



White Paper

Modernizing Workforce IAM

Why it's time to extend or gradually replace legacy
Identity and Access Management

Introduction.....	2
The Top Twelve Trends Shaping Work and Business.....	2
Addressing the Twelve Workforce Trends.....	4
Falling Short: Legacy IAM and Multiple Systems.....	5
Legacy Identity and Access Management.....	5
Multiple Disparate Systems and Silos.....	6
The Way Forward: Extend or Replace Legacy IAM with a Comprehensive Digital Identity Platform.....	6
Support the Twelve Trends by Modernizing Employee IAM.....	7
ForgeRock: Empowering Workforce Digital Transformation with Ease.....	7
Address All Digital Identity Needs With One Simple Yet Comprehensive Platform.....	8
Meet Modern Identity Requirements Without Ripping and Replacing Legacy IAM.....	8
Realize Proven Bottom-Line Results.....	9
Learn More About ForgeRock for Your Organization.....	9

Introduction

Within the past decade, there has been an explosive combination of technology, ingenuity, and social change — culminating in twelve workforce trends that are actively and interdependently shaping how business and work gets done. Anchored in the demand for security, accessibility, and ease, these trends have shifted the landscape that organizations must navigate. To attract and retain top talent and be a viable competitor in the market, organizations must be equipped to address each.

The Top Twelve Trends Shaping Work and Business

1. Multi-Generational Workforce

By 2020, there will be four generations within the workforce (Boomers, Gen Xs, Millennials, Gen Zs), each with their own work-style preferences. In 2020, [Gen Z will account for 36% of the workforce](#). This generation highly [values employers with positive brand associations](#).

2. High Employee Turnover

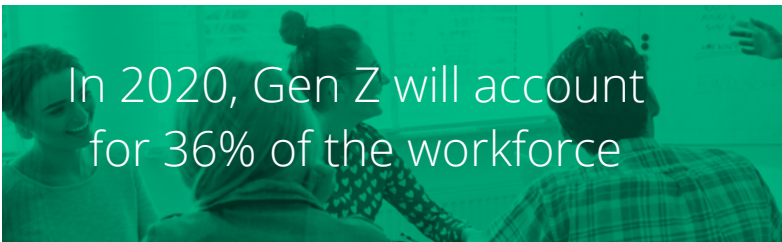
[Employees are changing employers at an unprecedented rate](#). To both attract and retain talent, organizations need to foster a positive brand and culture, address employee demands, and create delightful work experiences.

3. Strained IT Resources

IT departments are understaffed and overloaded. [According to Gartner®](#), “by 2020, 75 percent of organizations will experience visible business disruptions due to I&O [Infrastructure and Operations] skills gaps.”

A blue-tinted photograph of an office environment with several people working at desks. Overlaid on the image is the text "IT departments are understaffed and overloaded" in white.

IT departments are understaffed and overloaded

A green-tinted photograph of three young people, likely Gen Z, looking at a screen or whiteboard. Overlaid on the image is the text "In 2020, Gen Z will account for 36% of the workforce" in white.

In 2020, Gen Z will account for 36% of the workforce

4. The Experience Economy

The experience economy does more than just influence customer experiences —employees now demand the same level of delightful, secure, and frictionless experiences in their work lives that they enjoy in their personal lives.

5. Workplace Flexibility and Bring Your Own Device (BYOD)

Employees want to work easily from anywhere, using any device — including their personal devices.

6. The Gig Economy

According to [MBO Partners](#), the independent contract (freelance) workforce is expanding three times faster than the traditional, full-time employee workforce.


7. The Digital Workplace

Physical workplaces are now utilizing IoT 'things' at scale, such as beacons and sensors within corporate offices, geolocation trackers in workman helmets, and robots within manufacturing plants. These workplace 'things' can [collect employee data](#) and are often connected to a variety of internal systems.



8. Increasing Partnerships

To create the fluid services and experiences customers demand, [partnerships with outside organizations that create combined value-add solutions](#) and services are rapidly increasing.

A close-up photograph of a hand holding a smartphone. The image is overlaid with a blue tint and the text "Businesses are opening up their internal systems to be accessed by employees, contractors, and partners through APIs".

Businesses are opening up their internal systems to be accessed by employees, contractors, and partners through APIs

9. The API Economy

Businesses are opening up their internal systems to be accessed by both employees and other organizations to make it easier to build and access internal applications. A prime example of how even traditionally closed organizations are opening up to gain market share and publishing APIs, as well as satisfying regulatory requirements, are the PSD2 regulations and OpenBanking initiatives.

10. Cybercrime

The number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting. For example, according to the [U.S. Consumer Breach Support](#) published by ForgeRock, in 2018, more than 2.8 billion consumer data records were exposed in 342 breaches at an estimated total cost of more than \$654 billion. Unfortunately, a significant percentage of [hacks and breaches are attributed to employees](#), such as with the [Capital One hack in July of 2019](#).



11. Changing Regulatory Environment

Many organizations are utilizing technologies to [track employees' every move](#). However, just as with external personal user data, [employee personal data must be protected](#) according to numerous laws and regulations within the United States, the European Union's General Data Protection Regulation (GDPR), and others.

12. Cloud

The cloud enables the development and deployment of new applications faster than ever before. Because of this, cloud adoption has become ubiquitous, even within many regulated industries such as financial services.

Addressing the Twelve Workforce Trends

Together, the twelve trends are a dominating force, steering how business and work is done. To address the trends rather than get over-run by them, organizations must:

- › Maintain a positive brand and deliver delightful, secure, transparent, and frictionless experiences (during and after onboarding) in order to attract and retain top talent
- › Enable a digital workforce and support a variety of generational preferences by building trusted applications that can be accessed anywhere by employee, contract, and partner-owned devices (BYOD)
- › Give employees, contractors, and partners secure and appropriate level of access to resources, systems, and applications while constantly verifying that access
- › Secure digital workplace IoT devices, 'things', as well as their data and system integrations
- › Open externally to leverage third-party systems, applications, and identity driven API ecosystems
- › Decrease the strain on IT departments and resources
- › Support rapidly changing business needs with new applications and services while also maintaining business-critical legacy applications
- › Ensure security, privacy, and control capabilities meet regulatory mandates and supports users' trust
- › Enable rapid testing and deployment of new solutions easily and securely within the cloud



Organizations must be able to support the 12 workforce trends to survive and stay relevant

Unfortunately, achieving the above presents real challenges to most organizational ecosystems and system environments.

Falling Short: Legacy IAM and Multiple Systems

In the context of addressing the twelve trends, organizational leaders must understand the inventory of their current system environments as well as the processes used throughout their enterprise.

Legacy Identity and Access Management

Most organizations have large investments in traditional employee identity and access management (IAM) systems. Yet, traditional employee IAM uses static rules to make decisions and is built to solely support employee identities, not third-party systems and APIs, BYOD devices, and IoT 'things' — nor the data they amass. This results in latency, frustration, friction, and increased risk across the organization.

To address the twelve trends and support ongoing digital transformation while trying to mitigate risk, most organizations attempt to modify their legacy IAM systems. This is done mainly through complex integrations into back-end systems and data stores. However, if the process is not proven to be secure, fool-proof, and cost effective, most IAM and data protection professionals will not risk breaking their current systems, however slow and heavy, for new technology.

For example, some high-demand employee IAM capabilities such as multi-factor authentication and biometrics are difficult to integrate and test within a legacy environment, and selecting the right solution from the vast number of start-up vendors is extremely cumbersome.

All of this results in the digital transformation stagnation organizations seek to free themselves from.

Traditional employee IAM uses static rules to make decisions and is built to solely support employee identities, not third-party systems and APIs, BYOD devices, and IoT 'things' — nor the data they amass

“Attempting to adapt existing IAM systems that do not have the flexibility, extensibility or scalability required is a common pitfall of organisations...”

— ComputerWeekly*

*<https://www.computerweekly.com/news/450429018/Consumer-identity-management-will-benefit-business>

Multiple Disparate Systems and Silos

To collect and manage employee, freelance contract, and partner identities and data, most organizations are using a multitude of disparate systems across departments. For example, the Human Resources department alone may be using several software solutions that collect employee and contractor personal identifiable information (PII) for various needs. At the same time, the Marketing department may be integrating with third-party partner applications and using a variety of software to analyze and execute on PII data gathered through collaborated partnership initiatives. Meanwhile, IT uses multiple systems (including multiple IAM systems) to secure the organization itself, along with a patchwork of other systems to keep departmental solutions and the data they gather in check.

In total, the amount of disparate systems and siloed data within the modern enterprise is cause for alarm. Not only do disparate systems create a slow, un-unified work experience, they increase risk and make risk assessments more difficult. Also, managing disjointed legacy systems requires a vast amount of IT time and resources.

The Way Forward: Extend or Replace Legacy IAM with a Comprehensive Digital Identity Platform

Today's most advanced digital identity management platforms are designed to secure and manage identities and data of every kind (employees, contractors, partners, customers, devices, and 'things') as well as facilitate the use of new technologies.

The most thoughtfully crafted platforms can be implemented as a single, all-encompassing IAM solution across an organization for all use cases. They may also be used to easily extend and integrate existing IAM legacy systems according to an organization's unique needs. Additionally, they may be deployed within any environment, such as on-premises or within any cloud environment (public, private, hybrid-cloud, multi-cloud, bring-your-own cloud, or as-a-service).



Thoughtfully designed Digital Identity Platforms allow organizations to easily integrate with and extend existing legacy IAM systems.

Support the Twelve Trends by Modernizing Employee IAM

Either as a new all-encompassing IAM platform or used to extend and/or gradually sunset current legacy IAM, digital identity platforms must enable organizations to address the twelve workforce trends with modern IAM capabilities, such as:

- › Providing better user experiences through single sign-on, federation, a single view of a user and modern standards compliance
- › Identifying and protecting against fraudulent and malicious activities by adopting a Zero Trust and CARTA (continuous adaptive risk and trust assessment) model
- › Ensuring secure interactions across all users, externally owned devices, IoT 'things', APIs, applications, services, and integrations to support new business opportunities, workplace flexibility, and BYOD
- › Using automated provisioning, workflows, and governance to speed onboarding and decrease the development and administrative burden on IT teams
- › Integrating disparate systems (from departmental to security systems) to fully leverage current and new investments and create a single view of a user through directory services
- › Automating routine administrative tasks like the deployment of hardware (using cloud) and software (using DevOps) to enable business to run lean and efficient
- › Speeding development time by supporting a secure, microservices strategy within a monolithic environment
- › Integrating new and emerging technologies and advancements, such as artificial intelligence (AI) and machine learning (ML), easily into authentication flows

ForgeRock: Empowering Workforce Digital Transformation with Ease

Identified as an [Access Management and Federation Overall Leader](#) and the Overall Leader in all categories for Identity API Platforms by KuppingerCole, as well as a [leading visionary for access management by Gartner](#), the ForgeRock Identity Platform meets all of the workforce trends and empowers workforce digital transformation with ease.

“Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations.”

— KuppingerCole*

*<https://www.forgerock.com/resources/analyst-report/kuppingercole-leadership-compass-identity-api-platforms>

Address All Digital Identity Needs With One Simple Yet Comprehensive Platform

The ForgeRock Identity Platform is a flexible, unified solution that can be implemented across an organization for all use cases — employees, contractors, partners, customers, devices, and ‘things’. The ForgeRock Identity Platform consists of Identity Management, Identity Governance, Access Management, User-Managed Access, Directory Services, Edge Security, and an Identity Gateway. The full platform can be deployed as-a-service, on-premises or within any cloud environment including multi-cloud and hybrid-cloud for millions of identities in minutes. Importantly, the ForgeRock Identity Platform is able to fully address the twelve workforce trends.

Meet Modern Identity Requirements Without Ripping and Replacing Legacy IAM

Unlike most digital Identity solutions, with the ForgeRock Platform organizations don't need to suffer the pain, risk, and expense of ripping out existing Identity solutions to get the IAM modernization needed to compete in the digital landscape.

ForgeRock provides a flexible approach that enables organizations to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems like CA Single Sign-On (SiteMinder), Oracle, IBM and even homegrown identity systems. Additionally, ForgeRock Intelligent Access includes a pre-integrated ecosystem of technology partners, allowing organizations to add third-party capabilities such as biometrics or contextual signal collection with just a few clicks. ForgeRock and these technology partners take the responsibility of verifying these integrations with each release of the product. This enables low-risk rapid deployment of the latest innovative technologies at scale without the risks associated with adopting new technology, their upgrades and working with start-up companies — all while reducing cost and complexity.



The ForgeRock Identity Platform is a flexible, unified solution that can be implemented across an organization for all use cases — employees, contractors, partners, customers, devices, and ‘things’

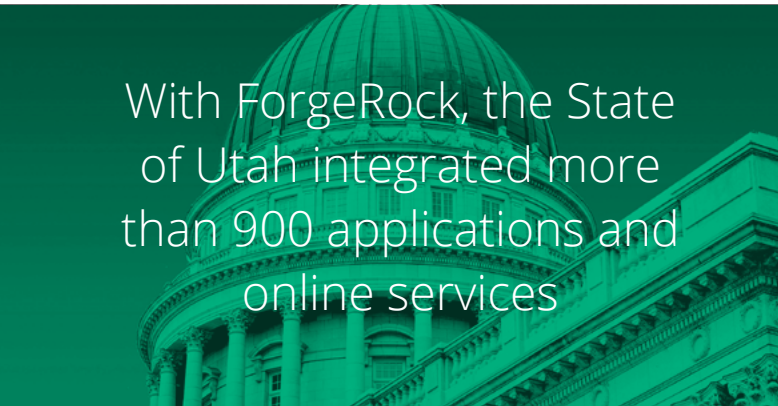
ForgeRock provides a flexible approach that enables organizations to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems

Realize Proven Bottom-Line Results

With ForgeRock, organizations realize tangible business benefits.

The State of Utah Saves Up To \$15 Million

The State of Utah sought to gain greater reliability and scalability in its identity and access management infrastructure to integrate more data and applications, and expand the number of online services available to employees, citizens, and businesses. After selecting the ForgeRock, they integrated more than 900 applications and online services, providing the flexibility and scalability to support all 1,400 of the states online services and a growing variety of additional applications and services, including those running in the cloud. Dave Fletcher, Utah's Chief Technology Officer, highlighted "We're looking at savings of up to \$15 million over five to six years tied directly to the efficiencies gained from having modernized our IAM infrastructure leveraging the ForgeRock Identity Platform."




With ForgeRock, the State of Utah integrated more than 900 applications and online services

HSBC Centralized and Replaced Over 400 Identity Systems

HSBC uses ForgeRock as a single identity platform across the entire HSBC Group globally. With the ForgeRock, they created a future-minded, digitally consistent, exceptional employee and customer experience across all lines of business for 100M identities by centralizing and replacing over 400 different identity systems onto the ForgeRock Identity Platform. Their results include GDPR, PSD2, and Open Banking compliance, increased security using technologies such as biometrics and adaptive risk, and future-preparedness for things like Alexa, IoT, and beyond. All contribute to business growth and competitive advantage.

These are just a couple examples among multitudes of how ForgeRock can make a real difference to the bottom line.



HSBC uses ForgeRock to create exceptional employee and customer experiences across all lines of business for 100M identities

Learn More About ForgeRock for Your Organization

ForgeRock is the [leading and most comprehensive](#) digital identity management provider — designed to support the workforce trends with modern employee IAM today and well into the future. As the most future-minded, flexible, and complete yet simple-to-use digital identity platform on the market, ForgeRock helps organizations grow business and competitive advantage, increase productivity, improve security, privacy, and compliance, and reduce costs.

[Contact us](#) to learn how ForgeRock can help your organization.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.



Copyright © 2020 ForgeRock, All Rights Reserved.

Follow Us

