

Nutzen Sie das Potenzial **agentischer KI**

Ein Guide für Führungskräfte zur nächsten
Stufe der KI-Entwicklung

Inhaltsverzeichnis

Einleitung

Die Möglichkeiten
durch agentische KI

3

Kapitel 2

Offener
Plattformansatz
für erfolgreiche
agentische KI

8

Weitere Informationen

Die autonome
Zukunft der
Unternehmensauto-
matisierung

14

Kapitel 1

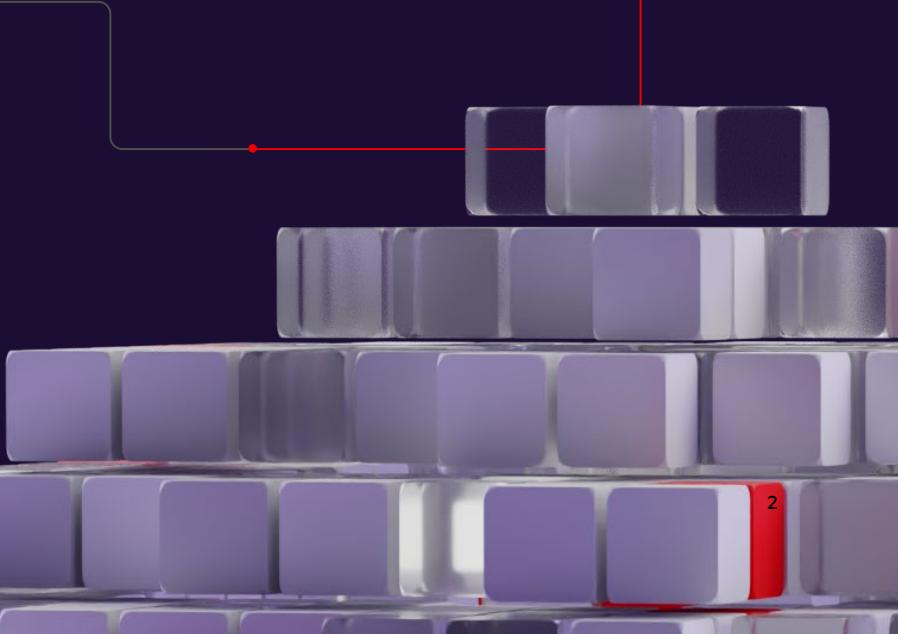
Die
Herausforderungen
agentischer KI für
Unternehmen

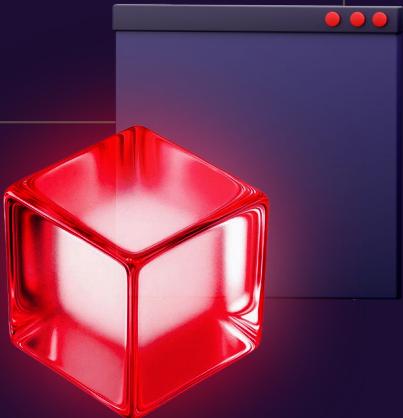
5

Kapitel 3

Planung Ihrer
Strategie für
agentische KI mit
Red Hat AI

11





Die Möglichkeiten durch agentische KI

Führungskräfte stehen aktuell vor einem entscheidenden Moment in der technologischen Entwicklung. KI hat bereits die Art und Weise neu definiert, wie wir mit Daten interagieren, Aufgaben automatisieren und Kundenservices anbieten. Die nächste Phase der KI hat bereits begonnen und sie geht über das Generieren von Inhalten und prädiktive Analysen hinaus.

Agentische KI ist eine Weiterentwicklung generativer Modelle zu autonomen Systemen mit größerer Anpassungsfähigkeit und der Fähigkeit für kontinuierliches Lernen. Sie kann eine physische Struktur, ein Softwareprogramm oder eine Kombination aus beidem sein. So können Agenten innerhalb vordefinierter Parameter in nahezu jedem Teil des Unternehmens wahrnehmen, entscheiden und handeln. Anstatt auf Eingabeaufforderungen zu reagieren, kann agentische KI Aufgaben mit mehreren Schritten

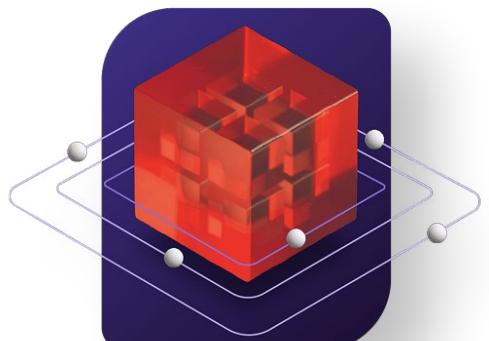
initiiieren, auf Tools und APIs zugreifen und sich im Laufe der Zeit verbessern. Dies kann beispielsweise die Bearbeitung von Kundenserviceanfragen über mehrere Plattformen hinweg, die Automatisierung von IT-Korrekturmaßnahmen oder die Verwaltung von Lieferkettenvorgängen in Echtzeit sein.

Führungskräfte müssen diesen Wandel verstehen, um auch in Zukunft wettbewerbsfähig zu bleiben.

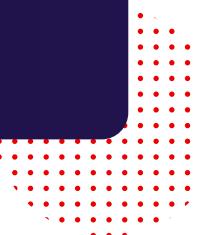
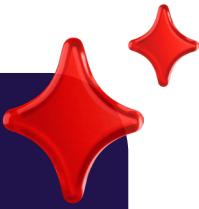
Funktionsweise agentischer KI

Agentische KI ist besonders nützlich für Aufgaben, die eine kontinuierliche Überwachung oder schnelle Entscheidungen erfordern. Sie können sich agentische KI als eine Möglichkeit vorstellen, Automatisierung mit Schlussfolgerungen, Entscheidungsfindung und den kreativen Fähigkeiten eines Large Language Models (LLM) zu kombinieren. Um agentische KI in die täglichen Abläufe einzuführen, müssen Unternehmen zunächst ein System erstellen, um einem LLM Zugriff auf externe Tools und Algorithmen zu geben, die Anweisungen für KI-Agenten liefern, die anderen Softwaretools aufsetzen und diese steuern.

KI-Agenten können dann je nach Framework mit Tools kommunizieren, die die Orchestrierung von Workflows umfassen. Dieser Ansatz ermöglicht es dem LLM, den besten Weg zur Beantwortung einer Frage zu prüfen und zu ermitteln.



Bis 2029 wird agentische KI 80 % der gängigen Probleme im Kundenservice ohne menschliches Eingreifen lösen, was zu einer Senkung der Betriebskosten um 30 % führt.¹



Zu den Vorteilen agentischer KI gehören:



Gesteigerte operative Effizienz durch autonome Workflows, die den Bedarf an manuellen Eingriffen reduzieren



Reduzierte Kosten durch minimierte menschliche Eingriffe und verbesserte Produktivität



Schnellere Entscheidungsfindung und Ausführung in verschiedenen Geschäftsbereichen sowie Echtzeitdaten und kontextbezogene Insights



Wettbewerbsdifferenzierung, da Unternehmen KI-Agenten orchestrieren und steuern können, um den Return on Investment (ROI) zu steigern

In einem Zeitalter, das von ständigen Disruptionen geprägt ist, können Unternehmen mit agentischer KI vorausschauend handeln, sich anpassen und eine Führungsrolle übernehmen.

Herausforderungen bei der Einführung

Von der Orchestrierung komplexer Agent-Workflows über die Aufrechterhaltung von Vertrauen und Zuverlässigkeit bis hin zur effizienten Skalierung dieser Innovationen im gesamten Unternehmen – die Integration agentischer KI in Ihr Unternehmen ist mit Herausforderungen verbunden. Da sich Geschäftsumgebungen jedoch immer schneller weiterentwickeln, ist die Einführung agentischer KI für Unternehmen, die ihren Wettbewerbsvorteil erhalten wollen, nicht mehr optional.

In diesem E-Book werden diese Herausforderungen und Möglichkeiten zu ihrer Bewältigung, die geschäftlichen Vorteile agentischer KI sowie umsetzbare Strategien zur Neugestaltung von Effizienz und Innovation in Ihrem Unternehmen mithilfe agentischer KI untersucht.



Die Herausforderung agentischer KI für Unternehmen

Unternehmen verfügen zunehmend über das nötige Wissen und nutzen KI zusehends häufiger. Gleichzeitig hat sich ein gewisses Maß an Reife eingestellt, sodass immer mehr Unternehmen den langfristigen geschäftlichen Nutzen dieser Technologie erkennen.

Tatsächlich sollen KI-gestützte Workflows – viele davon basierend auf agentischer KI – von 3 % im Jahr 2024 auf 25 % im Jahr 2026 ansteigen, da die Investitionen in KI weiter zunehmen.²

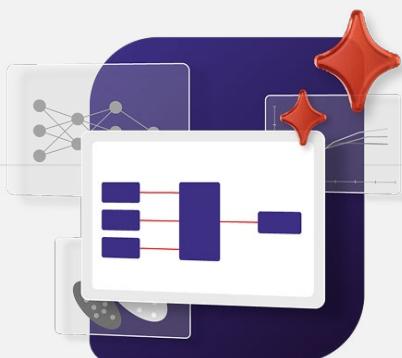
Doch Wandel war noch nie einfach. Es gibt echte Herausforderungen, die Unternehmen bewältigen müssen, bevor sie intelligente Agenten in großem Umfang und zuverlässig bereitstellen können.

Wenn Führungskräfte diese Herausforderungen frühzeitig erkennen, können sie die richtigen Fragen stellen, Pilotprogramme effektiv entwickeln und die Technologien auswählen, die ihnen zum Erfolg verhelfen.

Herausforderung 1: Orchestrierung komplexer Agenten-Workflows

Ein Hauptunterscheidungsmerkmal agentischer KI-Systeme im Vergleich zu anderen KI-Formen wie etwa gen KI besteht darin, dass sie nicht als Einzellösung gedacht sind.

KI-Systeme können Tools, APIs, Kommunikationsprotokolle, Datenquellen, Modelle für Machine Learning (ML), LLMs und KI-Agenten verstehen. Der KI-Agent ist die endgültige Entscheidung, aber dafür müssen die anderen Komponenten orchestriert werden.



² „From AI projects to profits: How agentic AI can sustain financial returns“. IBM, 9. Juni 2025.

Dieses Maß an Koordination führt zu neuen Komplexitätsebenen, unter anderem zu folgenden Notwendigkeiten:



Systemübergreifendes Management

Agentische KI muss Abhängigkeiten in verschiedenen Systemen managen, die unterschiedliche Protokolle, Sicherheitsmodelle und Performance-Parameter aufweisen können.



Agentenübergreifende Koordination

Die Zusammenarbeit mit mehreren Agenten muss sorgfältig synchronisiert werden, um redundante oder widersprüchliche Aktionen zu vermeiden.



Bereitstellung der richtigen Tools für Teams

Entwicklungs- und IT-Teams benötigen neue Tools, um diese Workflows schnell zu entwerfen, zu testen und zu iterieren, damit sie nicht immer von Grund auf neu entwickeln müssen.

Ohne ein einheitliches Framework und eine Strategie zur Integration agentischer KI in bestehende Workflows besteht die Gefahr, dass sie zu einer weiteren Technologie in einem scheinbar ständig wachsenden digitalen Toolkit wird.

Herausforderung 2: Aufrechterhaltung von Vertrauen und zuverlässigem Agentenverhalten

Bevor ein Unternehmen autonome Aktionen sicher zulassen kann, muss Vertrauen vorhanden sein. Im Gegensatz zu anderen Technologien, die mit minimaler menschlicher Interaktion arbeiten, wie etwa Automatisierung, bei der Ergebnisse vorhersehbar und vordefiniert sind, basieren KI-Agenten auf einer dynamischen Argumentation und Entscheidungsfindung. Der Hauptunterschied besteht darin, dass Agenten autonom Entscheidungen treffen können und so menschliches Verhalten nachahmen, was berechtigte Bedenken hinsichtlich Zuverlässigkeit, Transparenz und Compliance aufwirft.

Wichtige Überlegungen:



Wie lässt sich das Verhalten von Agenten in Echtzeit überwachen und kontrollieren?



Lässt sich sicherstellen, dass die Agenten weiterhin die Unternehmensrichtlinien und gesetzlichen Anforderungen einhalten?



Welche Maßnahmen hinsichtlich Verantwortlichkeit werden ergriffen, um die Entscheidungen eines Agenten zu regeln und zu erklären?

Beobachtbarkeit, Aufsicht und angemessene Sicherheitsvorkehrungen sind technische Voraussetzungen für die Akzeptanz sämtlicher Stakeholder.

Herausforderung 3: Effiziente Skalierung von Anwendungen agentischer KI

Selbst das effektivste Pilotprojekt kann in großem Umfang versagen. Implementierungen agentischer KI, insbesondere derjenigen, die auf LLMs basieren, erfordern erhebliche Rechenressourcen. Bedenken Sie den enormen Druck auf die IT-Infrastruktur, wenn Dutzende oder sogar Hunderte von Agenten gleichzeitig ausgeführt werden. Die einzelnen Agenten könnten gleichzeitig Modelle abfragen, auf Daten zugreifen und Tools aufrufen.

Für eine nachhaltige Skalierung agentischer KI müssen Unternehmen Folgendes sicherstellen:



Die Infrastruktur lässt sich effektiv vertikal und horizontal skalieren und das Unternehmen verfügt über Methoden zur Kostenkontrolle.



Es verfügt über die Flexibilität, Deployments in Hybrid- und Multi Cloud-Umgebungen, näher an Datenquellen oder Anwendungen, durchzuführen.



Governance, Sicherheit und Performance sind konsistent.

Mit einem Plattformansatz können Sie diese Herausforderungen bewältigen und ein Gleichgewicht zwischen Innovation und operativen Best Practices schaffen.





Offener Plattformansatz für erfolgreiche agentische KI

Die optimale Nutzung agentischer Workflows hängt von einer zuverlässigen Infrastruktur, operativer Transparenz, sicherheitsorientierten Deployments und Flexibilität in verschiedenen Umgebungen ab. Hier kann ein Plattformansatz weiterhelfen.

Red Hat® AI baut auf der jahrzehntelangen Führungsrolle im Bereich Open Source für Unternehmen auf und ist darauf ausgelegt, intelligente agentische Workflows zu unterstützen, die vom Experiment bis zur Orchestrierung im Produktionsmaßstab reichen. So können Unternehmen ein agentisches KI-System, einschließlich KI-Agenten, entwickeln, bereitstellen und warten.



Red Hat Enterprise Linux® AI
für individuelle Linux-
Serverumgebungen



Red Hat OpenShift® AI
für verteilte Kubernetes-
Plattformumgebungen



Red Hat AI Inference Server
für optimierte Inferenz von LLMs

Die Lösungen kombinieren die Leistungsfähigkeit von Open Source-Technologien mit führenden Open Source-Modellen und unterstützen Unternehmen dabei, die Entwicklung zu beschleunigen sowie den Zugriff auf neue Tools und Technologien zu demokratisieren.

Vereinfachte Zusammenstellung von Agenten-Workflows



Ein einheitliches API-Erlebnis

Durch standardisierte Interaktion von LLMs, offenen Agenten-Frameworks und [RAG-Pipelines \(Retrieval-Augmented Generations\)](#) erreichen Unternehmen die Interoperabilität zwischen verschiedenen Modellanbietern und Frameworks.

Der Erfolg agentischer KI basiert auf dem koordinierten Zusammenspiel von Planungsalgorithmen, Speicher, Tool-Orchestrierung und Lern-Feedbackschleifen. Red Hat vereinfacht den Aufbau dieser Stacks durch:



Dedizierte KI-Erlebnisse

Durch verbesserte Benutzererlebnisse können Engineers eine einzige Umgebung nutzen, um KI-Assets, -Agents und -Anwendungen zu verwalten sowie Prototypen zu erstellen.



Support durch IT-Ökosystem

Die native Kompatibilität mit führenden LLM-Frameworks wie LlamaStack und OpenAI-kompatiblen APIs ermöglicht Entwicklungsteams die Wahl der geeigneten Modellarchitektur, einschließlich offener und optimierter Optionen mit komplexem Integrationsaufwand.

Anpassbare und kontrollierte Agenten-Bereitstellung



Kontextbezogene Ausführung

Mithilfe des Model Context Protocol (MCP) können Agenten auf semantisch relevante Betriebsdaten zugreifen und absichtsorientierte Einschränkungen durchsetzen, wodurch sich die Nachvollziehbarkeit und Kontrolle über die Entscheidungsfindung verbessern lassen.

Mit der zunehmenden Autonomie von KI-Agenten sind umfassende Governance, Beobachtbarkeit und Erklärbarkeit von entscheidender Bedeutung.

Red Hat AI begegnet diesen Herausforderungen mit Funktionen, die zu einem verantwortungsvollen Deployment beitragen:



Integrierte Beobachtbarkeit und Durchsetzung von Richtlinien

Mit Monitoring-Tools und Role-based Access Control von Red Hat können Teams Verhaltengrenzen durchsetzen und Entscheidungen bis zu den Quellmodellen und -daten zurückverfolgen.



Interoperabilität mit bestehenden Unternehmens- und Compliance-Richtlinien

Interoperabilität stellt sicher, dass die Agentenaktivität in regulierten Umgebungen mit dem Sicherheitsstatus des Unternehmens übereinstimmt.

Mit Red Hat AI können Unternehmen autonome Agenten entwickeln, die leistungsstark und vorhersehbar auf die Absichten und Compliance-Anforderungen des Unternehmens ausgerichtet sind.



Skalierbare und kosteneffiziente KI-Plattform

Für die Skalierung agentischer KI bedarf es mehr als nur großer Modelle. Organisationen benötigen eine intelligente Infrastruktur. Diese Infrastruktur muss sich an wechselnde Workload-Anforderungen anpassen, Kompromisse bei Kosten und Performance optimieren und Support sowie Sicherheit aufrechterhalten können.

Red Hat AI bietet einen Ansatz, der Folgendes bietet:



Flexibilität in verschiedenen Umgebungen

Führen Sie Agenten im Rechenzentrum, in Cloud-Umgebungen, Clustern und auf Edge-Knoten aus.



Optimierte Computing-Orchestrierung

Unterstützen Sie Einsparungen bei den Inferenzkosten mit Red Hat AI Inference Server und reduzieren Sie die Gesamtbetriebskosten durch Neuverteilung von Aufgaben in Cloud- und On-Premise-Ressourcen mit Red Hat OpenShift AI zur Unterstützung intelligenter automatischer Skalierung.



Sicherheitsorientierte Skalierung

Erhalten Sie Support, Sicherheits-Patches und Kontinuitätsgarantien, die für das Deployment von KI in Branchen wie dem Finanzwesen, dem Gesundheitswesen und den Behörden entscheidend sind.

Red Hat AI bietet eine Plattform, die Tooling, Governance und Skalierbarkeit in einer einzigen Plattform vereint. Unabhängig davon, ob Sie autonome Agenten für IT-Abläufe, den Kundenservice oder branchenspezifische Aufgaben koordinieren möchten – Red Hat kann Sie in der jeweiligen Phase Ihrer agentischen Transformation unterstützen, damit Sie ohne Komplexität und mit Zuversicht agieren können.





Planung Ihrer agentischen KI- Strategie mit Red Hat AI

Mit der richtigen Basis kann agentische KI zur beschleunigten Bereitstellung, Kostensenkung und zu einem höheren ROI beitragen. Ein solcher Wandel geschieht jedoch nicht über Nacht. Ausgangspunkt ist ein strategischer Ansatz, der mit den geschäftlichen Prioritäten, der technischen Bereitschaft und den Governance-Anforderungen im Einklang steht.

Red Hat AI wurde entwickelt, um Unternehmen in den verschiedenen Phasen dieser Entwicklung zu unterstützen – von der Exploration bis hin zum unternehmensweiten Deployment. Unabhängig davon, ob Sie gerade erst mit der Evaluierung

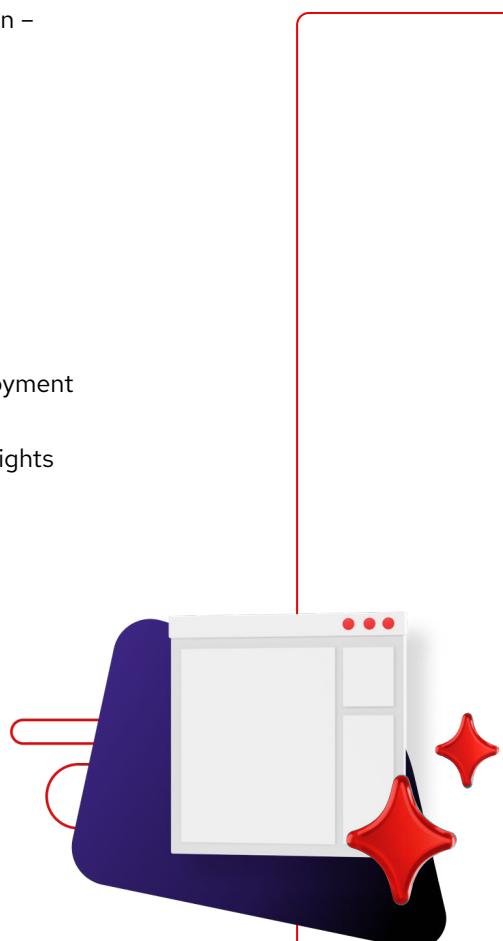
agentischer Workflows beginnen oder bereits KI-Initiativen skalieren – eine gut geplante Strategie sorgt dafür, dass Ihre Bemühungen und Investitionen auf das Generieren eines konkreten Geschäftswerts ausgerichtet sind.

Startpunkte

Der Weg zum autonomen Betrieb muss nicht mit einem vollständigen Deployment beginnen. Vielmehr ist eine schrittweise Einführung, die sich zunächst auf hochwertige, klar abgegrenzte Use Cases konzentriert, die in kurzer Zeit Insights bieten, oft am besten geeignet.

- Bearbeitung und Lösung von Kundensupport-Tickets
- Automatisierte Reaktion auf IT-Fehlerbehebung oder DevOps-Vorfälle
- Generierung von Compliance-Berichten für sämtliche Geschäftsbereiche
- Agenten für die interne Knowledgebase-Abfrage

Diese ersten Schritte bieten ein ideales Testfeld, um das Agentenverhalten zu bewerten, das Vertrauen bei Stakeholdern aufzubauen und die Performance Ihrer IT-Infrastruktur zu validieren.



Einschätzung der Bereitschaft Ihres Unternehmens

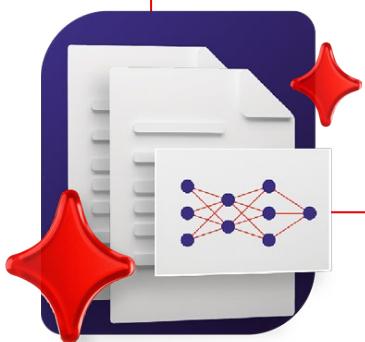
Berücksichtigen Sie folgende Punkte, um die Umgebung Ihres Unternehmens besser zu verstehen und Unterstützung bei der Einführung von Agenten zu erhalten:

1

Wo behindern sich wiederholende oder regelbasierte Entscheidungen meine Teams?

2

Auf welche Systeme, APIs oder Datenquellen müssten die Agenten zugreifen können?



3

Verfügen wir über die IT-Infrastruktur, um modellbasierte Workflows mit niedriger Latenz in großem Umfang zu unterstützen?

4

Welche Richtlinien und Rahmenbedingungen müssen für die Kontrolle autonomer Aktionen vorhanden sein?

5

Wie wird der Erfolg gemessen?
(Berücksichtigen Sie dabei Kosteneinsparungen, Geschwindigkeit, Genauigkeit und weniger Fehler bei der Automatisierung.)



Diese Liste ist zwar nicht vollständig, aber diese Fragen sind ein guter Ausgangspunkt, um erste Erfolge zu identifizieren und sicherzustellen, dass Sie eine einheitliche Ausrichtung zwischen IT, Operations und Führungskräften erreichen.

Strategische Überlegungen

Beachten Sie bei der Entwicklung Ihrer Strategie für agentische KI die folgenden Elemente, um Ihr Unternehmen auf Erfolgskurs zu setzen:



Interoperabilität

Die Wahl einer offenen, modularen Plattform, die Sie nicht an ein einzelnes Modell, eine einzelne Cloud oder ein einzelnes Toolset bindet, trägt dazu bei, dass Sie angesichts der technologischen Weiterentwicklungen flexibel bleiben.



Governance by Design

Legen Sie von Anfang an Richtlinien, Überwachung und Erklärbarkeit fest, um für Compliance und Vertrauen zu sorgen. Beispielsweise die Einhaltung des Health Insurance Portability and Accountability Act (HIPPA).



KI-Einbindung in die IT-Strategie

Behandeln Sie KI-Agenten als Teil Ihrer umfassenderen Digitalisierungs- und Automatisierungsstrategie, nicht als isoliertes Experiment.



Kompetenzentwicklung

Neue Technologien erfordern neue Kompetenzen. Stärken Sie Teams in den Bereichen Engineering, Operations und Business durch Training und Motivation für die Arbeit mit intelligenten Agenten.



Checkliste zur Bereitschaft für agentische KI

Angesichts der vielen Variablen kann es hilfreich sein, eine interne Checkliste zu entwickeln, um den Stand Ihres Unternehmens auf dem Weg zur agentischen KI zu beurteilen.



Haben wir mindestens eine Geschäftsfunktion ermittelt, die von autonomen Agenten profitieren würde?



Wissen wir, mit welchen Systemen und APIs ein Agent interagieren muss?



Kann unsere IT-Infrastruktur Modellinferenz-Workloads mit der erforderlichen Governance und Sicherheit unterstützen?



Haben wir die Unterstützung wichtiger Stakeholder, um agentische Workflows zu testen?



Verfügen wir über einen Plan für die Erfolgsmessung und die Skalierung bewährter Use Cases?

Die autonome Zukunft der Unternehmensautomatisierung



Unternehmen sollten die Zukunft der Automatisierung nicht als Mittel zur Eliminierung manueller Schritte betrachten, sondern als die Befähigung von Systemen, Entscheidungen zu treffen, sich an Veränderungen anzupassen und nach kontinuierlicher Verbesserung zu streben.

Agenten können komplexe Aufgaben übernehmen und schnell, präzise und autonom zur Verfolgung von Geschäftszielen agieren.

Für Führungskräfte bedeutet dieser Wandel eine neue Wettbewerbslandschaft. Unternehmen, die agentische KI nutzen, können neue Ebenen von operativer Agilität, Innovation und ROI erschließen. Die Einführung muss keineswegs kompliziert sein.

Red Hat AI bietet eine offene, hybride Basis, mit der Unternehmen erfolgreich sein können. Von der Vereinfachung von Agent-Workflows bis hin zur Kontrolle autonomen Verhaltens und der Optimierung der Infrastruktur in verschiedenen Umgebungen – Red Hat kann vorausschauende Führungskräfte dabei unterstützen, agentische KI auf praktische, skalierbare und zuverlässige Weise einzusetzen.

Bereit für den nächsten Schritt der KI-Einführung in Ihrem Unternehmen?

Erfahren Sie mehr über [agentische KI mit Red Hat AI](#) oder [kontaktieren Sie Red Hat](#).