ForgeRock

WHITE PAPER

MODERNIZING YOUR WORKFORCE IAM

Bigger Problems, Better Approach

One Platform, All Identities

Executive Summary

Digital transformation has revolutionized business and technology operations, enabling unprecedented advances in how we work and achieve business outcomes. Megatrends like remote working and the adoption of cloud-based applications and services are enabling more people to connect to more applications every day. However, these advancements have also created an identity data explosion, overwhelming risk and security professionals with an increasing volume of identities, roles, and entitlements that need to be continuously managed.

A traditional approach to IAM that relies on using and integrating disparate solutions to manage identities, access, and governance can no longer support the complexity of today's modern enterprise. Your organization requires a fully converged and innovative approach to IAM. Focused on addressing enterprise and large enterprise IAM requirements, ForgeRock Workforce IAM combines identity management, access management, and identity governance within a single solution, enabling your organization to secure user access, maximize productivity, and strengthen security.

Table of Contents

Today's Enterprise is Getting More Complex

Organizations are moving at a breakneck speed to keep pace with the demands of our digital world. Your workforce needs quick and easy access to the applications, tools, and platforms they require to perform their jobs and create business outcomes. However, the complexity of today's business environment is unprecedented, making it difficult to meet the on-demand identity and access needs of your workforce, while minimizing risk and meeting strict compliance regulations.

Numerous technology and business trends are contributing to the proliferation of identities that security and risk professionals must manage. Remote working has become the norm for most people, with more than half (58%) of the American workforce now conducting business outside of a traditional office.[1] In highly distributed work environments, there's an urgency to ensure business continuity and resiliency in the face of an unprecedented increase in internal and external cyber threats.

Across the board, enterprises have aggressively adopted cloud-based applications and services. Today, 94% of businesses already use some type of cloud service.[2] The cloud affords enterprises huge benefits, making it faster, easier, and less costly to implement new apps. But more apps also means more user accounts and increased pressure on security and risk professionals to manage a variety of applications with different security access controls.

Finally, enterprises are experiencing a high frequency of employee and contractor job changes. This constant state of flux means security and risk teams are forced to continuously manage changes associated with employees moving into new roles or business units, or requiring a different type of access. Most organizations struggle to keep up with these frequent access changes using traditional identity and access management (IAM) solutions.

Security and risk professionals are fatigued

These trends have resulted in an identity data explosion — where more and more new identities, roles, and permissions are created and changing every day. Consequently, today's security and risk professionals are fatigued as they try to manage an overwhelming number of identities, roles, and entitlements, while mitigating risk and maintaining compliance.

This identity explosion places a huge burden on security and risk teams, requiring them to ensure that each identity has only the access rights and privileges it needs. Without enterprise-wide visibility of the identity landscape or context around access requests and certifications, teams often find themselves overwhelmed. As a result, they are often forced to rubber-stamp access requests and certification approvals. They simply don't have the time to ensure that each request is truly necessary. But the consequences of not doing so can be dire — both from a security and compliance standpoint.

3.2 billion identities

The number of estimated identities and activities organizations have to manage and protect globally[3]

Security risks are on the rise

The scope, severity, and frequency of security breaches have dramatically increased over the past few years. For the fourth consecutive year, unauthorized access was the leading cause of breaches — 50% of all records breached. The scope is staggering with >2 billion usernames/passwords breached, a 35% increase over the year before.[4] The financial implications of breaches have also grown significantly. The average cost of a data breach in the U.S. has risen each year, more than doubling between 2018 and 2021 to $9.5 million — the highest in the world.[5] Beyond staggering fines, costs associated with breaches also include staff costs for remediation, user notification, loss of business, and more.

Compliance risks are escalating

To protect identity and data in this new norm, organizations worldwide face increased regulatory scrutiny and compliance requirements. Noncompliance fines for large enterprises can hit millions of dollars. For example, as of January 2021, a total of $331 million has been levied in penalties for GDPR violations against companies.[6] Penalties for regulatory noncompliance are equally impactful. A global insurance provider was recently fined $10 million for failure to comply with SOX regulations designed to ensure the proper identification of existing customers and their pension funds.[7] The U.S. Department of Health and Human Services, during an audit for HIPAA compliance, fined a Tennessee-based management company $2.3 million for a breach caused by compromised administrator credentials.[8]

The root of the problem for today's security and risk professionals is that existing identity and access management and governance solutions are slow, complex, and built on legacy concepts. They simply weren't designed to manage the complexity facing today's enterprises.

Enterprises have leveraged a best-of-breed IAM solution strategy to simplify the process of governing and managing users' access, roles, and permissions. Unfortunately, these solutions are siloed, difficult to administer, and costly because they are not optimized for interoperability. Additionally, while these best-of-breed solutions may be good on their own, they only provide a partial solution — identity management, access management, or identity governance. That means organizations must stitch together a patchwork of disparate solutions to cover all IAM requirements, which is time-consuming, highly expensive, and doesn't deliver on the promise of a strong return on investment

The effectiveness of these best-of-breed solutions erodes over time due to their human and manual-driven approach, which fails to keep up with the sheer volume and depth of new identities, applications, and permissions at scale in today's dynamic business environment. The result is that security and risk teams cannot keep up with manually processing all this new identity data to ensure appropriate access decisions are made in a timely fashion.

By 2023, 75% of security failures will result in inadequate management of identities, access, and privileges - up 50% from 2020.[9]

Gartner

The bottom line: Legacy IAM solutions are at an inflection point and need to evolve.

Why best-of-breed solutions are falling short

Best-of-breed IAM strategies are built on legacy concepts so they:

- Only provide a partial solution
- Are siloed, requiring patchwork of disparate solutions
- Are time consuming and expensive to manage
- Require human and manual-driven approach
- Fail to deliver promised ROI

ForgeRock's Modern Approach to Workforce IAM

The complexity facing today's organizations requires a fully converged and innovative approach to IAM. Comprised of three foundational pillars — identity management, access management, and identity governance — ForgeRock Workforce IAM enables your organization to secure user access, maximize productivity, and strengthen security. Focused on addressing enterprise and large enterprise IAM requirements, the unified solution is simple to use, AI-infused, and built on the scalable, high-performance ForgeRock Identity Cloud to help your organization leverage one platform for all identities.

> By 2025, 70% of new access management, governance, administrative, and privileged access deployments will be converged identity and access management platforms.[10]
>
> Gartner

Business benefits of Workforce IAM

Reduced operational costs
Save money and eliminate long deployments by simplifying cumbersome activities like application onboarding, access request reviews, and periodic certifications with an AI-infused governance process.

Stronger, more scalable security coverage
Deliver the security, scale, and resiliency needs of large, complex enterprises by leveraging fully isolated cloud resources with the power to process millions of permissions across thousands of applications in minutes.

Boost workforce productivity
Accelerate access to business applications and resources with automated day-one new hire access, and enable employees to work securely from any location on any device.

What business outcomes look like with Workforce IAM

The results of a converged IAM platform can be seen in real-world customer experiences all the time. While these business outcomes are focused solely on the automation savings in the first year, it is important to understand that the ongoing savings are equally impressive. The consolidation of legacy IAM solutions, achieving new levels of process automation, and reducing workloads can save enterprises massive direct costs and improve workforce productivity. Here is a business value example regarding ForgeRock's cloud-native governance solution.

CUSTOMER

- A global financial services organization
- $26 billion annual revenue
- 100K+ workforce identities
- 3,500+ applications

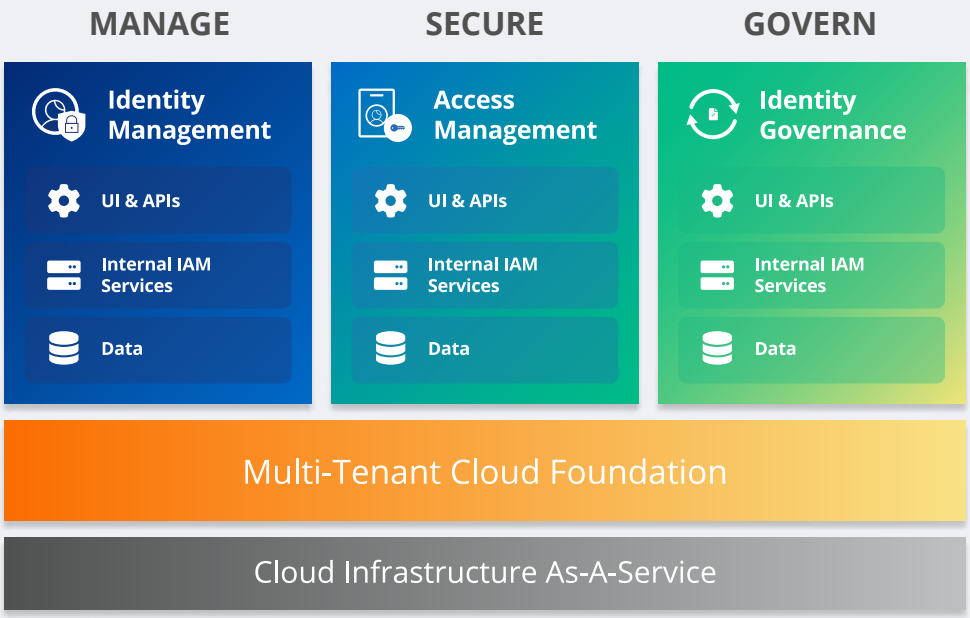
GOALS

- Replace 4 legacy IAM/IGA platforms
- Ensure compliance across end-user and privileged accounts
- Provide workflow-driven lifecycle management

BENEFITS

- **Time-Reduction:** Access certification campaigns created in less than an hour vs. weeks
- **Operational Savings:** Over $3M in operating costs saved due to hardware & software consolidation
- **Time Savings:** ~21% reduction in certification tasks through AI/ML automation findings

One Platform. All Identities.



Why ForgeRock Workforce IAM?

ForgeRock Workforce IAM is purpose-built to address large, complex enterprise use cases and requirements. The unique elements of the converged solution include:

Comprehensive IAM platform

A unified IAM workforce solution that helps manage, secure, and govern all identities throughout their entire lifecycle — all from a single platform. More effectively adhere to governance policies, enforce least-privileged access, and ensure a Zero Trust security environment.

Cloud hyperscale

Purpose-built cloud architecture rapidly processes and analyzes access data in order to meet the scale and resiliency needs of large, complex enterprises. Combined with a unique security and privacy model based on full tenant isolation, your data is protected from noisy neighbors at enterprise scale.

No-code access orchestration

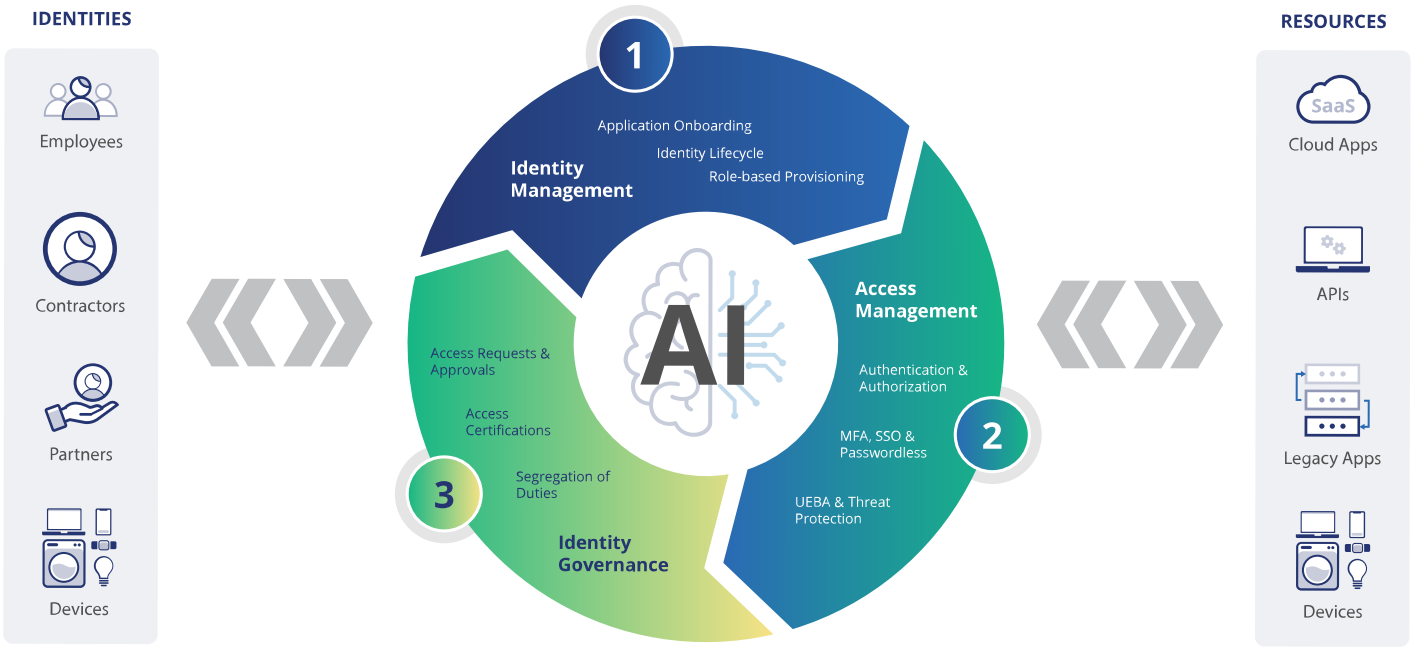
Quickly design flexible and seamless journeys to onboard users faster with a simple, drag-and-drop, no-code access orchestration designer. Built on ForgeRock Identity Cloud, you can save time and costs by creating the right journeys for the right users at the right time.

AI-infused IAM

Leverage AI and machine learning to facilitate end-to-end identity and access decisions with human oversight. Accelerate workforce access with AI-enabled access requests and certifications, automated low-risk approvals, and access control policy enforcement across the enterprise.

How ForgeRock Workforce IAM works

ForgeRock's modern IAM solution comprises three foundational pillars: identity management, access management, and identity governance. The unified IAM platform helps organizations manage, secure, and govern all identities and resources.



Manage identities

ForgeRock Identity Management helps enterprises manage user identities and their access to business applications and resources by automating the identity lifecycle management process. Organizations can create user accounts, manage access permissions, and offer self-service and password resets throughout the lifecycle of an identity within an organization. This allows your workforce to be more productive by providing them with quicker access to the business resources they need to do their jobs.

How it works

Application onboarding
Quickly onboard new business applications from a catalog of preconfigured application templates and automate user/application assignments with role-based provisioning.

Identity lifecycle
Automate and manage the joiner, mover, and leaver lifecycle stages for all users. Get all your employees, contractors, and partners up and running fast with access to the business applications and resources they need to do their jobs.

Identity workflows
Automate your organization's identity lifecycle processes with preconfigured, no-code identity orchestration workflow templates. Eliminate manual, error-prone processes and custom coding with a drag-and-drop configuration interface to accelerate users' access to business resources.

Secure access

ForgeRock Access Management secures access to business applications and resources, both modern and legacy, while delivering a seamless journey to the end users accessing them. With self-service registration, single sign-on (SSO), federation, and multi-factor authentication (MFA) capabilities, the platform helps to simultaneously deliver security and convenience.

How it works

Intelligent Access
An intuitive, no-code access orchestration visual designer allows you to drag and drop authentication configurations, making it easy for your teams to create, measure, and adjust any number of personalized user access journeys. This approach simplifies the process of creating the right user journey, while enabling secure user access from anywhere, at any time.

Multi-factor authentication (MFA)
Quickly verify users with password credentials using a second factor, such as a smartphone or biometric or passwordless authentication, to securely sign into workstations, servers, VPNs, and/or legacy applications.

Single sign-on (SSO)
Make it easy for users to login only once and securely access all of their business applications and resources. Securely federate one authentication session across multiple applications and trust boundaries using standard identity protocols or customized tokens for non-standard applications.

Authorization
Ensure just the right amount of access control is given to each employee, contractor, and partner in your organization with simple, coarse-grained, and/or fine-grained entitlement policies.

Federation
This service securely shares identity information across multiple domains or organizations, so users can access partner systems with the same authentication methods they use for their company.

Govern identities

ForgeRock Identity Governance is a cloud-native governance offering designed to help solve security and compliance challenges for large, complex enterprises at scale. The solution combines our unique cloud architecture and proprietary AI and ML with Google Cloud Platform (GCP) to determine whether employees should or shouldn't have access to applications and data. The solution creates AI-enabled recommendations and confidence scores to help organizations make faster and more informed decisions, and even automates low-risk decisions to reduce workloads for IT teams.

With ForgeRock Identity Governance, organizations can infuse AI into their governance processes and program to help:

- Reduce the high volume of extraneous access certification tasks
- Managers focus on the most important, high-risk access decisions
- Managers make quicker access decisions

ForgeRock's approach to identity governance creates the industry's most complete offering, combining three primary components: access certification, access requests, and segregation of duties.

How it works

Access certifications
Accelerate access decision-making with access certification campaigns that include remediation recommendations and confidence scores powered by AI.

Access requests
Empower users with a 24/7 self-service access request portal and automate application access with pre-configured workflow templates.

Segregation of duties
Enable least-privileged access by applying and enforcing segregation-of-duties policy checks — preventive and detective — to ensure regulatory compliance when and where you need it.

With ForgeRock Workforce IAM, enterprises can achieve a complete understanding of all their identity provisioning, administration, compliance, and employee access management needs. Coupled with AI and human oversight, organizations can more effectively adhere to governance policies, enforce least-privileged access, and ensure a Zero Trust security environment.

Rethinking Your IAM Strategy and Approach

Today's organizations have reached critical juncture. The continuous growth of users, access permissions, and applications have created an extraordinarily complex business environment. Security and risk professionals are overwhelmed as they try to manage this identity explosion while mitigating risk and maintaining compliance. That's why it is time to rethink your IAM strategy and approach.

ForgeRock's Workforce IAM solution is built to handle the complexity of today's digital business. It enables your organization to manage, secure, and govern all identities throughout their entire lifecycle — all from a single platform. With a converged IAM solution, you can quickly secure user access, maximize productivity, and strengthen security at enterprise-scale.

Now, is the time to change your IAM thinking, strategy, and approach. It's time for ForgeRock Workforce IAM.

We're here and ready to help. Contact us to get started.

Learn how security and risk professionals use ForgeRock to reduce operational costs, enable stronger, more scalable security coverage, and boost workforce productivity across the entire organization.

Contact us to learn more about how ForgeRock can help you.

[1] McKinsey, 2022, "**Americans are embracing flexible work—and they want more of it**"

[2] SG Analytics, 2020, "**94% of enterprises already use some type of cloud service - importance of Cloud Governance**"

[3] McKinsey, 2019, "**Digital identification, a key to inclusive growth.**"

[4,5] **2022 ForgeRock Consumer Identity Breach Report**

[6] Bank Info Security, 2021, **"Privacy Fines: Total GDPR Sanctions Reach $331 Million**"

[7] Compliance Week. 2019, "**Metlife to Pay $10M for 'longstanding' accounting errors**"

[8] HIPAA Journal, 2020, "**Business Associate Fined $2.3 Million for Breach of 6 Million Records and Multiple HIPAA failures**"

[9] Gartner, 2019, "**Is the Cloud Secure?**"

[10] Gartner, 2022, "**We've got your identity and access management needs covered**"

About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: **www.forgerock.com**.

Follow Us

ForgeRock