ForgeRock®

White Paper

How to Plan Your IAM Future with ForgeRock Identity Cloud

Introduction

As you evolve your overall cloud strategy, it's likely you're also rethinking your identity and access management (IAM) deployment models. A big challenge you need to consider is how to transition from your on-premises IAM solutions to the cloud, while maintaining full functionality.

If your organization was an early adopter of cloud-native IAM, you may have found that it couldn't scale to meet your growing business needs, and offered limited support for your on-premises, business critical applications.

Government agencies and highly regulated industries, like finance and healthcare, have tended to remain committed to their legacy IAM systems because they've been customized to support critical backend business processes. They may be required to keep on-premises systems to maintain compliance with data security standards. At the same time, there are compelling reasons to consider migrating legacy IAM and business critical systems to the cloud — including scalability, cost savings, operational efficiencies, availability, and flexibility.

The ForgeRock Identity Cloud is a comprehensive IAM platform for applications that can be deployed anywhere — on premises, in your own private cloud, or in your choice of public cloud.

To take advantage of the benefits offered by the cloud, you may have begun deploying legacy on-premises IAM solutions into private clouds, effectively using the cloud as another data center. Or, you might be an early adopter of cloud-native identity as a service (IDaaS) solutions to manage single sign-on, strong authentication, and other identity policies to support access to cloud services. These stopgap approaches may work for your tactical needs, but fall short of delivering a true IAM platform that meets your evolving longer-term strategic needs.

Over time, the shortcomings of these approaches have become more evident. Larger enterprises haven't been able to capitalize on the advantages of the cloud because legacy IAM systems are slow to evolve. Legacy systems fail to support newer protocols and cloud technologies, and they can't keep up with security risks that threaten customer data and privacy. Pure-play cloud IAM supports workforce access to thousands of cloud services, but offers limited support for on-premises business systems and business-to-consumer access. These "SaaS-delivered IAM" solutions are designed for ease of use, but require larger organizations to change their business processes or applications to fit the cloud solution. They lack the depth and breadth of features and functionality offered by enterprise IAM solutions.

Clearly, a different approach is needed to address the full range of identity and access needs and the evolving technology ecosystem. That approach — a full-featured,

enterprise-grade identity platform delivered as a cloud service — overcomes the shortcoming of both legacy on-premises and modern cloud IAM solutions. ForgeRock delivers that approach with the ForgeRock Identity Cloud, a true identity platform as a service.

The ForgeRock Identity Cloud is a comprehensive IAM service for applications that can be deployed anywhere — on premises, in your own private cloud, or in your choice of public cloud. Its capabilities and configurability surpass what analyst firm Gartner terms "SaaS-delivered IAM." Identity Cloud also reduces the operational risk and total cost of ownership associated with traditional IAM. You can embrace the cloud with a hybrid model and finally reap the benefits of the cloud while maintaining the benefits of a full-featured IAM solution.

The following are some of the problems you can solve with a comprehensive IAM solution for the cloud.

Balancing Security and Convenience

It's critical to have a solution that provides the right levels of access to the right users, while taking into account how many devices and workflows they're using to access your network. If you don't get it right, you can potentially put your security and user satisfaction at risk.

Faced with setting up and remembering yet another username and password, many users experience "security fatigue" and resort to careless behaviors like creating simple passwords and reusing them across multiple services and systems.[1] Weak credentials make it easier for malicious actors to piece together usernames and passwords obtained from other data breaches to gain unauthorized access to accounts and steal personally identifiable information (PII). Your organization needs better security, and your users need easier and safer access.

With the rise of smart devices and bring your own devices (BYOD), your users want to carry their personalized preferences — like their favorite music — from the office into their homes and vehicles. This requires a robust and comprehensive identity solution that supports not only workforce and customers, but also the internet of things (IoT).

The ForgeRock Identity Cloud balances security and convenience by reducing and even eliminating the need for username/password-based authentication. It provides dynamic and personalized user flows, authentication, and unique access experiences based on geography, device type, biometrics, and more.

SaaS Versus Legacy IAM

While some early SaaS-delivered IAM solutions are gaining traction and acceptance, it's understandable if you're unwilling or unable to rip and replace your entire backend infrastructure to fit into the constraints of a SaaS-delivered IAM solution.

The current SaaS-delivered IAM model is built on simplicity and ease of use but supports only limited use cases such as workforce, partner, and customer access to SaaS applications. They fall short of supporting identity for legacy on-premises systems, applications, and things.

Some legacy identity solutions offer fuller feature sets, but aren't investing enough in simplicity or compatibility with both on-premises and cloud solutions. You may find it challenging to deploy, maintain, and upgrade your legacy IAM systems when there is no clear roadmap of new features.

1 https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly

Planning for the Future

Digital transformation requires a comprehensive IAM solution that aligns with your priorities — whether it's cloud migration or maintaining a hybrid model with a simplified infrastructure footprint.

To plan for your organization's future in the cloud, you need a comprehensive, enterprise-grade identity platform that supports your priorities with a combination of usability, customizability, and operational cost savings. You need a range of configuration options so that you can choose the functionality you need.

As your organization grows, your IAM solution should grow along with it. You might find you need to secure identity for employees and, later, workforce, consumers, citizens, and things. You will need to manage access to cloud and on-premises apps, on-premises legacy systems, and a wide range of resource objects such as files, data in databases, and buttons or tabs in web pages and application programming interfaces (APIs).

Customizing your IAM solution is also important. If you are in a regulated industry, you will need a cloud IAM solution that can provide true data isolation, enable fine-grained transactional authorization, and integrate with leading anti-fraud solutions. If you are in healthcare, you will need to manage identity relationships (such as parent and child and doctor and patient) and incorporate these relationships into access and authorization decisions.

As your organization grows, your IAM solution should grow along with it. You might find you need to secure identity for employees and, later, workforce, consumers, citizens, and things.

ForgeRock Delivers the Future of IAM

The ForgeRock Identity Cloud is the market's first true identity platform as a service. ForgeRock is the only identity provider that offers a full suite of modern capabilities for any identity and access need in any business environment. Below are some of the features and benefits you will experience by deploying ForgeRock Identity Cloud.

The ForgeRock Identity Cloud is the market's first comprehensive true identity platform as a service.

A Single Platform for Cloud, On-Premises, and Hybrid Environments

When you think of "cloud" today, you may automatically think of SaaS solutions. But every organization that moves to the cloud has its own unique journey. **For large organizations, "cloud" actually encompasses a hybrid of SaaS, private cloud, and on-premises.**[2]

The ForgeRock Identity Cloud reduces the traditional operational expenses associated with maintaining on-premises servers. It offers security and redundancy for disaster recovery and the ability to scale as your business needs change. **Assets that must remain on premises for regulatory, compliance, or legacy reasons can remain on-premises, with identity and access managed from the cloud by ForgeRock.**

Identity Cloud reduces cost of ownership and accelerates time-to-value for identity services. Its flexible authentication and API integration patterns provide continuous security by integrating identity for workforce, customers, partners, things, and microservices.

2 https://www.zdnet.com/article/hybrid-cloud-rises-as-an-avenue-for-data-security-and-business-continuity/

The Same Great Features Everywhere

The ForgeRock Identity Cloud offers the same great features and capabilities as the ForgeRock Identity Platform. The consistency of the ForgeRock architecture across cloud and on premises means your team doesn't have to learn and manage multiple IAM solutions. You can extend authentication, authorization, provisioning, and other critical IAM capabilities from the cloud to any application running on premises, in the cloud, or in a hybrid environment.

Coexists With Legacy and Modern Systems and Apps

ForgeRock Identity Cloud can coexist with other legacy IAM solutions and augment legacy or home-grown applications with modern IAM capabilities. This gives you the time you need to execute on your cloud migration and security strategy.

ForgeRock Identity Cloud supports bi-directional identity sync between legacy solutions and the cloud to maintain a consistent user identity store. It can migrate apps group by group or individually, so you can plan and execute cloud migration at your own pace.

Identity for Everything

ForgeRock Identity Cloud gives you the power to manage multiple types of identities within a single implementation, including customers, partners, workforce, citizens, gig economy workers, and "non-person" identities, such as devices, bots, APIs, and microservices. The ForgeRock data model is object based and provides the flexibility to define many different schema and attributes and the relationships between each.

ForgeRock Identity Cloud gives you the power to manage multiple types of identities within a single implementation, including customers, partners, workforce, citizens, gig economy workers, and "non-person" identities, such as devices, bots, APIs, and microservices.

Compared to a monolithic application, a cloud application built from microservices can be a security challenge due to the higher number of endpoints that need to be both managed and secured. ForgeRock recognizes these risks and provides a full OAuth 2.0 authorization framework and two solutions that secure microservice-to-microservice, optimized to run in a containerized environment providing the required low latency responses. The ForgeRock Identity Cloud enables separation of the authentication and authorization security needs of microservices. It can also inspect and validate OAuth 2.0 tokens. These capabilities can be embedded inside the namespace of the applications to solve the complexities related to managing identity for microservices-based applications.

No Compromise on Security, Privacy, and Compliance

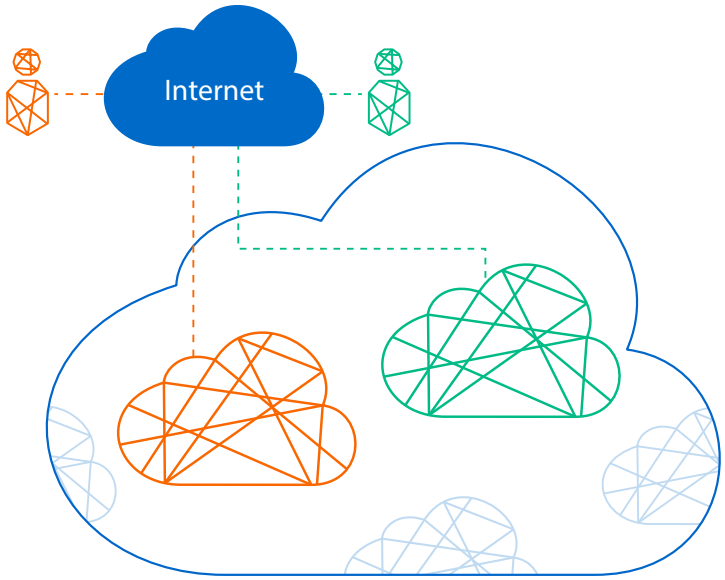
Speed, flexibility, and innovation can't come at the expense of security and compliance. ForgeRock ensures that identities are secure and meet privacy and compliance requirements at any scale.

The ForgeRock Identity Cloud platform provides full tenant isolation in a multi-tenant cloud service utilizing individual trust zones. Every customer's environment comprises a dedicated trust zone that shares no code, data, or identities with other customers' environments to prevent any accidental or malicious commingling. All data is encrypted at rest and in transmission to prevent unauthorized access and data breaches.

The ForgeRock Identity Cloud can also be used to address compliance with major national and international data regulations such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Identity Cloud has the same privacy and consent capabilities of the ForgeRock Identity Platform, including multi-tenancy, data isolation, and encryption.[3]

ForgeRock Identity Cloud also manages data residency requirements by allowing you to place data in the region of your choice. You can use the ForgeRock Identity Cloud to manage consumer data by allowing your consumers to download, update, or delete personal information and to allow customers to consent to use their data. You can quickly integrate the user UIs, SDKs, or APIs to integrate this capability into their applications. In addition, ForgeRock's extensive integration capabilities allows you to notify downstream applications of changes to user data and take action accordingly. ForgeRock Cloud deletes log, audit, and event data after 30 days, and only keeps data for the purposes of monitoring the system and ensuring uptime. During day-to-day operations of the system, ForgeRock site reliability engineers do not have visibility into customer environments.

ForgeRock has published a data protection addendum (DPA)[4] to help you with your GDPR responsibilities.



Full tenant isolation means that resources within a tenant are not shared with any other tenant, even within the same organization.

3 For more information, see The ForgeRock Identity Cloud Security White Paper: https://www.forgerock.com/resources/view/107430026/whitepaper/forgerock-identity-cloud-security-whitepaper.pdf

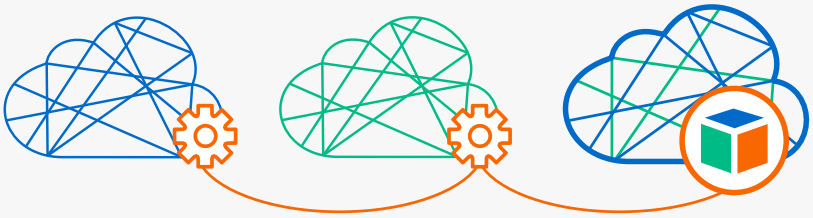
4 For more information, see The ForgeRock Data Protection Addendum: https://www.forgerock.com/resources/view/99022421/legal-document/ForgeRock%20Data%20Protection%20Addendum.pdf

Cost-Effective and DevOps Friendly

The cost-effectiveness of cloud versus on-premises IAM is widely accepted. According to Forrester research, organizations can reduce their IT operations and development costs by up to 80% by using cloud IAM solutions. Labor costs are also 80% to 90% lower for initial and ongoing maintenance and development of a cloud IAM solution.[5]

The ForgeRock Identity Cloud is both cost-effective and DevOps-friendly. The ForgeRock Identity Cloud offers three individual environments (development, testing, and production) for the cost of a single license, so you don't have to pay extra to license additional tenancies. ForgeRock also provides the necessary DevOps tooling, so developers don't have to expend effort building their own tooling to move configurations between environments. Developers spend less time learning IAM and more time focusing on your organization's strategic business initiatives. By using Agile software development methodologies, along with ForgeRock DevOps tooling, developers can make rapid, incremental changes to their applications while maintaining quality and control.

The ForgeRock Identity Cloud offers three individual environments (development, testing, and production) for the cost of a single license.



To assist with the knowledge and skill-set gap, the ForgeRock Identity Cloud also includes developer-friendly documentation: reference architectures, integration guides and videos, and benchmark performance data.

There is no API throttling that stops or slows down the user experience. To prevent surprise charges, there is no additional charge for overages of up to 10% of licensed users. You'll have a more predictable monthly spend even with occasional seasonal spikes. By using a single platform to manage IAM across multiple environments, you can minimize the costs of training and maintenance and customize ForgeRock Identity Cloud through its add-on packages, so you're only paying for the services you need.

ForgeRock Identity Cloud's architecture enables teams to consume all of the platform's capabilities without sacrificing rich features and extensibility. By delivering ForgeRock Identity Cloud as a cloud service, you can develop rapid and repeatable solutions to accelerate time to market, reduce development costs, and increase flexibility, availability, and scalability.

Comprehensive Yet Simple to Use

The ForgeRock Identity Cloud is a comprehensive solution that is also simple to use. Your organization can spin up your own instance of ForgeRock Identity Cloud in minutes. ForgeRock's drag-and-drop visual designer for user journeys, called **Intelligent Access** (also known as "**Trees**"), enables developers and non-developers alike to get their first project up and running quickly and scale from there. Intelligent Access Trees make it easy to configure, measure, and adjust user journeys using device, contextual, behavioral, user choice, analytics, and risk-based signals. Developers can also build their own customized user registration and authentication flows programmatically in JavaScript. They can integrate with any home-grown or custom risk analytics, Knowledge-Based Authentication (KBA), or other solutions that extend capabilities to meet their business needs.

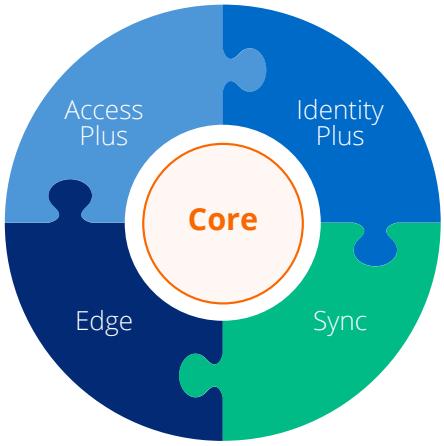
5 Forrester Research, "Making The Business Case For Identity And Access Management," 2019

Identity Cloud Packages

The ForgeRock Identity Cloud Core product provides all the technology that's essential for reinventing the digital customer experience. The Core package is designed to solve a majority of the customer use cases with a single offering. This includes identity management, access management, single sign-on (SSO) and federated SSO, adaptive and multi-factor authentication (MFA), and strong authentication factors, including one-time passcode (OTP), email confirmation, Mobile Push, Magic Link, and support for the ForgeRock Trust Network. Core integrates seamlessly with the ForgeRock Software Development Kit (SDK) for ease of implementation with customer applications.

ForgeRockIdentity Cloud Core can be customized to meet the needs of any organization through its upgrade packages: **Access Plus, Identity Plus, Edge**, and **Sync**.

Enterprises requiring more contextual and fine-grained authorization enforcement components can upgrade to the **Access Plus** package to enforce continuous and contextual authorization for transactions. Access Plus also makes it possible to introduce dynamic scopes and continuous risk monitoring capabilities to support Zero Trust and CARTA strategies.



The ForgeRock Identity Cloud Product Packages

Organizations wishing to modernize their customer-facing identity can choose the **Identity Plus** package, which supports social identity registration and login, personalization, delegation, user dashboards, privacy, and consent features. ForgeRock Identity Plus supports all leading social identity providers out of the box, along with other identity providers supporting OAuth2 or OpenID Connect.

The **Edge** package brings the security capabilities of the Identity cloud closest to legacy applications on premises, or to modern microservices running in the cloud. It includes capabilities of the ForgeRock Identity Gateway to create a secure perimeter for legacy applications and modern API traffic.

The **Sync** package includes a full-featured outbound provisioning engine with complete bi-directional and translatable synchronization to various systems and applications. Sync discovers new, changed, deleted, or orphaned accounts to determine user access privileges, and reconciles them seamlessly to ensure that user identity data including passwords are always accurate. It ensures that you have a stable hybrid environment where all identity data is consistent across all systems.

Conclusion

Your legacy, business-critical systems need modern IAM to bridge the gap between your on-premises deployments and your cloud offerings. Until now, there was no solution that could meet these needs with consistency and scalability. ForgeRock Identity Cloud is the industry's most comprehensive, fully customizable, and extensible identity platform as a service.

Using ForgeRock Identity Cloud, you can plan for your current and future business needs with a more attractive and predictable cost model and focus on the business. You can reduce operational risks by using a trusted software vendor, simplify your infrastructure footprint, and better align with your cloud strategy.

Contact ForgeRock today to learn more about the ForgeRock Identity Cloud.