

Enterprise-grade Agentic AI: Sicher, kontrolliert und souverän

Atos ermöglicht Unternehmen, Agentic AI sicher
und kontrolliert zu skalieren mit voller Transparenz
über Kosten, Nutzen und digitale Souveränität



Atos

C-Level-Briefing

Die Autonomie von KI entwickelt sich rasant. Die Antworten auf die entscheidenden Fragen noch nicht.

Agentic AI entwickelt sich mit enormer Geschwindigkeit. Gleichzeitig stehen C-Level-Führungskräfte vor zentralen Fragen: Wo entsteht belastbarer geschäftlicher Mehrwert? Wie lassen sich schreibberechtigte KI-Agenten sicher betreiben? Wo müssen Grenzen digitaler Souveränität gezogen werden? Und wie lässt sich Autonomie skalieren, ohne Kontrolle, Transparenz oder Planbarkeit zu verlieren? Zu viele Pilotprojekte überzeugen in Demos, kommen aber nicht in den produktiven Betrieb, weil industrielle Antworten auf Governance, Sicherheit, Architektur und Kostendisziplin zu spät kommen oder ganz fehlen.

Für global agierende Unternehmen werden diese Fragestellungen schnell zur operativen Realität. Daten befinden sich in unterschiedlichen Rechtsräumen mit teilweise widersprüchlichen Anforderungen an Datenresidenz und Datenzugriff. Agenten benötigen Schreibzugriffe auf ERP-, CRM-, ITSM- und OT-Systeme und vergrößern damit die potenziellen Auswirkungen kompromittierter Prompts, manipulierten Kontexts oder missbräuchlich genutzter Werkzeuge erheblich. Modelle, Werkzeuge und Komponenten von Drittanbietern erhöhen zusätzlich die Risiken innerhalb der Lieferkette. Gleichzeitig führt die einfache Erstellung neuer Agenten über Low-Code- und No-Code-Plattformen zu einer kaum kontrollierbaren Vermehrung autonomer Systeme, die Geschäftslogik duplizieren und Verantwortlichkeiten verwischen. Vorstände verlangen Nachvollziehbarkeit und klare Verantwortlichkeiten. CISOs benötigen wirksame Laufzeitkontrollen, die Möglichkeit, Berechtigungen sofort zu entziehen, sowie Notabschaltungen (Kill Switches). CFOs erwarten Transparenz über die Wirtschaftlichkeit und Instrumente, mit denen sich Kosten für Tokens, Werkzeuge und autonome Ausführungsschleifen kontrollieren lassen. Und all dies muss dort, wo es erforderlich ist, unter den Anforderungen digitaler Souveränität erfolgen – ohne Unternehmen dauerhaft an einen einzelnen Technologieanbieter zu binden.

Dieses Whitepaper zeigt einen pragmatischen Weg von der Vision zum produktiven Einsatz. Es beschreibt Agentic AI nicht als Experiment, sondern als produktionsreife Unternehmenssoftware und erläutert, wie sich autonome Systeme nur dann skalieren lassen, wenn geschäftlicher Nutzen, Sicherheit und Compliance jederzeit nachweisbar sind.

Im Mittelpunkt stehen dabei folgende Themen:

- Ein diszipliniertes Konzept für "Services as Software" mit Atos' Sovereign Agentic Studio, das Workflows schrittweise und kontrolliert in softwarebasierte Leistungen überführt
- Eine Steuerungs- und Kontrollebene für vertrauenswürdige Agentic AI mit Governance zur Laufzeit, Zero-Trust-Zugriffen, verhaltensbasierter Sicherheit, Notabschaltungen, umfassender Beobachtbarkeit und unveränderbaren Audit-Protokollen
- Digitale Souveränität als Architekturprinzip – einschließlich der Frage, an welchen Stellen Kontrolle erforderlich ist und wie sie über Daten, Modelle, Orchestrierung und Laufzeitumgebungen hinweg umgesetzt wird, beispielsweise in Air-Gap-, Private-Cloud-, Hybrid- oder rechtsraumspezifischen Bereitstellungsmodellen
- AgentOps und FinOps vom ersten Tag an - mit Transparenz über Wirtschaftlichkeit, Kostensteuerung und einem konsequenten Bezug zu geschäftlichen Kennzahlen, um unkontrolliertes Wachstum und unerwartete Betriebskosten zu vermeiden
- Datenqualität als unverzichtbare Voraussetzung für autonome Systeme. Nur kuratierte, vertrauenswürdige und klar gesteuerte Daten verhindern, dass Agentic AI bestehende Qualitätsprobleme weiter verstärkt
- Erfahrungen aus der Praxis zeigen, dass sich die Autonomie mit den Kontrollmaßnahmen skalieren lässt: kürzere Wiederherstellungszeiten (MTTR), geringere Ticketvolumina, einen höheren Anteil autonom gelöster Vorfälle sowie sinkende Betriebskosten auf Basis belastbarer, vertrauenswürdiger Steuerungsmechanismen

Wer Verantwortung für Geschäftsergebnisse und Risiken trägt, findet in diesem Whitepaper einen pragmatischen Ansatz, um Agentic AI unter den eigenen Rahmenbedingungen einzuführen – mit klarer Kontrolle über Nutzen, Sicherheit, digitale Souveränität und Wirtschaftlichkeit.



DAS VERSPRECHEN

Agentic AI ist für das moderne Unternehmen das, was Elektrizität und Internet für frühere Generationen waren:

Ein radikaler Sprung, der neu definiert, wie Organisationen funktionieren und Wert schaffen. Im Gegensatz zur klassischen Automatisierung besteht Agentic AI aus Systemen von Agenten, die unter menschlicher Aufsicht mit zunehmender Autonomie planen, lernen und handeln können. Diese Agenten übernehmen die Verantwortung für ganze Arbeitsabläufe und erzielen Ergebnisse mit beispielloser Geschwindigkeit und Präzision.

Für Geschäftsleitungen geht Agentic AI über theoretisches Potenzial hinaus und liefert messbare Wirkungen. Sie verkürzt Durchlaufzeiten, senkt Betriebskosten, verbessert die Servicequalität und erhöht Geschwindigkeit sowie Qualität von Entscheidungen – ohne dass der Personalbedarf im gleichen Maße wächst. Agentic AI schafft messbaren geschäftlichen Mehrwert und trägt unmittelbar zur Verbesserung der Profitabilität eines Unternehmens bei. Dies ist keine ferne Vision mehr. Laut Gartner®: "mindestens

15%

der täglichen Arbeitsentscheidungen werden bis 2028 autonom durch Agentic AI getroffen,

gegenüber 0% im Jahr 2024.¹ Führende Unternehmen richten ihre Strategien bereits heute auf dieses Zukunftsbild aus. Sie gestalten Geschäftsprozesse, Entscheidungsabläufe und Wertschöpfungsmodelle neu, um das Potenzial von Agentic AI umfassend zu nutzen. Gleichzeitig sind die meisten Organisationen strukturell noch nicht darauf vorbereitet, autonome Entscheidungen in diesem Umfang zu steuern, abzusichern und nachvollziehbar zu machen.

¹ Pressemitteilung von Gartner, 25. Juni 2025: Gartner prognostiziert, dass über 40% der agentischen KI-Projekte bis Ende 2027 eingestellt werden.

Die unterschätzten Risiken von Agentic AI: Vom Hype zur Risikolage

Die nahezu unbegrenzten Möglichkeiten von KI sind faszinierend – keine Frage.

Doch die Antwort besteht nicht darin, immer schneller immer mehr Agenten zu entwickeln. Entscheidend wird sein, ob es Unternehmen gelingt, mit Agentic AI einen klaren Geschäftsnutzen zu erzielen und sie gleichzeitig sicher, geschützt und skalierbar zu betreiben.

Als Führungskraft auf C-Level werden Sie nicht daran gemessen, die Erzählung anderer umzusetzen, sondern daran, belastbare Roadmaps, Risiken und Ergebnisse verantwortungsvoll zu steuern.

Trotz des Hypes ist Agentic AI für Unternehmensanforderungen immer noch unvollständig. Das Ökosystem rast voran mit Konzepten und Werkzeugen, die isoliert mächtig wirken, aber wenig belastbar sind, wenn sie realer Komplexität und Skalierung ausgesetzt sind.

Auf Systemebene führt Agentic AI zu einer grundlegend neuen Kategorie von Risiken.

In der Praxis führt dies zu bekannten, zugleich aber kritischen Fehlerszenarien: **Race Conditions, Ausführungs-Deadlocks, unvollständig abgeschlossenen Prozessen sowie nichtdeterministischem Verhalten**, das sich nur schwer reproduzieren, erklären oder auditieren lässt.

Fehlen eine explizite Orchestrierung, klar definierte Leitplanken sowie belastbare Wiederherstellungsmechanismen, geht das Vertrauen in die Lösung schnell verloren. Unternehmen bleiben dann in der Experimentierphase stecken und schaffen den Übergang in den produktiven Betrieb und die Skalierung nicht.

Agentic AI verändert das Bedrohungsmodell grundlegend und vergrößert das potenzielle Schadensausmaß erheblich. Im Gegensatz zu herkömmlichen KI-Lösungen verfügen diese Systeme über Schreibzugriffe, können Workflows auslösen und eigenständig über verschiedene Systeme hinweg handeln.

Ein kompromittierter Agent ist damit ein digitaler Insider. Er kann durch Prompt Injection, Manipulation von Speicher oder Kontext (Memory bzw. Context Tampering), Zielabweichungen (Goal Drift), den Missbrauch von Tools (Tool Misuse), Privilegienausweitung (Privilege Escalation), Schwachstellen in der Lieferkette oder sogar durch die Interaktion mit bösartigen Agenten kompromittiert werden. Das sind keine theoretischen Randfälle, sondern strukturelle Risiken agentischer Systeme und Unternehmen tragen die Verantwortung, diese Risiken zu steuern. Dennoch wenden viele Organisationen Governance-Ansätze von gestern auf Systeme an, deren Verhalten sich mit jedem Kontext ändert. Jede Tool-Nutzung erfordert daher den Wechsel von statischen Kontrollen hin zu begrenzter, überwachter Autonomie und verhaltensbasierten Schutzmechanismen.

Ein weniger beachtetes, aber ebenso grundlegendes Risiko ist die unkontrollierte Vermehrung von Agenten (Agentic Sprawl). Da No-Code- und Low-Code-Plattformen die Erstellung von Agenten vereinfachen, entstehen in vielen Organisationen durch Pilotprojekte von Endnutzern Hunderte oder Tausende eng gefasster, schwach verwalteter Agenten. Demokratisierung beschleunigt Experimente, führt ohne Kontrolle jedoch schnell zu doppelter Logik, inkonsistentem Verhalten, unklaren Verantwortlichkeiten und verborgenen Risiken. Fehlt die notwendige Disziplin, droht Agentic AI die gleichen Probleme zu wiederholen, die bereits frühere Automatisierungswellen geprägt haben: fragmentierte Systemlandschaften und unkontrollierte Schattenanwendungen – diesmal jedoch mit der Geschwindigkeit autonomer Systeme und einem deutlich größeren potenziellen Schadensausmaß.

Die unbequeme Wahrheit lautet daher: Das technologische Ökosystem entwickelt sich rasant weiter. Die wirklich schwierigen Fragen bleiben jedoch bei den Unternehmen selbst – nämlich wie sich geschäftlicher Nutzen, Cybersecurity, digitale Souveränität, Governance und Kostenkontrolle gleichermaßen sicherstellen lassen.

Möchten Sie das selbst testen? Bevor Sie eine weitere Agentic AI -Initiative freigeben, stellen Sie Ihren Teams diese 6 einfachen Fragen und achten Sie genau darauf, wie selbstbewusst oder vage sie antworten. Die Fragen zeigen, ob Agentic AI noch als Pilotprojekt behandelt wird oder für den produktiven Einsatz bereit ist.

1.

Identitäten, Zugriff und Kontrolle:

Sind Agenten eindeutig identifizierbar und verfügen sie ausschließlich über klar definierte Berechtigungen? Werden Zugriffe auf Tools und Unternehmenssysteme nach dem Zero-Trust-Prinzip zentral gesteuert und können Berechtigungen jederzeit entzogen werden? Sind privilegierte Aktionen kontrolliert, auditierbar und an menschliche Genehmigungsprozesse gebunden, sodass Agenten ihre Befugnisse nicht unbemerkt erweitern können?

2.

Security im Workflow:

Werden Sicherheitsmaßnahmen entlang des gesamten agentenbasierten Workflows umgesetzt – einschließlich Schutz vor Prompt Injection, Eingabevalidierung, Speicherisolation, Einschränkungen bei der Tool-Nutzung sowie einer abgesicherten Lieferkette für Agenten, Modelle und externe Komponenten? Oder beschränkt sich die Sicherheit ausschließlich auf das zugrunde liegende KI-Modell?

3.

Nachvollziehbarkeit und

Auditierbarkeit: Können sämtliche Aktionen eines Agenten vollständig nachvollzogen, auditiert und erklärt werden – in einer Form, die regulatorischen Anforderungen, Sicherheitsprüfungen und operativen Untersuchungen standhält?

4.

Data-Governance und Disziplin:

Arbeiten die Agenten auf kuratierten, verlässlichen und durch klare Governance-Regeln gesteuerten Datensätzen mit eindeutig definierten Verantwortlichkeiten und Qualitätskontrollen, oder setzen wir autonome Systeme inkonsistenten, veralteten oder nicht vertrauenswürdigen Daten aus?

5.

Orchestrierung und Disziplin:

Verfügt das Unternehmen über eine zentrale Orchestrierungsebene, welche die Zusammenarbeit von Agenten steuert, Zustände verwaltet, Übergaben koordiniert, Fehlerszenarien behandelt und Eskalationen kontrolliert? Oder basiert die Lösung auf fragilen Punkt-zu-Punkt-Integrationen?

6.

Kostenkontrolle und Lock-in-

Risiko: Existieren Mechanismen, um die stark schwankenden Kosten von Agentic AI – etwa für Tokens, Tools, Wiederholungen und Ausführungsschleifen – kontinuierlich zu überwachen, zu steuern und zu optimieren? Gleichzeitig: Ist sichergestellt, dass mit zunehmender Autonomie keine unumkehrbaren Herstellerabhängigkeiten entstehen, oder wird angenommen, dass Kosten und Abhängigkeiten auch künftig beherrschbar bleiben?

Diese Risiken sind real und beherrschbar.

Mit den richtigen Grundlagen können Unternehmen autonome Systeme sicher skalieren

Atos verfügt über umfassende Erfahrung bei der Lösung komplexer und geschäftskritischer Herausforderungen – sowohl in der Privatwirtschaft als auch im öffentlichen Sektor.

Dazu gehören gewachsene IT-Landschaften (Brownfield-Umgebungen), hochregulierte Branchen, geschäftskritische Betriebsumgebungen, souveräne Infrastrukturen sowie Ökosysteme, die einer permanenten Bedrohung durch Cyberangriffe ausgesetzt sind.

Ebenso umfasst dies Umgebungen mit höchsten Sicherheitsanforderungen – bis hin zu militärischen Standards – in denen Zuverlässigkeit, Resilienz, Sicherheit und vollständige Nachvollziehbarkeit unverzichtbar sind. Systeme müssen so ausgelegt werden, dass sie auch unter Angriffen, Ausfällen und extremen operativen Rahmenbedingungen funktionsfähig bleiben und jederzeit überprüfbar sind.

Warum Souveränität in Agentic AI wichtig ist

Souveräne KI bedeutet, jederzeit bewusst die Kontrolle über geschäftskritische Daten, Entscheidungen und das Verhalten von KI-Systemen zu behalten.

Atos unterstützt Unternehmen dabei, gezielt zu entscheiden, an welchen Stellen digitale Souveränität unverzichtbar ist – und wo standardisierte, marktübliche Ökosysteme eine wirtschaftlich sinnvolle Alternative darstellen.

So stellen wir sicher, dass Unternehmen sich nicht zwischen modernsten KI-Fähigkeiten und ihrer Unabhängigkeit von der Roadmap oder dem Rechtsraum eines einzelnen Anbieters entscheiden müssen.

Atos vereint eine Kombination von Kompetenzen, die in dieser Form nur selten zu finden ist: konsequente Governance, fundierte Orchestrierungskompetenz sowie jahrzehntelange Erfahrung im Betrieb geschäftskritischer und souveräner IT-Systeme. Wir verstehen Agentic AI als produktionsreife Unternehmenssoftware, die konsequent gesteuert, abgesichert und betrieben wird. So unterstützen wir Unternehmen dabei, autonome Systeme kontrolliert und schrittweise zu skalieren, ohne Transparenz, Nachvollziehbarkeit oder Vertrauen zu verlieren.

- ✓ Wir betreiben Agentic AI unter einem souveränen Governance-Modell mit fein abgestimmter Kontrolle über Datenqualität und Datenresidenz, die Bereitstellung von Modellen, Zugriffsgrenzen sowie – wo erforderlich – einer kontinuierlichen operativen Aufsicht.
- ✓ Unser Liefer- und Geschäftsmodell orientiert sich konsequent an messbaren Geschäftsergebnissen. Wertbeiträge werden kontinuierlich anhand definierter KPIs nachverfolgt und mit den Kosten sowie der Leistung der eingesetzten Agenten verknüpft.
- ✓ Dafür betreiben wir eine produktionsreife Plattform für das Management von Agentic AI. Sie basiert auf tiefgreifender Engineering-Kompetenz und sorgt für ein vorhersehbares Verhalten autonomer Agenten, technisch durchsetzbare Leitplanken zur Kostenkontrolle, eine richtliniengesteuerte Nutzung von Werkzeugen sowie eine resiliente Ausführung im Unternehmensmaßstab.
- ✓ Darüber hinaus bündeln wir Kompetenzen über die gesamte IT hinweg – von der Infrastruktur über Plattformen und Anwendungen bis hin zu Betrieb und Cybersecurity, um den vollständigen Technologie-Stack ganzheitlich zu adressieren.
- ✓ Wir machen Security zu einem Wettbewerbsvorteil – mit laufzeitbasierter Verhaltensanalyse, klaren Berechtigungsgrenzen, dem Entzug von Zugriffsrechten in Echtzeit, Schutzmechanismen gegen Kontextmanipulation sowie kontinuierlicher Nachvollziehbarkeit und Auditierbarkeit.
- ✓ Wir nutzen ein breites Partner-Ökosystem, in dem wir als Orchestrator fungieren und Hyperscaler, Unternehmensplattformen und spezialisierte Anbieter kombinieren, ohne architektonische Unabhängigkeit, Transparenz und Entscheidungsfreiheit für Sie einzuschränken.
- ✓ Wir verankern agentische Orchestrierung in einem menschenzentrierten Betriebsmodell und integrieren Veränderung, Verantwortlichkeit und ethische Leitplanken in die tatsächliche Arbeitsweise.

Wahrscheinlich haben Sie bereits erste Agenten getestet oder Pilotprojekte in Ihrer Organisation gestartet. Die eigentliche Frage ist, ob Sie diesen Agenten auch im großen Maßstab vertrauen können. **Was erfolgreiche Ergebnisse auszeichnet, ist nicht Ehrgeiz allein, sondern Disziplin in der Umsetzung.**

Hier kommt Atos ins Spiel. Seit Jahrzehnten betreiben wir komplexe, hochregulierte und geschäftskritische Systeme. Für Agentic AI gelten dieselben Anforderungen. Gemeinsam mit unseren Kunden schaffen wir die Grundlagen, auf denen sich autonome Systeme kontrolliert, vertrauenswürdig und mit nachweisbarem geschäftlichem Nutzen skalieren lassen.

Die folgenden Kapitel zeigen, wie dieser Ansatz in der Praxis umgesetzt wird und wie Agentic AI den Weg von einem vielversprechenden Konzept hin zu produktionsreifen Unternehmenslösungen findet.

Unsere Vision: Services für eine agentische Welt neu definieren

Atos verfolgt eine klare und konsequente Vision der Zukunft: Services as Software (SaS)

Wir sind überzeugt, dass Unternehmensservices und Unternehmenstechnologie zunehmend zu einer neuen Betriebsebene verschmelzen. Routineaufgaben, wiederkehrende Prozesse und datenintensive Tätigkeiten werden künftig überwiegend als Software erbracht – und immer seltener als manuelle, personengebundene Dienstleistungen. In diesem Modell verlagert sich der Wertschöpfungsfokus von der Bereitstellung personeller Kapazitäten hin zur Bereitstellung von Fähigkeiten. An die Stelle zeit- und ressourcenbasierter Leistungsmodelle (Time & Material) treten ergebnisorientierte Produkte und Services. Damit verändert sich grundlegend, wie Dienstleistungen entwickelt, erbracht und vergütet werden.

Atos bewegt sich bereits entschlossen in diese Richtung. Wir investieren in agentengestützte Delivery-Modelle für autonome Betriebsprozesse, beschleunigte Modernisierung, Software Engineering und Cyberabwehr. Grundlage hierfür ist eine durchgängige Agentic-AI-Plattformstrategie, mit der Dienstleistungen, die bislang überwiegend durch Menschen erbracht wurden, schrittweise zu softwarebasierten Produkten weiterentwickelt werden. Gleichzeitig gestalten wir unsere eigenen Delivery- und G&A-Prozesse (General & Administrative) konsequent nach dem Prinzip **Services as Software** neu. Dabei denken wir Arbeitsabläufe vollständig neu: Wir definieren, wie Tätigkeiten in Workflows zerlegt werden, wie Menschen und Agenten zusammenarbeiten, wie Ergebnisse gemessen werden und wie kontinuierliche Verbesserungen künftig über Software-Releases statt über klassische Prozessänderungen bereitgestellt werden.

Atos fordert Sie nicht auf, einen Weg zu gehen, den wir nicht selbst erprobt haben. Wir setzen dieses Modell bereits innerhalb unseres eigenen Unternehmens ein und agieren dabei als „**Client Zero**“. Dadurch sammeln wir praktische Erfahrungen bei der Orchestrierung von Agenten, der Kostensteuerung, der Absicherung autonomer Systeme und ihrer Governance. Ergänzt wird dieses Wissen durch unsere langjährige Erfahrung im Betrieb komplexer IT-Landschaften sowie durch anonymisierte Betriebsdaten aus realen Kundenumgebungen.

Diese Erkenntnisse bilden die Grundlage dafür, unsere Kunden bei der Industrialisierung von Agentic AI in realen Unternehmensumgebungen gezielt zu unterstützen.

Atos definiert neu, wie Agentic AI in Unternehmen und öffentlichen Institutionen betrieben wird.

Agentische Systeme nutzen Informationen nicht mehr nur zur Analyse, sondern leiten daraus eigenständig Handlungen ab und übernehmen zunehmend operative und strategische Entscheidungen innerhalb einer Organisation.

Atos schafft die Voraussetzungen dafür, dass diese Entscheidungen jederzeit kontrollierbar, nachvollziehbar, sicher und wo erforderlich souverän bleiben.

Unsere Vision basiert auf einer vertrauenswürdigen Steuerungs- und Kontrollebene für Agentic AI, die selbst den höchsten Anforderungen anspruchsvoller Unternehmens- und Behördenumgebungen gerecht wird.

So stellen wir sicher, dass Entscheidungen auch im großen Maßstab transparent, nachvollziehbar und mit regulatorischen sowie institutionellen Anforderungen vereinbar bleiben.



Verantwortungsvolle KI: Eine Voraussetzung für skalierbare Autonomie

Da agentische Systeme immer mehr operative und entscheidungsbezogene Aufgaben übernehmen, wird Responsible AI (RAI) zu einem zentralen Betriebsprinzip für die Entwicklung und den Betrieb digitaler Services. Agentic AI wird künftig deutlich weniger durch KI-spezifische Regulierung bestimmt als durch die bereits bestehenden fachlichen, branchenspezifischen und funktionalen Vorgaben für Unternehmensprozesse – beispielsweise in den Bereichen Datenschutz, Informationssicherheit, Finanzkontrollen, Personalwesen, Arbeitssicherheit oder Handel. Responsible AI beginnt daher mit den Grundlagen: Sicherheit, Datenschutz, Fairness, Genauigkeit und Erklärbarkeit. Sie muss sich zugleich darauf erstrecken, wie Autonomie explizit begrenzt, überwacht und angepasst wird, wenn sich Geschäftskontext, Vorschriften und Erwartungen weiterentwickeln.

In einer agentischen Welt wachsen Responsible AI und Governance zu einer gemeinsamen Disziplin zusammen. Verantwortung bedeutet, dass Agentensysteme an der Unternehmensstrategie und den Werten der Organisation ausgerichtet sind, auf Prozessebene überwacht werden und bewusst mit Human-in-the-Loop-Mechanismen sowie systemweiten Kontrollfunktionen entwickelt werden.

Menschen müssen in der Lage sein, Agenten und ganze Workflows zu genehmigen, zu übersteuern, zu unterbrechen oder auszusetzen, wenn Risiken oder Auswirkungen dies erfordern. So bleibt Autonomie im großen Maßstab mit Vertrauen vereinbar. Agentic AI wird nur dann zu einem dauerhaften Vorteil, wenn sie im täglichen Betrieb beobachtet, kontrolliert und zur Rechenschaft gezogen werden kann.

Vertrauen im großen Maßstab durch sichere Agentic AI

Sicherheit und KI-Governance stehen im Zentrum unserer Agentic AI Strategie, weil wir glauben, dass Autonomie ohne Kontrolle ein unkontrolliertes Risiko darstellt. Sobald Agentensysteme eigenständig Aufgaben über Anwendungen und Geschäftsprozesse hinweg ausführen, muss Vertrauen fester Bestandteil ihres Betriebsmodells sein. Es muss jederzeit eindeutig geregelt sein: wer die Verantwortung trägt, welche Handlungen zulässig sind, wie das Verhalten der Agenten überwacht wird, und wie ihre Aktionen überprüft und nachvollzogen werden können.

Deshalb betrachtet Atos Sicherheit und Governance nicht als nachgelagerte Kontrollinstanzen, sondern als integralen Bestandteil der Betriebsebene, auf der Agentic AI ausgeführt wird.

Unser Ziel ist es, Vertrauen skalierbar zu machen. Governance schafft die notwendige Disziplin über den gesamten Lebenszyklus hinweg: klare Verantwortlichkeiten, risikobasierte Leitplanken, menschliche Aufsicht, geregelte Änderungsprozesse und belastbare Nachweise. Dadurch bleiben Agenten auch dann an den Unternehmenszielen ausgerichtet, wenn Workflows erweitert oder neue Fähigkeiten hinzugefügt werden. Cybersecurity sorgt für die technische Durchsetzung dieser Vorgaben. Sie stellt sicher, dass Zugriffe, Aktionen und Datennutzung auch im produktiven Betrieb jederzeit kontrolliert bleiben. Erst das Zusammenspiel von Governance und Security ermöglicht es, den Grad der Autonomie schrittweise zu erhöhen und gleichzeitig Ausführung, Entscheidungen und Ergebnisse transparent, audittierbar und auch unter regulatorischen, sicherheitsrelevanten und souveränitätsbezogenen Anforderungen jederzeit nachvollziehbar zu halten.

Souveräne Agentic AI

Kontrolle,
WO
Autonomie
zählt



Souveräne KI bedeutet nicht technologische Isolation oder den Neuaufbau des KI-Stacks von Grund auf. Entscheidend ist vielmehr, die Kontrolle gezielt dort auszuüben, wo sie geschäftskritisch ist, und bewusst zu entscheiden, in welchen Bereichen standardisierte Technologien und Plattformen ausreichend sind. Die meisten Unternehmen werden auch künftig auf externe Modelle, Plattformen und Ökosysteme zurückgreifen – überall dort, wo keine differenzierenden Wettbewerbsvorteile entstehen. Souveränität wird unverzichtbar, wenn KI-Systeme zentrale Geschäftsentscheidungen steuern, autonom über Arbeitsabläufe agieren, sensible oder regulierte Daten verarbeiten oder proprietäres Wissen und Prozesse abbilden. Die Frage ist daher nicht „Sind wir souverän?“, sondern „Wo brauchen wir Souveränität und in welchem Ausmaß?“

Im Agentic AI Kontext kann Souveränität nicht auf einer einzigen Ebene adressiert werden. Wenn Agenten Maßnahmen ergreifen, Tools aufrufen, mit anderen Agenten interagieren und Systeme modifizieren können, wird jedes schwache Glied zu einer systemischen Schwachstelle. Souveräne Agentic AI muss daher im gesamten Stack durchgesetzt werden: Daten, Modelle, Orchestrierungsebenen, Anwendungen und im laufenden Betrieb. Dazu gehört die Steuerung des Verhaltens und der Entwicklung von Agenten, Transparenz und Rückverfolgbarkeit von Entscheidungen und Datenherkunft, vorhersehbares und robustes Modellverhalten sowie umfassende Kontrolle und Sicherheit der Daten in der Ausführung.

Digitale Souveränität ist damit keine einmalige Architekturentscheidung. Sie ist eine operative Disziplin, die fest in die kontinuierliche Überwachung, Begrenzung und Absicherung agentenbasierter Systeme integriert werden muss. Nur so bleibt Autonomie auch im großen Maßstab resilient, audittierbar und dauerhaft kontrollierbar.



Von der Vision zur Realität

Ein disziplinierter Weg zur Autonomie

Möglicherweise betreiben Sie geschäftskritische Umgebungen, die regulatorischen, branchenspezifischen, souveränitätsbezogenen und cybersicherheitsrelevanten Anforderungen unterliegen und in denen Ausfälle keine Option sind. Der Übergang zu einem Agentic-First-Betriebsmodell lässt sich unter diesen Rahmenbedingungen jedoch weder überstürzen noch erzwingen. Die Umsetzung unserer Vision erfolgt deshalb schrittweise, diszipliniert und verantwortungsvoll.

Es ist unsere Aufgabe, Unternehmen gezielt von den heute überwiegend menschenzentrierten Services über hybride Betriebsmodelle bis hin zu softwarebasierten Services zu begleiten – ohne dabei das zu gefährden, was bereits zuverlässig funktioniert. Wir erhöhen den Grad der Autonomie dort, wo ein messbarer Mehrwert entsteht. Wir halten den Menschen dort eingebunden, wo sein Urteilsvermögen erforderlich bleibt, und industrialisieren ausschließlich jene Prozesse, die sich sicher betreiben, wirksam steuern und objektiv messen lassen.

Ebenso wichtig ist, dass wir pragmatisch sind, wo Agentic AI wirklich einen Mehrwert schafft. Nicht jeder Workflow erfordert agentische Orchestrierung. Für hochdeterministische, standardisierte Prozesse können einfachere Automatisierungsansätze eine schnellere Rendite (ROI) mit geringerem Risiko und geringeren Overhead erzielen. Unsere Aufgabe besteht darin, Unternehmen dabei zu unterstützen, die richtigen Abwägungen zu treffen: Agentic AI dort einzusetzen, wo Anpassungsfähigkeit, Kontextverständnis und Urteilsvermögen den entscheidenden Unterschied machen – und bewährte Automatisierung dort zu nutzen, wo Vorhersehbarkeit, Stabilität und Effizienz im Vordergrund stehen.

Nicht alle Services werden sich in gleicher Weise oder mit derselben Geschwindigkeit weiterentwickeln. Das richtige Verhältnis zwischen menschlichem Urteilsvermögen und softwaregestützter Ausführung hängt von zwei Faktoren ab: der Komplexität der Aufgabe, und dem Maß an Empathie, Vertrauen und menschlicher Interaktion, das sie erfordert. **Die nachfolgende Service Value Matrix zeigt, welche Betriebsmodelle sich für unterschiedliche Arten von Services am besten eignen.**

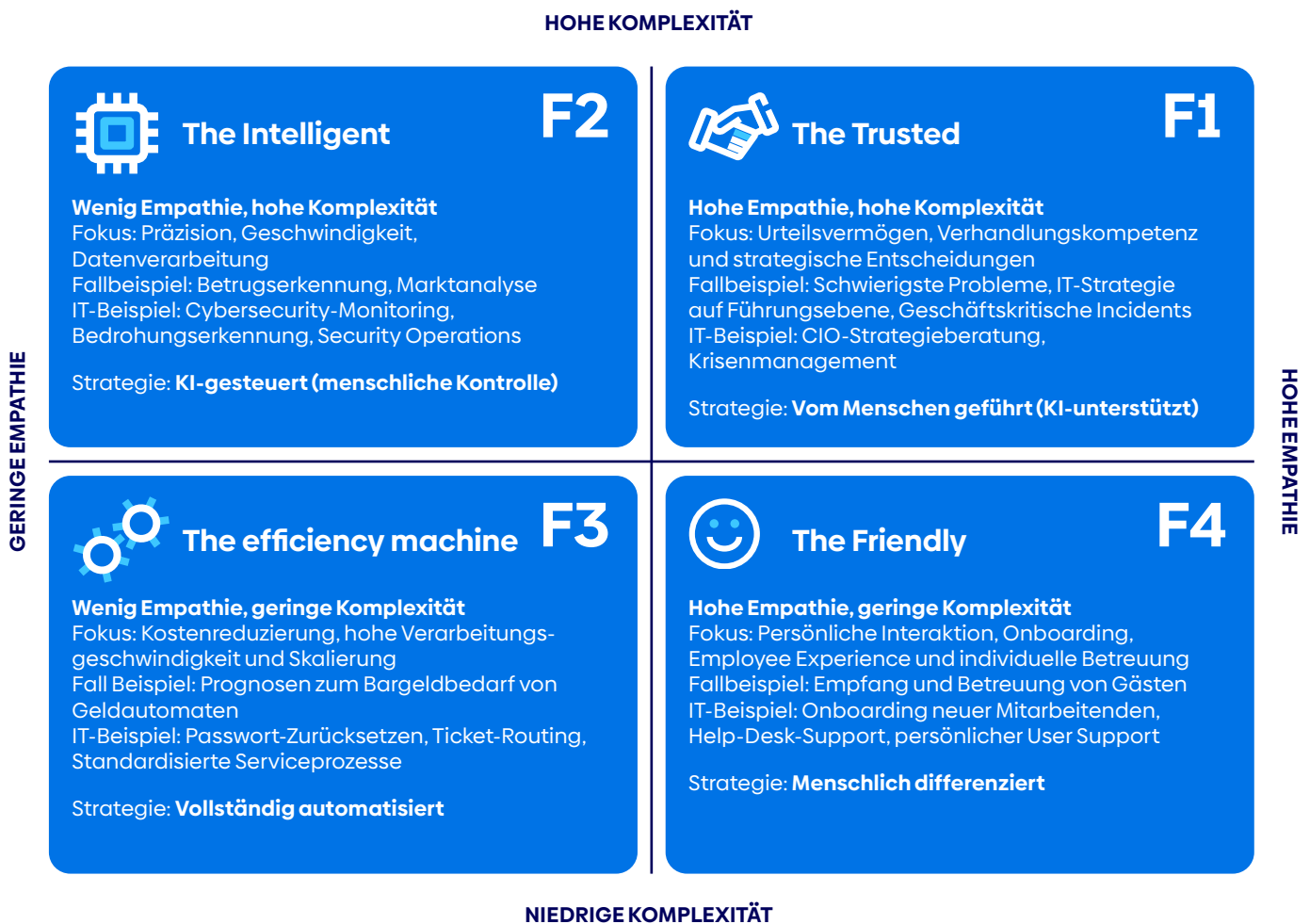


Abbildung 1. Wo Agentic AI wirklich Sinn macht, die Service Value Matrix

In der Praxis erfolgt der Wandel zu einem AI-native-Unternehmen schrittweise entlang eines klaren Reifegradmodells. Unternehmen entwickeln sich von einer menschengeführten Arbeitsweise, in der KI Analysen und Entscheidungen unterstützt, hin zu agentengestützten Betriebsmodellen, in denen Agenten klar definierte Aufgaben unter menschlicher Aufsicht ausführen.

Darauf aufbauend entstehen agentenorchestrierte Workflows, bei denen Menschen vor allem Ausnahmen steuern und die übergeordnete Aufsicht übernehmen. Erst danach wird eine kontrollierte Autonomie möglich, bei der Agenten vollständige End-to-End-Prozesse innerhalb klar definierter Leitplanken eigenverantwortlich ausführen.

Der Fortschritt entlang dieses Reifegradmodells hängt weniger von der Technologie als von den richtigen Entscheidungen ab. Jede Entwicklungsstufe erfordert bewusste Festlegungen hinsichtlich Verantwortlichkeiten, Governance, Architektur und Betriebsmodell. Genau an diesem Punkt stehen viele Unternehmen heute vor einer Richtungsentscheidung.

Die Industrialisierung von Agentic AI verlangt gleichermaßen Disziplin und Ambition. Unsere Erfahrungen aus Kundenprojekten und ersten großflächigen Implementierungen zeigen, dass nur wenige grundlegende Entscheidungen darüber bestimmen, ob Unternehmen den Schritt in den produktiven Betrieb schaffen – oder dauerhaft in der Experimentierphase verharren.



Die folgenden Dos and Don'ts beschreiben die wichtigsten Grundsätze für die verantwortungsvolle Skalierung von Agentic AI und die Erzielung nachhaltiger Geschäftsergebnisse.

Do's

- ✓ Agentic AI zu einem strategischen Transformationsprogramm auf CxO- bzw. Vorstandsebene machen, mit klar benannten fachlichen Verantwortlichen und eindeutig definierten ROI-Zielen.
- ✓ Mit einer kleinen Anzahl durchgängiger End-to-End-Workflows beginnen, die einen klaren geschäftlichen Nutzen, hohe Wiederholbarkeit und ein attraktives ROI-Potenzial aufweisen.
- ✓ Geschäftsrelevante KPIs bereits zu Beginn festlegen und sich auf messbare Zielwerte für den produktiven Betrieb verpflichten.
- ✓ AgentFinOps frühzeitig etablieren, einschließlich Transparenz über Kostenstrukturen, Ausgabenüberwachung, Anomalieerkennung und Mechanismen zur Begrenzung von Ausgaben, wenn der Grad der Autonomie zunimmt.
- ✓ In moderne Datenplattformen und eine konsequente Data Governance investieren, damit Agenten auf zuverlässige, sichere und qualitativ hochwertige Daten zugreifen können.
- ✓ Geschäftsprozesse konsequent AI-first neu gestalten, einschließlich Entscheidungslogik, Ausnahmebehandlung, Übergaben sowie der Zusammenarbeit zwischen Menschen und Agenten.
- ✓ Agenten klar definierte Verantwortungsbereiche, Entscheidungsbefugnisse, Eskalationsschwellen und Modelle menschlicher Aufsicht zuweisen.
- ✓ Robuste Kommunikations- und Orchestrierungsmechanismen etablieren, beispielsweise auf Basis von APIs, Messaging-Diensten und gemeinsam genutzten Zustandsinformationen (Shared State), damit Agenten und Systeme zuverlässig zusammenarbeiten.
- ✓ AgentOps von Beginn an einführen, einschließlich Observability, Audit-Trails, Rollback-Funktionen, Notabschaltungen (Kill Switches) und umfassender Sicherheitsmechanismen.
- ✓ Autonomie schrittweise und bewusst ausbauen: schnell pilotieren, noch schneller lernen und den Grad der Autonomie ausschließlich auf Grundlage belastbarer Erkenntnisse erweitern.
- ✓ Agentenspezifische Risiken durch laufzeitbasierte verhaltensorientierte Sicherheitsmechanismen absichern, ergänzt um Zugriffskontrollen, Verschlüsselung, Datenschutzmaßnahmen, Egress-Kontrollen sowie Schutzmechanismen gegen Context Poisoning, Goal Drift, Tool Misuse und Privilege Escalation.

Don'ts

- ✗ Agentic AI nicht als isoliertes IT-Pilotprojekt betreiben, während die Fachbereiche lediglich beobachten und Agenten ohne eindeutige Verantwortlichkeiten agieren.
- ✗ Nicht mit verstreuten Anwendungsfällen oder Pilotprojekten mit geringem geschäftlichem Nutzen beginnen, die keinen Bezug zu betriebswirtschaftlichen Ergebnissen besitzen.
- ✗ Sich nicht auf Demo-Ergebnisse, vereinzelte Produktivitätsbeispiele oder den Erfolg einzelner Pilotprojekte verlassen.
- ✗ Nicht zulassen, dass Kosten für Tokens, Tools oder agentenbasierte Ausführungsschleifen unkontrolliert wachsen.
- ✗ Agentic AI nicht auf fragmentierten oder unzureichend gesteuerten Datenlandschaften einsetzen und gleichzeitig konsistente, vertrauenswürdige Ergebnisse erwarten.
- ✗ Keine fehlerhaften Prozesse automatisieren oder Agenten lediglich auf bestehende Ineffizienzen aufsetzen.
- ✗ Keine unkontrollierte Autonomie zulassen und keine unklaren Verantwortlichkeiten für Ergebnisse oder Fehlverhalten akzeptieren.
- ✗ Sich nicht auf spontane Punkt-zu-Punkt-Interaktionen verlassen, die Koordinationsprobleme, doppelte Verarbeitung oder unbemerkte Fehler verursachen.
- ✗ Governance, Sicherheit und Compliance nicht auf spätere Projektphasen verschieben.
- ✗ Nicht vorschnell zu vollständig autonomen Betriebsmodellen wechseln und den notwendigen organisatorischen Wandel hin zu einer lernenden Organisation unterschätzen.
- ✗ Nicht davon ausgehen, dass allgemeine Schutzmechanismen für Generative KI ausreichen, um autonome Agenten mit Schreibzugriffen sicher zu betreiben. Agentic AI erfordert eigene Governance-, Sicherheits- und Kontrollmechanismen.

Governance, Sicherheit und Souveränität auf Unternehmensebene

Antworten auf die entscheidenden Fragen rund um Agentic AI – ein disziplinierter Weg zur kontrollierten Autonomie

Unsere Vision: Agentic AI wird sich nicht als bloße Orchestrierungsschicht über großen Sprachmodellen durchsetzen. Sie muss vielmehr als produktionsreife Unternehmenssoftware entwickelt, betrieben und gesteuert werden, die zuverlässig innerhalb produktiver Geschäftssysteme arbeitet. Die in diesem Whitepaper beschriebenen Fragestellungen sind keine theoretischen Überlegungen. Sie spiegeln reale Fehlerszenarien wider, mit denen Unternehmen konfrontiert werden, sobald sie den Schritt von Pilotprojekten in den produktiven Betrieb vollziehen. Die Agentic AI Lösungen von Atos wurden entwickelt, um genau diese Herausforderungen durch belastbare Architekturen, operative Disziplin und technisch durchsetzbare Kontrollmechanismen zu adressieren.



Identitäten, Zugriffssteuerung, Kontrolle und menschliche Aufsicht

Agenten arbeiten unter eindeutigen, nicht gemeinsam genutzten digitalen Identitäten und verfügen ausschließlich über klar definierte Berechtigungen. Der Zugriff auf Tools und Unternehmenssysteme erfolgt nach den Prinzipien einer Zero-Trust-Architektur. Berechtigungen werden zentral verwaltet, bei Bedarf zeitlich begrenzt (Just-in-Time Access) vergeben und können jederzeit in Echtzeit entzogen werden. Wege zur Ausweitung von Berechtigungen (Privilege Escalation) sind kontrolliert und vollständig audittierbar. Dadurch wird verhindert, dass Agenten ihre Befugnisse mit zunehmender Autonomie unbemerkt erweitern. Gleichzeitig lassen sich geschäftskritische Aktionen gezielt auf definierte Identitäten und Genehmigungsprozesse beschränken. Auch Ziele, Absichten und Handlungsgrenzen der Agenten werden eindeutig definiert und kontinuierlich überwacht. Änderungen an den Zielen eines Agenten unterliegen grundsätzlich einer menschlichen Freigabe. Ergänzend sorgen vertrauensbasierte Eskalationsmechanismen (Confidence-based Escalation) dafür, dass Agenten nicht unbemerkt von der ursprünglich vorgesehenen geschäftlichen Zielsetzung abweichen.



Datenqualität und Souveränität per Design

Agenten arbeiten auf kuratierten, kontrollierten und vertrauenswürdigen Datensätzen mit klar geregelten Verantwortlichkeiten und einem definierten Lebenszyklusmanagement. Bereits vor der Inbetriebnahme werden Datenqualität, Herkunft (Data Provenance), Anforderungen an die digitale Souveränität sowie Datenschutzvorgaben bewertet und anschließend kontinuierlich überwacht. So wird sichergestellt, dass autonome Systeme nicht inkonsistente, veraltete oder nicht vertrauenswürdige Informationen verstärken oder unkontrolliert weiterverarbeiten.



Orchestrierung und Architektur im großen Maßstab

Atos stellt eine dedizierte Orchestrierungsebene sowie Referenzarchitekturen bereit, einschließlich sicherer Zero-Trust Multi Context Protocol (MCP)-Server, um die Zusammenarbeit zwischen Agenten, Unternehmenssystemen und Menschen zuverlässig zu steuern. Zustandsinformationen, Übergaben zwischen Agenten, Eskalationslogiken und Wiederherstellungsmechanismen werden explizit entwickelt und umgesetzt, einschließlich deterministischer Rollback-Verfahren, Notabschaltungen (Kill-Switch) und kontrolliertem Neustart von Agenten und kompletten Arbeitsabläufen. Dadurch werden fragile Punkt-zu-Punkt-Integrationen vermieden und ein vorhersehbares Verhalten im großen Maßstab ermöglicht.



Sicherheit über den gesamten Workflow hinweg – mit einer abgesicherten Agentic-Lieferkette

Atos entwickelt agentenbasierte Workflows als verteilte Systeme, deren Orchestrierung, Zustandsverwaltung und Fehlerbehandlung von Beginn an explizit definiert werden. Sicherheitsmaßnahmen wie der Schutz vor Prompt Injection, Eingabevalidierung, Speicherisolation sowie Einschränkungen bei der Tool-Nutzung werden auf Ebene des gesamten Workflows umgesetzt – nicht nur auf Ebene des Sprachmodells. Diese Schutzmechanismen umfassen die vollständige Verarbeitungskette: Eingaben, Retrieval-Prozesse, Arbeitsspeicher, Koordination zwischen Agenten, sowie die Ausführung externer Tools. Architektonische Sicherheitsmechanismen sorgen dafür, Fehler zu isolieren und zu verhindern, dass sich Schwachstellen unkontrolliert über mehrere Agenten oder Systeme hinweg ausbreiten. Dies schließt ausdrücklich auch die Lieferkette von Agentic AI ein. Agenten von Drittanbietern, Partnerkomponenten, Modellabhängigkeiten und externe Werkzeuge werden wie produktive Softwarekomponenten behandelt: Sie werden geprüft, versioniert und unter Governance gestellt. Kontinuierliche Integritätsprüfungen verhindern, dass kompromittierte Komponenten in produktive Workflows gelangen.



Nachvollziehbarkeit, Verantwortlichkeit und Reaktionsfähigkeit

Jede Aktion eines Agenten ist vollständig beobachtbar und nachvollziehbar. Entscheidungen, Tool-Nutzung, Datenzugriffe und Ergebnisse werden so protokolliert, dass sie sowohl operative Analysen als auch regulatorische Berichtspflichten und Sicherheitsuntersuchungen unterstützen. Diese durchgängige Nachvollziehbarkeit bildet die Grundlage für eine wirksame Reaktionsfähigkeit. Sie ermöglicht eine schnelle Ursachenanalyse, kontrollierte Rollback-Verfahren sowie gezielte Eingriffe, sobald Anomalien, Richtlinienverstöße oder Fehlfunktionen erkannt werden. Dadurch können Unternehmen nicht nur nachvollziehen, **was** ein Agent getan hat, sondern auch **warum**, **auf welcher Grundlage** und **mit welchen Auswirkungen** eine Entscheidung getroffen wurde.



Kostendisziplin und wertgebundene Skalierung

AgentOps und FinOps werden von Anfang an implementiert und mit geschäftlichen Kennzahlen verknüpft. Die Betriebskosten von Agenten werden kontinuierlich mit KPIs verknüpft, wie Durchlaufzeit, Cost-to-Serve, Durchsatz, Servicequalität und Geschäftsergebnissen und in Beziehung gesetzt, sodass mit zunehmender Autonomie jederzeit nachvollziehbar bleibt, welchen wirtschaftlichen Beitrag Agentic AI tatsächlich leistet. Echtzeitüberwachung und -kontrollen sind vor der Skalierung vorhanden, sodass Teams Budgets zuweisen und Ausgaben auf der richtigen Ebene (Feature, Workflow, Projekt, Programm, Geschäftseinheit) drosseln oder stoppen können. Wiederverwendbare, verwaltete Agenten werden kuratiert und über eine kontrollierte Bibliothek geteilt, was die Wiederverwendung statt Duplikation fördert, und Agenten-Sprawl verhindert, während die Zeit zur Wertschöpfung beschleunigt wird. Dies ermöglicht es Teams, Token-Verwendung, Toolaufrufe, Retries und Ausführungsschleifen zu steuern, während die Entscheidungsfreiheit erhalten bleibt und das Lock-in begrenzt wird.

Atos' Agentic AI Ansatz

Vom Bauplan zum industriellen Maßstab mit Atos Sovereign Agentic Studios

Atos' Ansatz für Agentic AI basiert auf einer einfachen Überzeugung: Die Skalierung von Agentic AI ist weit mehr als eine technologische Herausforderung. Ebenso entscheidend sind das Geschäftsmodell, das Betriebsmodell und die Menschen, die mit diesen Systemen arbeiten. Erfolgreiche Implementierungen folgen einem klaren Vorgehensmodell, das wir bei führenden Unternehmen beobachtet und in unserem eigenen Leistungsportfolio sowie unserer internen Transformation konsequent umgesetzt haben.

In der Praxis wird dieses Vorgehensmodell durch das Atos **Sovereign Agentic Studio** realisiert. Dabei handelt es sich um eine produktionsreife Plattform zum Entwickeln, Betreiben und Steuern agentenbasierter Systeme in realen Unternehmensumgebungen. Gleichzeitig beschleunigt sie die Wertschöpfung durch Agentic AI mithilfe einer mehrschichtigen Architektur. Der Aufbau folgt einer klaren Struktur:



Geschäftsinteraktion und Wertschöpfung bilden die oberste Ebene. Orchestrierung und Governance bilden den operativen Kern. Agentenintelligenz und Datenkontext stellen die fachliche Grundlage bereit. Souveränitätsfähige Infrastruktur bildet das technologische Fundament. **Auf diese Weise begleitet Atos Unternehmen beim Übergang von menschenzentrierten Betriebsmodellen hin zu einer AI-native-Unternehmensorganisation.**



Darüber hinaus verfolgen wir einen disziplinierten End-to-End-Ansatz für die Transformation der Arbeitsweise. Wir beginnen mit einem klar definierten geschäftlichen Nutzen und priorisierten End-to-End-Prozessen, gestalten diese konsequent nach einem AI-First-Ansatz neu, schaffen vertrauenswürdige und sichere Grundlagen und skalieren anschließend den Einsatz von Agentic AI kontrolliert und verantwortungsvoll.

Die folgende Abbildung fasst zusammen, wie Atos Unternehmen Schritt für Schritt von menschenzentrierten Betriebsmodellen hin zu einer AI-native-Unternehmensorganisation begleitet.

1 Nutzen & strategisches Mandat

Die Transformation mit Agentic AI beginnt mit der Identifizierung der Bereiche, in denen Autonomie die Unternehmensleistung nachhaltig verbessern kann. Gleichzeitig wird die Verantwortung auf Managementebene klar verankert und an messbare Geschäftsergebnisse gekoppelt

2 Prozesse und Workflows neu gestalten

Workflows müssen AI-first neu gestaltet werden, indem Entscheidungen und Aktionen von Anfang bis Ende zerlegt werden, anstatt Automatisierung auf fragmentierte Altprozesse zu lagern

3 Organisations- und Fähigkeitsmodell

Rollen, Entscheidungsbefugnisse und Kompetenzen müssen gezielt weiterentwickelt werden. Menschen wechseln dabei von der operativen Ausführung hin zur Orchestrierung, Überwachung und verantwortlichen Steuerung agentenbasierter Systeme

4 Governance und Betriebsmodell

Autonomie darf nur innerhalb klar definierter Steuerungs- und Kontrollstrukturen skaliert werden. Dazu gehören eindeutig festgelegte Human-in-the-Loop-Schwellenwerte, Mechanismen zur Überprüfung agentenbasierter Entscheidungen sowie eine kontinuierliche Überwachung von Leistung, Verhalten und Geschäftsergebnissen

5. Architektur- und Sourcing-Strategie

Unternehmen müssen bewusst entscheiden, welche Komponenten selbst entwickelt, welche eingekauft und welche gemeinsam mit Partnern bereitgestellt werden. Dies ist Grundlage für Interoperabilität, digitale Souveränität und eine skalierbare Orchestrierung über den gesamten Technologie-Stack hinweg

Atos-Beschleuniger

- Auswahlkriterien für Agentic AI
- Framework zur Priorisierung von Anwendungsfällen
- Bewertung der Datenbereitschaft für KI (AI Data Readiness Assessment)
- Digital Data Engineer
- Frictionless Operations
- Digital Engineer
- Knowledge Pilot



Executive Sponsoring über CEO, CTO und CHRO ist entscheidend für die nachhaltige Transformation

Nächste Schritte

Der Vorschlag für den Einstieg in die Umsetzung umfasst ein AI Readiness Assessment (Daten, Integrationen, Mitarbeitende, etc.)

Wie Atos dies in der Praxis umsetzt

Die Agentic AI Lösungen von Atos wurden als produktionsreife Plattform entwickelt, um autonome Agenten zu konzipieren, bereitzustellen und zu betreiben, die vollständige Geschäfts- und IT-Prozesse Ende zu Ende ausführen. Es baut auf den bestehenden Leistungsbausteinen von Atos auf. Dazu gehören unsere Digital Engineer-gestützten Managed Services, die Digital Transformation Engineer-gestützten Modernisierungslösungen, branchenspezifische Lösungen sowie die Atos Polaris Acceleration Platform. Die Plattform wurde für den Einsatz autonomer Agenten in produktiven Unternehmensumgebungen entwickelt – einschließlich regulierter, souveräner und geschäftskritischer Einsatzszenarien. Sie basiert auf neun zentralen Bausteinen, die gemeinsam die Grundlage für den sicheren, skalierbaren und produktionsreifen Einsatz von Agentic AI bilden:

1. Agentic launchpad

Atos beginnt jedes Vorhaben mit einer umfassenden Analyse der geschäftlichen und technologischen Ausgangssituation. Dabei werden der Reifegrad der Geschäftsprozesse, die Daten- und Anwendungslandschaft, die Integrationsfähigkeit bestehender Systeme, Anforderungen an die digitale Souveränität sowie die aktuelle Cyber-Risikolage bewertet. Ein zentraler Bestandteil ist das Agentic Readiness Assessment. Es kombiniert das Bewertungsmodell der Atos Group mit ausgewählten Partnerwerkzeugen, um den Reifegrad in den Bereichen Menschen, Prozesse, Daten, Architektur, Cybersecurity und Betriebsmodell systematisch zu bewerten.

Anschließend werden Geschäftsprozesse konsequent nach einem AI-First-Ansatz neu gestaltet. Ziel ist es, die Anwendungsfälle mit dem höchsten Geschäftsnutzen zu identifizieren, messbare Erfolgskriterien festzulegen und eine priorisierte Roadmap zu entwickeln – von kontrollierten Pilotprojekten bis hin zum produktiven Einsatz im großen Maßstab. Diese fundierte Analyse stellt sicher, dass das Atos Sovereign Agentic Studio von Beginn an auf Wertschöpfung ausgerichtet ist und in einer Umgebung eingeführt wird, die sich sicher steuern, absichern und nachhaltig betreiben lässt.

2. Souveränitätsfähige Build-and-Run-Umgebung

Atos stellt eine souveränitätsfähige Umgebung bereit, in der agentenbasierte Workflows entwickelt, getestet und betrieben werden können – unabhängig davon, ob sie auf Public-, Hybrid-, Private- oder souveränen Cloud- beziehungsweise KI-Infrastrukturen ausgeführt werden. Die Plattform kombiniert Low-Code-Werkzeuge für Prozessverantwortliche mit kuratierten Konnektoren zu bestehenden Unternehmenssystemen wie ERP-, CRM-, OT- oder Ticketing-Lösungen. Darüber hinaus ermöglicht sie den sicheren Zugriff auf unterschiedliche KI-Modelle und Werkzeuge, um Abhängigkeiten von einem einzelnen Technologie-Stack zu vermeiden. Für besonders sensible Anwendungsfälle können datenschutzwahrende Verschlüsselungstechnologien aktiviert werden, sodass vertrauliche Daten und Workloads während der gesamten Verarbeitung geschützt bleiben. Wo regulatorische oder organisatorische Anforderungen dies erfordern, unterstützt die Plattform außerdem On-Premises-, Private-Cloud-, Hybrid-Cloud- und souveräne Bereitstellungsmodelle, die Anforderungen an Datenresidenz und Compliance erfüllen.

3. Agenten-Orchestrierung und Referenzarchitektur

Atos entwirft und implementiert die Orchestrierungsebene auf Basis des Digital Engineer Autonomous Agentic Operations Frameworks, das es mehreren Agenten, Systemen und Menschen ermöglicht, zuverlässig und

maßstabsgetreu zusammenzuarbeiten. Dazu gehört die Definition von Referenzarchitekturen für agentische Systeme, Koordinationsmuster zwischen Agenten, Zustands- und Kontextmanagement, Fehlerbehandlung, Eskalationslogik und Human-in-the-Loop-Übergaben. Diese Architektur basiert auf einem **Reference Agent Framework**, das Rollen, Interaktionsmuster, Zustandsverwaltung und Abschlussbedingungen von Agenten standardisiert. Darüber hinaus nutzt es **MCP-konforme Kommunikationsmodelle (Model Context Protocol)**, um Interoperabilität und ein vorhersehbares Verhalten über unterschiedliche Agenten und Werkzeuge hinweg sicherzustellen. Die Orchestrierungsebene sorgt dafür, dass Agenten nicht als voneinander isolierte Komponenten arbeiten, sondern als Teil eines kontrollierten End-to-End-Systems mit klaren Verantwortlichkeiten und definierten Fehlerszenarien. Die **Atos Polaris AI Platform** stellt hierfür die grundlegenden Plattformdienste bereit – darunter gemeinsame Kontextdienste, die Nachverfolgung von Ausführungszuständen, vertrauensbasierte Eskalationsmechanismen sowie kontrollierte Wiederholungs- und Rollback-Verfahren. Sie kombiniert die nativen Fähigkeiten führender Hyperscaler mit ausgewählten Open-Source-Technologien zu einer vorintegrierten Plattform für sichere, skalierbare und zuverlässige Agenten-Orchestrierung.

4. Security- und Governance-Control-Plan

Atos stellt eine einheitliche Steuerungs- und Kontrollebene für Sicherheit und Governance bereit, über die agentenbasierte Systeme im produktiven Betrieb überwacht und gesteuert werden. Diese Kontrollebene setzt Sicherheitsrichtlinien und Governance-Vorgaben unmittelbar während der Laufzeit durch. Sie definiert eindeutig, welche Aktionen Agenten ausführen dürfen, unter welchen Bedingungen diese zulässig sind, welche Genehmigungen erforderlich sind, und welche Eskalations- und Freigabeprozesse gelten. Sie umfasst außerdem Laufzeit-Governance, verhaltensbasierte Sicherheitsmechanismen, Richtliniendurchsetzung, Observability, unveränderbare Audit-Protokolle sowie Funktionen zum sofortigen Entzug von Berechtigungen und zur Notabschaltung (Kill Switch). Dadurch wird sichergestellt, dass autonome Agenten ihre Aufgaben jederzeit innerhalb klar definierter technischer und organisatorischer Leitplanken ausführen – unabhängig von ihrer Komplexität oder dem eingesetzten KI-Modell.

5. MCP-Integrationsservices

Atos bietet umfassende Model Context Protocol (MCP)-Integrationsservices – von der Architektur und Implementierung über die Integration bis hin zum Betrieb im Unternehmensmaßstab. Die MCP-Integrationsservices bilden eine durchgängige Implementierungslösung, die KI-Modelle, Cloud-Plattformen, Daten und Unternehmenssysteme miteinander verbindet. Sie stellen sicher, dass MCP-basierte Services von Beginn an produktionsreif, sicher, resilient und unter klarer Governance betrieben werden können. Damit schaffen sie die Grundlage für eine sichere, kontrollierte und durchgängig gesteuerte Kommunikation zwischen Agenten über den gesamten End-to-End-Prozess hinweg.

6. KI-gestützte Application Modernization

Atos unterstützt Unternehmen bei der Modernisierung und Weiterentwicklung von Anwendungen im großen Maßstab – von teilweise automatisierten Verfahren bis hin zu nahtlosen, autonomen und intelligenten Services für die Transformation von Anwendungslandschaften. Der Digital Transformation Engineer ist eine Agentic-AI-gestützte Plattform, die autonome, zielorientierte KI-Agenten einsetzt, um die Analyse, Planung und Umsetzung von Anwendungsmodernisierungen deutlich zu vereinfachen und zu beschleunigen. Dabei kombiniert die Plattform die Präzision von Agentic AI mit der Sicherheit menschlicher Aufsicht und unterstützt Unternehmen auf ihrem Weg zu einem AI-gestützten Software Development Lifecycle (AI-SDLC).

7. AI Agents Marketplace

Kunden greifen auf eine kuratierte Bibliothek produktionsreifer Agenten zurück. Diese umfasst sowohl von der Atos Group entwickelte Agenten als auch Lösungen ausgewählter Technologiepartner sowie kundenspezifische Agenten. Die Bibliothek deckt horizontale und branchenspezifische Anwendungsfälle gleichermaßen ab. Jeder Agent verfügt über einen klar definierten Einsatzbereich, technische und fachliche Leitplanken, standardisierte Integrationsmuster sowie messbare Leistungskennzahlen. Dadurch verkürzt sich die Zeit bis zur Wertschöpfung erheblich, ohne Kompromisse bei Governance oder Kontrolle einzugehen. Gleichzeitig entsteht ein wiederverwendbares Portfolio, das individuelle Entwicklungen mit standardisierten Komponenten kombiniert und eine herstellerübergreifende

Orchestrierung ermöglicht, während digitale Souveränität, Verantwortlichkeit und Wahlfreiheit erhalten bleiben.

8. Prozess-Redesign, AgentOps und Change Management

Atos entwickelt gemeinsam mit Fachbereichen, IT, Risiko-, Personal- und Security-Teams neue, KI-gestützte Arbeitsabläufe. Diese werden anschließend mithilfe von AgentOps industrialisiert. Governance, Observability, Kostenkontrolle und Richtlinienmanagement werden dabei von Beginn an integriert. Gleichzeitig unterstützen wir Unternehmen beim Kompetenzaufbau ihrer Mitarbeitenden sowie bei der Entwicklung einer AI-First-Unternehmenskultur. So gelingt der schrittweise Übergang von menschengeführten Prozessen hin zu agentenorchestrierten Abläufen – wobei Menschen dort eingebunden bleiben, wo ihre Erfahrung und ihr Urteilsvermögen erforderlich sind. Der Grad der Autonomie wird ausschließlich dann erweitert, wenn Sicherheit, Auditierbarkeit und messbare Geschäftsergebnisse nachgewiesen sind.

9. Breites Partner-Ökosystem

Unser Liefermodell basiert auf einem breiten und kuratierten Partner-Ökosystem. Atos bietet plattformneutrale Orchestrierung über Hyperscaler, Modellanbieter und Unternehmenssysteme hinweg, um echte Entscheidungsfreiheit zu gewährleisten und sowohl auf der Orchestrierungs- als auch auf der Infrastrukturebene Lock-in zu vermeiden. Durch die Verbindung führender Hyperscaler, etablierter Unternehmensplattformen und innovativer Agentic-AI-Technologien kombiniert Atos leistungsfähige KI-Infrastrukturen mit den jeweils besten verfügbaren Agentenkomponenten. Wir unterstützen Public-, Hybrid-, Private- und souveräne Cloud-Umgebungen gleichermaßen. Dabei nutzen wir Hyperscaler für Skalierbarkeit und Rechenleistung, integrieren Agenten direkt in bestehende Geschäftsprozesse über Unternehmensplattformen und ergänzen diese durch spezialisierte Partner für Agenten-Frameworks, Orchestrierungsbeschleuniger und den Betrieb im großen Maßstab. Dieser ökosystembasierte Ansatz ermöglicht es Atos, Abhängigkeiten von einzelnen Anbietern zu vermeiden, für jeden Anwendungsfall die optimale Technologiekombination bereitzustellen und gleichzeitig eine einheitliche Steuerungs- und Kontrollebene für Governance, Sicherheit, Kostenmanagement und digitale Souveränität bereitzustellen.

Über die Technologie hinaus fungiert das Sovereign Agentic Studio als Motor für Co-Innovation und Orchestrierung. Es vereint angewandte Spitzenforschung, ausgewählte Start-ups und neue agentische Frameworks mit Plattformen auf Enterprise-Niveau und ermöglicht es Atos, agentische Lösungen schnell zu erproben, zusammenzustellen und zu industrialisieren, sodass sie für den skalierbaren Einsatz bereit sind.

Kunden profitieren von Innovationen, ohne die Kosten, Risiken und die Fragmentierung tragen zu müssen, die mit der eigenständigen Navigation durch dieses Ökosystem verbunden sind.

4. Agentic AI bereits im produktiven Einsatz

Eine Atos-Fallstudie

In den Bereichen IT-Betrieb, Software Engineering und Transformationsprogramme hat Atos die Pilotphase bereits hinter sich gelassen und agentenbasierte Systeme eingeführt, die unter klar definierten Sicherheits-, Governance- und Human-in-the-Loop-Vorgaben eigenständig vollständige Workflows übernehmen. Die folgenden Beispiele zeigen, wie wir die operative Umsetzung bereits heute neu gestalten und wie Unternehmen den Übergang von KI-gestützter Assistenz zu kontrollierter, orchestrierter Autonomie schrittweise vollziehen können.

FALLSTUDIE

Skalierung der Incident Resolution unter SLA-Druck mit Agentic-AI-basierten Digital Engineers (DE/DTE)

Geschäftliche Herausforderungen:

In großen, geschäftskritischen IT-Umgebungen ist das Incident Management zu einem strukturellen Leistungsengpass geworden. Mit steigender Release-Frequenz und zunehmend komplexen Systemlandschaften geraten Engineering-Teams durch wachsende Alarmvolumina, manuelle Triage-Prozesse und fragmentierte Diagnoseverfahren über verschiedene Tools hinweg zunehmend unter Druck.

Die Ursachenanalyse hängt dabei oft von individueller Expertise und implizitem Organisationswissen ab. Das führt zu uneinheitlichen Ergebnissen und erschwert eine nachhaltige Skalierung.

In diesem Umfeld liegt die **Mean Time to Repair (MTTR)** häufig bei drei bis vier Stunden. Gleichzeitig nehmen SLA-Verletzungen zu, während die Betriebskosten weiter steigen, da Unternehmen versuchen, die Belastung durch zusätzliche personelle Ressourcen zu kompensieren.

Atos' Lösung:

Gemeinsam mit dem Kunden hat Atos die Abläufe im Incident Management grundlegend neu gestaltet. Anstatt KI lediglich zur punktuellen Unterstützung von Engineering-Teams einzusetzen, wurde eine agentische Ausführungsebene eingeführt, die die Verantwortung für den Incident-Resolution-Prozess selbst übernimmt – innerhalb klar definierter Sicherheits-, Governance- und vertrauensbasierter Kontrollmechanismen.

Die Agentensysteme überwachen kontinuierlich Observability-Daten, korrelieren Warnmeldungen über Anwendungen und Infrastrukturebenen hinweg, analysieren aktuelle Deployments und Serviceabhängigkeiten und identifizieren mithilfe historischer Incident-Daten und betrieblicher Runbooks die wahrscheinlichsten Fehlerursachen. Erreicht die Analyse zuvor definierte Vertrauensschwellen (Confidence Thresholds), führen die Agenten freigegebene Gegenmaßnahmen automatisch aus – beispielsweise Neustarts von Diensten, Skalierungsmaßnahmen, Rollbacks oder das Aktivieren bzw. Deaktivieren von Feature Toggles. Bestehen Unsicherheiten, wird der Incident mit einer vollständigen Diagnose und konkreten Handlungsempfehlungen an einen Engineer eskaliert. Dadurch können sich Mitarbeitende auf komplexe Entscheidungen und Ausnahmesituationen konzentrieren, anstatt Zeit mit wiederkehrenden Analyseaufgaben zu verbringen. Der Übergang von einer reaktiven, menschengeführten Incident-Bearbeitung hin zu einer agentengesteuerten Ausführung führte im produktiven Betrieb zu messbaren Ergebnissen:

20-40%

geringere Mean Time To Repair (MTTR) durch schnellere Ursachenanalyse und automatisierte Fehlerbehebung

55-75%

der Incidents wurden unter vertrauensbasierten Kontrollmechanismen vollständig ohne menschliches Eingreifen bearbeitet

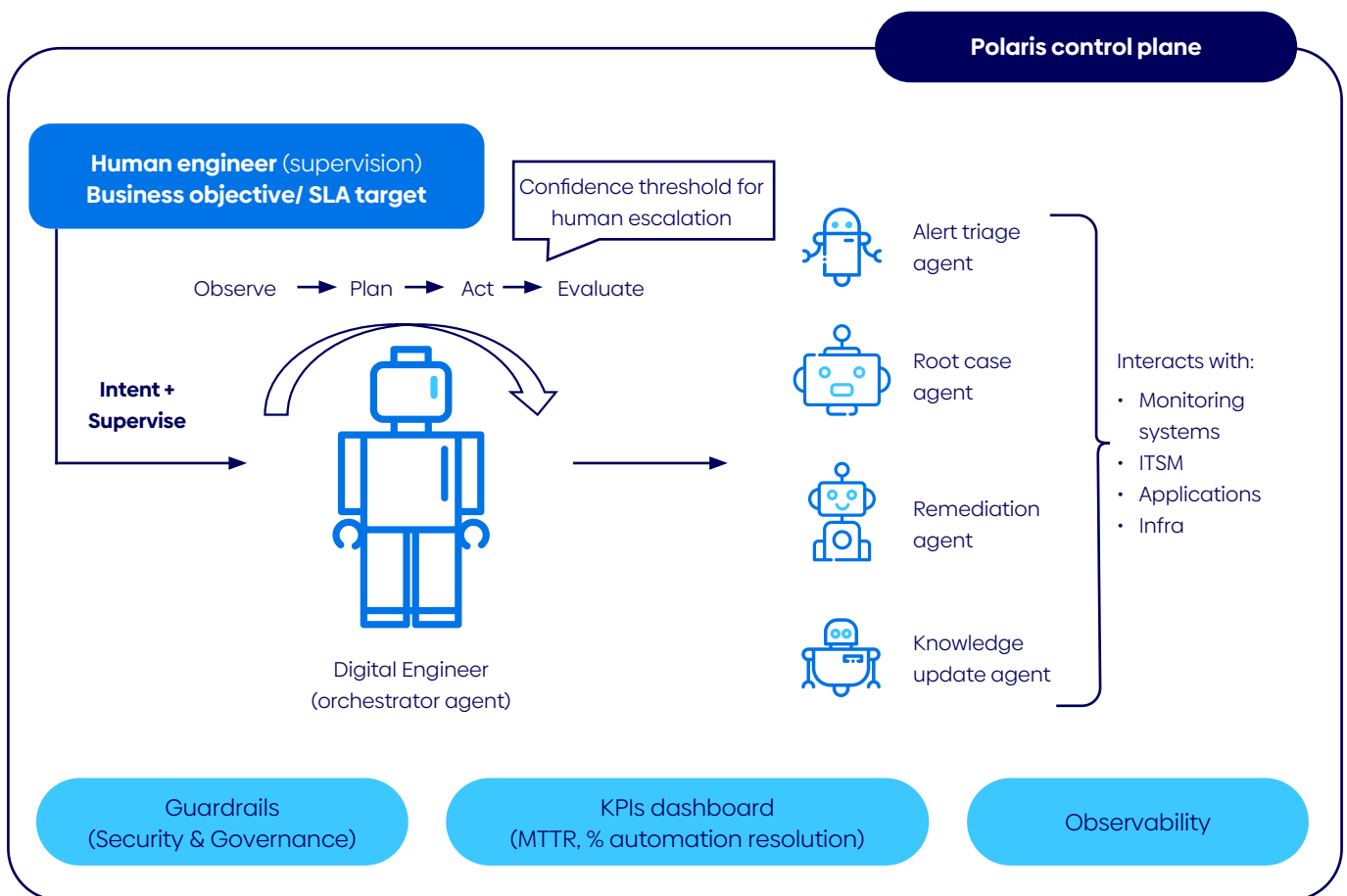
40-60%

Reduzierung des L1-/L2-Ticketvolumens, verbunden mit einer deutlichen Verringerung von Operational Noise und Alert Fatigue

20-35%

geringere Betriebskosten bei gleichzeitig höherer Servicequalität und besserer Einhaltung der vereinbarten Service Levels (SLAs)

Die erzielten Verbesserungen gingen weit über die reinen Kennzahlen hinaus. Das gesamte Betriebsmodell veränderte sich grundlegend. Engineers mussten sich nicht länger überwiegend mit reaktiver Fehlerbehebung beschäftigen. Stattdessen konnten sie sich auf die Überwachung autonomer Systeme, die kontinuierliche Optimierung von Abläufen sowie den gezielten Ausbau der Resilienz konzentrieren. Dieses Beispiel zeigt einen grundlegenden Wandel: Agentic AI ersetzt qualifizierte Fachkräfte nicht. Vielmehr übernimmt sie wiederkehrende operative Aufgaben und schafft Freiräume für Tätigkeiten, bei denen menschliches Urteilsvermögen, Erfahrung und Innovationskraft den größten Mehrwert liefern. Der Erfolg beruhte dabei nicht allein auf dem Einsatz von KI, sondern auf einer konsequenten Kombination aus Governance, Cybersecurity, vertrauensbasierten Entscheidungsmechanismen und einer klar definierten Zusammenarbeit zwischen Menschen und KI-Agenten. Gerade diese Kombination ermöglichte es, autonome Ausführung sicher in produktive Unternehmensumgebungen zu integrieren und gleichzeitig Transparenz, Nachvollziehbarkeit sowie die Einhaltung der vereinbarten Service Levels sicherzustellen. Die Fallstudie verdeutlicht, dass Agentic AI bereits heute messbaren geschäftlichen Nutzen liefern kann – vorausgesetzt, sie wird als produktionsreife Unternehmenssoftware entwickelt, gesteuert und betrieben und nicht lediglich als Technologieexperiment betrachtet.



Glossar

APIs: Schnittstellen, die es Softwaresystemen ermöglichen, Daten auszutauschen und Aktionen auszulösen

Agil: Ein iterativer Ansatz zur Entwicklung und Bereitstellung von Lösungen, der auf kurzen Entwicklungszyklen, regelmäßigem Feedback und kontinuierlicher Verbesserung basiert

FinOps: Praktiken zur Prognose, Verfolgung und Optimierung der Kosten für den Betrieb von KI-Agenten (Tokens, Tools, Infrastruktur)

Agentenorchestrierung: Die koordinierte Steuerung mehrerer Agenten, Tools und Systeme, um End-to-End-Workflows zuverlässig und kontrolliert auszuführen

Agentic AI: KI, die Agenten nutzt, um zu planen, zu entscheiden und mithilfe von Werkzeugen Aufgaben mit unterschiedlicher Autonomie zu erfüllen

AgentOps: Betriebsmodell zur sicheren Bereitstellung, Überwachung, Steuerung und Verbesserung von Agenten im Unternehmensmaßstab

Autonome Agenten: Softwareagenten, die Aktionen mit minimalem menschlichem Eingreifen innerhalb festgelegter Richtlinien ausführen können

Brownfield (Softwareentwicklung): Die Entwicklung, Modernisierung oder Erweiterung von Lösungen innerhalb bestehender, komplexer IT- und Anwendungslandschaften

CRM: Customer Relationship Management System, das zur Verwaltung von Vertrieb, Konten und Kundeninteraktionen verwendet wird

DevOps: Methoden, Prozesse und Werkzeuge, die Softwareentwicklung und IT-Betrieb verbinden, um Anwendungen kontinuierlich, zuverlässig und effizient bereitzustellen

ERP: Enterprise Resource Planning System, das Kernprozesse wie Finanzen, Beschaffung und Lieferkette betreibt

G&A: Gemeinkosten für zentrale Unternehmensfunktionen wie Finance, HR, Legal & Compliance und Unternehmenssteuerung

GenAI: Generative KI, die Inhalte (Text, Code, Bilder) aus Eingabeaufforderungen und Kontext erzeugt

Hyperscaler: Globale Cloud-Anbieter, die hochskalierbare Rechen-, Speicher- und Plattfordmdienste bereitstellen, beispielsweise Microsoft Azure, Amazon Web Services (AWS) oder Google Cloud Platform (GCP)

Infrastruktur-Stack: Gesamtheit der technischen Ebenen, auf denen Anwendungen betrieben werden – einschließlich Rechenleistung, Speicher, Netzwerke, Plattformen und Laufzeitumgebungen

Kill Switches: Kontrollmechanismen, mit denen ein Agent oder ein Workflow sofort gestoppt werden kann, sobald Risiken, unerwünschtes Verhalten oder Fehlfunktionen erkannt werden

LLM: Ein Large Language Model (LLM) ist ein KI-Modell, das auf sehr großen Mengen von Texten – und teilweise auch Code, Bildern oder Audiodaten – trainiert wurde, um Sprache zu verstehen und zu generieren. In der Praxis kann ein LLM Eingaben interpretieren, Fragen beantworten, Inhalte zusammenfassen, Texte erstellen, übersetzen sowie Aufgaben durch schrittweise Verarbeitung und Generierung von Sprache bearbeiten

MCP: Model Context Protocol ist ein offenes Protokoll, das standardisiert, wie eine KI-App (ein "LLM-Client/Host") sich über MCP-Server mit externen Tools und Datenquellen verbindet, sodass das Modell Live-Kontext abrufen und Dinge wie das Ausführen eines Tools, eine Systemabfrage oder das Abrufen einer Datei/Ressource auf konsistente Weise tun kann

Missionskritische Kontexte: Systeme und Abläufe, die zuverlässig mit strengen Anforderungen an Resilienz und Compliance laufen müssen

MTTR (Mean Time To Restore/Repair): Mittlere Zeit zur Wiederherstellung/Reparatur, durchschnittliche Zeit zur Wiederherstellung des Dienstes nach einem Vorfall

Orchestrierungsschicht: Die Laufzeit, die Aufgaben routet, den Zustand verwaltet, Richtlinien durchsetzt und Werkzeuge/Systeme integriert

OT (Operational Technology): Betriebstechnologie, Industrie-/Steuerungssysteme, die physische Geräte und Prozesse überwachen oder steuern

Referenzagenten: Standardisierte, wiederverwendbare Agentenmuster/Vorlagen mit definiertem Umfang, Kontrollen und KPIs

Service as a software: Bereitstellung eines operativen Services hauptsächlich durch Softwareautomatisierung statt manuellen Aufwands

Souveränität: Anforderungen, die sicherstellen, dass Daten, Modelle, Entscheidungen und Betriebsprozesse unter einer definierten nationalen, regulatorischen oder organisatorischen Kontrolle verbleiben

Token: Eine Texteinheit, die von einem LLM verarbeitet wird und zur Messung von Nutzung und Kosten verwendet wird



Lassen Sie uns ins Gespräch kommen!

Mit der zunehmenden Verbreitung von Agentic AI werden diejenigen Organisationen erfolgreich sein, die Autonomie und Kontrolle gleichermaßen beherrschen. Dafür müssen agentische Systeme von Anfang an als Produktionssoftware verstanden und betrieben werden – mit einer Governance-First-Architektur, Zero-Trust-Zugriff, verhaltensbasierter Sicherheit, umfassender Auditierbarkeit und konsequenter Kostendisziplin.

Das Atos Sovereign Agentic Studio schafft die industrielle Grundlage, um genau dies auch in regulierten und missionskritischen Umgebungen zu ermöglichen. Es unterstützt Unternehmen dabei, Souveränität, Transparenz und technologische Entscheidungsfreiheit zu bewahren und gleichzeitig messbare Geschäftsergebnisse zu erzielen.

Gemeinsam mit Ihnen identifizieren wir einen wertstiftenden End-to-End-Workflow, bewerten die Datenreife, definieren Entscheidungsrechte und Human-in-the-Loop-Prozesse, etablieren AgentOps- und FinOps-Mechanismen und setzen einen produktionsnahen Piloten mit umfassender Observability, Rollback-Fähigkeiten und Kill-Switch-Kontrollen auf. Anschließend skalieren wir gezielt die Ansätze, die ihren Mehrwert in der Praxis nachgewiesen haben.

Nächster Schritt: Sprechen Sie mit Atos darüber, wie Sie einen geeigneten Value Stream identifizieren und die erforderliche Kontroll- und Governance-Ebene aufbauen können, um Agentic AI sicher, souverän und skalierbar in Ihrem Unternehmen einzusetzen.

Nehmen Sie Kontakt auf unter:
agenticaai@atos.ai

Die Tech-Ambition der Atos Group

Die Strategie der Atos Group basiert auf drei eng miteinander verknüpften Prioritäten: Agentic AI für Mission-Critical-Umgebungen, digitaler Souveränität und Security. Gemeinsam schaffen sie die Voraussetzungen dafür, dass Organisationen mit Zuversicht innovieren, die Kontrolle über ihre kritischen digitalen Assets bewahren und in einer zunehmend komplexen Welt sicher agieren können. Getragen wird dieser Anspruch durch die komplementären Stärken von Atos, Atos Amplify und Eviden.

Atos

Atos ist die Marke der Atos Group für KI-gestützte, sichere und ganzheitliche digitale Services. Atos entwirft, entwickelt und betreibt kritische digitale Umgebungen, die Leistungsfähigkeit, Ausfallsicherheit und Souveränität fördern. So unterstützt Atos öffentliche und private Organisationen weltweit dabei, die Kontrolle über ihre Daten und IT-Infrastrukturen zu bewahren und gleichzeitig regulatorische Anforderungen zu erfüllen.

Atos unterstützt Kunden bei der Modernisierung ihrer zentralen IT-Systeme, der Beschleunigung ihrer Cloud- und Datentransformation, der Stärkung ihrer Cybersicherheit sowie der Bereitstellung sicherer digitaler Arbeitsplatzlösungen.

Als vertrauenswürdiger Partner beim Betrieb komplexer und geschäftskritischer Umgebungen unterstützt Atos Organisationen in stark regulierten und souveränen Kontexten.

atos.ai



Atos Amplify ist die auf KI ausgerichtete Consulting- und Advisory-Einheit der Atos Group. Sie unterstützt Organisationen dabei, strategisch wichtige Entscheidungen zu treffen und diese in messbare Geschäftsergebnisse zu überführen.

Durch die Verbindung von tiefem Branchenwissen, unternehmerischem Verständnis und KI-getriebener Innovation arbeitet Atos Amplify gemeinsam mit seinen Kunden daran, Transformationsstrategien zu entwickeln, die Einführung neuer Technologien zu beschleunigen und Mehrwert aus Daten, KI und digitalen Plattformen zu erschließen. Der Consult-to-Build-Ansatz verbindet Strategie und Umsetzung und unterstützt Organisationen dabei, Komplexität zu bewältigen, digitale Souveränität zu stärken, ihre Resilienz zu erhöhen und nachhaltiges Wachstum zu fördern.

Auf Grundlage menschenzentrierter Werte und verantwortungsvoller KI-Prinzipien ermöglicht Atos Amplify Organisationen, Transformation mit Vertrauen, Transparenz und Verantwortlichkeit zu gestalten.

atos.ai/atos-amplify

EVIDEN

Eviden ist die Marke der Atos Group mit Schwerpunkt auf Cybersecurity-Produkten, Mission-Critical Systemen und Vision AI.

Als vertrauenswürdiger Partner für Organisationen im öffentlichen und privaten Sektor setzt Eviden fortschrittliche Analysefähigkeiten ein und unterstützt seine Kunden dabei, die Widerstandsfähigkeit, Kontinuität und Resilienz ihrer Betriebsabläufe sicherzustellen.

Das Portfolio kombiniert fortschrittliche Cybersecurity-Technologien, Lösungen für digitale Identitäten, Fähigkeiten zum Schutz von Daten sowie Mission-Critical Systeme für besonders anspruchsvolle Einsatzumgebungen mit KI-gestützten Echtzeit-Monitoring- und Analysefähigkeiten.

Mit mehr als 2.200 Expertinnen und Experten sowie über 720 Patenten trägt Eviden dazu bei, Menschen, Daten und kritische Infrastrukturen weltweit zu schützen – an der Schnittstelle von Intelligenz, Souveränität und Vertrauen.

eviden.com

Über Atos Group

Die [Atos Group](#) ist ein weltweit führender Anbieter im Bereich der digitalen Transformation. Mit ca. 56.000 Mitarbeitenden und einem Jahresumsatz von ca. 7,2 Mrd. EUR (auf Basis des künftigen Unternehmenszuschnitts) agiert das Unternehmen in 54 Ländern unter zwei Marken: Atos für Services und Eviden für Produkte und Systeme. Als europäische Nummer eins in der Cybersicherheit und führend im Bereich Cloud arbeitet die Atos Group für eine sichere und dekarbonisierte Zukunft und bietet maßgeschneiderte KI-gestützte End-to-End Lösungen für alle Branchen. Atos Group ist an der Euronext Paris notiert.

Erfahren Sie mehr über uns
[atos.ai](#)

Beginnen Sie das Gespräch mit uns



Atos Group ist eine eingetragene Marke der Atos Group. © Atos Group. Vertrauliche Informationen, die der Atos Group gehören und nur vom Empfänger verwendet werden dürfen. Dieses Dokument oder ein Teil davon darf ohne vorherige schriftliche Genehmigung der Atos Group nicht reproduziert, kopiert, verbreitet und/oder verteilt oder zitiert werden.

107924 - EM + HC - AGENTIC-AI

The Atos logo is displayed in a large, bold, blue font. The letters 'A', 't', 'o', and 's' are connected, with the 't' and 'o' having a unique, stylized shape.