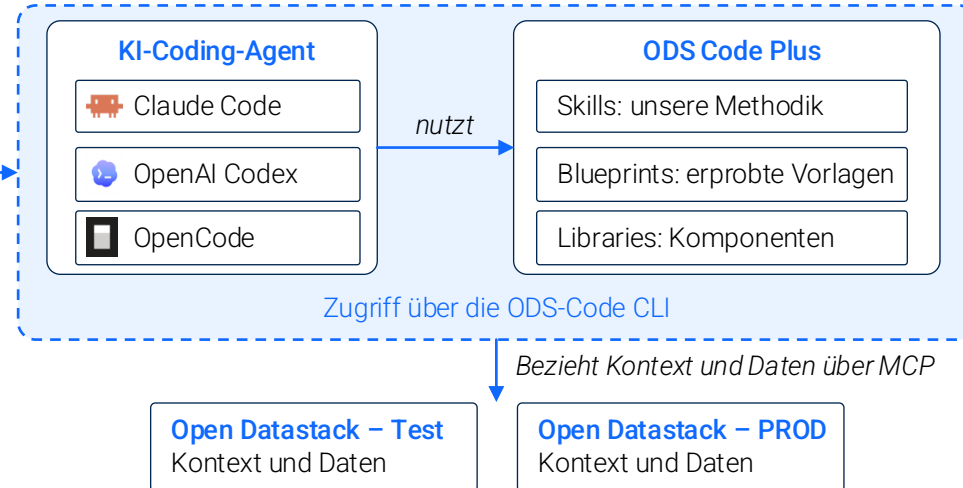
01 LLM Ihrer Wahl

Extern, privat oder lokal betrieben



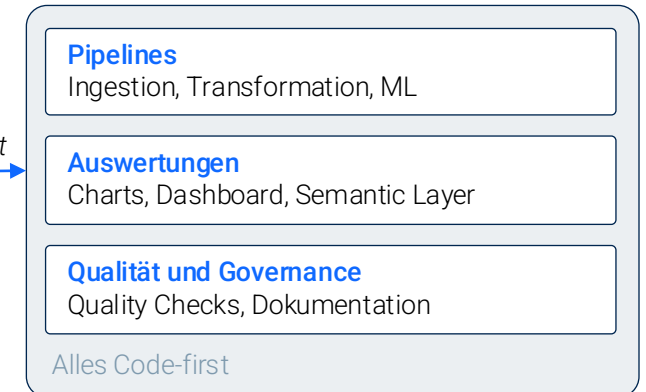
02 Lokal auf dem Entwickler-Laptop

Agent und ODS Code Plus laufen komplett lokal. Keine Daten verlassen das Gerät.



03 Zentrales Git-Repository

Versioniert, überprüfbar, einheitlich aufgebaut



 **Vereinfachte Wartung**
mit KI-gestützter Fehlerbehebung

 **Konsistentes Vorgehen**
Gleiche Methodik und Struktur im ganzen Team

 **Kontext und Transparenz**
Umfangreiche stets aktuelle Dokumentation

 **Weniger Ausfälle und Fehler**
mit eingebauter Qualitätssicherung



Effizienzgewinne von 30-70% von Quellen anbinden bis zur Visualisierung*

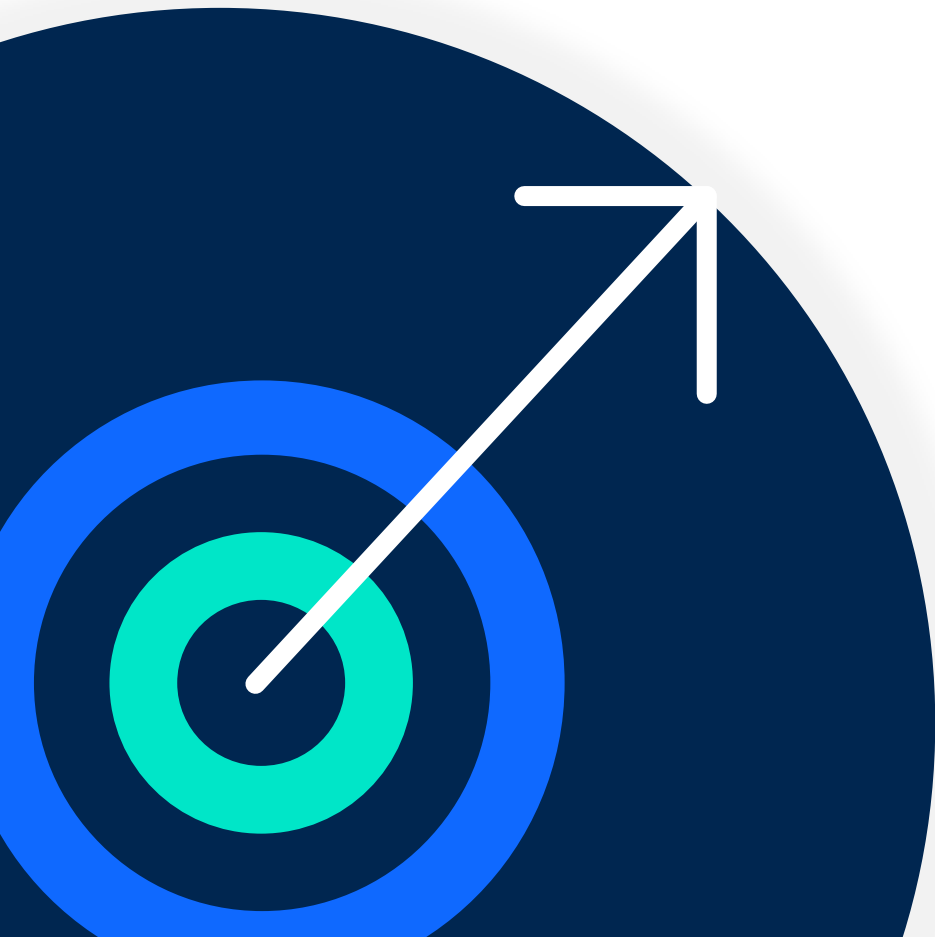
* Erfahrungswerte aus Kundenprojekten.

KI-gestützte Entwicklung mit Open Datastack in 90 Sekunden erklärt



Open Datastack

Vorteile im Überblick



- 01**  **Souverän betreibbar mit klaren Exit Optionen**
Aus der Schweiz. SaaS, eigener Cloud-Tenant und on-premises bis air-gapped. Open-Source-Kern und fachliche Logik bleiben beim Kunden
- 02**  **Planbar mit Kostensicherheit**
Eine Lizenz für Datenplattform und Reporting. Kein Kostenrisiko je Anbieter und je Abfrage
- 03**  **Alles in einer Plattform, ohne Medienbruch**
30 – 70 % schneller von Rohdaten zum Dashboard.* Aufbereitung, Governance und Reporting an einem Ort, mit Kommentaren und Qualitätsstatus im Dashboard.
- 04**  **KI nutzen und Kontrolle behalten**
Geregelte Datenbasis, self-hostbare MCP-Schnittstelle für LLMs und Agenten Ihrer Wahl, KI-Use Cases mit Human-in-the-Loop.

* Effizienzgewinne sind abhängig von der Komplexität des jeweiligen Use Cases. Je geringer die Komplexität, desto höher die Effizienzgewinne.

Souveräne KI als konsequente Ergänzung Dieselben Prinzipien wie bei der Datenplattform



Datenhoheit

Self-hosted Open-Weight-Modelle (Llama, Mistral, Qwen ...): Prompts und sensible Daten bleiben im eigenen Rechtsraum.



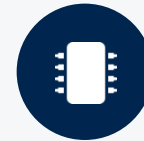
Modell-Lock-in

Frei fine-tun- und betreibbar – unabhängig von Roadmap, Preis und Deprecation des Anbieters.



Betriebskontrolle

Eigene Modell-Betrieb statt Rate Limits und ToS-Änderungen – zum Preis von MLOps-Kompetenz und GPU-Infrastruktur.



Grenze: Hardware & Capability

Souveränität endet an der GPU-Ebene (NVIDIA, Exportkontrollen); Frontier-Leistung ist noch überwiegend closed.

Dualer AI-Ansatz

Geschwindigkeit nutzen. Souveränität sichern



AI-Harness

Eine gemeinsame Steuerungs- und Kontrollschicht verbindet beide Welten



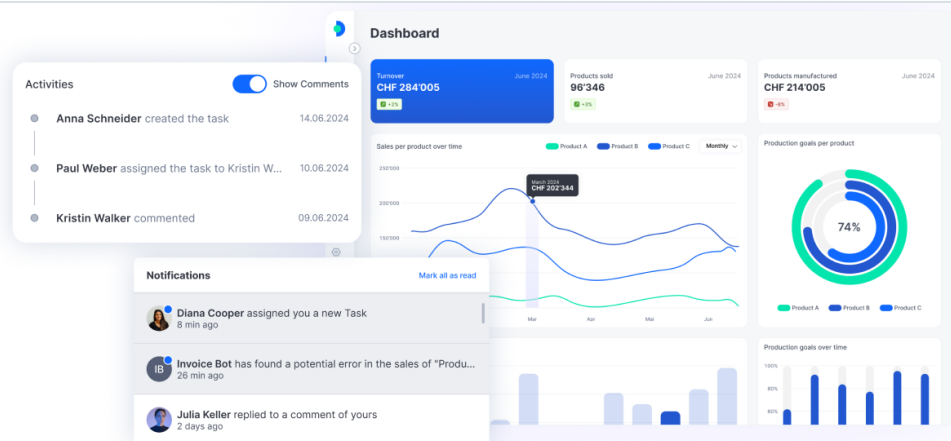
Souverän, wo notwendig Self-hosted. Open Weight.

- Sensible Daten und Standardaufgaben
- RAG, Klassifikation, Extraktion, interne Assistenten
- Volle Daten-, Technologie- & Betriebskontrolle



Spitzenleistung, wo sinnvoll Abgesicherte API. Frontier.

- Hochkomplexe Aufgaben bei Bedarf
- Zugriff auf die stärksten Frontier-Modelle
- Über gesicherte, vertraglich geregelte Schnittstellen



[Open Datastack](#)

Die Datenplattform, die Souveränität und intuitive BI vereint

ti&m



Jetzt entdecken und Demo
vereinbaren
ti8m.com/datastack

Digitale Souveränität: Wie abhängig sind Schweizer Unternehmen?

6. Okt. 2026, Hochschule Luzern

HSLU

ti&m



Jetzt anmelden
tinyurl.com/4jzvvhfk

Wir digitalisieren Ihr Unternehmen.

Gemeinsam in eine digital souveräne Zukunft!

Nico Kaiser
Lead Consultant, Digital Sovereignty Lead
Nico.kaiser@ti8m.ch
+41 44 497 73 70

David Furrer
Product Owner Open Datastack
David.furrer@ti8m.ch
+41 44 497 76 98

ti&m AG
Flüelastrasse 30
8047 Zürich
SCHWEIZ
+41 44 497 75 00

ti&m AG
Helvetiastrasse 17
3005 Bern
SCHWEIZ
+41 31 960 15 55

ti&m AG
Elisabethenanlage 9
4051 Basel
SCHWEIZ
+41 61 501 29 99

ti&m GmbH
Schaumainkai 91
60596 Frankfurt am Main
DEUTSCHLAND
+49 69 24745268-0

ti&m GmbH
Kesselstraße 3
40221 Düsseldorf
DEUTSCHLAND
+49 211 90989580

ti&m Pte. Ltd.
18 Robinson Road #15-01
Singapore 048547
SINGAPORE
+65 6983 9530

ti8m.com

ti&m