

ForgeRock: Ihr Katalysator für die Unternehmenstransformation

Für den weltweit steigenden Bedarf an digitalen Verbindungen braucht es eine fortschrittliche und umfassende Identitätsplattform

Zusammenfassung	2
Von der Evolution zur Revolution: Das neue Tempo der digitalen Transformation	3
Digitale Identität: Ein Katalysator für die Unternehmenstransformation	3
Das Legacy-Dilemma	4
Der Weg in die Zukunft mit ForgeRock	5
Erlebnisse ohne Brüche	7
ForgeRock Intelligent Access: Einfach und umfassend.....	7
Registrierungserfahrungen.....	8
Abschied von Passwörtern – und Benutzernamen.....	8
Ein neues Konzept für vergessene Zugangsdaten.....	9
Unvergleichliche Intelligenz mit ForgeRock Autonomous Identity	10
Kompromisslose Sicherheit	11
Ein leistungsstarkes Technologie-Ökosystem.....	12
Datenschutz und Compliance.....	13
Moderne Enterprise-Cloud	14
Identität an der Peripherie	15
Beliebig einsteigen und weiterwachsen mit ForgeRock	16

Zusammenfassung

Menschen jeden Alters sind heute darauf angewiesen, mobil arbeiten, lernen und leben zu können. Der Anstieg mobiler Aktivitäten hat auch zu einer drastischen Zunahme von Cyberkriminalität und Betrug geführt. Durch diese neue Realität werden digitale Erlebnisse, Sicherheit und Datenschutz für Verbraucher, Mitarbeiter und vernetzte Dinge wichtiger als je zuvor. Das hat Unternehmen dazu veranlasst, ihre digitale Transformation mit beispiellosem Tempo voranzutreiben.

Identity and Access Management (IAM) ist die Grundlage für den Geschäftserfolg. Ein gutes IAM kann ein Katalysator der Digitalisierung sein. Ein schlechtes kann den Fortschritt behindern. Organisationen, die die unternehmerischen „Checks and Balances“ umgehen, um schneller voranzukommen, könnten später Verzögerungen bei der Integration erleben.

Die meisten Unternehmen haben in punkto IAM dieselben Anforderungen und Zielsetzungen:

- › Den Umsatz bei gleichzeitiger Kostensenkung und kürzerer Amortisierungszeit ankurbeln
- › Auf dem digitalen Marktplatz durch hervorragende Nutzererlebnisse wettbewerbsfähig sein
- › Risiko und Compliance ohne Abstriche beim Nutzererlebnis effektiv managen
- › Moderne Geschäftsanwendungen entwickeln und Altsysteme elegant auslaufen lassen
- › Verfügbarkeit von neuen Arbeitskräften an entfernten Standorten sichern und einen effizienten intelligenten Zugang zu internen Systemen gewährleisten

Als anerkannter Branchenführer verhilft ForgeRock Menschen durch außergewöhnliche digitale Erfahrungen und kompromisslose Sicherheit, Datenschutz und Compliance zu einem sicheren und problemlosen Zugriff auf die vernetzte Welt. Die [ForgeRock Identity-Plattform](#) ist die einzige vollständige digitale Identitätsplattform, die:

- › beispiellose KI-Fähigkeiten (Künstliche Intelligenz, KI) bietet
- › umfassende IAM- und Identity Governance und Administrationsfähigkeiten (IGA) aufweist
- › in einer Organisation für alle Identitäten und Anwendungsfälle (Mitarbeiter, Verbraucher, Dinge) implementiert werden kann
- › alle wesentlichen IAM-Funktionen in einer beliebigen Kombination von unserer Cloud, Ihrer Cloud oder der Public Cloud bietet

Dieses Whitepaper beschreibt die aktuellen Trends und zeigt, wie die einzigartigen Fähigkeiten der ForgeRock-Plattform Organisationen dabei helfen, ihre Herausforderungen in den Bereichen IAM und Identity Governance and Administration (IGA) innerhalb ihrer individuellen Umgebungen, Zeitpläne und Handlungsräume zu meistern.



Von der Evolution zur Revolution: Das neue Tempo der digitalen Transformation

Die aktuelle neue Realität hat Unternehmen dazu veranlasst, ihre digitale Transformation mit beispiellosem Tempo voranzutreiben. Bis vor kurzem verfolgten die meisten Unternehmen einen evolutionären Weg zur digitalen Transformation. Nun hat sie die Notwendigkeit zu einer [digitalen Revolution](#) gezwungen.

COVID-19 hat den Online-Datenverkehr nachhaltig nach oben getrieben, und zwar auf einem Niveau, das normalerweise im Zusammenhang mit Großveranstaltungen wie dem Black Friday oder den Olympischen Spielen zu beobachten ist – Veranstaltungen, die traditionell Monate oder Jahre im Voraus geplant wurden. Das ist heute die Realität in den Bereichen Online-Handel, Bildung, Gesundheitswesen, Bankwesen, Telekommunikation und anderen Branchen, da sich Menschen aller Altersgruppen auf eine neue, mobile Lebens- und Arbeitsweise einstellen.

Während diese neue Realität Unternehmen dazu gezwungen hat, sich durch Bürokratie und Verwaltungsaufwand zu kämpfen, hat sie auch neue Risiken mit sich gebracht. Betrugsfälle haben zugenommen, denn Cyberkriminelle profitieren von Unternehmen, die in dem verzweifelten Bemühen, mit der Entwicklung Schritt zu halten, auf die üblichen Vorsichtsmaßnahmen verzichten. Organisationen, die

Im Zuge der COVID-19-Pandemie erfolgte ein massiver Übergang von „persönlichen“ zu digitalen Beziehungen. So verzeichnete beispielsweise ein großes Finanzinstitut eine Zunahme beim Online-Banking von 300 %, während der Kundenverkehr in den örtlichen Filialen gleichzeitig um 51 % zurückging.

typische Schranken und Überprüfungen zugunsten eines schnellen Agierens umgehen, laufen Gefahr, Insektlösungen einzuführen, die später in die Unternehmensarchitektur integriert werden müssen.

Durch die unerwartete Beschleunigung der digitalen Transformation stehen Unternehmen stärker als zuvor vor existenziellen geschäftlichen Aufgaben. Da [praktisch alle und alles miteinander verbunden ist](#), sind digitale Erlebnisse, die sicher sind und Datenschutz gewährleisten, wichtiger als je zuvor. Das gilt für alle Identitätsarten - Verbraucher, Mitarbeiter oder Dinge. Die Transformation ist nur dann erfolgreich, wenn gute digitale Erlebnisse mit Sicherheit und Datenschutz einhergehen.

Bis 2022 werden Unternehmen, die ein herausragendes Kundenerlebnis bieten, schätzungsweise 20 % mehr Umsatz erzielen als Unternehmen mit einem weniger optimalen Kundenerlebnis.¹

Digitale Identität: Ein Katalysator für die Unternehmenstransformation

Organisationen nutzen digitale Identität, um zur richtigen Zeit den richtigen Zugang zu den richtigen Personen und Dingen zu ermöglichen – wo, wann und wie sie ihn benötigen – und gleichzeitig unberechtigten Zugriff zu verhindern. Dies wird gemeinhin auch als Identity and Access Management oder IAM bezeichnet. Und da für die meisten Online-Transaktionen ein bekannter Nutzer verlangt wird, ist IAM sowohl für Anwendungsfälle mit Verbrauchern als auch mit Mitarbeitern von entscheidender Bedeutung. Für Kunden müssen Unternehmen einfache und sichere Omnichannel-Erlebnisse bieten, um sie zufriedenzustellen und an sich zu binden. Auch das Mitarbeitererlebnis muss hervorragend sein, wobei in diesem Fall ist das Ziel darin besteht, ihre Produktivität zu erhalten und sie zu schützen.

¹ Gartner-Konferenz zum Thema „Identity and Access Management“, Keynote: „The Future Identity and Access Management in 2019 and Beyond“, Gregg Kreizman und Mary Ruddy.

In jüngster Zeit hat sich IAM aufgrund seiner direkten Auswirkungen auf das Geschäft zu einer Top-Priorität entwickelt. Auch wenn einige Organisationen ihre IT-Ausgaben kürzen, hat IAM nach wie vor höchste Priorität, wobei die meisten Initiativen im Bereich Identity and Access Management sogar mit noch größerem Nachdruck vorangetrieben werden.

Das Thema Identität richtig zu handhaben bedeutet, Ihren Kunden und Mitarbeitern die digitale Verbindung zu Ihnen zu erleichtern – dazu gehören eine einfache Anmeldung, ein problemloses Zurücksetzen von Passwörtern, personalisierte digitale Inhalte sowie die Wahrung von Sicherheit und Privatsphäre.

Identität kann auch Ihre Unternehmensentwicklung beeinflussen und Ihre Marke zu einem Begriff werden lassen. Bis 2022 werden Unternehmen, die ein herausragendes Kundenerlebnis bieten, schätzungsweise 20 % mehr Umsatz erzielen als Unternehmen mit einem weniger optimalen Kundenerlebnis.²

“Unsere Partnerschaft mit ForgeRock ist für Telkomsel einer der Bausteine von digitalen Transformationsinitiativen. Der Anforderungsumfang und eine schnelle Einführung waren mit die Hauptgründe für Telkomsel, eine Partnerschaft mit ForgeRock einzugehen.“

– Telkomsel CIO Pak Bharat Alva

Das Legacy-Dilemma

Im heutigen von Budgetknappheit geprägten Umfeld ist der Druck, [sichere moderne Identitäts- und Zugangserfahrungen](#) zu bieten, größer denn je. Neue Anforderungen machen neue Technologien notwendig, die über digitale Ökosysteme hinweg interoperabel und in der Lage sind, Ihre Zielgruppe an jedem Berührungspunkt zu kennen und sicher zu bedienen. IAM ist die Grundlage für digitalen Erfolg, doch viele Unternehmen kämpfen mit veralteter IAM-Software.

Alte IAM-Software bremsen die digitale Transformation. Siloartige und unflexible Identity-Lösungen erhöhen die Sicherheitsrisiken und bieten suboptimale Nutzererfahrungen, während Interoperabilitäts- und Skalierungsprobleme die Betriebskosten in die Höhe treiben. Legacy-Software kann jedoch nicht von jetzt auf gleich ersetzt werden. Das Risiko, die Kosten und die Zeit, die erforderlich sind, um diese Lösungen außer Betrieb zu nehmen und völlig neue Lösungen zu implementieren, stellen für die meisten Unternehmen eine große Herausforderung dar.

Es muss nicht mehr zwischen IAM-Teillösungen entschieden werden, die zwar einen geschäftlichen Problembereich angehen, andere jedoch vermeiden, oder schlimmer noch, zu neuen Problemen führen.

Die Umstellung auf eine neue Lösung ist eine beängstigende Vorstellung. Es muss keine Einzellösung mehr gewählt werden, die ein Geschäftsproblem löst, andere jedoch nicht.

Heute ist ein unternehmensweiter, strategischer Ansatz in punkto digitale Identität möglich. Dazu gehören bessere Nutzererlebnisse, die die Helpdesk-Kosten senken und zugleich die Kundentreue und Konversionsraten erhöhen, die Produktivität der Mitarbeiter steigern, mehr Sicherheit und Datenschutz bieten, Risiken reduzieren und die Einhaltung gesetzlicher Regelungen verbessern.

² Gartner-Konferenz zum Thema „Identity and Access Management“, Keynote: „The Future Identity and Access Management in 2019 and Beyond,“ Gregg Kreizman und Mary Ruddy.

KuppingerCole [bezeichnet diesen strategischen Ansatz](#) als „Identity Fabric“ (Identitätsgefüge):

„Digitale Identitäten sind das Herzstück der digitalen Transformation. Ohne die Fähigkeit, Identitäten zu vereinheitlichen und den Zugang aller zu allen digitalen Diensten effektiv zu verwalten, werden Transformationsansätze scheitern. Unternehmen können es sich nicht leisten, diese Funktionen auf einer Pro-Dienst-Basis zu implementieren – das erhöht die Kosten, verlangsamt die Markteinführung und führt zu neuen Identitätssilos, was wiederum das Benutzererlebnis beeinträchtigt. Durch die Einrichtung eines Identitätsgefüges, das Identitätsdienste für die neuen digitalen Geschäftsservices bereitstellt, können Unternehmen die Anforderungen digitaler Transformationsansätze schnell umsetzen und gleichzeitig eine schrittweise Migration ihres alten IAM ermöglichen.“

– KuppingerCole³

Der Weg in die Zukunft mit ForgeRock

Wir von ForgeRock helfen Menschen dabei, sicher und einfach die vernetzte Welt zu betreten. Die [ForgeRock Identity-Plattform](#) hilft Ihrem Unternehmen, mit der branchenweit einzigen umfassenden [KI-gesteuerten Plattform](#) alle IAM-Funktionen, einschließlich [Identity Management](#), [Governance](#) und [Access Management](#) grundlegend zu verbessern und zu skalieren.

Fallstudie: Die BBC musste während COVID-19 stark skalieren, um Millionen von Zugriffsanfragen von Bürgern zu bewältigen, die den Sender zu verschiedenen Tageszeiten für Live-Nachrichten und Streaming-Inhalte einschalteten. Mit ForgeRock waren sie in der Lage, [auf einem völlig neuen Niveau zu skalieren](#) und die [IAM-Anforderungen](#) problemlos zu erfüllen.

ForgeRock ermöglicht nahtlose personalisierte digitale Erlebnisse dank Funktionen wie [ForgeRock Go](#). Dabei handelt es sich um einen einzigartigen Lösungsansatz für die hohen Kosten im Zusammenhang mit vergessenen Zugangsdaten. Mit unserer auf künstlicher Intelligenz (KI) basierenden Plattform, die das Identitätsmanagement und die Governance optimiert, helfen wir Ihnen zudem, Risiken zu reduzieren und die operative Effizienz zu steigern. Das gilt für jede Identität – [Verbraucher](#), [Mitarbeiter](#) und [Dinge](#) – mit allen wesentlichen Funktionen, die Sie in beliebiger Kombination von unserer Cloud, Ihrer Cloud oder Public Cloud benötigen.

³ <https://www.forgerock.com/resources/whitepaper/kuppingercole-digital-transformation-requires-modern-identity-fabric>

Die KI-gestützte ForgeRock Identity-Plattform:



Abbildung 1: Die ForgeRock Identity-Plattform

Die IAM-Plattform von ForgeRock ist einzigartig in der Branche. Die ForgeRock-Identity-Plattform vereint eine Reihe fortschrittlicher Technologien, die den Anforderungen eines jeden Unternehmens gerecht werden, darunter Identitätsmanagement, Governance und Analytik, Zugriffsmanagement, [Verzeichnisdienste](#), [benutzerverwalteter Zugriff](#), [Edge-Sicherheit](#) sowie ein [Identitäts-Gateway](#).

„Aufgrund der Effizienzgewinne durch die Modernisierung unserer IAM-Infrastruktur mithilfe der ForgeRock Identity Plattform haben wir Kosteneinsparungen von bis zu 15 Millionen US-Dollar über einen Zeitraum von fünf bis sechs Jahren zu verzeichnen.“

– Dave Fletcher, Chief Technology Officer, Bundesstaat Utah

Erlebnisse ohne Brüche

Sich für ein neues Konto anmelden oder Benutzernamen und Passwörter eingeben, macht niemand gerne. Schleppende, mühsame Nutzererlebnisse schaden Ihrem Geschäft. Der Standard beim digitalen Erlebnis ist heute, auf „Kaufen“ zu klicken und am nächsten Tag ein Amazon-Prime-Paket in Empfang zu nehmen. ForgeRock liefert das Fachwissen und den Umfang, um Ihr Unternehmen dabei zu unterstützen, ähnlich hervorragende digitale Erlebnisse zu bieten. Wenn jeder Klick zählt, ist ein IAM-System erforderlich, das reibungslos läuft und zugleich umfassend genug ist, um auch die komplexesten Integrationen zu bewältigen.

„...war es für uns außerordentlich wichtig, dass die Benutzerauthentifizierung im Fahrzeug das gleiche Erscheinungsbild wie das Online-Portal hat und die gleichen Zugangsdaten verlangt.“

– Kostas Gkirkizas, Senior Project Manager, Car IT – Information Systems, Toyota Motor Europe

ForgeRock Intelligent Access: Einfach und umfassend

[ForgeRock Intelligent Access](#) unterstützt Unternehmen bei der Bereitstellung nahtloser und sicherer Erlebnisse, die sich in Echtzeit an die Bedürfnisse des Benutzers anpassen. Mit unserer Lösung lässt sich dies leicht erreichen: IT-Mitarbeiter müssen keinen Code mehr eingeben, sondern können mithilfe einfacher Drag-and-Drop-Authentifizierungsbäume Login-Prozesse per Klicks einfach konfigurieren, messen und anpassen. Das beinhaltet digitale Signale wie geräte- und kontextabhängige Faktoren sowie verhaltens-, benutzerauswahl-, analyse- und risikobasierte Faktoren.

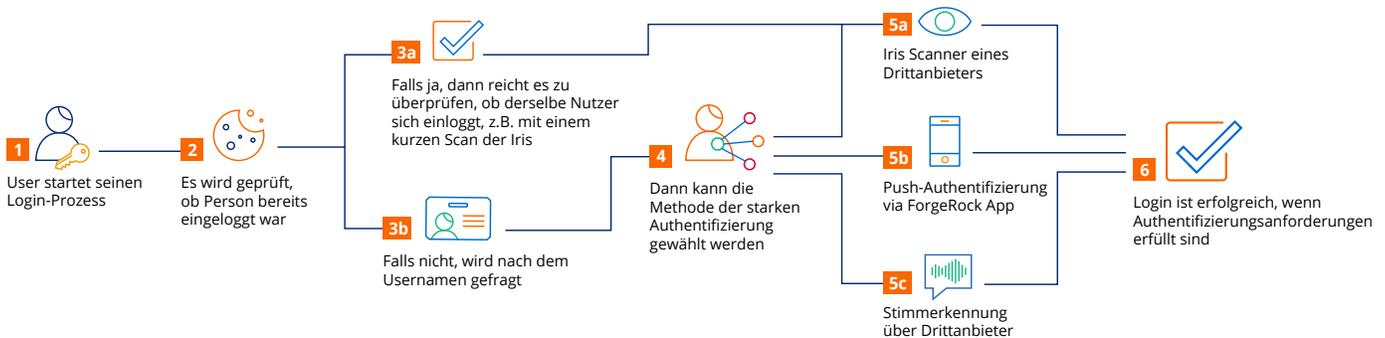


Abbildung 2: ForgeRock Intelligent Access für Authentifizierungsprozesse

Wann immer es Probleme mit dem IAM gibt, wenden sich Kunden an ForgeRock. Denn hinter unseren Drag-and-Drop-Konfigurationen verbirgt sich die umfassendste und leistungsfähigste IAM-Plattform der Branche. Wenn Altsysteme, neue Anwendungen und Anforderungen an das Benutzererlebnis zusammenkommen, ist eine maßgeschneiderte Konfiguration die einzige Lösung. Mit seiner überzeugenden Erfolgsbilanz bei Erweiterbarkeit, branchenführenden APIs und einem Identity Gateway, das wie kein anderes die Kluft zwischen IAM-Generationen überbrücken kann, bietet Ihnen ForgeRock die passende Unterstützung.

Hinter unseren Drag-and-Drop-Konfigurationen verbirgt sich die umfassendste und leistungsfähigste IAM-Plattform der Branche.

Registrierungserfahrungen

Für Verbraucher ist die Registrierung der erste und mitunter mühsamste Schritt beim Betreten der digitalen Welt. Mit unserer Intelligent Access-Lösung hilft ForgeRock Ihnen, mit einer schrittweisen Registrierung Ihre Kunden zu ihren Bedingungen besser kennen zu lernen. Das bedeutet, Nutzer müssen bei der Kontoeinrichtung zu Beginn nur wenige Informationen angeben. Im Laufe der Zeit, und nur wenn erforderlich, werden weitere Daten gesammelt. Für die IT-Mitarbeiter bleibt der Konfigurationsprozess gleich. Sie verwenden unsere einfachen Drag-und-Drop-Authentifizierungsbäume für allgemeine Abläufe mit erweiterbaren Optionen für kundenspezifische Anforderungen.

Abschied von Passwörtern – und Benutzernamen

In der Vergangenheit waren für Anwendungen Benutzernamen und Passwörter notwendig, um sicherzustellen, dass eine Person in der digitalen Welt tatsächlich die Person ist, die sie zu sein vorgibt. Mit unserer neuen ForgeRock Go-Lösung (Bestandteil von ForgeRock Intelligent Access) können Sie Ihre digitalen Erlebnisse verbessern, indem Sie Benutzern eine Authentifizierung ohne Kennwort und Benutzernamen ermöglichen.

Die Verwendung von ForgeRock Go zur Authentifizierung ist vergleichbar mit der Verwendung einer Debitkarte beim Einkaufen. Die Tatsache, dass Sie im Besitz der Karte sind und Ihre PIN kennen, bietet eine ausreichende Authentifizierungssicherheit, um die Transaktion abschließen zu können. Die endgültige Bestätigung erfolgt, wenn die Transaktion durch den Zahlungsabwickler autorisiert wird.

Wie bei der Verwendung einer Debitkarte ermöglicht ForgeRock Go Ihnen sich zu authentifizieren, indem Sie etwas angeben, das Sie wissen und/oder haben, anstatt auf Benutzernamen und Passwörter zu setzen. Sie können dazu ein physisches Gerät mit einer PIN verwenden,

z. B. einen YubiKey oder ein Smartphone. Biometrie, wie Fingerabdruck- oder Gesichtserkennung, kann ebenfalls zum Einsatz kommen. An Ihre Person gekoppelte Dinge zu wissen und/oder in deren Besitz zu sein, ermöglicht dann die Authentifizierung. Die Eingabe von Benutzernamen oder Kennwort ist nicht mehr erforderlich. Anschließend wird Ihr Login nahtlos durch ForgeRock Intelligent Access verifiziert.

Da die Notwendigkeit von Benutzernamen und Passwörtern entfällt, ermöglicht Ihnen ForgeRock Go:

- › Ihren Nutzern ein reibungsloses Zugangserlebnis zu bieten
- › die Sicherheit zu erhöhen, da die Gefahr von Phishing und jeglichem Diebstahl von Benutzernamen und Passwörtern sowie von Replay-Angriffen eliminiert wird
- › Helpdesk-Kosten für vergessene Benutzernamen und Passwörter zu senken

„ForgeRock hat es in unseren Augen verstanden, ein modernes, erstklassiges Web-Erlebnis für unseren großen und äußerst vielfältigen Kundenstamm zu schaffen.“

– **Greg Kalinsky, Senior Vice President und Chief Information Officer, GEICO**



Die Implementierung von ForgeRock Go in Ihrer Organisation ist ebenfalls ein Kinderspiel. ForgeRock Go ist in unsere Intelligent Access-Bäume integriert und lässt sich mit unserer Drag-and-Drop-Oberfläche einfach für Anwendungen konfigurieren, was IT-Administratoren die Arbeit erleichtert.

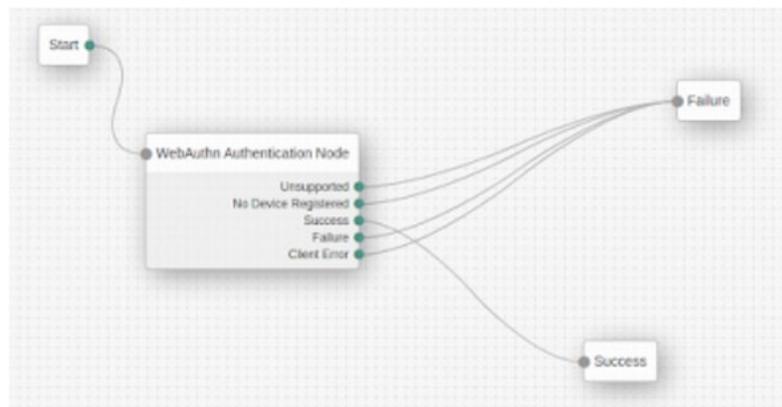


Abbildung 3: Benutzernamenloser Login-Baum

Ein neues Konzept für vergessene Zugangsdaten

Laut Forrester sind Kennwörterücksetzungen und IAM-bezogene Fragen die häufigste Ursache für Helpdesk-Anrufe, und diese Anrufe sind kostspielig. Kundenberichten zufolge belaufen sich die Kosten für einen Helpdesk-Anruf im Zusammenhang mit IAM auf 20 bis 60 US-Dollar und können sich in einem Jahr auf mehr als 1 Million US-Dollar summieren. Anstatt Benutzer zwischen den Prozessen hin- und herwechseln zu lassen, bietet ForgeRock die Möglichkeit, das Problem verlorener Security Tokens, Benutzernamen oder Passwörter innerhalb einer Online-Sitzung zu lösen.

Fallstudie: Bei einem großen, multinationalen Kommunikationsdienstleister stiegen die erfolgreichen Anmeldungen von lediglich 59 % auf 94 %, und das innerhalb von drei Wochen nach Einführung des ForgeRock Identity Provider-Dienstes (IDP). Dies wirkte sich unmittelbar auf die Kundenabwanderungsrate von 40 % aufgrund mehrfach fehlgeschlagener Anmeldungen aus und führte zu einer verstärkten Nutzung von Online-Inhalten, höheren Bindungsraten und mehr Upselling. Darüber hinaus gingen ihre Login-Support-Chats um 76 % bzw. 91.000 pro Jahr zurück.

Nehmen wir einmal an, Sie haben Ihr Passwort vergessen. Anstatt auf eine separate Seite zu einem separaten Vorgang weitergeleitet zu werden, können Sie wählen, wie Sie auf demselben Bildschirm Ihr Passwort zurücksetzen möchten. In diesem Fall entscheiden Sie sich dafür, einen Einmal-Code zu erhalten und ein neues Passwort zu erstellen – auf ein und demselben Bildschirm. Meistens müssen Benutzer zwischen Bildschirmen hin und her wechseln oder Registerkarten durchsuchen und sich ein zweites Mal mit dem neuen Passwort anmelden, das sie soeben erstellt haben. Bei ForgeRock werden Sie nach Bestätigung des neuen Passworts automatisch authentifiziert und können an der Stelle fortfahren, wo Sie stehen geblieben waren – z.B. „zur Kasse gehen“ – und zwar von demselben Bildschirm aus.

Anstatt Benutzer zwischen den Prozessen hin- und herwechseln zu lassen, bietet ForgeRock die Möglichkeit, Benutzernamen wiederzuerlangen oder Passwörter innerhalb einer Online-Sitzung zurückzusetzen.

Unvergleichliche Intelligenz mit ForgeRock Autonomous Identity

ForgeRock Intelligent Access bietet Unternehmen die Möglichkeit, Benutzererlebnisse mit einer Drag-and-Drop-Oberfläche einfach zu kodifizieren, aber das ist erst der Anfang. Heutzutage müssen Risikomanager von IT-Teams Tausende von Mitarbeiteranfragen bezüglich Zugang zu Informationen und Anwendungen bearbeiten -- ein langwieriger und manuell gesteuerter Prozess. Herkömmliche Ansätze zur Verwaltung von Zugriffsrechten in Unternehmen erhöhen das Risiko eines unbefugten Zugriffs auf Unternehmensressourcen. Dieser [führt zu Datenschutzverletzungen](#), die Unternehmen hinsichtlich Kapital, Ruf und Verbrauchervertrauen teuer zu stehen kommen.

[ForgeRock Autonomous Identity](#) ist eine KI-gesteuerte Identitätsanalyselösung, die unternehmensweite Sichtbarkeit, Kontrolle und Korrektur beim Benutzerzugriff bietet. Mithilfe maschinellen Lernens sammelt und analysiert Autonomous Identity Identitätsdaten wie beispielsweise Konten, Rollen und Zugriffsrechte, um Risiken im Bereich Zugriffssicherheit zu identifizieren. Die Lösung bietet Organisationen tiefe Einblicke in das Risiko, das mit einem Benutzerzugriff verbunden ist, indem es unternehmensweite kontextbezogene Transparenz, eine Sensibilisierung für Hochrisiko-Nutzer und Korrektorempfehlungen bereitstellt.

Fallstudie: Ein multinationaler Finanzdienstleister identifizierte und automatisierte 91 % der Zugriffsberechtigungen für eine wichtige Enterprise Resource Planning-Anwendung (ERP).

Im Einklang mit der Zielsetzung der branchenweit umfassendsten IAM-Plattform fügt sich Autonomous Identity nahtlos in die Identitätsmanagement- und Governance-Funktionen unserer Plattform ein.

Darüber hinaus kann Autonomous Identity im Gegensatz zum Konkurrenzprodukt, falls Sie bereits über ein Identitätsmanagement- und/oder Governance-System verfügen, direkt integriert werden, wodurch sich der Geschäftswert Ihrer vorhandenen Lösungen und Infrastrukturinvestitionen erhöht.

Autonomous Identity hebt sich von Wettbewerbern zudem durch die gleichzeitige automatisierte Modellierung von mehreren zehn Millionen Datenpunkten ab, wodurch weniger manuelle Eingriffe notwendig sind. Das Ergebnis ist ein Datenmodell, das die Ist-Zugangslandschaft widerspiegelt, in der alle Identitätsdaten berücksichtigt werden. Dies ist ein umfassenderer Ansatz im Vergleich zu anderen Lösungen, die statische rollenbasierte und Peer-Group-Analysen verwenden, bei denen jeweils nur ein Teil der Identitätsdaten berücksichtigt wird.

Autonomous Identity kann direkt in bestehende Identitätssysteme integriert werden, wodurch sich der Geschäftswert bestehender Lösungen und Infrastrukturinvestitionen erhöht.

Erfahren Sie mehr über [ForgeRock Autonomous Identity in diesem Whitepaper](#).

Kompromisslose Sicherheit

Herausragende Benutzererlebnisse lassen sich nur erreichen, wenn ein ausgewogenes Maß an Sicherheit gegeben ist. Laut dem [2020 ForgeRock Consumer Identity Breach Report](#) haben die Anzahl, Größe und Häufigkeit externer Verstöße, kompromittierter Daten und Geschäftsziele exponentiell zugenommen. Damit steigen zugleich auch die Kosten und der Zeitaufwand, um Organisationen vor diesen Bedrohungen zu schützen.

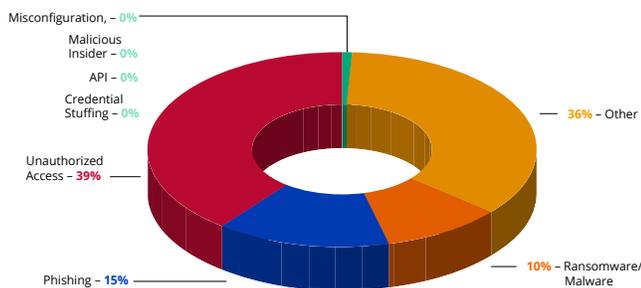


Abbildung 4: Sicherheitsverletzungen aufgeschlüsselt nach Art des Sicherheitsrisikos

Ein vertrauenswürdiges Netzwerk oder Gerät gibt es nicht. In der heutigen Bedrohungslandschaft ist ein dynamischer Sicherheitsansatz, wie z. B. [Zero Trust oder Continuous Adaptive Risk and Trust Assessment \(CARTA\)](#) gefragt. Zero Trust ist ein Sicherheitsmodell, bei dem kein Benutzer oder Gerät von vornherein vertrauenswürdig ist.

Mit ForgeRock können Sie auf dynamische Art und Weise die perfekte Balance zwischen Erlebnis und Sicherheit wahren, die von den Gegebenheiten des jeweiligen Moments beeinflusst wird.

Das von Gartner eingeführte CARTA-Konzept baut auf dieser Idee auf, indem es eine risiko- und vertrauensbasierte Entscheidungsfindung in Echtzeit mit flexiblen Reaktionen unterstützt. Zero Trust und CARTA sind beliebte Themen im Bereich IAM und gehören häufig zur Roadmap einer Organisation. Angesichts des schnelleren Tempos der digitalen Transformation kürzen Organisationen jedoch den Zeitplan für die Umsetzung dieser Initiativen um ein Jahr oder mehr.

Dieselben Intelligent Access-Bäume, die mithilfe einer Drag-and-Drop-Oberfläche die Benutzererlebnisse optimieren, ermöglichen es auch Ihrem IT-Personal, Zero Trust und CARTA nicht nur über dieselbe Schnittstelle, sondern im Rahmen derselben User Journey nahtlos zu integrieren. Dies ist ein entscheidender Faktor, der die Kunden von ForgeRock so erfolgreich macht. Sie können auf dynamische Art und Weise die perfekte Balance zwischen Erfahrung und Sicherheit wahren, die von den Gegebenheiten des jeweiligen Moments beeinflusst wird.

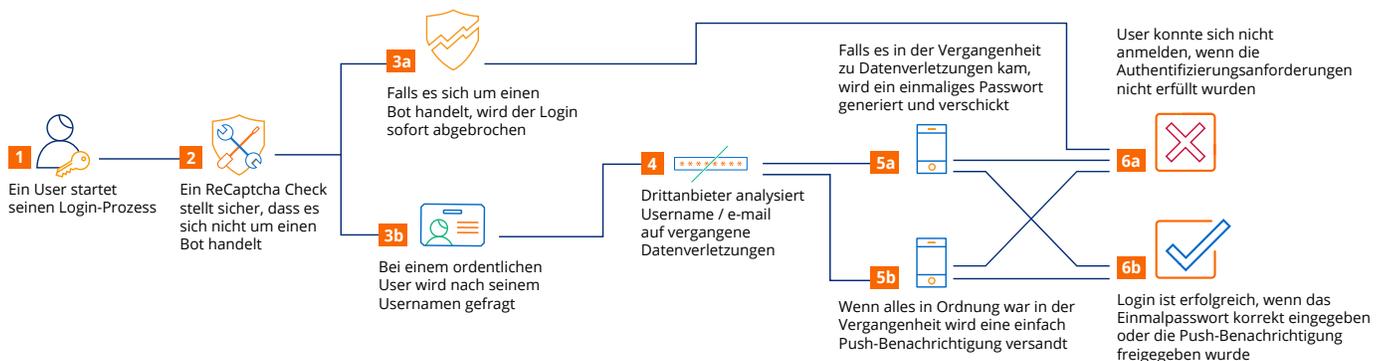


Abbildung 5: Zero Trust und CARTA integriert in den Intelligent Access-Prozess

Manchmal rechnen Nutzer mit einer gewissen Reibung. So erwarten sie etwa bei einer größeren Finanztransaktion einen zusätzlichen Validierungsschritt, bevor sie fortfahren können. Das gibt ihnen ein Gefühl von mehr Sicherheit.

ForgeRock verhindert Betrug und unbefugten Zugriff durch die Platzierung von Sicherheitsknotenpunkten im Rahmen von Intelligent Access an wichtigen Stellen der User Journey basierend auf den jeweiligen Anforderungen einer bestimmten Anwendung. Der Intelligent Access-Baum beurteilt daraufhin, ob eine weitere Verifizierung erforderlich ist, ob die Transaktion abgelehnt oder der Vorgang ohne weitere Aktionen fortgesetzt werden sollte. Hierfür lassen sich folgende Beispiele nennen:

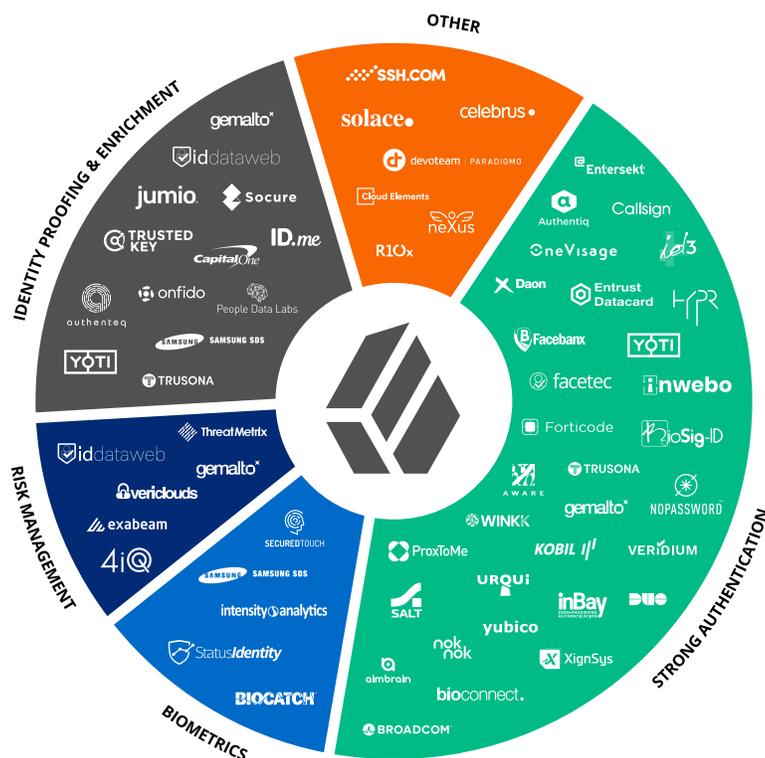
- › Erfassen und Auswerten von Kontext, wie z.B. eines Risk Score, einer Gerätesignatur oder einer IP-Adresse
- › Speichern von Kontext für einen zukünftigen Vergleich
- › Kontinuierliche Autorisierung – IT-Administratoren können Intelligent Access mit der leistungsstarken Autorisierungs-Engine von ForgeRock integrieren, um Entscheidungen auf der Grundlage häufig wechselnder Variablen wie Standort oder Art der Netzwerkverbindung neu zu bewerten
- › Aufrufen von Step-up-Authentifizierung, Identitätsprüfung, Sitzungsbeendigung, Datenredaktion, Datendrosselung⁴ und mehr

Ein leistungsstarkes Technologie-Ökosystem

Das [ForgeRock Trust Network](#) ist ein Technologie-Ökosystem von mehr als 80 Partnern, das Zugriff auf umfangreiche Funktionen für digitales Identitätsmanagement mithilfe der ForgeRock Identity-Plattform bietet. Zu den Technologiepartnerkategorien zählen strenges Authentifizierungs-, Risiko- und Betrugsmanagement, Verhaltensbiometrie sowie Identitätsnachweise und Identitätsbereicherung. Integrationen des ForgeRock Trust Network sind kostenlos in der ForgeRock Identity-Plattform inbegriffen.

Fallstudie: Ein Kunde aus dem Finanzdienstleistungssektor entschied sich für die ForgeRock-Identity-Plattform aufgrund der darin enthaltenen zahlreichen Tools für die Identitätsprüfung und das Risikomanagement. Durch den Einsatz von Intelligent Access und ForgeRock Trust Network konnte der Kunde die Authentifizierungsabläufe in seiner Umgebung leicht integrieren und ändern.

Das ForgeRock Trust Network



⁴ Auch bei der Datenredaktion und Datendrosselung kommen die Fähigkeiten des ForgeRock Identity Gateway zum Tragen.

Datenschutz und Compliance

Datenschutz und Compliance sind ebenfalls ein entscheidender Bestandteil jeder Risikomanagementstrategie. Verbraucher tauschen mehr Informationen aus als je zuvor und haben höhere Erwartungen, was die Verarbeitung persönlicher Daten und ihre Nutzung durch Organisationen anbelangt. Deshalb wurden gesetzliche Bestimmungen wie die allgemeine EU- Datenschutz-Grundverordnung (EU- DSGVO) und das kalifornische Verbraucherschutzgesetz (CCPA) verabschiedet und weitere werden folgen. Die Datenschutzerfordernungen ändern sich häufig und werden für internationale Unternehmen immer komplexer, insbesondere wenn sie in mehreren Rechtssystemen tätig sind.

Die Bereitstellung von Profil- und Datenschutzeinstellungen trägt dazu bei, eine engere Beziehung zu den Kunden aufzubauen, da diese genau sehen können, welche persönlichen Daten ein Unternehmen speichert und warum.

Für die meisten Implementierungen mit Schnittstelle zum Kunden ist es wichtig, den Benutzern die Möglichkeit zu geben, ihr eigenes Profil und ihre eigenen Datenschutzeinstellungen zu verwalten. Zudem ist das nicht nur gesetzlich vorgeschrieben (z. B. bei der EU- DSGVO und dem CCPA), sondern trägt auch zur Senkung der Kundensupport-Kosten bei. Durch die Bereitstellung von Profil- und Datenschutzeinstellungen kann vor allem eine engere Beziehung zu den Kunden aufgebaut werden, da diese genau sehen können, welche persönlichen Daten ein Unternehmen speichert und warum.

Die ForgeRock Identity-Plattform verfügt über ein umfassendes [standardbasiertes Dashboard](#) für die [Profil- und Datenschutzverwaltung](#). Benutzer können ihre Profildaten in Eigenregie verwalten, die mit ihrem Konto verbundenen Geräte, Anwendungen, die sie mit ihrem Konto verbinden wollen, wie sie Daten teilen wollen und welche persönlichen Daten an externe Datenbanken, wie z. B. Marketingautomatisierungsplattformen, weitergegeben werden. Die Plattform berücksichtigt auch zahlreiche andere Benutzeranforderungen im Zusammenhang mit wichtigen Vorschriften wie der EU- DSGVO. So können Benutzer ihre Profildaten lokal speichern und von ihrem Recht Gebrauch machen, ihr Profil zu löschen.

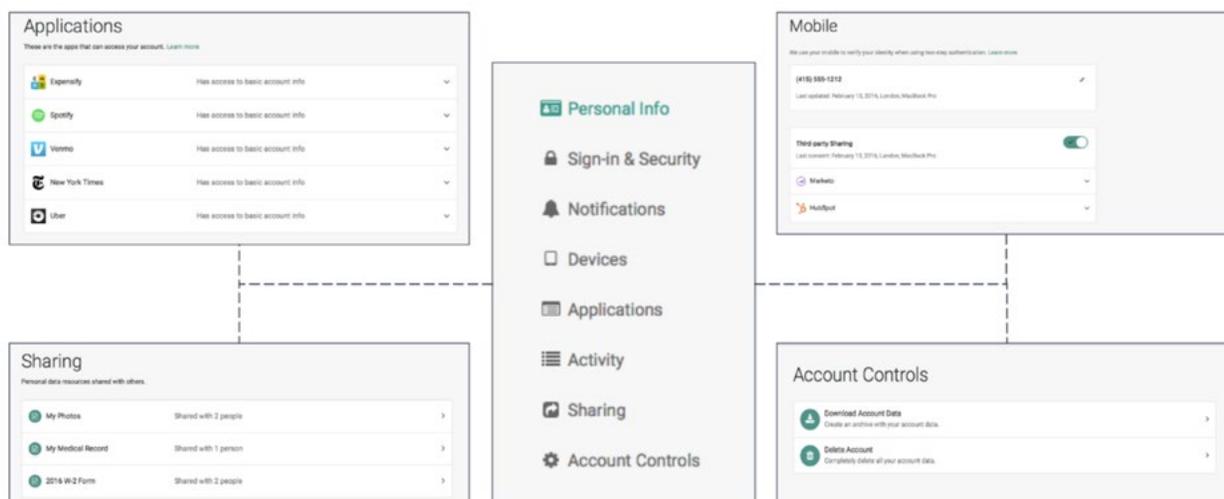


Abbildung 6: Das ForgeRock Profile and Privacy Dashboard

Moderne Enterprise-Cloud

Im Zuge der rasanten Weiterentwicklung der Cloud-First-Strategie Ihres Unternehmens werden Sie vielleicht auch Ihre IAM-Bereitstellungsmodelle auf den Prüfstand stellen. Häufig drängt sich die Frage auf, wie man von standortgebundenem IAM (eine erhebliche Investition über viele Jahre) auf Cloud-Dienste umstellen kann, ohne bestehende Investitionen aufzugeben und wichtige Funktionen zu verlieren. Darüber hinaus muss alles von Deployment-Architekturen bis hin zu individuellen Topologien, die organisch und anorganisch in Unternehmen entstanden sind, berücksichtigt werden.

Bislang haben viele Organisationen auf dem Weg in die Cloud einen hybriden Ansatz verfolgt. Häufig haben sie ihre vorhandenen lokalen IAM-Lösungen in ihren eigenen privaten Clouds implementiert und diese dann mit Public Clouds als weiteres Rechenzentrum ergänzt.

Die Verwaltung einer bunten Mischung von On-Premise- und im Einsatz eingefassten kostspieligen Legacy-Cloud-Lösungen ist nicht mehr praktikabel.

Manche von ihnen setzen auf reine Cloudidentität mit Identity-as-a-Service-Lösungen (IDaaS) – ein Begriff, dessen Bedeutung sich in den letzten Jahren gewandelt hat. Das größte Problem mit dieser eng begrenzten frühen IDaaS-Lösung besteht darin, dass sie am Ende eine weitere lästige IAM-Lösung von vielen anderen ist, die ein Unternehmen zu verwalten hat. Die Kosten dieser Lösungen werden bei der Größenordnung, die große Unternehmen benötigen, untragbar. Mit der Entwicklung hin zu einem strategischeren IAM-Ansatz in den Unternehmen ist die Verwaltung einer bunten Mischung von On-Premise- und begrenzten kostspieligen Legacy-Cloud-Lösungen nicht mehr praktikabel.

ForgeRock liefert eine moderne Unternehmens-Cloud mit allen entscheidenden Funktionen, die Sie in beliebiger Kombination von unserer Cloud, Ihrer Cloud oder der Public Cloud benötigen. Die [ForgeRock Identity Cloud](#) bietet die Leistungsfähigkeit einer echten Identity-Plattform, die als umfassender und anpassbarer Cloud-Service bereitgestellt wird. Sie bietet Ihnen die ultimative Kontrolle darüber, wie Sie Identitäten verwalten und auf Ihre Umgebungen anwenden, und macht diese gleichzeitig zukunftssicher, wenn sich ihre Bedürfnisse ändern. Unabhängig von [Nutzung und/oder Einsatz](#) der [ForgeRock-Plattform](#) verfügt sie über dieselbe Schnittstelle, dieselben Endpunkte, dasselbe Menü von Edge-Enforcement-Funktionen und dieselben Software Development Kits (SDKs).

Dies ist ein starkes Alleinstellungsmerkmal und für die IAM-Strategie einer Organisation von entscheidender Bedeutung, denn während die Ebene der Identitätskontrolle in die Cloud verlagert wird, muss die Durchsetzung und – in zunehmendem Maße – die Entscheidungsfindung nahe an der Peripherie bleiben.

Unabhängig von Nutzung und/oder Einsatz der ForgeRock-Plattform verfügt sie über dieselbe Schnittstelle, dieselben Endpunkte, dasselbe Menü von Edge-Enforcement-Funktionen und dieselben SDKs.

Identität an der Peripherie

Die Verwaltung einer hybriden Umgebung, bei der das IAM in Ihrem Rechenzentrum abläuft, eine öffentliche Cloud-Infrastruktur und Cloud-Abonnementdiensten mit einer Kombination aus Legacy-, selbst entwickelten und verschiedenen anderen IAM-Punktlösungen zum Einsatz kommt, kann kompliziert und kostspielig werden. Sie brauchen eine Lösung, die die Lücken schließt und dabei die Sicherheit an allen Netzwerkrändern aufrechterhält.

[ForgeRock Edge Security](#) verbindet alle Teile miteinander und fungiert als Brücke zwischen unserer Plattform und Ihrem übrigen IAM-Umfeld. Dazu gehört die Fähigkeit, die Identitäten, Authentifizierung und Autorisierung von IoT-Geräten zu registrieren und zu verwalten, einschließlich [des Aufbaus von Beziehungen zwischen Geräten und den Personen, Organisationen und Ressourcen](#), mit denen diese interagieren.

Im Rahmen unserer Edge Security ermöglicht Ihnen das [ForgeRock Identity Gateway](#) auch, Intelligent Access auf den Netzwerkrand auszuweiten.

Mit einer ähnlichen Drag-and-Drop-Oberfläche können Ihre IT-Mitarbeiter wertvolle Zeit sparen, indem sie visuelle Abläufe erstellen, mit denen Sie wichtige IAM-Szenarien am Rande des Netzwerks verwalten können. Das ermöglicht eine beispiellose Skalierbarkeit. So zeigt Abbildung 4 unten, wie eingehender Datenverkehr von Verbrauchern anders geleitet und behandelt wird als Datenverkehr von Mitarbeitern.

Fallstudie: Ein großes

Telekommunikationsunternehmen setzt ForgeRock Edge Security ein, um Anfragen von Kundenservice-Mitarbeitern abzufangen, die auf Kundenkontodaten zugreifen und über die mobile Anwendung des Kunden eine Autorisierungsanfrage in Echtzeit an den Kunden senden möchten. Nur wenn der authentifizierte Kunde seine Zustimmung gibt, erlaubt das ForgeRock Identity Gateway dem Kundenservice-Mitarbeiter den Zugriff auf die Kontoinformationen des Kunden.

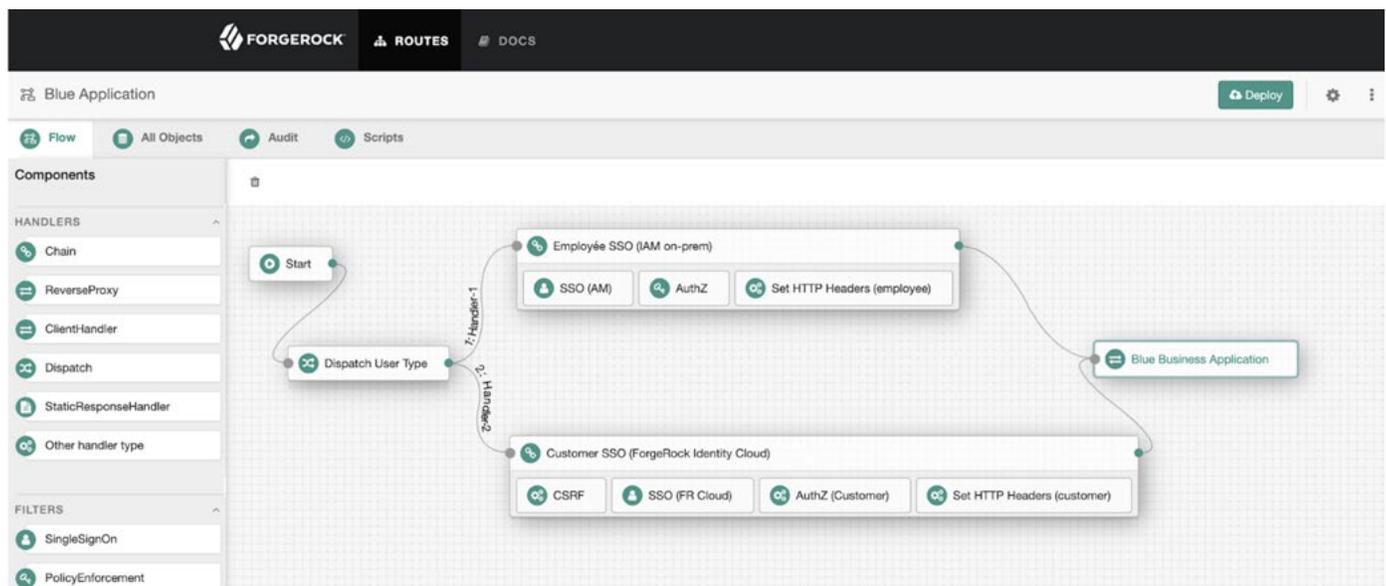


Abbildung 7: Intelligent Access am Netzwerkrand mit dem ForgeRock Identity Gateway

Beliebig einsteigen und weiterwachsen mit ForgeRock

Nutzen Sie ForgeRock zunächst für Ihr größtes Problem, lösen Sie es und gehen Sie dann schrittweise von einem Punkt zum nächsten Punkt weiter – alles mit einer einzigen Plattform.

Fallstudie: Bei einer großen amerikanischen Gesundheitsorganisation gab es ein großes Problem, wenn Nutzer ihr Kennwort zurücksetzen wollten. Die Kunden riefen den Helpdesk an und wurden in der Regel mehrmals weitergeleitet, bevor sie schließlich mit dem richtigen Ansprechpartner verbunden waren. Dieser bat nun die Kunden mindestens zum zweiten Mal innerhalb eines einzigen Telefonats um einen Identitätsnachweis. Diese Organisation entschied sich für ForgeRock und begann mit diesem einen Anwendungsfall. Sie führten eine mobilfunkfähige Self-Service-Kennwortrücksetzung ein, was die Kundenzufriedenheit erheblich verbesserte und gleichzeitig die Anzahl und Kosten der Helpdesk-Anrufe reduzierte.

Nach diesem Erfolg weitete die Organisation den Einsatz von ForgeRock weiter aus, indem sie Kundenauthentifizierung und Datenschutzkontrollen implementierte. Aufgrund dieses Erfolgs beschlossen sie, in einem nächsten Schritt, ihr altes [Single Sign-on-System \(SSO\)](#) für ihre Mitarbeiter durch ForgeRock zu ersetzen.

Jede Organisation verfolgt einen anderen IAM-Ansatz. Die Bedürfnisse großer Unternehmen sind jedoch häufig dieselben:

- › Umsatz ankurbeln bei gleichzeitiger Kostensenkung und kürzerer Amortisierungsdauer
- › Auf dem digitalen Markt durch hervorragende Nutzererlebnisse wettbewerbsfähig sein
- › Risiko und Compliance ohne Abstriche beim Nutzererlebnis effektiv managen
- › Moderne Geschäftsanwendungen erstellen, während Legacy-Systeme langsam auslaufen
- › Verfügbarkeit von neuen Arbeitskräften an entfernten Standorten sichern und einen effizienten Zugang zu internen Systemen mit geringsten Privilegien gewährleisten

Obwohl es heute am Markt eine Vielzahl von IAM-Alternativen gibt, deckt keine von ihnen mehr IAM-Bedürfnisse ab bzw. bietet keine mit einer einzigen Plattform mehr Wert als ForgeRock.

Obwohl es heute am Markt eine Vielzahl von IAM-Alternativen gibt, deckt keine von ihnen mehr IAM-Bedürfnisse ab bzw. bietet keine mit einer einzigen Plattform mehr Wert als ForgeRock. Von den anspruchsvollsten Legacy-Systemen bis hin zu den modernsten Anwendungen – ForgeRock ist Ihr Katalysator für Geschäftstransformation. [Werden Sie noch heute Teil unserer Community](#) und starten Sie in die Zukunft.

Über ForgeRock

ForgeRock, der führende Anbieter im Bereich digitale Identität, liefert moderne und umfassende Identitäts- und Zugangsmanagement-Lösungen für Verbraucher, Mitarbeiter und Dinge und bietet so einen einfachen und sicheren Zugang zur vernetzten Welt. Mit ForgeRock orchestrieren, verwalten und sichern mehr als tausend globale Unternehmen den gesamten Lebenszyklus von Identitäten, angefangen bei dynamischen Zugriffskontrollen, Verwaltung, APIs bis hin zur Speicherung autoritativer Daten – verwendbar in jeder Cloud- oder Hybridumgebung. Das Unternehmen befindet sich in Privatbesitz mit Hauptsitz in San Francisco, Kalifornien, und hat Niederlassungen weltweit. Besuchen Sie für weitere Informationen und kostenlose Downloads www.forgerock.com oder folgen Sie ForgeRock in den sozialen Medien.



Folgen Sie uns

