Generative KI: Wachstum, Herausforderungen & Lösungen

- Herausforderungen
  - Innovationshemmnisse
    - Prozessbeschränkungen
    - Fehlender Fokus
    - Überarbeitungsschleifen
    - 50% Zeit für Compliance
    - Ineffizientes Arbeiten
    - Wiederholungen & Einzellösungen
  - Scheitern bei der Skalierung
    - Sicherheits- & Risikobedenken
    - Kostenüberschreitungen
    - Entgleisen ganzer Programme
  - Sicherheitsherausforderungen bei KI-Agenten
    - Neue Risiken durch Aktionen
  - Unrealistische Erwartungen an KI-Agenten
    - 99% Genauigkeit nicht ausreichend
    - Open-World-Probleme zu komplex
    - Hype führt zu Lähmung
  - Fragmentierte IT-Landschaften
  - Rechtliche Unsicherheiten
  - Zögerliche Cloud-Nutzung
- Lösungen & Empfehlungen
  - Zentralisierte Plattform
    - Self-Service-Portal
      - Sicherer & schneller Zugang zu Tools
      - Fördert Effizienz
      - Dokumentation & Schulungen
    - Offene Architektur
      - Wiederverwendbare Dienste & Module
      - Reduziert Kosten, maximiert Effizienz
      - Flexible & anpassbare Architektur
      - Integration verschiedener Anbieter
    - Automatisierte Schutzmaßnahmen
      - Governance-Mechanismen
      - Sicherstellung der Compliance
      - Minimierung von Risiken
      - Kostenüberwachung
      - Zentrale KI-Gateway-Lösung
      - Automatisierung von Audits
  - Qualitätsbewertung von Trainingsdaten
  - Fokus auf Closed-World-Probleme
  - Architektur-Ansatz für Agenten
  - Determinismus in Agenten
  - Vorteile Multi-Agenten-Systeme
- Beispiele & Trends
  - Dust (KI-Plattform)
    - Jahresumsatz 6 Mio. $, versechsfacht
    - Automatisierung kompletter Arbeitsabläufe
    - Erstellen von GitHub-Issues
    - Planen von Meetings
    - Aktualisieren von CRM-Daten
    - Überprüfen von Code
    - Basierend auf Claude-Ökosystem & MCP
    - Entwicklung spezialisierter Unternehmensanwendungen
    - Kunden zahlen 40-50 $/Nutzer/Monat
    - Nativ Berechtigungsschicht & Zero-Data-Retention
    - Beispiel für 'KI-native Startups'
  - Agentic AI
    - Paradigmenwechsel in Automatisierung (Genpact)
    - Geht über RPA hinaus
    - Dynamisch, eigenständige Entscheidungen, lernt kontinuierlich
    - End-to-End-Automatisierung in Echtzeit
    - Datenintensive, fehleranfällige Prozesse
    - Beispiele: Accounts Payable, Record to Report, Order to Cash
    - Voraussetzung: Konsolidierte, hochwertige Datenbasis
    - AWS setzt verstärkt auf Agentic AI
    - BMW, Zalando nutzen für Code-Entwicklung, Artikelverwaltung
    - Model Context Protocol (MCP), Strands-Framework
  - TNG Technology Consulting GmbH
    - DeepSeek-TNG R1T2 Chimera (KI-Modell)
    - Open-Source-Technologie (DeepSeek)
    - Kombiniert drei Modelle (AoE-Methode)
    - 200% schneller, 60% weniger Tokens
    - Geringere Infrastrukturkosten
    - Hohe Intelligenz, reduzierte Antwortlänge
    - MIT-Lizenz, modifizierbar
    - Modularität für Anpassungen
    - Optimiert für allgemeine Aufgaben
    - Verfügbar auf Hugging Face
  - Pendo - Agent Analytics
    - Messung der Leistung von KI-Agenten
    - Erfassung von Nutzerverhalten, Konversationen, Prompt-Trends
    - Erkennt nicht-konformes Verhalten
    - Unterstützt eigene & externe Agenten, klassische Software
    - Zuordnung von Aufgabenabschlüssen zu Agentennutzung (ROI)
    - Kontroll- & Monitoringfunktionen auf Enterprise-Level
    - Anwendungen: Prozessautomatisierung, industrielles Monitoring
  - KI-Modellpass (Gesundheitswesen)
    - AI MODEL PASSPORT Framework
    - Digitale Identität & Verifizierungstool für KI-Modelle
    - Erfasst Metadaten über gesamten Lebenszyklus
    - Eindeutige Identifizierung, Verifizierung, Verfolgung, Überwachung
    - AIPassport (MLOps-Tool)
    - Automatisiert Metadatenerfassung
    - Gewährleistet Versionierung
    - Schließt Lücke zw. Dokutools & MLOps-Lösungen
    - Einhaltung EU-Regulierungen (EHDS, Digitaler Produktpass)
  - Hexagon - Humanoider Roboter Aeon
    - Für industrielle Anwendungen
    - Sensorik, KI-Technologie, Fortbewegung, räumliche Intelligenz
    - Präzise Manipulation, Inspektion, Realitätserfassung
    - Schnelle Bewegung, hochpräzise Arbeit
    - Einsatz in Automobil, Luft- und Raumfahrt, Fertigung, Logistik
    - Aufgaben: Objekte entnehmen, Scannen, digitale Zwillinge
    - Innovativer Batteriewechselmechanismus
    - Testphase mit SchaeSler & Pilatus
    - Partner: Nvidia, Microsoft (Azure), Maxon
- BSI und KI-Sicherheit
  - KI und IT-Sicherheit
    - IT-Sicherheit für KI (Schutz von KI-Systemen)
    - IT-Sicherheit durch KI (Einsatz von KI)
    - Angriffe durch KI (Verstärkung von Cyberangriffen)
  - Forschung und Kooperation
    - Zusammenarbeit mit Standardisierungsgremien
    - Workshops (Prüfbarkeit von KI)
    - Studien zu XAI, formalen Methoden, Sicherheit von KI
  - Kompetenzzentrum Künstliche Intelligenz
    - Entwicklung von Sicherheitsstandards
    - AI Cloud Service Compliance Criteria Catalogue
    - Fokus: Robustheit, Fairness, Transparenz, Datenqualität
  - KI in sicherheitskritischen Bereichen
    - Autonomes Fahren, biometrische Identifikation
    - Spezifische Anforderungen (z.B. Verkehrsschilderkennung)
  - Generative KI
    - Chancen und Risiken (LLMs)
    - Risikoanalyse und Sicherheitsleitfäden
  - Praktische Leitfäden
    - Publikationen für Entwickler (AI Security Concerns)
    - Empfehlungen für sichere Entwicklung & Einsatz
  - Spezifische Studien und Projekte
    - Einsatz von KI in Kryptografie, Codeanalyse
    - Sicherheit in Szenarien (Adversarial Learning)
  - Erklärbarkeit und Transparenz
    - Forschung zu erklärbarer KI
    - Förderung von Transparenzanforderungen (EU-KI-VO)