KI-gestützte Observability

Wenn Automatisierung Vertrauen schafft

Agentic AI verspricht schnellere Entscheidungen, weniger manuelle Arbeit und eine neue Qualität operativer Effizienz. In komplexen IT- und Produktionsumgebungen entsteht Vertrauen jedoch nicht durch Autonomie allein. Wo Ausfälle, Fehlkonfigurationen oder Sicherheitsvorfälle direkte Folgen für Betrieb, Sicherheit und Geschäftskontinuität haben, ist Zurückhaltung kein Zeichen mangelnder Innovationsbereitschaft. Sie ist Ausdruck professioneller Verantwortung.

Für Unternehmen stellt sich deshalb nicht die Frage, wie schnell sich Agentic AI einführen lässt, sondern unter welchen Bedingungen KI-gestützte Automatisierung belastbar, kontrollierbar und sicher wird. Genau hier wird Observability entscheidend, denn nur Systeme, die Abhängigkeiten, Laufzeitverhalten und operative Zusammenhänge in Echtzeit verstehen, können Automatisierung ermöglichen, die nachvollziehbar und vertrauenswürdig bleibt.

Wie Unternehmen Vertrauen in Agentic AI aufbauen

Viele Diskussionen rund um Agentic AI konzentrieren sich auf theoretische Möglichkeiten autonomer Systeme. In der Praxis sind Unternehmensumgebungen jedoch selten sauber standardisiert oder vollständig vorhersehbar. Moderne IT-Landschaften bestehen aus hybriden Infrastrukturen, cloud-nativen Architekturen, Legacy-Systemen, APIs, Containern und hochdynamischen Workloads über verschiedene Umgebungen hinweg. Diese Komplexität erzeugt ein grundlegendes Problem für autonome Systeme, denn Entscheidungen, die technisch isoliert betrachtet sinnvoll erscheinen, können problematisch werden, sobald betriebliche Abhängigkeiten, Sicherheitsrichtlinien oder geschäftliche Prioritäten berücksichtigt werden müssen. Ein automatisierter Neustart eines Workloads kann ein lokales Problem lösen, gleichzeitig aber nachgelagerte Services beeinträchtigen oder Compliance-Vorgaben verletzen.

Verantwortung übernehmen

Skepsis ist deshalb häufig kein Zeichen von Innovationsfeindlichkeit, sondern von operativer Reife. Unternehmen mit kritischen Produktionsumgebungen, Finanzsystemen oder komplexen Lieferketten können sich unkontrollierte Experimente nicht leisten. Sie benötigen Transparenz, Nachvollziehbarkeit und vorhersehbares Verhalten, bevor Automatisierung über isolierte Pilotprojekte hinausgeht. Hinzu kommt, dass viele Unternehmen keinen klaren Einstiegspunkt für Agentic AI erkennen. Das eigentliche Hindernis ist oft nicht die Technologie selbst, sondern die Unsicherheit rund um Governance, Sicherheit, Verantwortlichkeiten und die Zuverlässigkeit KI-gestützter Entscheidungen.

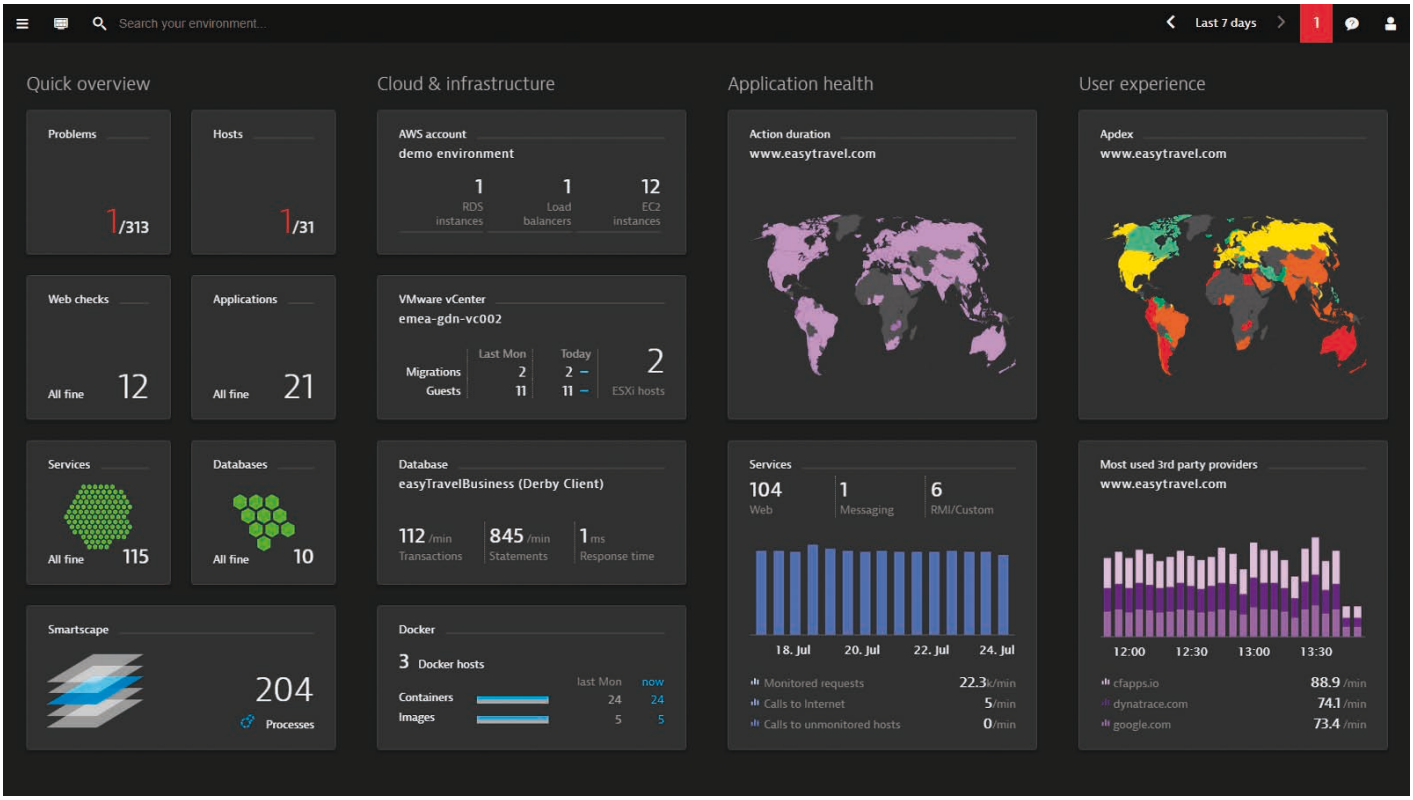
Der kontrollierte Einstieg

Ein kontrollierter Einstieg beginnt deshalb mit einem einfachen Grundsatz: Automatisierung muss erklärbar bleiben. Systeme müssen nachvollziehbar machen können, warum Entscheidungen getroffen werden, welche Signale diese ausgelöst haben und welche Auswirkungen daraus entstehen können. Ohne diese Transparenz wird Autonomie schnell selbst zum operativen Risiko.

Wo Automatisierung heute schon Mehrwert schafft

Die sinnvollsten Anwendungsfälle für Agentic AI beginnen nicht mit Vollautonomie. Sie beginnen bei operativen Aufgaben mit hohem Kontextbedarf, wiederkehrenden Analysen und klar definierten Grenzen. Ein Beispiel ist die Priorisierung von Vorfällen. Moderne IT-Umgebungen erzeugen täglich tausende Alerts, Logs und Telemetriedaten. Für operative Teams wird es zunehmend schwieriger, zwischen isolierten Auffälligkeiten und tatsächlich geschäftskritischen Problemen zu unterscheiden.

Autor:
Roman Spitzbart
VP Solutions Engineering EMEA
Dynatrace
www.dynatrace.com



KI-gestützte Systeme können kontinuierlich Zusammenhänge zwischen Anwendungen, Infrastruktur, Nutzererfahrung und Laufzeitverhalten analysieren und dadurch relevante Vorfälle schneller identifizieren.

Ursachenanalyse

Ein weiterer realistischer Einstiegspunkt ist die Ursachenanalyse über verteilte Systeme hinweg. In cloud-nativen Architekturen bleiben Probleme selten auf einzelne Komponenten beschränkt. Performance-Probleme können durch Netzwerklatenzen, Konfigurationsänderungen, Ressourcenengpässe oder Fehler in anderen Teilen der Umgebung entstehen. Agentische Systeme korrelieren Logs, Traces, Metriken und Topologie-Daten in Echtzeit und beschleunigen die Ursachenanalyse deutlich. Viele Unternehmen nutzen KI-gestützte Automatisierung zudem zunächst nicht für autonome Ausführung, sondern zur Vorbereitung operativer Maßnahmen. Systeme erzeugen beispielsweise Handlungsempfehlungen, bereiten Rollback-Prozesse vor, schlagen Infrastruktur-Anpassungen vor oder orchestrieren definierte Workflows, die weiterhin menschliche Freigaben benötigen.

Bessere Beherrschung wachsender Komplexität

Für den praktischen Einsatz ist diese Unterscheidung zentral. Erfolgreiche Einführung entsteht meist nicht dadurch, dass Unternehmen maximale Autonomie anstreben. Sie entsteht dort, wo operative Reibung reduziert wird, ohne menschliche Kontrolle zu verdrängen. Ziel ist nicht die Ersetzung operativer Teams, sondern die bessere Beherrschung wachsender Komplexität. In vielen Umgebungen erzeugt dieser Ansatz bereits heute messbaren Mehrwert: Schnellere Ursachenanalyse reduziert Ausfallzeiten, bessere Priorisierung verringert Alarmmüdigkeit und automatisiert vorbereitete Maßnahmen beschleunigen die Reaktion auf Vorfälle, ohne Governance-Strukturen auszuhebeln. Das Ergebnis ist keine vollständig autonome Infrastruktur, sondern resilienterer Betrieb durch intelligente Unterstützung.

Observability schafft den Kontext für sichere Automatisierung

Agentische Systeme können nur dann belastbare Entscheidungen treffen, wenn sie den operativen Kontext verstehen, in dem diese Entscheidungen stattfinden. Genau dadurch verändert sich die Rolle von Observability grundlegend. Traditionelles Monitoring konzentriert sich primär auf isolierte Metriken und definierte Schwellenwerte. Moderne Observability geht deutlich weiter: Sie verbindet Logs, Metriken, Traces, Topologien, Laufzeitabhängigkeiten, Sicherheitsereignisse und Geschäftskontext zu einem einheitlichen operativen Gesamtbild. Dieser Kontext ist die Voraussetzung für vertrauenswürdige Automatisierung.

Eine einzelne Auffälligkeit erklärt selten den tatsächlichen Zustand eines Systems. Erst der Zusammenhang zwischen Abhängigkeiten, Infrastrukturverhalten, Workloads und historischen Mustern erzeugt ein realistisches Lagebild. Ein Anstieg von Latenzen ist beispielsweise nicht automatisch kritisch. Erst in Verbindung mit Deployment-Aktivitäten, Ressourcenengpässen, ungewöhnlichem Traffic-Verhalten oder Transaktionsfehlern wird die tatsächliche operative Bedeutung sichtbar. Observability verwandelt isolierte Telemetriedaten in handlungsfähige operative Erkenntnisse.

Kontinuierliche Veränderung

In dynamischen Cloud-Umgebungen verschärft sich diese Anforderung. Cloud-native Architekturen skalieren kontinuierlich, verschieben Workloads und verändern Abhängigkeiten in Echtzeit. Starre Automatisierungsregeln stoßen dort schnell an Grenzen, weil sich Betriebszustände permanent verändern. Observability-Plattformen liefern das Echtzeitverständnis, das sichere Automatisierung überhaupt erst möglich macht. KI-Systeme erkennen dadurch nicht nur, dass sich etwas verändert hat, sondern auch, ob daraus ein operatives Risiko, erwartbares Verhalten oder ein Sicherheitsproblem entsteht.

Kausale KI

Hier spielt insbesondere kausale KI eine wichtige Rolle. Reine Korrelation reicht in hochverteilten Systemen nicht aus, weil viele Ereignisse gleichzeitig auftreten. Kausale KI hilft dabei, zwischen Symptomen und tatsächlichen Ursachen zu unterscheiden, indem sie Abhängigkeiten und operative Zusammenhänge analysiert.

Dadurch entstehen präzisere Empfehlungen, schnellere Lösungswege und geringere operative Unsicherheit. Observability entwickelt sich damit von einer passiven Monitoring-Disziplin zu einer aktiven operativen Kontrollschicht. Sie wird zum Mechanismus, der Automatisierung erklärbar, messbar und mit der Realität komplexer Systeme vereinbar macht.

Sichere Automatisierung braucht klare Leitplanken

Je größer der operative Handlungsspielraum autonomer Systeme wird, desto wichtiger wird Governance. Sicherheit darf deshalb nicht erst nachträglich ergänzt werden. Agentic AI erweitert die Rolle von Systemen grundlegend: Sie analysieren nicht mehr nur Umgebungen, sondern greifen zunehmend aktiv in Entscheidungs- und Betriebsprozesse ein. Damit steigen gleichzeitig Möglichkeiten und Risiken. Unternehmen müssen deshalb früh klare operative Leitplanken definieren. Dazu gehören Zugriffsrechte, Freigabeprozesse, Auditierbarkeit, Rollback-Mechanismen und Richtlinien für automatisierte Eingriffe.

Human-in-the-Loop-Ansätze

Gerade in regulierten Branchen wird Nachvollziehbarkeit entscheidend. Teams müssen verstehen können, warum Maßnahmen ausgelöst wurden, welche Datenquellen die Entscheidung beeinflusst haben und ob automatisierte Änderungen regulatorischen oder internen Vorgaben entsprechen. Das erklärt auch die wachsende Bedeutung von Human-in-the-Loop-Ansätzen. In geschäftskritischen oder sicherheitsrelevanten Szenarien ist vollständige Autonomie oft weder notwendig noch sinnvoll. Stattdessen analysieren KI-Systeme Situationen, erzeugen Empfehlungen und bereiten Maßnahmen vor, während operative Teams die finale Kontrolle behalten.

Dieser Ansatz reduziert Risiken, ohne die Effizienzgewinne intelligenter Automatisierung zu verlieren. Gleichzeitig stärkt er das Vertrauen innerhalb der Organisation, weil Menschen weiterhin aktiv in Entscheidungsprozesse eingebunden bleiben. Hinzu kommt die zunehmende Verschmelzung von Observability und Security Operations. Moderne Cyberbedrohungen nutzen operative Komplexität, Konfigurationsfehler und fragmentierte Transparenz gezielt aus. KI-gestützte Observability hilft Unternehmen dabei, Anomalien frühzeitig zu erkennen, Risiken zu priorisieren und potenzielle Angriffspfade im operativen Gesamtkontext sichtbar zu machen.

Security-Teams erhalten dadurch nicht nur schnellere Warnungen, sondern ein präziseres Verständnis der tatsächlichen Auswirkungen eines Vorfalls. Das verbessert Reaktionsfähigkeit, Resilienz und operative Sicherheit. Vertrauen entsteht deshalb nicht durch größere Modelle oder rigorosere Automatisierung. Vertrauen entsteht durch Kontrolle, Transparenz und operative Verantwortlichkeit.

Der Weg zur vertrauenswürdigen Automatisierung

Viele Unternehmen zögern, weil sie Agentic AI mit einer radikalen Transformation verbinden. Erfolgreiche Einführung erfolgt in der Praxis jedoch meist schrittweise. Ein realistischer Ansatz orientiert sich an operativen Reifegraden statt an technologischen Visionen. Die erste Phase konzentriert sich häufig auf Transparenz und Analyse. KI unterstützt operative Teams dabei, Anomalien zu erkennen, Ereignisse zu korrelieren und kontextbezogene Empfehlungen zu erzeugen. Die nächste Stufe erweitert diese Fähigkeiten um vorbereitete Maßnahmen. Systeme schlagen Workflows vor, orchestrieren definierte Abläufe oder automatisieren operative Teilprozesse, während die finale Entscheidung weiterhin beim Menschen liegt.

Erst wenn Datenqualität, Governance-Strukturen und operative Prozesse belastbar etabliert sind, sollte der Handlungsspielraum autonomer Systeme erweitert werden. Selbst dann bleibt Automatisierung meist auf klar definierte Bereiche mit kontrollierbaren Risiken beschränkt. Der stufenweise Ansatz reduziert nicht nur technische Risiken. Unternehmen können Datenqualität validieren, Governance-Strukturen schärfen und Vertrauen in die Systeme aufbauen, bevor weitergehende Automatisierung eingeführt wird. Gleichzeitig verhindern sie, dass neue operative Komplexität durch unkontrollierte KI-Nutzung entsteht.

Kontrollierte Weiterentwicklung bestehender Betriebsmodelle

Vor allem aber orientiert sich dieser Ansatz an der Realität moderner Unternehmensumgebungen. Operative Reife lässt sich nicht durch Technologie ersetzen. Unternehmen, die Agentic AI als kontrollierte Weiterentwicklung bestehender Betriebsmodelle verstehen, erzielen langfristig belastbarere Ergebnisse als Organisationen, die sofort maximale Autonomie anstreben. Die Relevanz von Agentic AI wird deshalb künftig nicht daran gemessen werden, wie viele Entscheidungen Systeme allein treffen können. Ausschlaggebend ist, ob Unternehmen Automatisierung mit belastbarem Kontext, klaren Regeln und operativer Resilienz verbinden.

Observability bildet dafür die Grundlage. Sie hilft Systemen, Komplexität nicht nur zu erfassen, sondern in belastbaren Kontext zu übersetzen. Erst daraus entstehen Entscheidungen, die erklärbar, steuerbar und auditierbar bleiben. Die Zukunft von Agentic AI liegt deshalb nicht in maximaler Autonomie, sondern in intelligenter Automatisierung innerhalb klarer Leitplanken. Genau dort entsteht Vertrauen.

Über den Autor

Roman Spitzbart ist VP Solutions Engineering EMEA bei Dynatrace. Er begleitet Unternehmen bei der Modernisierung ihrer IT-Operationen, beim Aufbau resilienter digitaler Services und beim Einsatz von AI-powered Observability in komplexen Cloud- und Hybridumgebungen. ◄