Cloud im Griff

Das industrielle Datenökosystem stabil halten

© Unsplash / Flexera

© Jesse Stockall

Autor:
Jesse Stockall
Chief Architect
Flexera
https://www.flexera.de/

SaaS-Anwendungen, Plattformdienste und virtuelle Assets – die Datenströme der Industrie 4.0 reichen längst weit über die Fabrikhallen hinaus. Die Cloud bildet das Rückgrat eines zukunftsfähigen Datenökosystems. Umso wichtiger ist es, Transparenz, Compliance, Sicherheit und effizientes Kostenmanagement in dieser neuen Infrastruktur sicherzustellen.

Die Cloud ist integraler Bestandteil industrieller Datenökosysteme. Produzierende Unternehmen nutzen Public-Cloud-Plattformen wie Azure, AWS oder Google Cloud, um ERP- und MES-Systeme auszulagern und Rechenressourcen flexibel zu skalieren. Parallel dazu etabliert sich mit Edge- und Factory Clouds eine neue Ebene der Datenverarbeitung: Bereitgestellte Rechenleistung direkt an der Maschine, nah an den Produktionsprozessen.

Schnelle Verfügbarkeit

Anwendungen wie Predictive Maintenance oder Predictive Quality profitieren von kurzen Latenzzeiten und der schnellen Verfügbarkeit großer Datenmengen. Ergänzend ermöglichen Datenräume den sicheren und kontrollierten Austausch sensibler Informationen entlang der gesamten Wertschöpfungskette – ein entscheidender Faktor, um Kooperationen zu stärken und Innovationen im Sinne der Industrie 4.0 abzusichern.

Cloud-Komplexität verstehen

Die Wahl der Cloud-Architektur ist zentral. Die Mehrzahl der Unternehmen blickt dabei auf eine sehr komplexe Landschaft. Hybrid-Cloud zum Beispiel bezeichnet den Einsatz von Private- und Public-Cloud. Multi-Cloud wiederum bezieht sich auf den parallelen Einsatz mehrerer Anbieter. Beide Ansätze kommen häufig kombiniert zum Einsatz. Laut State of the Cloud Report von Flexera [1] nutzen 70 Prozent der Unternehmen hybride Strategien mit mindestens einer Public- und einer Private-Cloud-Umgebung. Die Mehrheit großer Organisationen setzt zusätzlich auf Multi-Cloud-Konzepte. Diese Architekturvielfalt bietet Flexibilität, erhöht aber auch die Komplexität.

Hinzu kommt: Was in der Praxis pauschal als „Cloud“ bezeichnet wird, umfasst in Wirklichkeit eine Vielzahl von einzelnen Cloud-Assets. Dazu zählen neben SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) und IaaS (Infrastructure-as-a-Service), aber auch Bereitstellungsmodelle wie spezialisierte Cloud-Instanzen sowie Anwendungen im Edge-Computing, die direkt in der Nähe von Maschinen und Prozessen laufen.

Drei Phasen im FinOps-Ansatz: Inform, Optimize und Operate © Flexera

Diese Vielfalt erhöht die Abhängigkeit von verschiedenen Providern und Technologien und erschwert eine konsistente Übersicht über Assets. Unterschiedliche Lizenzmodelle, Sicherheitsanforderungen, SLAs und Schnittstellen fragmentieren das Gesamtbild. Ohne zentrale Sicht und Steuerung in diesem komplexen Umfeld, riskieren Unternehmen nicht nur unnötige Kosten, sondern sehen sich schnell Sicherheits- und Compliance-Risiken gegenüber.

Achtung Cloud Hürden

Um diese Risiken zu entschärfen, gilt es drei zentrale Herausforderungen zu adressieren und so das volle Potenzial der Cloud zu entfalten:

• Sicherheit im industriellen Cloud-Umfeld

In industriellen Cloud-Umgebungen zählt Schwachstellenmanagement zu den Grundpfeilern einer robusten Sicherheitsarchitektur. Insbesondere der Einsatz zahlreicher Drittanbieteranwendungen birgt Risiken. Ein Großteil bekannt gewordener Sicherheitslücken lässt sich auf unzureichend geschützte SaaS-Dienste, fehlerhafte Konfigurationen oder veraltete Komponenten zurückführen. Vor allem in Produktionsumgebungen, in denen IT und OT (Operational Technology) zunehmend verschmelzen, können solche Schwächen gravierende Auswirkungen auf Verfügbarkeit und Betriebssicherheit haben.

Durchgängiges, risikobasiertes Schwachstellenmanagement

Ein bewährter Ansatz zur Reduktion dieser Risiken besteht in einem durchgängigen, risikobasierten Schwachstellenmanagement. Dieses umfasst die kontinuierliche Erkennung und Klassifizierung potenzieller Schwachstellen, eine Priorisierung anhand von Bedrohungslagen sowie automatisierte Workflows zur Behebung. Ergänzend sorgen klare Verantwortlichkeiten und ein abgestimmtes Patch-Management für Transparenz und Reaktionsgeschwindigkeit – auch bei komplexen hybriden Cloud-Infrastrukturen.

Besonders effektiv zeigt sich dieser Ansatz, wenn Sicherheitsprozesse direkt in bestehende IT- und DevOps-Strukturen integriert sind. Eine zentrale Asset-Datenbasis, kombiniert mit regelmäßigen Scans und Compliance-Prüfungen ermöglicht nicht nur eine bessere Risikoabschätzung, sondern auch die zielgerichtete Zuweisung von Maßnahmen. So lässt sich eine dauerhafte Sicherheitskultur als integraler Bestandteil eines resilienten industriellen Datenökosystems etablieren.

• Compliance: Lizenzmanagement

Die Cloud verändert nicht nur den IT-Betrieb, sondern auch die Regeln für Software-Lizenzierung. Klassische Abrechnungsmodelle pro Installation oder Nutzer, weichen zunehmend flexiblen Metriken wie Transaktionen, Datenvolumen oder Funktionsumfang. Gleichzeitig können sich Lizenzbedingungen in der Cloud ändern – eine Herausforderung für Unternehmen, die Compliance sicherstellen und wirtschaftliche Risiken vermeiden wollen.

Unterschiedliche Modelle wie „Bring your own license“ (BYOL) oder „Pay as you go“ (PAYG) gelten je nach Anbieter und Nutzungskontext. Während SaaS-Dienste zwischen verschiedenen Nutzertypen und Feature-Paketen differenzieren, basieren Infrastrukturangebote häufig auf CPU-Zeit oder Workload-Dauer. Ohne vollständige Transparenz über vorhandene Lizenzen, tatsächliche Nutzung und vertragliche Spielräume drohen Überlizenzierung, Fehlzuweisungen oder ungewollte Regelverstöße.

Wirkungsvolles Lizenzmanagement

Ein wirkungsvolles Lizenzmanagement in der Cloud erfordert daher präzise Inventare, automatisierte Nutzungsanalysen und klar definierte Zuständigkeiten. Nur wenn Unternehmen nachvollziehen können, welche Anwendungen tatsächlich genutzt werden, lassen sich überdimensionierte Lizenzpakete erkennen und gezielt anpassen. Die Entscheidung für das passende Modell, etwa zwischen BYOL und PAYG, erfolgt idealerweise auf Basis konkreter Nutzungsszenarien. So entsteht eine belastbare Compliance-Struktur, die Transparenz schafft und zugleich wirtschaftliche Spielräume eröffnet.

• Kosten und Effizienz: Gezielte Cloud-Nutzung

Cloud-basierte Infrastrukturen bieten prinzipiell hohe Flexibilität, erschweren aber die langfristige Planung und Kontrolle der Betriebskosten. Besonders industrielle Umgebungen leiden häufig unter fehlender Transparenz bei Ressourcennutzung, Bereitstellungsmodellen und Auslastung. Unter anderem, weil digitale Services parallel zu produktionsrelevanten Systemen betrieben werden. Schnell entstehen versteckte Kosten durch überdimensionierte Instanzen, fehlgeschaltete Services oder dauerhaft aktive Entwicklungsumgebungen. Skalierbarkeit wird dann zur Kostenfalle.

Großer Handlungsbedarf

Wie groß der Handlungsdruck ist, zeigt eine aktuelle Flexera-Umfrage: Demnach investieren 29 Prozent der Unternehmen mittlerweile mehr als eine Million US-Dollar monatlich in Cloud-Anwendungen. Zwar sinkt der Anteil nicht genutzter Ressourcen leicht. Nach wie vor bewerten 24 Prozent der Unternehmen jedoch einen signifikanten Teil ihrer Cloud-Ausgaben als nicht wertschöpfend. Diese Diskrepanz zwischen Investition und Nutzen verdeutlicht die Wichtigkeit, wirtschaftliche Steuerung mit technischer Transparenz zu verbinden.

FinOps-Modell

Ein strukturierter Kostenmanagement-Ansatz orientiert sich dabei zunehmend am FinOps-Modell – einer Methodik zur wirtschaftlich fundierten Steuerung von Cloud-Infrastrukturen. In der ersten Phase („Inform“) geht es darum, Ausgaben sichtbar zu machen und Verantwortlichkeiten zu klären. Darauf folgt die Optimierungsphase („Optimize“). Hier können Unternehmen ungenutzte oder überdimensionierte Ressourcen identifizieren, anpassen oder bei Bedarf entfernen. Die Steuerungsphase („Operate“) sorgt abschließend dafür, dass Optimierungen dauerhaft greifen – etwa durch automatisiertes Monitoring, klare Richtlinien und ein organisationsweites Kostenbewusstsein.

Dies ist keine einzelne Aktivität, sondern vielmehr ein kontinuierlicher Prozess. Auf diese Weise wird das Cloud-Kostenmanagement zu einem integralen Bestandteil der datengesteuerten Wertschöpfung, und die Infrastruktur ist stets an die aktuellen Anforderungen optimiert.

Fazit

Industrielle Cloud-Ökosysteme bieten enorme Potenziale, sie erfordern aber ebenso ein hohes Maß an Steuerung. Wer Sicherheit, Lizenz-Compliance und Wirtschaftlichkeit nicht systematisch adressiert, riskiert nicht nur Betriebsrisiken und regulatorische Konflikte, sondern auch unnötige Kosten. Entscheidend ist daher eine integrierte Herangehensweise, die technische Transparenz, organisatorische Verantwortung und wirtschaftliche Steuerung verbindet. Automatisierte Managementplattformen spielen hierbei eine zentrale Rolle – sie schaffen die nötige Übersicht, setzen Governance-Vorgaben durch und entlasten operative Teams. Nur so entfaltet die Cloud ihren vollen Mehrwert – als verlässliche Grundlage für Innovation und Effizienz in der Industrie 4.0.

Wer schreibt:

Jesse Stockall ist Chief Architect bei Flexera. Er verfügt über mehr als 20 Jahre Branchenerfahrung in der Leitung agiler Teams – von der Konzeption über die Umsetzung bis hin zur Einführung von Softwarelösungen. Zuvor hatte er Positionen bei Symbium, CRYPTOCard, der kanadischen Regierung und Digital Equipment Corp. inne.

Referenz

[1] Flexera State of the Cloud Report 2025 ◄