ForgeRock

WHITEPAPER

Sechs Trends für die Zukunft der Cloud

Ein Leitfaden für Identity und Access Management-Experten

Executive Summary

Aktuellen Daten zufolge steigt eine rekordverdächtige Anzahl von Unternehmen auf Cloud-Lösungen um. Bis 2024 werden schätzungsweise 45 % der IT-Ausgaben in die Cloud fließen.[1] Gleichzeitig tritt allmählich ein tieferliegendes Problem zutage: Manche Cloud-Implementierungen sind nicht besonders erfolgreich. Tatsächlich ist es sogar so, dass 80 % der CIOs angaben, mit der Migration in die Cloud nicht die gewünschte geschäftliche Agilität erreicht zu haben.[2]

Dieses Whitepaper beleuchtet die sechs wichtigsten Trends, die Identitätsexperten bei der Planung ihrer Cloud-Strategie berücksichtigen sollten. Für ein exponentielles Wachstum müssen Sie nicht nur den Trends voraus sein, sondern auch Wege finden, wie Sie diese vollumfänglich implementieren können, um positive Ergebnisse zu erzielen.

[1]https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/
[2]https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/unlocking-business-acceleration-in-a-hybrid-cloud-world

Sechs Trends für die Zukunft der Cloud

Ein Leitfaden für Identity and Access Management-Experten

Einführung

Der Vormarsch der Cloud ist nicht mehr aufzuhalten. Konfrontiert mit der Aufgabe, neue digitale Initiativen vor der Konkurrenz umzusetzen, stehen viele Unternehmens- und IT-Leiter unter dem Druck, sich die Geschwindigkeit, Flexibilität und Kostenersparnis der Cloud zunutze zu machen. Gartner schätzt, dass „siebzig Prozent der Workload in Unternehmen bis 2024 in der Cloud liegen werden – und dennoch verfügen drei von vier Unternehmen nicht über eine geeignete Cloud-Strategie“. Damit Ihre Cloud-Implementierung ein Erfolg wird, sollten Sie die folgenden wichtigen Trends berücksichtigen, die die Zukunft der Cloud bestimmen werden.

> By 2024, more than 45% of IT spending will shift from traditional solutions to the cloud.
>
> Gartner®

Sechs Cloud-Trends

1. Innovation und Kostenersparnis

Durch den Wechsel in die Cloud, spart Ihr Unternehmen Geld. Damit verlagert sich der Schwerpunkt jedoch von Investitionskosten auf Betriebskosten. Gleichzeitig bringen die weitreichenden Innovationen in der Cloud die traditionellen Verfahren Ihres IT-Managements ins Wanken, was eine Anpassung und Veränderung der Prozesse erfordert.

2. Multi-Cloud-Strategie

Minimieren Sie Ihre Abhängigkeit von einem einzigen Cloud-Anbieter und bewahren Sie sich gleichzeitig Flexibilität und Kontrolle.

3. Hybrid-Cloud

Eine sinnvolle Cloud-Migrationsstrategie erfordert, dass die Ausführung Ihrer geschäftskritischen Anwendungen vor Ort unterstützt wird, während Sie in die Cloud wechseln, was zu einer Hybrid-Cloud-Umgebung führt.

4. Cloud-native Architekturen

Indem Sie Microservice-Architekturen und Funktionen der Cloud-nativen Architektur nutzen, können Sie Ihre Agilität erhöhen und Ihre Kosten senken.

5. Sicherheit und Datenschutz

Sie benötigen eine sichere Cloud mit vollständiger Mandantenisolierung, um eine optimale Leistung zu gewährleisten, das Risiko eines versehentlichen oder böswilligen Ausspähens zu verringern und die Einhaltung der gesetzlicher Vorschriften sicherzustellen.

6. Identität als einzige Sicherheitsgrenze

Die Zunahme von Online-Shopping und Home Office bringt ein höheres Risiko mit sich und erfordert Sicherheitsvorkehrungen, die über die Netzwerkgrenzen hinausgehen. Der Schutz geschäftskritischer Anwendungen ist nur durch eine identitätsbasierte Sicherheitsstrategie zu erreichen.

Die sechs wichtigsten Cloud-Trends und ihre Auswirkungen auf IAM

Für IAM-Experten (Identity and Access Management) bedeutet der Wechsel in die Cloud tiefgreifende Veränderungen, die sowohl ihre Aufgaben als auch ihre Arbeitsabläufe auf den Kopf stellen. Branchen- und länderübergreifend haben sich aktuelle Trends im Cloud-Kontext herauskristallisiert. All diese Trends beeinflussen die Art und Weise, wie IAM-Experten ihre Arbeit heute und in Zukunft ausüben.

TREND 1

Innovation und Kostenersparnis

Die Hauptgründe für den Wechsel in die Cloud sind: Schnelligkeit, einfache Innovation und Senkung der IT-Kosten. In einer Cloud-Umgebung kann Ihr Entwicklungsteam neue Angebote schneller bereitstellen. Sie können Ihr Portfolio an Anwendungen, Produkten und Diensten auf einfache Weise erweitern und neue Features einführen, um die Funktionalität und Benutzerfreundlichkeit zu verbessern. Und da Sie keine eigene IT-Infrastruktur einrichten oder eigene Server betreiben, verwalten oder warten müssen, spart Ihr Unternehmen sowohl Investitions- als auch Betriebskosten.

Dennoch setzen Unternehmen im Durchschnitt 30 % ihrer Cloud-Ausgaben nicht mit der richtigen Priorität ein[3] und müssen neue und bessere Wege zur Optimierung ihrer Cloud-Lösungen finden.

„Ich wollte eine flexible Lösung, die für unseren globalen B2B2C-Markt geeignet ist. Ein erstklassiges Kundenerlebnis ist das A und O unseres Geschäfts. Damit uns dies gelingt, müssen wir viele Dinge über den Nutzer, seine Identität und sein Anliegen kennen."

Daryl Robbins
Senior Director of Global Architecture, Calabrio

Die IAM-Anforderungen Ihres Unternehmens übersteigen die Möglichkeiten vieler Cloud-Angebote – insbesondere solcher, die sich auf begrenzte Anwendungsfälle konzentrieren und mit unvorhersehbaren Kosten verbunden sind. Eine moderne Identitätslösung ist das Rückgrat, um sichere, einfache und innovative Lösungen in einer komplexen Umgebung zu realisieren. Die ideale IAM-Lösung bietet eine erweiterbare Integration mit Systemen und Unterstützung für Anwendungsprogrammierschnittstellen (APIs), Microservices und IoT-Geräte (Internet of Things). Eine moderne IAM-Lösung verfügt zudem über fortschrittliche

Durch den Einsatz einer modernen Identity and Access Management-Plattform zur Unterstützung von Multi-Cloud-Initiativen können die Implementierungskosten um bis zu 25 % gesenkt und der ROI um 50 % gesteigert werden.

Funktionen zur Unterstützung von Innovationen, No-Code- und Low-Code-Orchestrierung für das Onboarding, passwortlose Self-Service-Authentifizierung und erweiterte Autorisierungsrichtlinien. Um Ihre Kosten zu senken, sollten Sie sich für eine Identitätslösung entscheiden, die einfache und flexible Abonnements mit vorhersehbaren Preisen bietet.

TREND 2

Multi-Cloud-Strategie

Knapp 81 % der Unternehmen nutzen derzeit mehrere Cloud-Anbieter oder planen dies für die nächsten 12 Monate; vor der globalen Pandemie waren es lediglich 12 %.[4]
In den Anfangstagen der Umstellung auf die Cloud hat sich Ihr Unternehmen möglicherweise für einen einzigen Cloud-Anbieter entschieden. Wie die meisten großen Unternehmen benötigen Sie jedoch eine Multi-Cloud-Strategie, um anbieterspezifische Beschränkungen zu überwinden, die Abhängigkeit von einem bestimmten Anbieter zu vermeiden und die Kontrolle und Flexibilität des Unternehmens in Bezug auf Daten und Kosten zu verbessern. Ganz gleich, ob Sie eine Kombination aus

[3]https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/
[4]https://www.zdnet.com/article/research-multicloud-deployment-increases-among-enterprises/

beliebten Cloud-Service-Anbietern wie Microsoft Azure, Amazon Web Services (AWS) oder Google Cloud Platform nutzen: Indem Sie die richtige Plattform für jede Ihrer spezifischen Anwendungen und Anforderungen auswählen, können Sie die spezifischen Funktionen der einzelnen Plattformen optimal nutzen.

Wenn Identitäten isoliert vorliegen und jeder Cloud-Anbieter nur für sein eigenes Ökosystem IAM-Funktionen anbietet, ist die versprochene Agilität von Multi-Cloud-Umgebungen begrenzt. Eine umfassende, integrierte IAM-Plattform, die Hybridumgebungen vereinen, integrieren und sichern kann, überbrückt hingegen die Kluft zwischen On-Premises- und Cloud-Umgebungen und ermöglicht Ihnen somit nahtlose Abläufe.

> „Die Zukunft liegt nicht allein in der Cloud, sondern in der Hybrid-Cloud. Diese versetzt Unternehmen in die Lage, ihr Geschäftsmodell neu zu gestalten und schneller zu modernisieren. IAM muss dabei im Mittelpunkt stehen, damit die Zukunft ebenso reibungslos wie sicher verläuft."
>
> **Hamidou Dia**
> **Vice President, Global Head of Solutions Engineering, Google Cloud at Google**

TREND 3

Hybrid-Cloud

Während eine Multi-Cloud-Strategie mehrere Cloud-Anbieter umfasst, besteht eine Hybrid-Cloud-IT-Architektur aus Anwendungen, Diensten und Systemen, die sich in privaten und öffentlichen Clouds sowie in lokalen Umgebungen befinden. Die Hybrid-Cloud trägt der Notwendigkeit Rechnung, einige Daten und Anwendungen vor Ort und unter strenger Kontrolle zu halten, während andere in die Cloud verlagert werden. Auch Anforderungen an die Datenhoheit können eine Rolle spielen, z. B. wenn das Unternehmen sicherstellen muss, dass bestimmte Daten nur in spezifischen geografischen Regionen gespeichert werden.

Ein kürzlich veröffentlichter Bericht von Forrester zeigt, dass fast ein Viertel der befragten IT-Entscheider weltweit bereits eine Hybrid-Cloud-Lösung eingeführt haben und dass weitere 52 % der Befragten beabsichtigen, innerhalb der nächsten zwei Jahre eine Hybrid-Cloud-Lösung einzuführen oder deren Einsatz auszuweiten.[5]

Eine IAM-Lösung, die sowohl On-Premises- als auch Cloud-Anwendungen unterstützt und mit älteren und selbstentwickelten Anwendungen koexistieren und diese ergänzen kann, ist für die Sicherheit einer Hybrid-Cloud-Umgebung von entscheidender Bedeutung. Sie müssen sich darauf verlassen können, dass ein IAM-Service alle digitalen Identitäten in einer hybriden IT-Umgebung ausführen, vereinen und sichern kann.

TREND 4

Cloud-native Architekturen

Durch die Nutzung von Cloud-nativen Technologien wie Containern, dynamischer Orchestrierung, Microservices und serverlosen Architekturen können Sie Ihre Agilität erhöhen, die Markteinführung beschleunigen und die Kosten weiter senken. Gartner prognostiziert, dass bis 2023 70 % der Unternehmen weltweit mehr als zwei containerisierte Anwendungen in der Produktion einsetzen werden – im Vergleich zu weniger als 20 % im Jahr 2019. Nach Prognosen von IDC werden bis 2021 sogar 95 % der neuen Microservices in Containern bereitgestellt werden.[6]

Mithilfe von Containern können Sie eine Anwendung mit allen benötigten Komponenten – Bibliotheken, Code und anderen abhängigen Elementen – bündeln und als ein Paket bereitstellen. So können Sie sich auf das Schreiben von Code konzentrieren, ohne sich Gedanken über das System zu machen, auf dem dieser ausgeführt wird, was wiederum die Bereitstellung beschleunigt, die Sicherheit erhöht und die Skalierbarkeit verbessert.

Microservices bieten einen äußerst skalierbaren, flexiblen Ansatz für die Erstellung von Cloud-Anwendungen, da sie die Aufteilung einer Anwendung in einzelne Dienste

IAM-Plattformen müssen selbst Cloud-nativ sein und einige dieser Funktionen nutzen, wie z. B. eine dynamische containerisierte Architektur, die auf Kubernetes-Clustern ausgeführt wird, und serverlose Implementierungen, um diese Cloud-nativen Architekturen zu skalieren und zu unterstützen.

[5]https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam
[6]https://www.entrepreneur.com/article/345826

Um die Sicherheit in einer Cloud-Umgebung zu gewährleisten, dürfen die Daten Ihres Unternehmens keinesfalls mit den Daten anderer Unternehmen vermischt werden. Eine IAM-Lösung mit vollständiger Mandantenisolierung gewährleistet, dass Identitäten aus einer Umgebung in keiner anderen gültig sind. So ist sichergestellt, dass ein versehentlicher oder böswilliger Zugriff auf eine andere Kundenumgebung keine Auswirkungen auf Ihre Umgebung hat.

ermöglichen. Mit Microservices können Ihre Entwickler Anwendungen leicht ändern, ersetzen oder skalieren. Zudem sind die Testzyklen kürzer und die Zusammenarbeit einfacher, sodass Ihr Unternehmen schnell auf veränderte Anforderungen reagieren kann.

Microservices und die zunehmende Verwendung von APIs bedeuten, dass Sie die Sicherheits- und Identitätsanforderungen auf ähnliche Weise verwalten müssen, wie Sie die Identitätsanforderungen Ihrer Benutzer verwalten. Sie benötigen folglich eine einzige IAM-Plattform, die für die Skalierung und Ausführung in der Cloud Ihrer Wahl die Cloud-native Architektur nutzen kann, um diese APIs und Microservices zusammen mit den Benutzeridentitäten zu sichern.

TREND 5

Kostenexplosion durch immer strengere gesetzliche Vorschriften

Die Sicherung der Cloud hat nach wie vor höchste Priorität. Gartner geht davon aus, dass die Ausgaben für Cloud-Sicherheit im nächsten Jahr von 595 Millionen US-Dollar auf 841 Millionen US-Dollar steigen werden – ein Zuwachs von 41,2 %.[7] Gleichzeitig nennen viele Unternehmen Sicherheitsprobleme als eines der größten Hindernisse[8] für die Einführung der Cloud. Möglicherweise haben auch Sie beim Wechsel in die Cloud angenommen, dass Ihre Daten durch redundante, diversifizierte Server, die von einem Drittanbieter verwaltet werden, gut geschützt sind. Es reicht jedoch nicht aus, die Daten während der Speicherung und Übertragung zu verschlüsseln. Um zu verstehen, wo und wie Ihre Daten gespeichert werden und wie sich dies auf Ihre Anwendungen auswirkt, wenn Sie die Daten abrufen, müssen Sie etwas genauer hinschauen.

In einer mandantenfähigen Cloud-Umgebung müssen Sie sicherstellen, dass andere Mandanten die Leistung Ihrer geschäftskritischen Funktionen nicht beeinträchtigen können. Dieses Problem – auch „Noisy Neighbor" genannt – tritt auf, wenn ein Mandant die verfügbaren Ressourcen in Beschlag nimmt und dadurch Leistungsprobleme für andere Mandanten verursacht, die die gleiche Infrastruktur nutzen.

TREND 6

Identität als einzige Sicherheitsgrenze

Mitarbeiter, Partner, Auftragnehmer und Kunden benötigen jeweils unterschiedliche Zugriffsrechte auf die Anwendungen, die lokal und in der Cloud ausgeführt werden. Die veränderten Unternehmensgrenzen in Verbindung mit der immensen Anzahl von Benutzern, Geräten und Anwendungen führen zu vielen potenziellen Fehlerquellen. Vorbei sind die Zeiten eines fest definierten Netzwerks, das an den Grenzen geschützt werden kann. Ihr

„Identitätsbasierte Richtlinien ermöglichen eine wesentlich differenziertere und schnellere Kontrolle des Netzwerkzugriffs, um die Angriffsfläche insgesamt zu verringern. Darüber hinaus bietet Zero Trust Edge (ZTE) eine deutlich höhere Transparenz über die Identitäten von Personen und Maschinen/Workloads, die auf beliebige Hybrid-Cloud- oder On-Premises-Ressourcen zugreifen."

The Top Trends Shaping Identity and Access Management in 2021, Forrester[9]

[7]https://www.techrepublic.com/article/cybersecurity-spending-to-hit-150-billion-this-year/
[8]https://cloudsecurityalliance.org/press-releases/2021/03/30/cloud-security-alliance-releases-latest-survey-report-on-state-of-cloud-security-concerns-challenges-and-incidents/
[9]https://www.forrester.com/report/The+Top+Trends+Shaping+Identity+And+Access+Management+In+2021/RES166097

Netzwerk beginnt, sobald Benutzer auf eine Anwendung zuzugreifen versuchen, egal ob sie zu Hause, im Büro oder in einem Café arbeiten. Deshalb ist in der heutigen Zeit Zero-Trust-Sicherheit auf der Grundlage von Benutzeridentitäten unerlässlich. Das heißt:

Die Identität ist heute die einzige Sicherheitsgrenze. Eine gut implementierte IAM-Plattform stellt sicher, dass geschäftskritische Daten geschützt sind – sowohl in der Cloud als auch bei einem Wechsel von einem Cloud-Service zu einem anderen.

Viele Unternehmen greifen diesen Trend auf und wissen, dass robuste Sicherheit mit der Nutzung der nativen Sicherheitsfunktionen des Dienstanbieters beginnt – aber das ist erst der Anfang. Um unbefugte Zugriffe und Datenschutzverletzungen zu verhindern, braucht es darüber hinaus umfangreiche, identitätsspezifische Authentifizierungs- und Autorisierungsrichtlinien. Das Prinzip der minimalen Zugriffsrechte, d. h. die Gewährleistung, dass Benutzer, Anwendungen und Geräte nur auf die Daten und Ressourcen zugreifen können, die sie für ihre berechtigten Zwecke unbedingt benötigen, ist der Schlüssel zum Schutz der neuen Grenzen. Daraus ergibt sich die Notwendigkeit eines umfassenden und strengen IAM, das Identitäten über On-Premises- und Cloud-Umgebungen hinweg vereinheitlichen und verwalten kann – und zwar für alle Benutzer und zu jeder Zeit.

ForgeRock Identity Cloud: Hohes Vertrauen und großartige Erlebnisse mit Hilfe dieser Trends

ForgeRock Identity Cloud ist eine umfassende Identity and Access Management-Plattform, die als Service bereitgestellt wird. Identity Cloud unterstützt Ihr Unternehmen auf vielfältige Weise:

1. Bereiten Sie erstklassige Erlebnisse, minimieren Sie die Risiken und senken Sie die Kosten durch eine umfassende Identitätsplattform.
2. Profitieren Sie von modernstem Identitätsmanagement, ohne sich um Wartung, Patches und Upgrades kümmern zu müssen.
3. Steigern Sie Ihre Produktivität, indem Sie eine einzige Plattform für alle Identitäts- und Zugriffsanforderungen nutzen: Benutzer, Geräte, Dinge, APIs, Dienste und vieles mehr.
4. Unterstützen Sie geschäftskritische Anwendungen, die lokal und in der Cloud ausgeführt werden, um ein sicheres hybrides Unternehmen zu erschaffen.
5. Nutzen Sie eine patentierte Sicherheitsarchitektur mit Datenisolierung, die Ihnen die volle Kontrolle bietet.
6. Treiben Sie Innovationen und Wachstum in Ihrem Unternehmen voran ohne kostspielige Überschreitungsgebühren – jetzt und in Zukunft.

Mit Identity Cloud meistern Sie spielend die sechs Cloud-Trends, die zur Unterstützung Ihrer Cloud-Strategie unerlässlich sind. Das Ergebnis: erstklassige Benutzererlebnisse, unübertroffene Sicherheit und niedrigere Kosten.

Zusammenfassung

Die sechs Cloud-Trends verdeutlichen die tiefgreifenden, rasanten Auswirkungen der Cloud auf Ihr Unternehmen und die Notwendigkeit eines dynamischeren, sichereren und effizienteren Identitätsmanagements. Identity Cloud bietet IAM für das hybride Unternehmen – damit Ihr Unternehmen alle digitalen Identitäten mit einer einzigen Plattform in einer hybriden IT-Umgebung verwalten, vereinen und schützen kann.

Nächste Schritte

Planen Sie jetzt die Zukunft Ihres Unternehmens in der Cloud und verschaffen Sie sich einen Wettbewerbsvorteil durch die frühzeitige Einführung von Hybrid IAM. Die als Download verfügbare ForgeRock Identity Cloud Checkliste enthält eine ausführliche Liste der zehn wichtigsten Überlegungen und Best Practices für Ihre Identity Cloud-Strategie.