Gartner

Die 10 wichtigsten strategischen Technologie-trends 2026

Navigieren durch eine KI-gesteuerte, hypervernetzte Welt

Die Technologieführer werden 2026 mit einem entscheidenden Jahr konfrontiert werden, in dem Disruption, Innovation und Risiko sich mit beispielloser Geschwindigkeit beschleunigen werden. Die Top 10 der strategischen Technologietrends für 2026 von Gartner sind mehr als nur Technologiewandel – sie sind Katalysatoren für Unternehmenstransformation, die eine Reaktion auf der Geschäftsführungsebene erfordern.

Die diesjährigen Trends spiegeln die Realitäten einer KI-gesteuerten, hypervernetzten Welt wider, in der eine einzelne Fähigkeit nicht ausreicht. Sie sind in drei Themenbereiche aufgegliedert, die definieren, wie führende Unternehmen innovieren, im Wettbewerb bestehen und Werte schützen werden:

Der Architekt

Baut sichere, skalierbare und anpassungsfähige digitale Fundamente mit KI-nativen Entwicklungsplattformen, KI-Supercomputing und Confidential Computing auf.

Der Synthetiker

Orchestriert diverse Technologien – von Multiagenten-Systemen bis hin zu domänenspezifischen Sprachmodellen und physischer KI – zur Erschließung neuer Wertschöpfungsquellen.

Der Vorreiter

Erhöht Vertrauen, Governance und Sicherheit mit präventiver Cybersicherheit, digitaler Herkunft, KI-Sicherheitsplattformen und Geopatriation.

Berücksichtigen Sie bei der Erkundung dieser Trends, wie sie mit den strategischen Ambitionen Ihres Unternehmens übereinstimmen und wie sie in Ihre Planung integriert werden können, um nachhaltiges Wachstum und einen Wettbewerbsvorteil zu erlangen.

Gene Alvarez
Distinguished Vice President,
Business and Technology Insights, Gartner

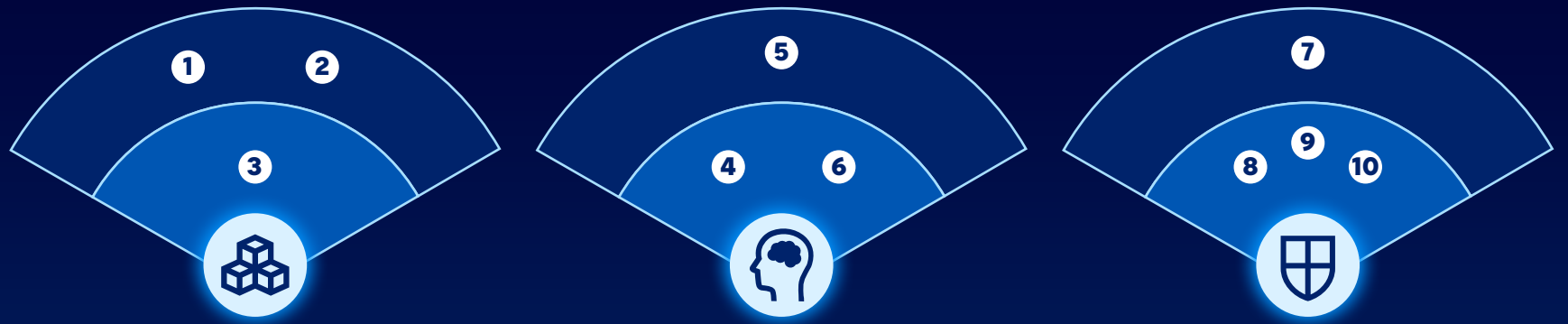
Die wichtigsten strategischen Technologietrends von Gartner für 2026

Gartner hat diese 10 Trends sorgfältig auf Basis ihres Potenzials für das Vorantreiben von Innovation, die Stärkung von Resilienz und die Steigerung des Vertrauens in einer KI-gesteuerten, hypervernetzten Welt ausgewählt.

Sie stellen strategische Imperative dar, die durchdachte Überlegungen und entschlossenes Handeln von den Technologieführern erfordern.

Jetzt
1 bis 3 Jahre

Bald
3 bis 5 Jahre



Der Architekt

1. KI-native Entwicklungsplattformen
2. KI-Supercomputing-Plattformen
3. Confidential Computing

Der Synthetiker

4. Multiagenten-Systeme
5. Domänenspezifische Sprachmodelle
6. Physische KI

Der Vorreiter

7. Präventive Cybersicherheit
8. Digitale Herkunft
9. KI-Sicherheitsplattformen
10. Geopatriation

Der Architekt

Baut sichere, skalierbare und anpassungsfähige digitale Fundamente auf.

Zum Beschleunigen von Innovation und Resilienz müssen Technologieführer Plattformen und Infrastruktur modernisieren. Der Architekt richtet den Fokus auf den Aufbau KI-bereiter Fundamente, die Geschwindigkeit, Sicherheit und Skalierbarkeit ermöglichen. Dies ist entscheidend, um in einer KI-gesteuerten, hypervernetzten Welt erfolgreich zu sein.

1

KI-native Entwicklungs-plattformen

Worum geht's?
KI-native Entwicklungsplattformen nutzen generative KI, um Software schneller und einfacher als je zuvor zu entwickeln. Diese Plattformen reichen von „One Shot"-Tools, die Software auf einen einzigen Befehl hin erzeugen, über „Vibe Coding"-Tools, die eine Softwareentwicklung ohne profunde technische Kenntnisse ermöglichen, bis hin zu KI-Agenten, die zusammen orchestriert werden, um Software zu entwickeln.

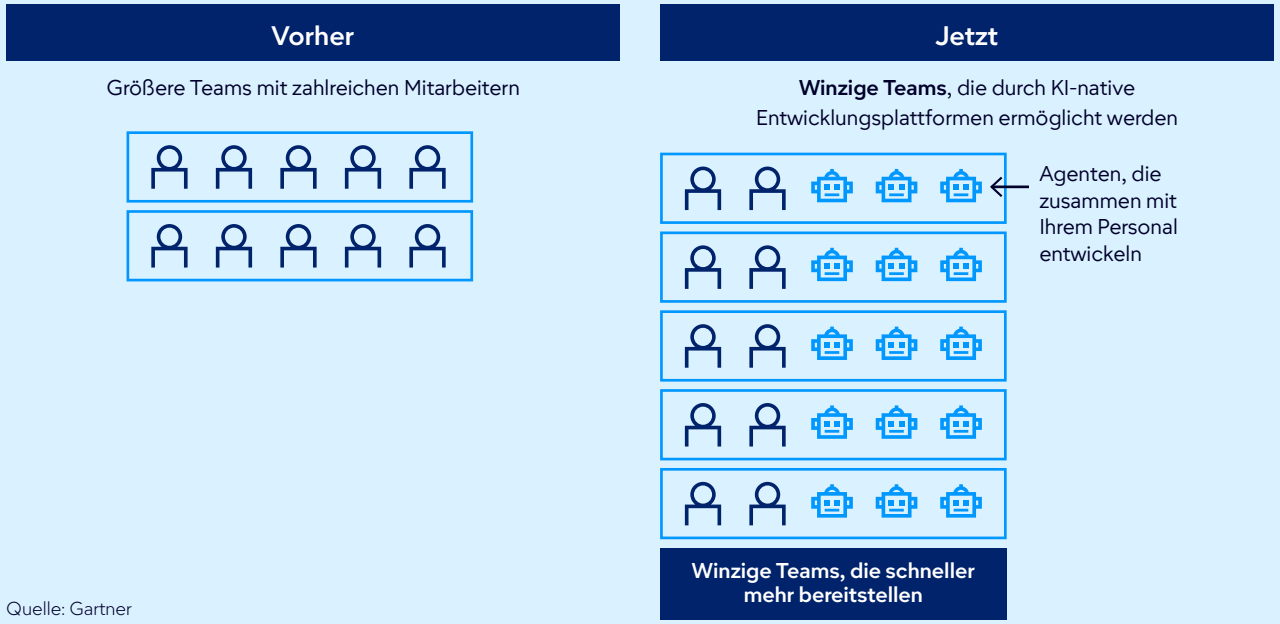
Gründe für diesen Trend
CIOs sind begeistert von schnellerer Softwareverfügbarkeit und Produktivitätssteigerungen, während CEOs und CFOs das Potenzial für Kosteneinsparungen sehen. KI-native Entwicklungsplattformen ermöglichen „winzigen Teams", mehr Anwendungen mit denselben Ressourcen zu entwickeln – wobei beispielsweise fünf Zweier-Teams in die Lage versetzt werden, fünf Anwendungen auf einmal bereitzustellen. Dieser Trend hilft CIOs bei der Bewältigung von Rückständen und verschiebt die „Entwickeln vs. Kaufen"-Gleichung in Richtung Entwickeln.

Was kommt als Nächstes?

80 % der Unternehmen werden bis 2030 große Teams für Software-Engineering in kleinere, KI-gestützte Teams umwandeln.

40 % der Anwendungsportfolios der Unternehmen werden bis 2030 maßgeschneiderte Anwendungen beinhalten, die unter Verwendung KI-nativer Plattformen entwickelt wurden (von 2 % im Jahr 2025).

Winzige Teams



Quelle: Gartner

1

Erzielen von Ergebnissen mit KI-nativen Entwicklungsplattformen

Aktionsplan zur Steigerung der Geschwindigkeit, zum Einsparen von Kosten und zur Förderung von Innovation

Schritte	1 Einrichtung eines Plattformteams	2 Implementierung von Sicherheitsvorkehrungen	3 Durchführung von Pilotprojekten zur KI-nativen Entwicklung	4 Übernahme eines KI-orientierten Mindsets	5 Weiterbildung und Befähigung von Teams
Erwartetes Ergebnis	Zentralisierte Beaufsichtigung gewährleistet konsistente Standards und Governance.	Verringertes Risiko eines unsicheren oder nichtkonformen Codes.	Schnelle Erfolge, die den Wert demonstrieren und Vertrauen aufbauen.	Beschleunigte Bereitstellung und optimierte Innovationskapazität.	Breitere Akzeptanz und effektive Kooperation.
Aktion	Bildung eines speziellen Teams für die Verwaltung von KI-nativen Plattformen und ausgewählten KI-Modellen.	Integration von KI-Governance-Plattformen für Code-Überprüfung und Compliance-Prüfungen.	Einführung von Projekten mit geringem Risiko, um die Produktivitätssteigerungen zu validieren.	Priorisierung von KI-nativen Tools für neue Entwicklungsinitiativen.	Schulung von Entwicklern und Geschäftspartnern in Prompt Engineering und Governance.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Partner: Definition einer KI-orientierten Strategie und eines Governance-Frameworks.

Kooperieren: Abstimmung der Plattformfähigkeiten mit den Unternehmensprioritäten.

Führen: Gewährleistung von Compliance- und Sicherheitsvorkehrungen für eine KI-native Entwicklung.

IT-Partner

Platform Engineering: Verwaltung von KI-nativen Tools, Integrationen und Leistung.

Sicherheit: Implementierung von KI-Governance für Code-Prüfung und Risikomanagement.

Beschaffung: Bewertung und Auswahl von Anbietern und Services für KI-native Plattformen.

Geschäftspartner

Produktinhaber: Bereitstellung von Domänenexpertise und Validierung von KI-gesteuerten Lösungen.

Finance: Abstimmung von Finanzierungsmodellen zur Unterstützung von KI-nativen Entwicklungsinitiativen.

2

KI-Supercomputing-Plattformen

Worum geht's?
KI-Supercomputing-Plattformen bieten die enorme Rechenleistung, die für das Training und den Betrieb fortschrittlicher KI-Modelle erforderlich ist. Diese Systeme kombinieren Hochleistungsrechner (High-Performance Computing, HPC), spezialisierte Prozessoren und skalierbare Architekturen zur Bewältigung datenintensiver Workloads.

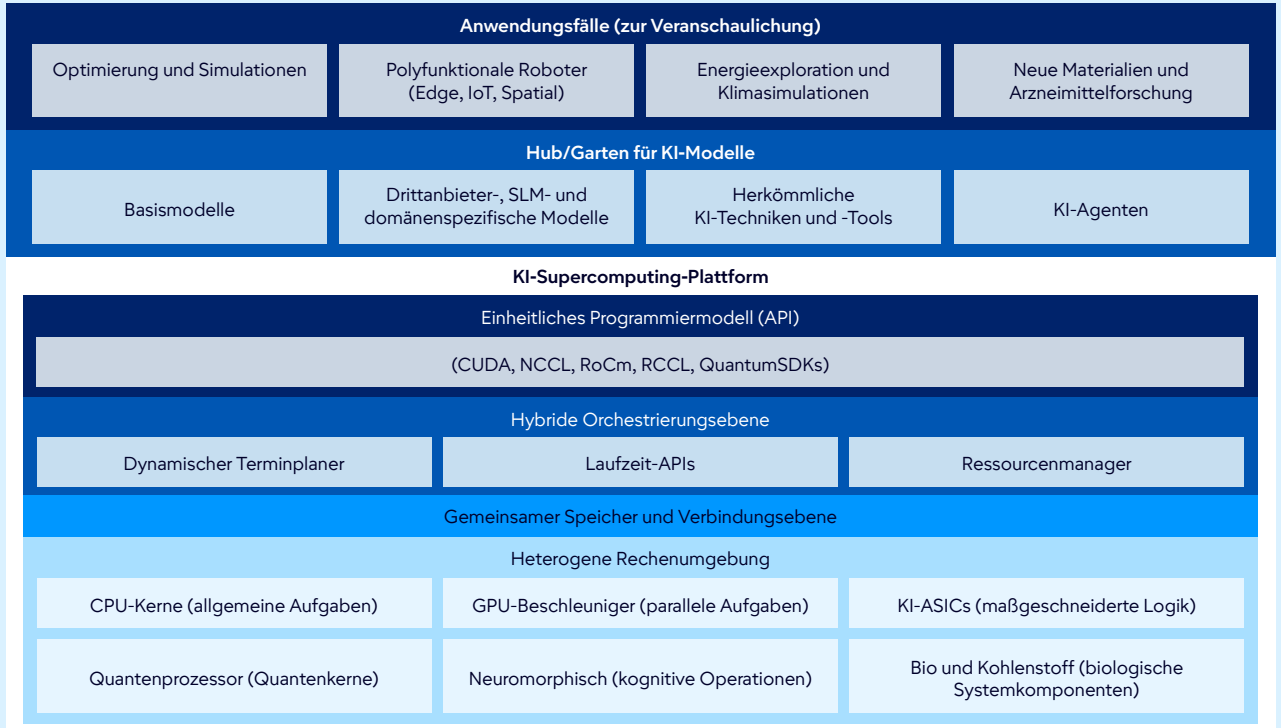
Gründe für diesen Trend
Die Nachfrage nach KI-Supercomputing steigt rapide an, da Unternehmen immer größere und komplexere Modelle entwickeln, die die Grenzen herkömmlicher Infrastrukturen überschreiten.

Was kommt als Nächstes?

40 % der Unternehmen werden bis 2028 hybride Computing-Architekturen einführen (gegenüber 8 % heute).

Über 20 Anbieter werden unter Verwendung von Supercomputing-Umgebungen bis 2028 einheitliche Entwicklerplattformen anbieten.

KI-Supercomputing-Plattform



Quelle: Gartner

2

Erzielen von Ergebnissen mit KI-Supercomputing-Plattformen

Aktionsplan zur Freisetzung enormer Verarbeitungsleistung

Schritte	1 Identifizierung von Workloads mit hoher Auswirkung	2 Investitionen in einheitliche Software-Stacks	3 Entwicklung einer schrittweisen Integrationsstrategie	4 Optimierung der Entwicklung über verschiedene Umgebungen hinweg	5 Einplanung von Governance und Compliance
Erwartetes Ergebnis	Demonstration von Wert und Entwicklung interner Fachkompetenz.	Vereinfachte Integration und flexible Workload-Platzierung.	Zukunftsfähige Infrastruktur und Belegschaft.	Beschleunigte Bereitstellung und reduzierte Reibung.	Geringeres Risiko und verbesserte Aufsicht.
Aktion	Durchführung von Pilotprojekten unter Verwendung hybrider Orchestrierung.	Einführung offener Standards in bestehende und neue Systeme.	Schrittweise Einführung neuer Rechenparadigmen und Schulung des IT-Personals.	Ermutigung von Teams zur Einführung hybrider Plattformen und zusammensetzbarer Architekturen.	Entwicklung von Sicherheits- und Compliance-Strategien auf Systemebene.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer hybriden Orchestrierungsstrategie, die auf die geschäftlichen Prioritäten abgestimmt ist.

Sicherstellung der Governance für Workload-Platzierung, -Sicherheit und -Compliance.

Zusammenarbeit mit Unternehmensleitern, um Workloads mit hoher Wirkung zu priorisieren.

IT-Partner

Infrastruktur und Operations: Integration neuer Beschleuniger in bestehende Systeme.

Sicherheit: Implementierung von Governance für Multiarchitektur-Umgebungen.

DevOps: Einführung einheitlicher Software-Stacks und Orchestrierungstools.

Geschäftspartner

Produkt: Identifizierung von Anwendungsfällen für hybrides Computing (z. B. Simulationen, KI-gestützte Apps).

Finance: Abstimmung der Finanzierung auf Ziele der schrittweisen Integration und Nachhaltigkeit.

Operations: Vorbereitung auf KI-gesteuerte Arbeitsabläufe in wichtigen Prozessen.

3

Confidential Computing

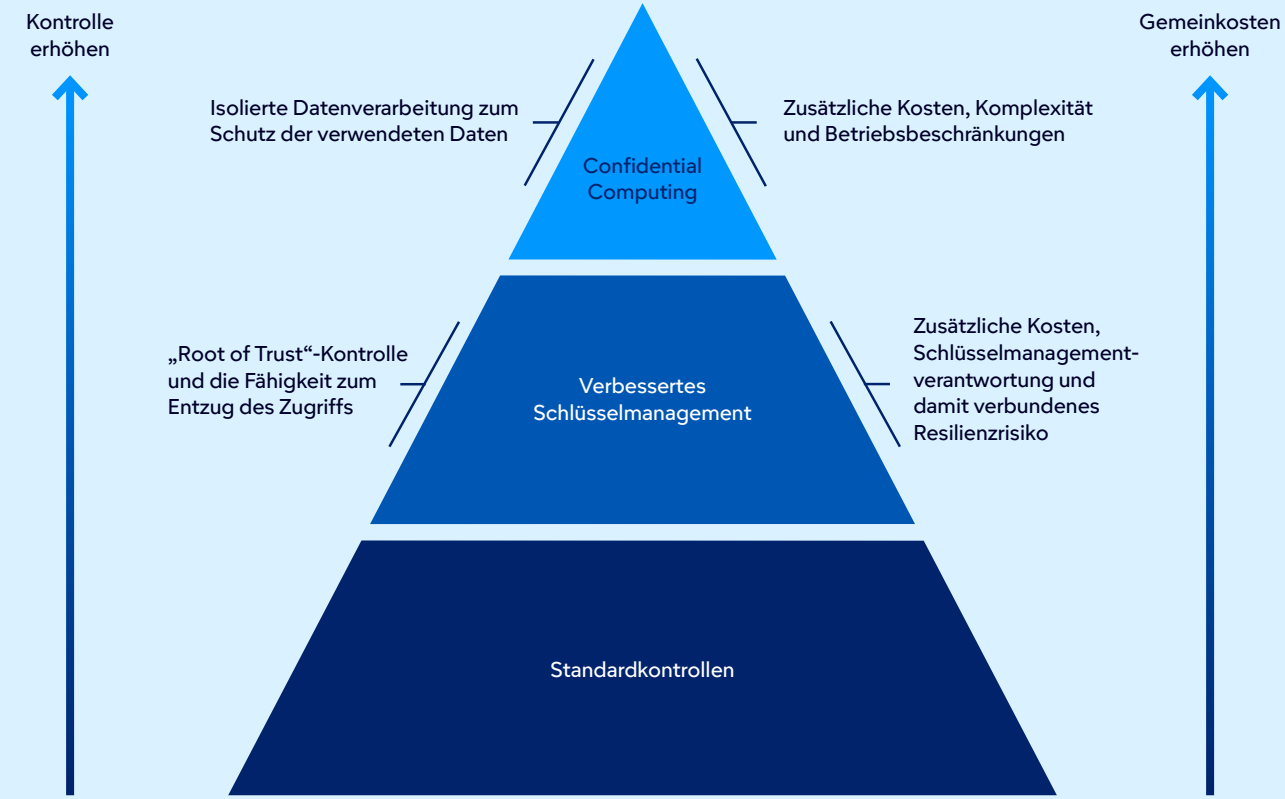
Worum geht's?
Confidential Computing nutzt hardwarebasierte vertrauenswürdige Ausführungsumgebungen (VAU) um Daten während ihrer Verarbeitung zu schützen und unbefugten Zugriff zu verhindern – selbst von Cloud-Anbietern.

Gründe für diesen Trend
Strengere Datenschutzgesetze, Vorschriften zur Datenlokalisierung und der Einsatz von KI machen den Schutz während der Nutzung unerlässlich. Confidential Computing ermöglicht sichere Cloud-Strategien und Compliance für sensible Workloads.

Was kommt als Nächstes?

75 % der Verarbeitung in nicht vertrauenswürdigen Infrastrukturen werden bis 2029 durch Confidential Computing gesichert sein.

Kontrollen zur Beschränkung des Zugriffs auf CSP-Daten



Quelle: Gartner

3

Erzielen von Ergebnissen mit Confidential Computing

Aktionsplan zur Sicherstellung einer ortsunabhängigen sicheren und konformen Datenverarbeitung

Schritte	1 Prüfung sensibler Workloads	2 Durchführung von Pilotprojekten zu VAU für KI-Modelle	3 Sicherstellung einer sicheren Zusammenarbeit	4 Einrichtung eines unabhängigen Schlüsselmanagements	5 Vorbereitung auf Integrationsherausforderungen
Erwartetes Ergebnis	Identifizierung der Stellen, an denen ein Schutz während der Nutzung erforderlich ist.	Stärkung der Vertraulichkeit und des Schutzes geistigen Eigentums.	Austausch von Insights ohne Offenlegung von Rohdaten.	Volle Kontrolle über den Datenzugriff.	Reibungslose Bereitstellung in allen Umgebungen.
Aktion	Abbildung von Workloads, die Datenschutz- oder Lokalisierungsvorschriften unterliegen.	Prüfung von VAU mit exklusiven und Open-Source-KI-Modellen.	Verwendung von Confidential Computing für Analytics- und BI-Projekte.	Implementierung von unternehmenseigenen kryptografischen Schlüsselsystemen.	Planung der Orchestrierung über mehrere Chipsätze und Anbieter hinweg.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer Strategie für Confidential Computing, die mit Datenschutz-, Compliance- und Cloud-Zielen im Einklang steht.

Zusammenarbeit mit Rechts- und Compliance-Teams, um Anforderungen hinsichtlich Datenlokalisierung und -hoheit zu erfüllen.

Überwachung der Governance für VAU und Sicherstellung der Integration in bestehende Sicherheitsframeworks.

IT-Partner

Infrastruktur und Operations: Bereitstellung von VAU in Hybrid- und Multicloud-Umgebungen.

Sicherheit: Implementierung von Beglaubigungsprozessen und kryptografischer Schlüsselverwaltung.

DevOps und Plattform: Anpassung der Workloads für Confidential Computing und Überwachung der Leistung.

Geschäftspartner

Compliance: Validierung der Einhaltung gesetzlicher Vorschriften und Audit-Bereitschaft.

Finance: Ausrichtung der Finanzierung für die Einführung von Confidential Computing und Risikominderung.

Dateninhaber: Identifizierung sensibler Workloads für den Schutz während der Nutzung und zur Priorisierung von Projekten.

Der Synthetiker

Orchestriert verschiedene Technologien für neue Werte.

Um neue Quellen der Differenzierung zu erschließen, müssen Technologieleiter spezialisierte Modelle, Multiagenten-Systeme und physische KI für domänenspezifische Lösungen integrieren. Die Trends des Synthetikers konzentrieren sich auf die Orchestrierung verschiedener Technologien zur Schaffung anpassungsfähiger, intelligenter Ökosysteme, die Innovationen in Arbeitsabläufen, Produkten und Erfahrungen vorantreiben.

4

Multiagenten-Systeme

Worum geht's?
Multiagenten-Systeme (Mulitagent Systems, MAS) verwenden Sammlungen spezialisierter KI-Agenten, die zusammenarbeiten, um komplexe Arbeitsabläufe zu erledigen. Jeder Agent übernimmt eine bestimmte Aufgabe, wodurch die Effizienz und Skalierbarkeit im Vergleich zu monolithischen KI-Lösungen verbessert wird.

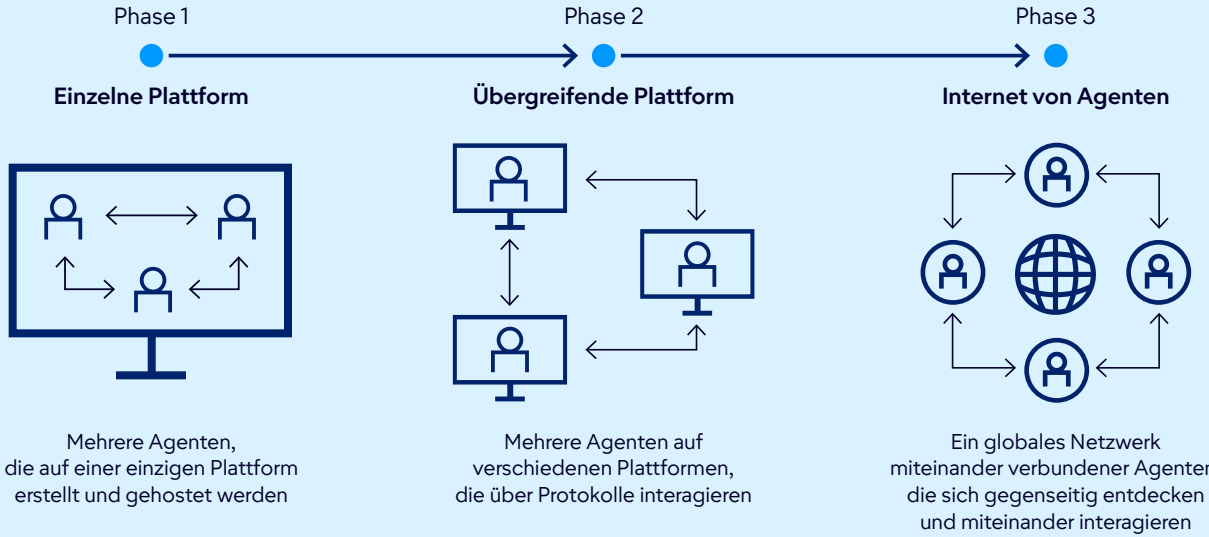
Gründe für diesen Trend
Während KI mit einem einzigen Agenten mit mehrstufigen Prozessen zu kämpfen hat, ermöglichen MAS eine modulare Automatisierung und plattformübergreifende Integration. Wir verzeichnen einen Anstieg der MAS-Anfragen um 1.445 % vom 1. Quartal 2024 bis zum 2. Quartal 2025, was auf ein rasch wachsendes Unternehmensinteresse hindeutet.

Was kommt als Nächstes?

70 % der MAS werden bis 2027 hochspezialisierte Agenten einsetzen, wodurch die Genauigkeit verbessert wird, aber die Komplexität der Koordination zunimmt.

60 % der MAS werden bis 2028 die Interoperabilität zwischen verschiedenen Anbietern unterstützen und so Innovation und Flexibilität fördern.

Die Entwicklung von Multiagenten-Systemen



Quelle: Gartner

4

Erzielung von Ergebnissen mit Multiagenten-Systemen

Aktionsplan zur Förderung modularer Automatisierung und nahtloser Integration

Schritte	1 Identifizierung hochwertiger Anwendungsfälle	2 Entwicklung modularer Agenten	3 Implementierung von Governance und Beobachtbarkeit	4 Einführung von Interoperabilitätsstandards	5 Weiterbildung von Teams
Erwartetes Ergebnis	Messbare Wirkung und schnellere Einführung.	Verbesserte Zuverlässigkeit und Skalierbarkeit.	Geringeres Risiko und bessere Kontrolle.	Zukunftssichere MAS-Investitionen.	Effektive Bereitstellung und Risikominderung.
Aktion	Einrichtung von klar definierten Arbeitsabläufen für MAS-Pilotprojekte.	Entwicklung von spezialisierten Agenten anstelle von monolithischen Lösungen.	Anwendung leistungsstarker API-Governance- und Monitoring-Tools.	Verwendung neuer Protokolle für die Zusammenarbeit zwischen Agenten verschiedener Anbieter.	Schulung der Mitarbeiter zu MAS-Frameworks und Change-Management.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer MAS-Strategie für hochwertige Arbeitsabläufe und Abstimmung mit den Geschäftsprioritäten.

Etablierung einer Governance für die Interoperabilität, Sicherheit und Compliance von Agenten.

Kommunikation von Change-Management-Plänen zur Beilegung der Bedenken der Belegschaft.

IT-Partner

Plattform und DevOps: Entwicklung modularer Agenten und Verwaltung von Orchestrierungstools.

Sicherheit: Implementierung von API-Governance und Überwachung von Agenteninteraktionen.

Integrationsteams: Einführung von Standards für Interoperabilität und Beobachtbarkeit.

Geschäftspartner

Prozessinhaber: Identifizierung von Arbeitsabläufen für MAS-Pilotprojekte und Validierung der Ergebnisse.

Finance: Verwaltung unvorhersehbarer Kosten und Finanzierung von Beobachtbarkeitstools.

Operations: Unterstützung von Initiativen zur Zusammenarbeit zwischen Menschen und Agenten sowie zu Schulungen.

5

Domänenspezifische Sprachmodelle

Worum geht's?
Domänenspezifische Sprachmodelle (Domain-Specific Language Models, DSLMs) sind KI-Modelle, die auf speziellen Datensätzen für bestimmte Branchen oder Geschäftsfunktionen trainiert wurden und eine höhere Genauigkeit und Compliance bieten als generische große Sprachmodelle (Large Language Models, LLMs).

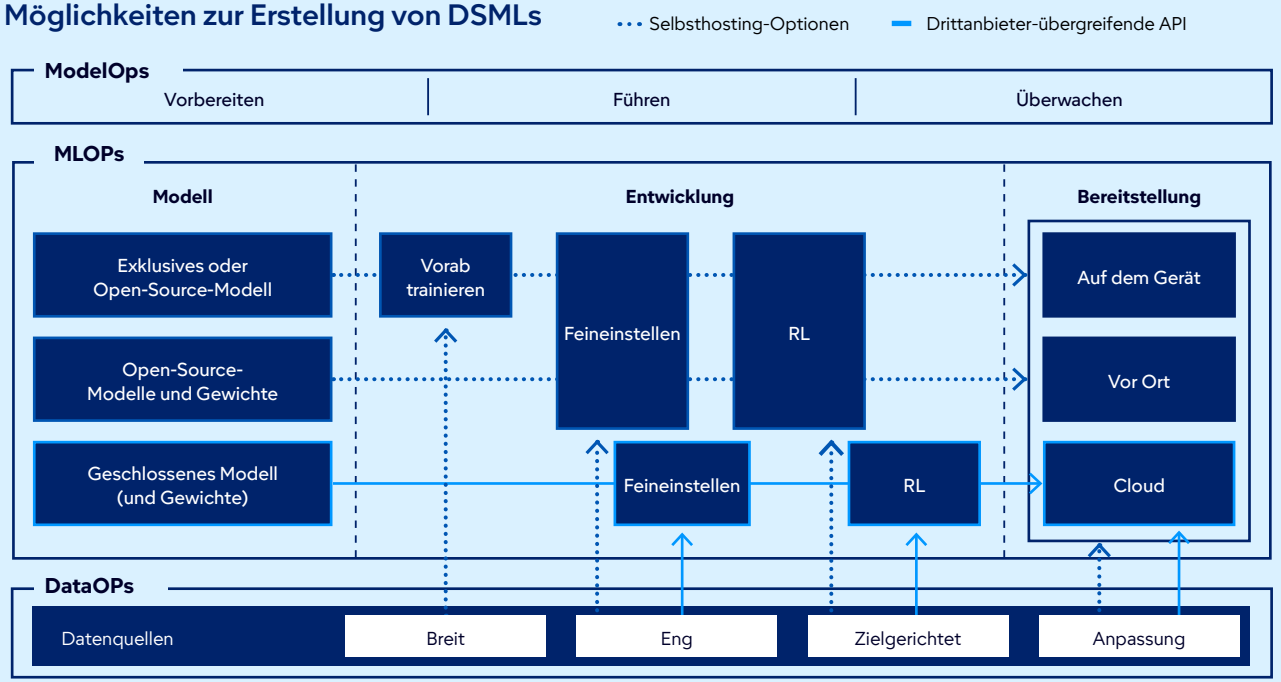
Gründe für diesen Trend
CIOs benötigen messbaren Geschäftswert aus KI. DSLMs reduzieren Fehler, beschleunigen die Bereitstellung und senken die Kosten für wichtige Arbeitsabläufe in den Bereichen Finance, Gesundheitswesen und HR.

Was kommt als Nächstes?

Über 60 % der GenAI-Modelle von Unternehmen werden bis 2028 domänenspezifisch sein.

30% der GenAI-Workloads werden bis 2028 DSLMs vor Ort oder auf Geräten ausführen.

Möglichkeiten zur Erstellung von DSMLs



Quelle: Gartner

5

Erzielen von Ergebnissen mit DSLMs

Aktionsplan zur Einhaltung präziser, branchenspezifischer Compliance-Vorgaben

Schritte	1 Identifizierung von Anwendungsfällen mit hoher Wirkung	2 Stärkung der Data-Governance	3 Durchführung von DSLM-Pilotprojekten in wichtigen Domänen	4 Entwicklung funktionsübergreifender Teams	5 Monitoring und Optimierung
Erwartetes Ergebnis	Schnellerer ROI und verbesserte Genauigkeit.	Zuverlässige und konforme DSLM-Outputs.	Demonstration eines messbaren Geschäftswerts.	Reibungslose Integration und Einführung.	Nachhaltige Leistung und Kostenkontrolle.
Aktion	Ermittlung von Workflows, bei denen generische LLMs unterdurchschnittlich abschneiden.	Implementierung robuster Datenschutz- und Qualitätskontrollen.	Einführung von Finance-, Gesundheits- oder HR-Prozessen.	Aufnahme von IT, KMU und Compliance in DSLM-Projekte.	Anwendung von Erklärbarkeits- und Compliance-Frameworks.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer DSLM-Strategie für regulierte und hochwertige Domänen.

Sicherstellung der Governance hinsichtlich Genauigkeit, Compliance und Erklärbarkeit.

Ausrichtung der DSLM-Einführung auf ROI- und Risikomanagementziele.

IT-Partner

Data und Analytics: Vorbereitung domänenspezifischer Datensätze und Sicherstellung der Qualität.

ModelOps: Verwaltung von Feinabstimmung, Monitoring und Lebenszyklus-Governance.

Sicherheit: Durchsetzung von Datenschutz und Compliance für DSLM-Bereitstellungen.

Geschäftspartner

Domänenexperten: Validierung der DSLM-Outputs hinsichtlich Genauigkeit und Relevanz.

Finance: Planung eines Budgets für die DSLM-Einführung und -Kostenoptimierung.

Compliance: Sicherstellung der Einhaltung gesetzlicher Vorschriften.

6

Physische KI

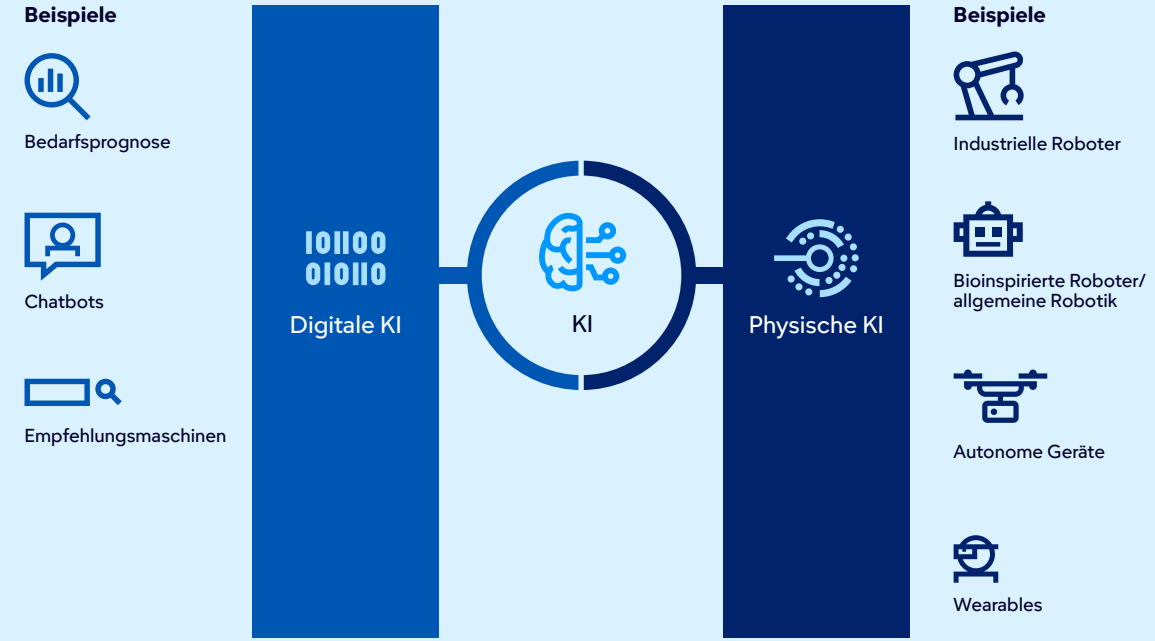
Worum geht's?
Physische KI bringt Intelligenz in die reale Welt – durch Roboter, Drohnen, Fahrzeuge und intelligente Geräte, die wahrnehmen, entscheiden und handeln. Diese Systeme kombinieren Sensoren, Aktuatoren und KI-Modelle zur Automatisierung physischer Aufgaben.

Gründe für diesen Trend
Unternehmen möchten die Produktivität digitaler KI auf physische Umgebungen anwenden. Bis 2028 werden fünf der zehn führenden KI-Anbieter physische KI-Produkte anbieten.

Was kommt als Nächstes?

80 % der Lagerhäuser werden bis 2028 Robotik oder Automatisierung einsetzen.

Kategorisierung von KI



Quelle: Gartner

6

Erzielen von Ergebnissen mit physischer KI

Aktionsplan zur Automatisierung realer Aufgaben und zur Steigerung der Produktivität in allen Bereichen

Schritte	1 Audit von Betriebsbereichen	2 Durchführung von Pilotprojekten zu physischen KI-Systemen	3 Entwicklung funktionsübergreifender Teams	4 Aufklärung von Stakeholdern	5 Planung für Multiagenten-Koordination
Erwartetes Ergebnis	Identifizierung von Bereichen für Automatisierung und Kosteneinsparungen.	Validierung der Leistung und des ROI.	Effektive Governance und Integration.	Vermeidung von Verwirrung und fehlgeleiteten Investitionen.	Zukunftssichere Bereitstellungen.
Aktion	Fokussierung auf Logistik, Wartung und Sicherheitsabläufe.	Verwendung von Simulationen und digitalen Zwillingen vor der Live-Bereitstellung.	Aufnahme von IT, Operations und Engineering in die Planung.	Klärung der Unterschiede zwischen physischer KI, eingebetteter KI und Edge-KI.	Erkundung von Orchestrierungsplattformen für Geräteflotten.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer physischen KI-Strategie, die auf die Betriebsziele abgestimmt ist.

Sicherstellung der Governance für Sicherheit, Zuverlässigkeit und Erklärbarkeit.

Zusammenarbeit mit Operations und Engineering bei der Integration und dem Risikomanagement.

IT-Partner

Infrastruktur und Operations: Integration physischer KI in IoT- und Altsysteme.

Sicherheit: Implementierung von Schutzmaßnahmen für autonome Systeme.

Data und Analytics: Unterstützung der Prüfung von Simulationen und digitalen Zwillingen.

Geschäftspartner

Operations: Identifizierung hochwertiger Anwendungsfälle und Validierung der Leistung.

Finance: Planung des Budgets für Investitionen in Robotik und Automatisierung.

Compliance: Sicherstellung der Einhaltung von Sicherheits- und Regulierungsstandards.

Der Vorreiter

Erhöht Vertrauen, Governance und Sicherheit.

In einer Zeit steigender Risiken und verschärfter behördlicher Kontrollen ist Vertrauen unerlässlich. Die Vorreitertrends konzentrieren sich auf proaktive Sicherheit, transparente Governance und digitale Integrität. So können Unternehmen ihren Ruf schützen, Compliance sicherstellen und das Vertrauen ihrer Stakeholder bewahren, während sie gleichzeitig KI und digitale Transformation vorantreiben.

7

Präventive Cybersicherheit

Worum geht's?
Präventive Cybersicherheit (Preemptive Cybersecurity, PCS) nutzt fortschrittliche KI-gestützte Techniken, um Cyberangriffe zu antizipieren, zu unterbinden und zu neutralisieren, bevor sie stattfinden – und geht damit über herkömmliche Erkennungs- und Reaktionsmaßnahmen hinaus.

Gründe für diesen Trend
KI-gestützte Bedrohungen nehmen exponentiell zu und zielen auf Netzwerke, Anwendungen und IoT-Systeme ab. Bis 2029 werden Technologieprodukte ohne präventive Cybersicherheit ihre Marktrelevanz verlieren, da proaktive Verteidigung zu einer universellen Anforderung wird.

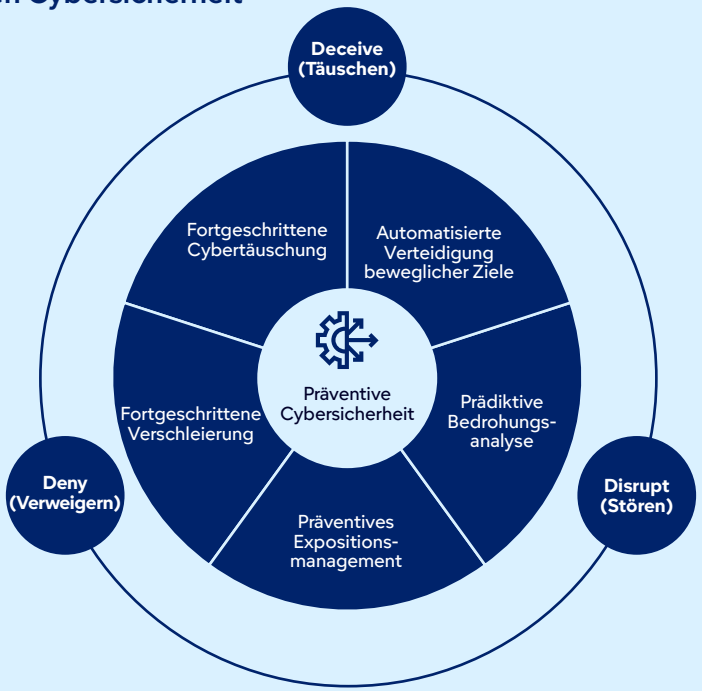
Benötigen Sie maßgeschneiderte Insights in Technologie- und Dienstleistungsunternehmen? Lesen Sie unseren Artikel über präventive Cybersicherheit für Anbieter: **Zögern Sie nicht mit der Entwicklung präventiver Cybersicherheitslösungen.**

Was kommt als Nächstes?

50 % der Ausgaben für Sicherheitssoftware werden bis 2030 für präventive Lösungen aufgewendet werden.

1 Mio. Dokumentierte Sicherheitslücken werden bis 2030 voraussichtlich 1 Million pro Jahr überschreiten.

Die 3 Ds der präventiven Cybersicherheit



Quelle: Gartner

7

Erzielen von Ergebnissen mit präventiver Cybersicherheit

Aktionsplan zum Schutz von Vermögenswerten vor dem Auftreten von Bedrohungen

Schritte	1 Beurteilung der aktuellen Sicherheitsarchitektur	2 Durchführung von PCS-Pilotprojekten in hochriskanten Bereichen	3 Definition der Anbieterauswahlkriterien	4 Sozialisierung der PCS-Strategie	5 Integration von PCS mit bestehenden Tools
Erwartetes Ergebnis	Identifizierung von Lücken und Priorisierung von PCS-Investitionen.	Demonstration einer messbaren Risikominderung.	Sicherstellung einer zukunftssicheren PCS-Einführung.	Aufbau von Unterstützung auf Führungs- und Vorstandsebene.	Maximierung des ROI und Beschleunigung der Einführung.
Aktion	Durchführung einer Risikoanalyse und Bereitschaftsüberprüfung.	Implementierung von prädiktiver Bedrohungsprävention und Täuschung.	Erfordernis von detaillierten Roadmaps für präventive Fähigkeiten.	Kommunikation der geschäftlichen Auswirkungen und des ROI von PCS.	Kombination von PCS mit aktuellen Sicherheits- und Compliance-Prozessen.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Förderung eines Wandels von reaktiven zu präventiven Sicherheitsstrategien.

Definition von Kaufkriterien für PCS-Fähigkeiten und Aufklärung der Kollegen in der Führungsebene.

Überwachung der Governance für aggressive Abwehrmaßnahmen und Compliance.

IT-Partner

Sicherheit: Einsatz von Technologien zur prädiktiven Bedrohungsabwehr und Täuschung.

Infrastruktur und Operations: Integration von PCS in Cloud-, OT- und cyberphysische Systeme.

Risiko und Compliance: Sicherstellung der Einhaltung von Datenschutz- und Regulierungsstandards.

Geschäftspartner

Finance: Zuweisung von Budgets für PCS-Pilotprojekte und langfristige Akzeptanz.

Operations: Unterstützung von Initiativen zur sicheren digitalen Transformation.

Produkt: Integration präventiver Sicherheit in Angebote zur Marktdifferenzierung.

8

Digitale Herkunft

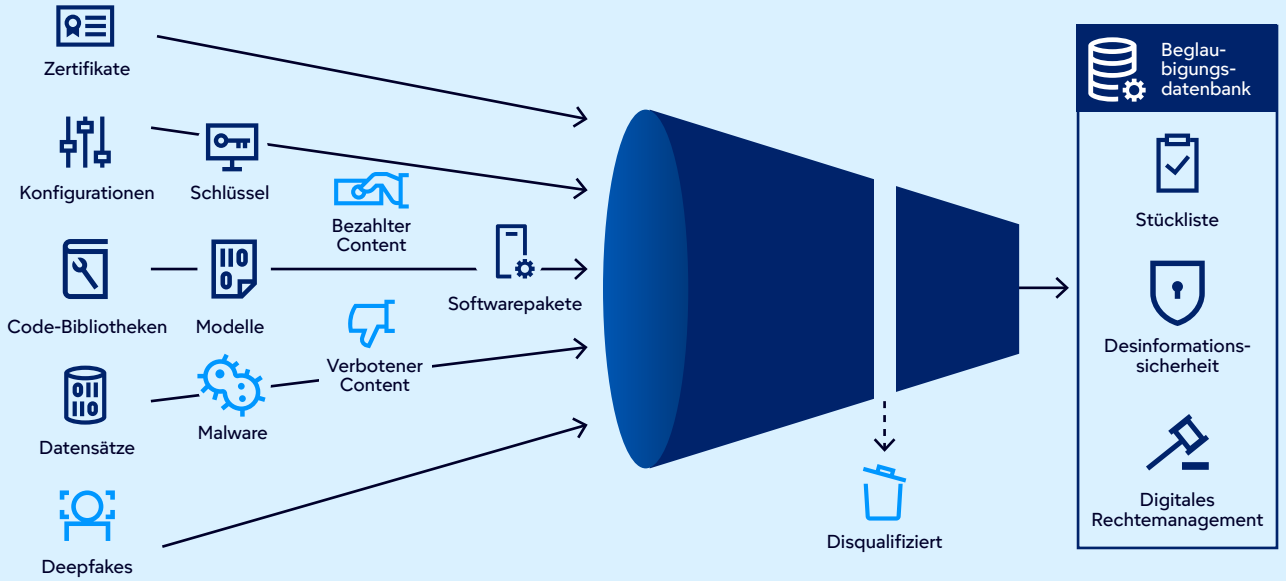
Worum geht's?
Die digitale Herkunft verifiziert den Ursprung und die Integrität von Software, Daten und Medien mithilfe von Tools wie Stücklisten (Bills of Materials, BOMs), Beglaubigungsdatenbanken und Wasserzeichen. Sie gewährleistet Transparenz und Vertrauen in Systeme, die auf Komponenten von Drittanbietern und KI-generiertem Content basieren.

Gründe für diesen Trend
Unternehmen sehen sich zunehmenden Risiken durch Code-Manipulationen, aufgegebene Open-Source-Projekte und Deepfake-basierte Desinformation ausgesetzt.

Was kommt als Nächstes?

Zunehmende regulatorische Vorgaben (z. B. KI-Gesetz der EU) erfordern Wasserzeichen und Herkunftsverfolgung für KI-generierten Content.

Filterung nach digitaler Herkunft



Quelle: Gartner

8

Erzielen von Ergebnissen mit digitaler Herkunft

Aktionsplan zum Aufbau von Vertrauen durch Überprüfung der Authentizität von Daten und Inhalten

Schritte	1 Einsatz von Stücklisten	2 Implementierung von Beglaubigungsdatenbanken	3 Einführung von Desinformationssicherheitstools	4 Anwendung von digitalen Wasserzeichen	5 Stärkung der Governance
Erwartetes Ergebnis	Ermöglichung der Einsicht in Softwareherkunft, -transparenz und -sicherheit.	Zentralisierte, vertrauenswürdige Herkunftsnachweise.	Schutz vor Identitätsdiebstahl und Betrug.	Compliance mit den Vorschriften für KI-Content.	Geringeres rechtliches Risiko und Reputationsrisiko.
Aktion	Implementierung von Software-Stücklisten (SBOMs) für Software- und Machine-Learning-Stücklisten (MLBOMs) für KI-Modelle.	Speicherung kryptografisch signierter Herkunftsnachweise.	Integration der Erkennung synthetischer Identitäten in Pläne zur Erkennung und Reaktion auf Identitätsbedrohungen.	Kennzeichnung von KI-generierten Medien in maschinenlesbaren Formaten.	Zusammenarbeit zwischen IT-, Compliance- und Marketingteams.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer digitalen Herkunftsstrategie, die auf Compliance und Risikomanagement abgestimmt ist.

Überwachung der Implementierung von BOMs und Beglaubigungsdatenbanken.

Zusammenarbeit mit CISO und CMO bei der Bekämpfung von Desinformation und beim Schutz der Reputation.

IT-Partner

DevOps: Integration von SBOMs und MLBOMs in Lieferpipelines.

Sicherheit: Einsatz von Tools zum Schutz vor Desinformation und für digitales Rechtemanagement (Digital Rights Management, DRM).

Daten: Dokumentation der Herkunft der Trainingsdaten für KI-Modelle.

Geschäftspartner

Compliance: Sicherstellung der Einhaltung neuer Vorschriften.

Rechtsabteilung: Validierung der Compliance mit Urheberrechten und Lizenzen.

Marketing: Verwaltung von Reputationsrisiken im Zusammenhang mit Deepfakes und synthetischem Content.

9

KI-Sicherheits-plattformen

Worum geht's?
KI-Sicherheitsplattformen (AI Security Platforms, AISPs) konsolidieren Kontrollen, um sowohl KI-Dienste von Drittanbietern als auch maßgeschneiderte KI-Anwendungen zu sichern. Sie befassen sich mit KI-spezifischen Risiken wie Prompt Injection, betrügerischen Handlungen von Agenten und Datenlecks.

Gründe für diesen Trend
Angesichts der zunehmenden Verbreitung von KI reichen herkömmliche Sicherheitstools nicht mehr aus, um KI-Arbeitsabläufe zu schützen.

Was kommt als Nächstes?

Über 50 % der Unternehmen werden bis 2028 AISPs einführen.

80 % der nicht autorisierten KI-Transaktionen werden auf Verstöße gegen interne Richtlinien zurückzuführen sein, nicht auf externe Angriffe.

Abbildung der Fähigkeiten von KI-Sicherheitsplattformen

Quelle: Gartner

9

Erzielen von Ergebnissen mit KI-Sicherheitsplattformen

Aktionsplan zum Schutz sich weiterentwickelnder KI-gesteuerter Geschäftsabläufe

Schritte	1 Bewertung der KI-Risikolandschaft	2 Durchführung von Pilotprojekten für AISP-Lösungen	3 Bevorzugung einheitlicher Plattformen	4 Integration von Sicherheitstests	5 Überwachung der Innovationen von Anbietern
Erwartetes Ergebnis	Identifizierung von Lücken im aktuellen Sicherheitsstack.	Validierung der Wirksamkeit und des ROI.	Vereinfachung der Verwaltung und Reduzierung der Komplexität.	Verbesserung der Widerstandsfähigkeit gegen Prompt Injection.	Antizipation neuen Bedrohungen.
Aktion	Abbildung von KI-spezifischen Risiken über Arbeitsabläufe hinweg.	Einführung risikoreicher KI-Dienste und benutzerdefinierter Apps.	Auswahl von AISPs, die die Kontrolle der KI-Nutzung sowie die App-Sicherheit abdecken.	Hinzufügung automatisierter KI-Sicherheitstests zu Pipelines.	Verfolgung von Start-ups und etablierten Unternehmen hinsichtlich erweiterter Funktionen.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer KI-Sicherheitsstrategie, die sowohl KI-Anwendungen von Drittanbietern als auch maßgeschneiderte KI-Anwendungen umfasst.

Auswahl von Anbietern, die eine einheitliche KI-Nutzungskontrolle und -Anwendungssicherheit bieten.

Kommunikation der KI-Risikolage und Compliance-Anforderungen an den Vorstand.

IT-Partner

Sicherheit: Einsatz von Sicherheitsvorkehrungen für Prompt Injection und zur Erkennung betrügerischer Agenten.

DevOps: Integration von KI-Sicherheitstests in Entwicklungs-Pipelines.

Infrastruktur und Operations: Sicherstellung der Kompatibilität mit Cloud- und On-Premises-Umgebungen.

Geschäftspartner

Compliance: Anpassung der AISPs an regulatorische Frameworks (z B. KI-Gesetz der EU).

Finance: Planung eines Budgets für die Plattformeinführung und Risikominderung.

Produkt: Integration von Sicherheitsfunktionen in KI-gestützte Angebote.

10

Geopatriation

Worum geht's?
Geopatriation ist die Verlagerung von Workloads aus globalen Hyperscale-Clouds in souveräne oder lokale Umgebungen, um geopolitische Risiken zu reduzieren. Dazu gehören Strategien wie die Verlagerung in souveräne Cloud-Regionen oder die Rückführung von Workloads in On-Premises-Umgebungen.

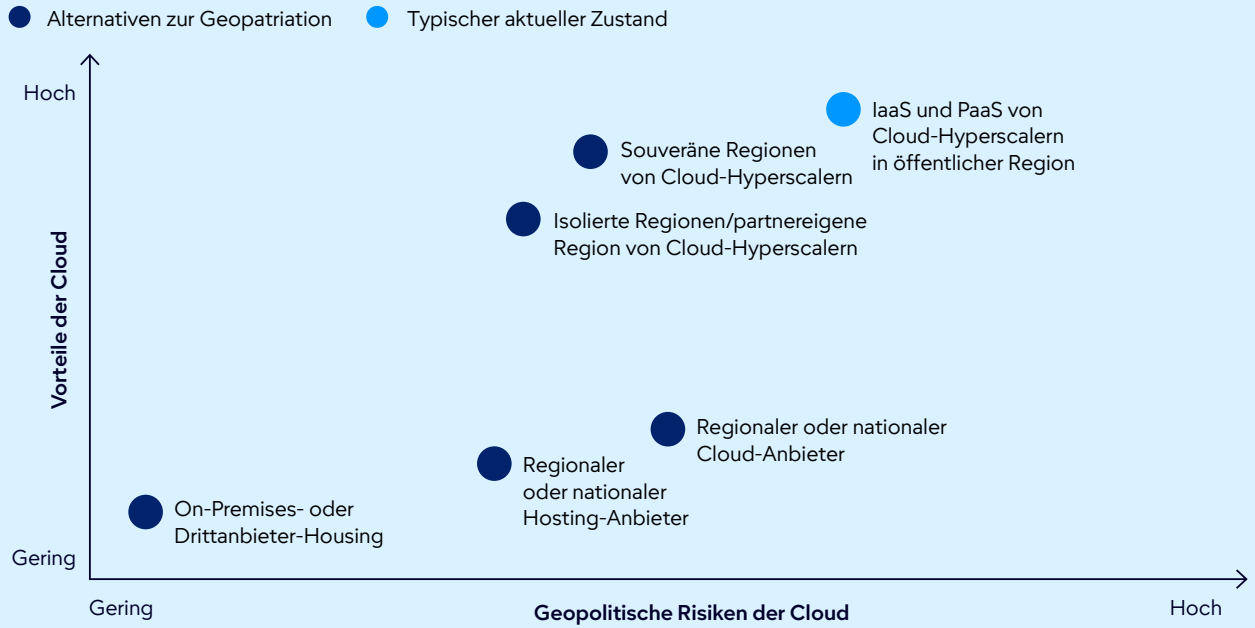
Gründe für diesen Trend
Geopolitische Turbulenzen und regulatorische Vorgaben veranlassen Unternehmen dazu, ihre Abhängigkeit von der Cloud neu zu bewerten.

Was kommt als Nächstes?

75 % der Unternehmen werden bis 2030 ihre Workloads geografisch auslagern.

Souveräne Cloud-Angebote von Hyperscalern und lokalen Anbietern nehmen rapide zu.

Vorteile und geopolitische Risiken der Cloud



Quelle: Gartner

10

Erzielen von Ergebnissen mit Geopatriation

Aktionsplan zur Risikominderung durch Lokalisierung kritischer digitaler Workloads

Schritte	1 Beurteilung der Workload-Kritikalität	2 Bewertung souveräner Optionen	3 Planung hybrider Strategien	4 Implementierung von Governance-Kontrollen	5 Überwachung geopolitischer Trends
Erwartetes Ergebnis	Priorisierung der Geopatriation für risikoreiche Vermögenswerte.	Ausgewogenheit von Agilität und Souveränität.	Erhaltung der Widerstands- und Leistungsfähigkeit.	Reduzierung von Compliance- und Sicherheitsrisiken.	Proaktive Anpassung der Strategie.
Aktion	Bewertung von Workloads anhand ihrer Sensibilität und geopolitischen Risiken.	Gegenüberstellung von Souvereign-Cloud-Hyperscaler-Angeboten und lokalen Anbietern.	Kombination von Sovereign Cloud mit On-Premises- oder Drittanbieter-Housing.	Einführung von Beglaubigungs- und Souveränitätsframeworks.	Aktualisierung der Workload-Verteilung bei sich ändernden Risiken.

Wichtige Akteure zur Unterstützung des Implementierungserfolgs

CIO

Definition einer Geopatriationsstrategie, die Souveränität, Agilität und Resilienz in Einklang bringt.

Bewertung der Kompromisse zwischen lokalen Anbietern und den Sovereign-Optionen globaler Hyperscaler.

Überwachung der Risikobewertung für kritische Workloads und der Compliance-Abstimmung.

IT-Partner

Infrastruktur und Operations: Planung von Migrationspfaden und Integration in Altsysteme.

Sicherheit: Validierung von Souveränitätskontrollen und Sicherstellung der Compliance.

Cloud-Architekten: Optimierung der Workload-Platzierung für Leistung und Resilienz.

Geschäftspartner

Compliance: Überwachung regulatorischer Änderungen und Hoheitsmandate.

Finance: Erstellung eines Budgets für Migrationskosten und Investitionen zur Risikominderung.

Operations: Sicherstellung der Kontinuität während der Workload-Umverteilung.

Umsetzbare, objektive Insights

Entdecken Sie diese zusätzlichen, ergänzenden Ressourcen und Tools für IT-Leiter:

Vorlage

Erstellung eines strategischen IT-Plans

Setzen Sie Ihre Strategie in die Tat um – mit dieser Vorlage für die Planung auf einer Seite.

Vorlage aufrufen

Tool

Benchmarking und Diagnostik von Gartner

Entdecken Sie Benchmarking für bessere IT-Entscheidungen.

Mehr erfahren

Insights

Gartner Hype Cycle™ 2025

Der Hype Cycle 2025 für KI geht über GenAI hinaus.

Jetzt erkunden

Insights

Aktuelle Fragen zu KI und neuen Technologien

Gartner-Experten geben schnelle Antworten auf kürzlich gestellte Kundenfragen zu neuen Technologien.

Antworten überprüfen

Bereits Kunde?
Erhalten Sie über Ihr Kundenportal Zugang zu weiteren Ressourcen. **Anmelden ↗**

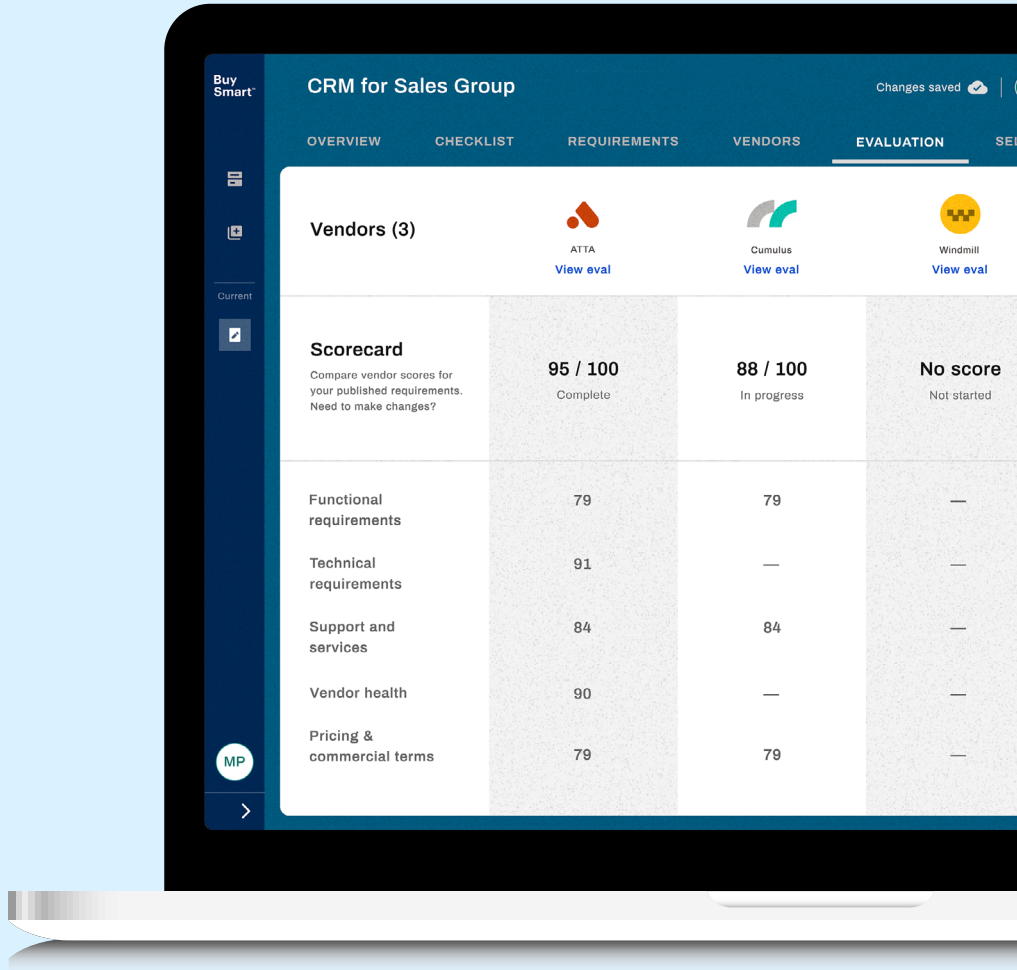
Gartner®

Gartner BuySmart™

Optimieren Sie den Weg Ihres Teams zu besseren Kaufentscheidungen im Technologiebereich

Was Sie erhalten:

- Zugriff auf über 100 Vorlagen für die wichtigsten Technologiemärkte
- Vordefinierte, vollständig anpassbare Checklisten und Anforderungen
- Kollaborationsfunktionen zur Unterstützung der Arbeitsabläufe Ihres Teams an einem Ort
- Standardisiertes Scoring für mehr Vertrauen in Ihre Anbieterauswahl



Mehr erfahren ↗ Studie Auswahlliste Bewerten Verhandeln

Ihr Kontakt zu uns

Erhalten Sie umsetzbare, objektive Geschäfts- und Technologie-Insights, die zu intelligenteren Entscheidungen und besserer Performance bei Ihren geschäftskritischen Prioritäten führen.

USA: 1 855 811 7593

International: +44 (0) 3330 607 044

Sprechen Sie mit einem Spezialisten

Erfahren Sie mehr über Gartner für CIOs und IT-Leiter
gartner.com/en/chief-information-officer

Bleiben Sie in Kontakt, um die neuesten Insights zu erhalten

Nehmen Sie an einer Gartner-Konferenz teil
Konferenz anzeigen

Gartner®