

Sechs Risiken für die Cloud-Strategie

und wie man sie vermeidet

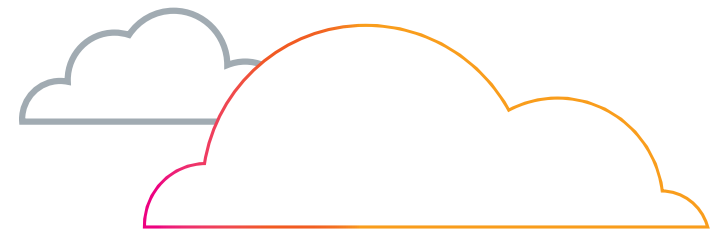
Die größten Vorteile der Cloud
können sich ohne eine starke Cloud-
Datenstrategie schnell zum
Nachteil entwickeln

Momentan lösen Unternehmen in praktisch allen Branchen ihre bisherigen lokalen Rechenzentren auf und verlagern ihre Workloads und Daten in die Cloud. Sie versuchen so, die Kosten zu senken und neue Lösungen bereitzustellen, um die sich schnell ändernden Anforderungen und Erwartungen von Mitarbeitern und Kunden zu erfüllen. Dazu entwickeln sie Cloud-Strategien, deren Fokus auf der Modernisierung ihres Technologie-Stacks durch Multi-Cloud-Umgebungen und auf der Einführung Cloud-nativer Anwendungen liegt.

Die Cloud-Nutzung kann weitreichende und entscheidende Vorteile haben. Die Cloud sorgt für niedrigere Kosten, verbessert und beschleunigt Innovationen und lässt Unternehmen agiler auf Markttrends und den Wettbewerbsdruck reagieren. Selbst etablierte Unternehmen setzen auf die Digitalisierung und investieren dazu kräftig in die entsprechende Technologie, um die Kundenerwartungen zu erfüllen. Das ist notwendig, um in extrem umkämpften Märkten mit digitalen Startups und wirtschaftlichen Schwankungen zu bestehen.

Doch wie jede Technologie bringt auch die Cloud gewisse Herausforderungen und Risiken mit sich, die nicht nur die erwarteten Vorteile einer Cloud-Strategie, sondern auch das gesamte Kundenerlebnis gefährden können. Der Schlüssel zur Cloud-Nutzung mit maximalem Mehrwert besteht in erster Linie darin, wie effektiv ein Unternehmen sein zunehmend komplexes Anwendungsportfolio und die damit verbundene Infrastruktur verwaltet. Nur wenn die von Cloud-basierten Systemen erzeugten riesigen Datenmengen angemessen verwaltet und analysiert werden, kann eine Cloud-Strategie dem Unternehmen den versprochenen Nutzen bringen.

Um dieses Ziel zu erreichen, müssen sich Unternehmen darüber im Klaren sein, wie sie die Fallstricke der Cloud-Nutzung umgehen. Wir haben sechs der größten Risiken identifiziert und hoffen, Ihnen mit diesem Leitfaden das Rüstzeug für eine erfolgreiche Cloud-Nutzung geben zu können.



Vorteile und Risiken der Cloud-Nutzung

Risiko 1: Die Kosten laufen aus dem Ruder

Einer der meistgenannten Vorteile der Cloud-Nutzung ist die Möglichkeit, Kosten einzusparen und gleichzeitig Kapital für Investitionen (CapEx) in den operativen Geschäftsbetrieb (OpEx) zu verlagern. Doch ohne angemessene Kontrollen können die Ausgaben für Cloud-Services schnell aus dem Ruder laufen.

Vorteil

Es ist ein wichtiger Vorteil der Cloud-Technologie, dass Unternehmen die Ausgaben für die Unterstützung ihrer Anwendungen anders verteilen können – und zwar weg von festen Investitionsausgaben hin zu Betriebskosten, die direkt an die Nutzung gekoppelt sind. Angesichts der langen Beschaffungsvorlaufzeiten und der hohen Fixkosten vieler IT-Abteilungen sind IaaS- und PaaS-Angebote überzeugende Alternativen. Die Cloud gibt Unternehmen die Möglichkeit, den Betrieb entsprechend der Nachfrage zu skalieren, sodass die Kosten genau mit dem Bedarf übereinstimmen.

Risiko

Die nutzungsbasierte, verbrauchsabhängige Preisgestaltung kann kosteneffizienter als der Betrieb einer lokalen Infrastruktur sein. Die Kosten können jedoch schnell aus dem Ruder laufen, wenn Unternehmen schlecht planen und kein angemessenes Monitoring für ihre Cloud-Umgebungen einrichten. Das Hauptproblem ist dabei häufig die mangelnde Transparenz bei der Nutzung von Cloud-Instanzen und -Services. Bei vielen Unternehmen dürfen separate Gruppen eigene Cloud-Umgebungen einkaufen bzw. verwalten. Diese Strategie gibt den entsprechenden Einzelpersonen oder Teams zwar die Freiheit, zu experimentieren und die Umgebung auf ihre Bedürfnisse zuzuschneiden, führt aber auch zu erheblichen Lücken bei der Kontrolle. Dies kann dazu führen, dass Services überprovisioniert werden, Lizenzen ungenutzt bleiben und Cloud-Server unnötigerweise doppelt eingerichtet werden

– und all dies treibt die Kosten in Höhe. Tatsächlich wurde 2019 **ein Drittel der Cloud-Kosten für ungenutzte oder überprovisionierte Cloud-Ressourcen verschwendet**. Noch schlimmer ist, dass Unternehmen dabei oftmals – entweder absichtlich oder versehentlich – verschiedene Cloud-Anbieter nutzen, wodurch ein Kostenvergleich auf Workload-Basis kaum möglich ist. Häufig lässt sich nicht nur schwer feststellen, wohin Ausgaben fließen – auch der konkrete Nutzen, den die Organisation davon hat, ist kaum zu beziffern.

Datenstrategie

Es ist wichtig, eine Datenstrategie für Ihre Cloud-Strategie zu entwickeln. Ihre Organisation muss die Cloud-Ausgaben exakt prognostizieren und überwachen, um die Rendite (ROI) zu maximieren und sicherzustellen, dass die Kosten dem geplanten Budget entsprechen. Wenn Sie die Gesamtkosten für Ihre Cloud-Services zentralisieren, können Sie ineffiziente Jobs, doppelte Workloads und andere unnötige Ausgaben identifizieren, bevor sie überhandnehmen. Hierbei sind Möglichkeiten zur Beobachtung (Stichwort: Observability) unerlässlich, um das Wo und Warum dieser fehlerhaften Prozesse in immer komplexer werdenden Systemen zu verstehen. Mit der richtigen Observability-Plattform können Sie Nutzungsberichte normalisieren und konsolidieren, ganz gleich, wo die Cloud-Services genutzt werden. Wenn Sie jede Implementierung einer Cloud-Anwendung wie eine unabhängige Geschäftsentscheidung behandeln, können Sie einzelne Gruppen weiterhin autonom arbeiten lassen und dennoch unangenehme Überraschungen bei der Cloud-Abrechnung vermeiden.

Risiko 2: Ein höheres Innovationstempo auf Kosten der Stabilität

Die Einführung Cloud-nativer DevOps-Verfahren beschleunigt Innovations- und Transformationsprozesse, bringt potentiell aber auch neue Fehlerquellen mit sich.

Vorteil

In einer herkömmlichen Umgebung mit lokalem Rechenzentrum wird die Infrastruktur hauptsächlich von periodischen Budgetzyklen bestimmt. Neue Ideen, die zusätzliche Hardware- oder Software-Ressourcen erfordern, aber außerhalb der standardmäßigen Budgetierungsabläufe entstehen, müssen bis zur Bereitstellung der Infrastruktur hinten angestellt werden – das bremst das Innovationspotential und mindert die Wettbewerbsfähigkeit. Cloud-Infrastruktur und -Services können dagegen im Handumdrehen hochgefahren werden, um ein hohes Innovationstempo zu unterstützen.

Risiko

Wenn ein Unternehmen auf agile Entwicklung und DevOps-Methoden umstellt, ist damit auch der Wechsel von eher seltenen Releases monolithischer Anwendungen zu viel häufigeren Releases dezentraler, Cloud-nativer Anwendungen verbunden. Die zusätzliche Komplexität lässt sich eventuell nur schwer managen, da es bei Cloud-nativen Anwendungen mit ihren diffizilen gegenseitigen Abhängigkeiten und ihrem dezentralen Design ein höheres Fehlerpotential gibt. Außerdem hängen viele dieser neuen Cloud-Apps von bestehenden Backend-Systemen ab und erweitern diese, was zu einer komplexen Bereitstellungs-pipeline führt. Die Fehlerbehebung in einer solchen Umgebung kann schnell überfordernd sein. Tatsächlich zeigte ein kürzlich veröffentlichter [Bericht](#), dass „620 Millionen Entwicklerstunden pro Jahr

für die Fehlersuche bei Softwareproblemen verschwendet werden.“ Oder anders gesagt: fehlgeschlagene Tests kosten den Markt für Unternehmenssoftware jährlich 61 Milliarden US-Dollar. Außerdem kann ein höheres Entwicklungstempo ohne die nötige Transparenz die Stabilität verringern und die Cloud-Nutzung beeinträchtigen.

Datenstrategie

Wenn neue Service- und Anwendungsarchitekturen implementiert werden, bedeutet das auch, dass die neu entstandenen Datenströme erfasst werden müssen. Diese neuen Datenströme aus Quellen wie serverlosen Funktionen und Microservices enthalten potenziell Antworten auf Probleme, die in Ihren Cloud-Umgebungen auftreten könnten. Es ist daher enorm wichtig, alle Daten über alle Cloud-Plattformen und bestehenden Abhängigkeiten hinweg beobachten zu können. Auch hier ist Observability der Schlüssel. Wenn es Ihnen nicht möglich ist, sich in Echtzeit und auf Basis sämtlicher Daten ein klares Bild von den Abläufen zu machen, können Sie im laufenden Betrieb auch nicht die richtigen Maßnahmen ergreifen. Das Ziel ist es, nicht nur das „bekannte Bekannte“, sondern auch das „unbekannte Unbekannte“ identifizieren und überwachen zu können. Richtig umgesetzt, sind Sie in der Lage, die Kernursache von Problemen schnell zu lokalisieren und gleichzeitig die gewünschte Entwicklungsrate zu fördern, die Skalierbarkeit zu verbessern und die Effektivität Ihrer Geschäftsprozesse insgesamt zu erhöhen. So vereinen Sie Geschwindigkeit und Stabilität.

„Bisher hat uns die fehlende Transparenz immer ausgebremst“, erklärt Jishnu Kinwar. „Doch Splunk unterstützt die Geschwindigkeit des Teams, sodass wir Produkte und Features schneller entwickeln und guten Gewissens früher veröffentlichen können.“

—Jishnu Kinwar, VP Cloud Platform Engineering, Arlo

[Erfolgsbericht von Arlo lesen](#)

Risiko 3: Eine Cloud-Strategie ohne passende Sicherheitsstrategie

Während die Anbieter selbst ein erstklassiges Sicherheitsniveau aufweisen, priorisieren Cloud-native Lösungen und DevOps ein schnelles Arbeits- und Anpassungstempo – wodurch die Sicherheit zur Nebensache wird.

Vorteil

Geprüfte Cloud-Anbieter haben vorherige Security Checks bestanden und ermöglichen Sicherheitsteams, Entwicklungs- und Infrastrukturanforderungen schnell und zuverlässig zu genehmigen. Cloud-Anbieter erfüllen einseitig strenge Compliance-Anforderungen und unterhalten dank ihrer Größe oftmals Security-Teams, die selbst über die Möglichkeiten technisch versierter Unternehmen hinausgehen. Zudem bieten sie Tools, die für Transparenz bei der Speicherung und Verarbeitung Ihrer Daten sorgen. Da Unternehmen so weniger Zeit und Geld für die Sicherheit ihrer Infrastruktur aufwenden müssen, hat die Verlagerung in die Cloud geringere Kosten und eine schnellere Wertschöpfung zur Folge.

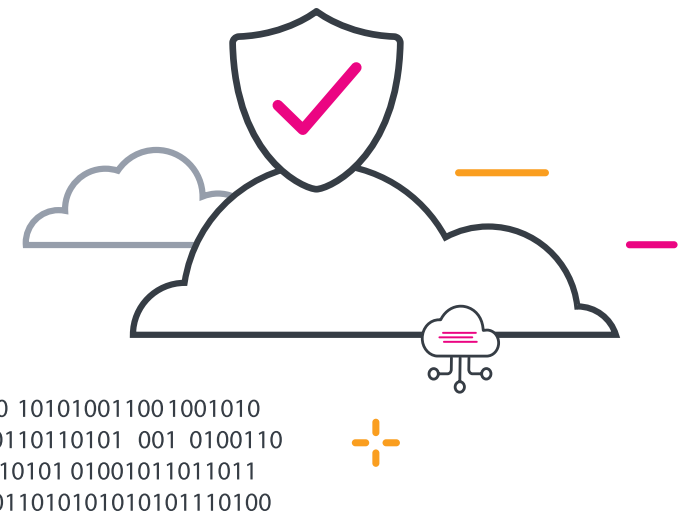
Risiko

Eine sichere Plattform allein bringt nichts, wenn sie nicht richtig verwaltet wird. Laut **Gartner** besteht die Herausforderung nicht in der Sicherheit der eigentlichen Cloud, sondern in den **Richtlinien** und Technologien für die Sicherheit und Kontrolle der Technologie. In fast allen Fällen ist es der Anwender und nicht der Cloud-Anbieter, der die zum Schutz der Unternehmensdaten eingerichteten Kontrollmechanismen nicht richtig verwaltet. Die Fragestellung von CIOs muss daher nicht „Ist die Cloud sicher“ lauten, sondern „Nutze ich die Cloud auf eine sichere Art und Weise?“

Während die Cloud tatsächlich ein solides Sicherheitsniveau und ein bestimmtes Maß an Transparenz hinsichtlich der Datenspeicherung und -verarbeitung bietet, weisen manche Bereiche eine gewisse Intransparenz auf. In Kombination mit einer größeren Angriffsfläche führt dies eventuell zu einer insgesamt schwachen Sicherheitslage. Werden die Daten einer Organisation dann zusätzlich auf mehrere Clouds und eigene Rechenzentren verteilt, wird das Thema Sicherheit noch komplexer und schwerer zu kontrollieren. Hinzu kommt, dass Teams Digitalisierungsprogramme gerne mit Volldampf vorantreiben und sich dabei auf die Erfüllung eigener Sicherheitsanforderungen konzentrieren, allgemeine Sicherheitsanforderungen aber nicht selten übersehen. In Summe führt all dies zu einem höheren Risiko, besonders, wenn das Unternehmen in puncto Netzwerkkontrollen, Zugriffsverwaltungssysteme oder Konfigurationsoptionen nicht auf dem aktuellsten Stand ist. Wer ist für das Risikomanagement verantwortlich? Was, wenn sich niemand darum kümmert?

Datenstrategie

Eine starke Cloud-Security-Strategie ist das Fundament einer soliden Cloud-Datenstrategie: Sie sorgt dafür, dass Sie die Kontrolle über Ihre Daten behalten, während den richtigen Personen dennoch der nötige Handlungsspielraum für ihren Beitrag zum Handling der Sicherheitsrisikos gewährt wird. Dies gilt nicht nur für die üblichen Betriebsdaten, die im klassischen Sinne mit dem Thema Security in Verbindung gebracht werden, sondern auch für sensible Kunden- und Geschäftsdaten. Die Cloud- und Security-Strategie müssen Hand in Hand gehen. Nur so wird sichergestellt, dass Geschäftsanforderungen erfüllt und gleichzeitig Sicherheitskontrollmaßnahmen über verschiedene, an unterschiedlichen Digitalisierungsprojekten arbeitende Teams hinweg umgesetzt werden. Teams sollten die Möglichkeit haben, an verschiedenen Standorten entstehende Probleme unabhängig vom Anwendungstyp mithilfe einer einzelnen, zentralisierten Plattform zu erkennen und zu beheben. Dazu setzen Sie am besten eine Datenplattform ein, die Ihnen ein Sicherheitsniveau mit einheitlicher Cloud-Security bietet und für Transparenz bei all Ihren Datenkontrollen innerhalb einer Multi-Cloud-Umgebung sorgt.



„Der Hauptvorteil für uns war der Schutz des Netzwerk-Edge“, sagt David Bell. „Dadurch war es nicht mehr nötig, dass einzelne Entwicklungsteams Edge-Sicherheitsmodelle für öffentlich zugängliche Endpunkte entwickelten.“

—David Bell, Manager, Infrastructure and Cloud Services, REI

[REI-Erfahrungsbericht lesen](#)

Risiko 4: Neue Tools ohne schlüssiges Konzept

Cloud-Lösungen beinhalten eigene, zweckspezifische Management-Tools, die nur für ihr eigenes Service-Erlebnis optimiert sind, andere Anbieter oder bestehende IT-Management-Tools aber nicht berücksichtigen.

Vorteil

Die Cloud-Technologie ermöglicht Kosteneinsparungen, die zum Teil dadurch entstehen, dass bisherige, lokale Tools und Anwendungen nicht mehr benötigt werden. Aufgrund des insgesamt geringeren Managementaufwands, der in den zur gewählten Cloud-Plattform gehörenden Tools begründet ist, können IT- und Sicherheitsteams ihre Energie auf andere Aufgabenbereiche konzentrieren und somit zeitliche Ressourcen effektiver nutzen und Ausgaben senken.

Risiko

Anbieterorientierte, Cloud-basierte Management-Tools sind in den seltensten Fällen auf die Kompatibilität mit Multi-Cloud-Umgebungen ausgelegt. Daher werden Unternehmen, die voll und ganz auf die Cloud-Technologie umsteigen wollen, oftmals feststellen, dass sie ein gewisses Maß an bereits bestehender Technologie nutzen müssen, um die Lücken zu schließen. In diesem Fall kann es vorkommen, dass ein Unternehmen mehr Zeit damit verbringt, sein vorhandenes Toolset anzupassen, als die tatsächlichen Möglichkeiten der Cloud für die Transformation zu nutzen. Da diese traditionellen Tools zudem nicht dafür konzipiert wurden, die durch die Cloud ermöglichten, modernen Anwendungsarchitekturen zu unterstützen, liefern sie nur bruchstückhafte, ungenaue Ergebnisse. Das bedeutet für das Unternehmen letztlich weniger operative Transparenz, längere Reaktionszeiten, die mehr Ausfallzeiten verursachen, häufiger auftretende Performance-Probleme und ein insgesamt höheres Risiko.

Datenstrategie

Unternehmen benötigen Tools, mit denen sie wettbewerbsfähig bleiben. Das ist jedoch nur mit einem umfassenden Konzept möglich, bei dem auch die bestehende Infrastruktur berücksichtigt wird. Eine adäquate Cloud-Datenstrategie sollte die alten und neuen Systeme mithilfe einer einzelnen Datenplattform zusammenzuführen, womit eine Gesamtübersicht erleichtert wird. Die Plattform sollte auf KI und Machine Learning basierende, belastbare Möglichkeiten bieten, mit denen alle unterschiedlichen Cloud-Services einer Organisation kontinuierlich im Kontext analysiert werden können. Dies gilt vor allem, wenn auch weiterhin bereits bestehende Legacy-Tools verwendet werden sollen. Nur dann kann ein Unternehmen die Identifizierung, Klassifizierung, Prognose und Selbstheilung verschiedener technischer und geschäftlicher Schwierigkeiten wirklich automatisieren, bevor diese zu echten Problemen werden. Erst wenn ein Unternehmen nicht mehr nur auf Probleme reagiert und ältere Technologie zur Lösung moderner Probleme anzupassen versucht, ist es wirklich auf dem Weg der Modernisierung.

Risiko 5: Sich in zu vielen Punktlösungen verzetteln

Es gibt jede Menge Cloud-basierte Punktlösungen – und wenn Sie nicht aufpassen, haben Sie plötzlich alle abonniert.

Vorteil

Wenn Sie damit beginnen, voll und ganz in Cloud-Technologie zu investieren, ist es leicht, zunächst dem Motto „Cloud First“ zu folgen und sich dann auf „Cloud Always“ zu verlegen. Da ist es ganz gleich, mit welchem Problem Ihr Unternehmen konfrontiert wird – es gibt höchstwahrscheinlich eine Cloud-basierte Lösung dafür. Außerdem können Sie bei Bedarf zu anderen Lösungen wechseln. Mit einem ganzen Arsenal an Cloud-basierten Apps und Services sind Organisationen für alles gerüstet und können IT Operations, die Entwicklung des Sicherheitsniveaus und letztendlich das Geschäftsmodell als solches verbessern.

Risiko

Es gibt wahrscheinlich wirklich eine Cloud-Lösung für jedes Problem, aber keine Einzellösung für alles. Ohne umfassende Monitoring- und Observability-Strategie hat Ihr Unternehmen unter Umständen Schwierigkeiten, einen genauen Überblick über den Zustand und die Verfügbarkeit Ihrer Cloud-Services zu behalten. Haben einzelne Teams die Freiheit, die für sie ideale Punktlösung zu kaufen, kann dies schnell zur Silobildung und zu einer Datenüberflutung führen. Analysten sehen sich dann einer exponentiell wachsenden Zahl von Daten-Feeds und Warnmeldungen gegenüber – und das ganz ohne umfassenden Plan, der ihnen bei der Bewältigung dieser Situation

hilft. Dies kann letztlich dazu führen, dass ein Unternehmen feststellen muss, dass die Cloud-Technologie zu einer komplexeren, teureren Umgebung geführt hat, deren Monitoring eine große Herausforderung darstellt. Ihr Unternehmen und ihre Teams fühlen sich eventuell überlastet und können die Vielfalt der Lösungen nicht effizient verwalten.

Datenstrategie

Es ist von entscheidender Bedeutung, dass Einzelpersonen und Teams ihre eigenen Anforderungen definieren können. Dafür braucht es allerdings eine Datenplattform, die eine einzelne, zentrale Ansicht bietet. Diese Plattform sollte nicht nur mehrere externe Plattformen verbinden, sondern auch eine zentrale Oberfläche bieten, mit der IT, Security, DevOps und verschiedene Unternehmensfunktionen einen transparenten Einblick erhalten, um bei Bedarf auf Probleme reagieren zu können. Mit einer zentralen Managementplattform können alle Beteiligten die Zunahme des Datenvolumens und die steigende Geschwindigkeit der Datenerzeugung beobachten und verwalten und so leichter entscheiden, welche Cloud-Lösungen sinnvoll bzw. unnötig sind. Das Ziel ist eine schlanke Infrastruktur – sowohl lokal als auch in der Cloud – ohne aufgeblähte Technologie-Stacks mit mehreren Lösungen, die eigentlich demselben Zweck dienen und nur die Gesamtkomplexität erhöhen.

„Vor Splunk war die Protokollierung unzusammenhängend. Da ein einheitlicher Ansatz fehlte, war es schwierig, sich ein Gesamtbild zu verschaffen. Wir reifen mit dem System und es hat sich gezeigt, dass Splunk die Lösung für unsere grundlegenden Probleme ist.“

—Antonio Guedes, Security Analytics Senior Lead, Mars, Inc.

[Erfolgsbericht von Mars lesen](#)

Risiko 6: Wert der Daten wird nicht ausgeschöpft

Ihrem Unternehmen entgehen Chancen, die sich aus der Verwertung großer Datenmengen ergeben, wenn Sie die Daten nicht effizient auswerten und konkreten Nutzen daraus ziehen.

Vorteil

Die Cloud-Technologie ermöglicht es Organisationen, mehr Interaktionen zu digitalisieren, Apps auf neue Arten und Weisen zu entwickeln und mehr Daten als je zuvor zu erfassen. Werden die Daten richtig genutzt, können sie ganz neue Impulse setzen und eine Vielzahl von Erkenntnissen bieten, die dem Unternehmen zuvor nicht zur Verfügung standen. Dies kann zu Verbesserungen bei der Kundenbindung, der Mitarbeiterproduktivität und der Uptime sowie zu optimierten Prozessen führen. Unternehmen, die verstärkt auf Datennutzung setzen, steigern ihren Jahresumsatz laut [einer Studie von Splunk und ESG](#) um durchschnittlich 5,32 %.

Risiko

Der Wert der Daten wird uns leider nicht auf einem Silbertablett präsentiert. Die Daten müssen verarbeitet, analysiert und verstanden werden, damit sich ihr Wert offenbart. Viele der in Unternehmen erzeugten Daten sind sogenannte **Dark Data** – also unerschlossene, ungenutzte oder unentdeckte Daten. Viele Unternehmen sind schlicht nicht in der Lage, die riesigen, von Cloud-gestützten Systemen generierten Datenmengen effektiv und effizient zu verwerten. In solchen Fällen bleibt die vielgepriesene digitale Transformation aus. Stattdessen entsteht ein

Datenökosystem, das komplexer denn je ist und Kosten verursacht, ohne Mehrwert zu generieren. Wenn Informationen auf mehrere Systeme verteilt und in Silos organisiert sind, ohne dass es eine Strategie für die Datenauswertung gibt, bedeutet dies immense Zusatzkosten.

Datenstrategie

Ohne tiefgreifendes Verständnis der Daten Ihrer Organisation können Sie keine Digitalisierungsprogramme anstoßen. Dark Data – die sowohl von technischen als auch von Business-Systemen generiert werden – müssen organisiert und zentral für den Zugriff verfügbar gemacht werden, damit sie sinnvoll genutzt werden können. Bei einer effektiven Auswertung können diese Daten Optimierungen anstoßen, die von kürzeren Reaktionszeiten bei Serviceunterbrechungen bis hin zu einem besseren Kundenangebot reichen. Woher kommt Dark Data? Dark Data stammt aus mobilen Apps und Microservices, aus neu verbundenen Systemen wie mobilen POS-Systemen, aus Cloud-Monitoring-Tools, aus neuen Systemintegrationen und vielem mehr. Mit dem Einsatz einer Plattform, die solche Echtzeit-Daten-Feeds nutzen kann, sind Unternehmen für einen erfolgreichen Weg in die Cloud gerüstet.

„Wir haben jetzt eine Granularitätsstufe erreicht, bei der wir uns an jeder beliebigen Position der Flughafen-Sicherheitskontrolle ein umfassendes Bild der Performance machen können. Unsere Daten liefern Antwort auf Fragen wie etwa: „Wie können wir die gestrige Ontime Performance verbessern?“ „Was war der Grund für etwaige Defizite?“

—Alex Webber und Paul Bannister, IT Development Specialists, Gatwick Airport

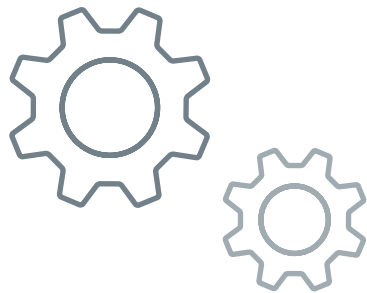
[Erfolgsbericht von Gatwick Airport lesen](#)

Eine intelligente Cloud-Strategie erfordert eine Data-to-Everything Plattform

Die Entwicklung zu einem Cloud-nativen Unternehmen ist nicht immer automatisch eine Garantie für schnellen Erfolg. Bei der Cloud-Nutzung gibt es nicht zu unterschätzende Herausforderungen, auf die Sie vorbereitet sein sollten, um ausufernde Kosten, komplexe Managementprobleme und eine Datenüberflutung zu vermeiden. Einer der zentralen Faktoren für den langfristigen Erfolg in der Cloud besteht darin, dass alle einzelnen Datenquellen – vom Multi-Cloud-System über Sensordaten bis hin zu Kundeninteraktionen – für die Schlüsselpositionen im Unternehmen sofort zur Verfügung stehen und einsehbar sind.

Das ist einfacher gesagt, als getan und lässt sich nur mit der richtigen Plattform erfolgreich realisieren. Splunk, die Data-to-Everything Plattform, wurde dafür entwickelt, Sie bei jedem Schritt in die Cloud zu unterstützen. Splunk erkennt, ob sich Informationen in Ihrem lokalen Rechenzentrum, auf einer öffentlichen oder privaten Cloud-Plattform oder in den umsatzgenerierenden Anwendungen befinden, die Sie entwickeln und verwalten. Damit können Sie einen umfassenden Datenzugriff

in Echtzeit, leistungsstarke Analysen und eine automatisierte Datenerfassung durchführen. Sie können so kritische Unternehmensdaten sofort indizieren und konfigurierbare Warnmeldungen einrichten, die Sie auf potenzielle Schwachstellen und Probleme aufmerksam machen. Bei Unternehmen, die auf Modernisierung und Cloud-native Architekturen setzen, können Plattformen wie Splunk zum Kernstück für die operative Widerstandsfähigkeit werden und dafür sorgen, dass Sie echten Mehrwert aus Ihrer Infrastruktur, Ihren Ressourcen und Ihren Daten ziehen können. Nur mit der richtigen Datenplattform können Sie Risiken auf dem Weg in die Cloud vermeiden und ein robustes Daten-Rückgrat als Basis für echte Innovationen errichten.





Wie können Sie diese sechs Risiken am schnellsten hinter sich lassen? Untersuchen, überwachen, analysieren und handeln Sie mit Splunk Cloud.

Weitere Informationen

Splunk, Splunk>, Data-to-Everything, D2E und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern. © 2020 Splunk Inc. Alle Rechte vorbehalten.

20-14077-SPLK-6-Cloud-Strategy-Pitfalls-How-to-Avoid-Them-103-LS

splunk>
turn data into doing™