ForgeRock

SOLUTION BRIEF

Modernize IT to Empower and Secure an Agile Workforce

ForgeRock Workforce Access Management Solutions

The ForgeRock Workforce Access Management solution helps organizations achieve their digital transformation and business growth goals, protect the organization's users against breaches, enable regulatory compliance, and empower an efficient and increasingly remote workforce.

Legacy enterprise access management solutions – whether homegrown or commercial – are becoming obsolete. Rip-and-replace is rarely the best option for most enterprises working on a limited budget. Fortunately, a new, modern approach to workforce access management is available from ForgeRock that will help global organizations achieve their goals for digital transformation and business growth.

The State of Enterprise Workforce Access

Today's enterprise CIO needs to support a growing, diverse, and increasingly remote workforce. The remote workforce has been steadily growing, and, since 2020, the percentage of remote office workers has increased from 39% before the COVID-19 pandemic to 77% after work from home orders were implemented.[1] Some organizations have decided to allow "work from home forever."[2]

But not every organization is ready for remote workers: 50% of employees are unhappy and less productive because they can't easily connect to the workplace. A mixture of legacy and cloud access management systems creates disjointed authentication experiences. These create separate identity silos that prevent IT teams from getting a comprehensive view of their user base. IT costs for upgrades, customizations, and maintenance strain budgets. In 2019 alone, more than 60% of IT budgets were spent on maintaining legacy technology.[3]

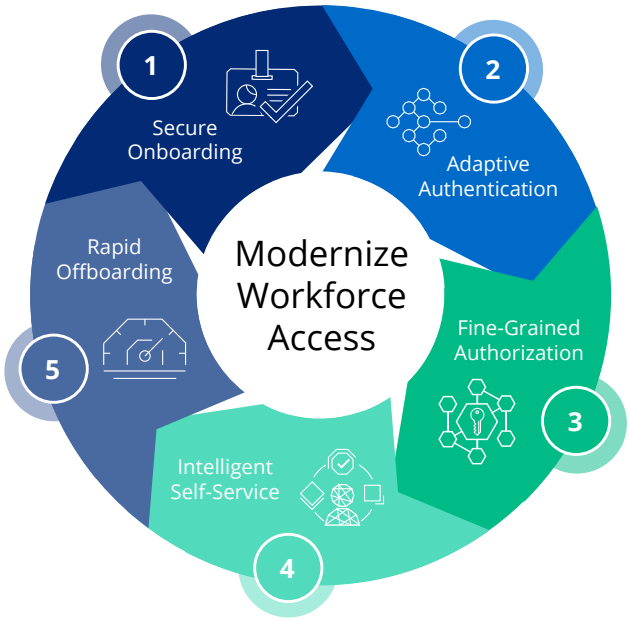
Securing how remote workers access their work environment is not just a "nice to have" – 80% of data breaches start from stolen credentials.[4] A massive uptick of users and devices makes it harder to distinguish actual humans from bots, while an unsecured IoT device, weak password, or "bring-your-own-device (BYOD)" policy can lead to unauthorized access, attacks, and damaged reputations. IT needs to protect their organization, safeguard data, and improve audit controls to avoid fines for noncompliance.

Organizations need to juggle multiple priorities when it comes to workforce access: support remote workers, improve the overall security posture, and modernize their legacy systems – all without disrupting the business.

Modernizing IT for Business Agility

Modernizing IT doesn't have to require a rip and replace. The right access management solution should help organizations coexist with legacy systems, help them migrate to more modern systems over time, while maintaining a consistent and transparent end user experience.

In a modern IT environment, CIOs can empower their remote workforce to work efficiently from the day they start until they depart. On day one, secure onboarding gives them access to the applications and systems they need. Adaptive access controls enable administrators to set policies on who, what, and how users receive elevated access when they need to perform more sensitive transactions. Fine-grained and contextual authorization policies protect the organization by continuously validating every interaction between users and applications. Intelligent self-service capabilities give users the ability to manage their own password resets and preferences, reducing both end-user friction and IT support costs. When workforce users leave the organization, IT can rapidly remove all their accounts and privileges, thus safeguarding the organization's sensitive data against unauthorized, "lingering" access.



[1] https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html
[2] https://www.forbes.com/sites/danabrownlee/2020/05/18/twitter-square-announce-work-from-home-forever-optionwhat-are-the-risks/
[3] https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html
[4] Verizon 2020 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir/

Why ForgeRock?

Every customer has unique needs, and they want a workforce access management solution that fits with their unique business processes. ForgeRock's philosophy is to meet customers where they are and help them move to their desired next stages of digital transformation.

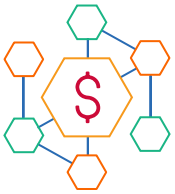
ForgeRock Workforce Access Management is a modern identity and access management solution that allows organizations to quickly modernize their legacy environments, empower the workforce towards greater efficiency, and protect the organization against data breaches due to unauthorized access. Here are some of the reasons why customers choose ForgeRock.

Here are some of the reasons why customers choose ForgeRock:

A single platform for all digital identity needs, that is comprehensive and extensible for any identity at any scale

The ForgeRock platform supports all identity types; accommodates past, present, and future technologies without breaking the bank; and supports the simplest to the most complex use cases.

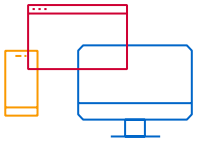
- An international, nonprofit scientific association that had a mixture of "easy" modern applications and "difficult" legacy on-premises applications required customizations that were not possible with a cloud only service. Using the ForgeRock workforce access management solution, they were able to go live in 60 days, supporting both modern and legacy applications.



Simpler and faster time to value using a flexible deployment in the cloud, on-premises, or in hybrid deployments

Providing faster time to value for simple, cloud-only use cases is easy. It's a much bigger challenge to do the same thing for highly complex, hybrid use cases. ForgeRock delivers the most in-depth cloud functionality, while providing IT teams with the ability to design workforce access management journeys quickly.

- A financial customer switching over from a legacy IAM system saved 75% on implementation time and completed the project using half the resources as their previous implementation using ForgeRock DevOps capabilities and modernization accelerators.



Modernized, Consolidated, and Integrated Legacy Systems

Today, enterprises are overwhelmed trying to manage their legacy IAM and integrate new applications and platforms. An increasing share of IT budgets are being tied up in legacy infrastructure. What's at stake is the ability to keep the organization agile to take advantage of new business opportunities when they emerge.

- A large U.S.-based telecommunication company replaced their legacy CA SiteMinder environment with ForgeRock to support their 275,000 employees and a projected savings of 50% on infrastructure costs alone.

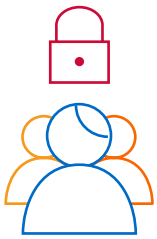
"We're looking at savings of up to $15 million over five to six years tied directly to the efficiencies gained from having modernized our IAM infrastructure leveraging the ForgeRock Identity Platform."

Dave Fletcher,
CTO, State of Utah

Benefits

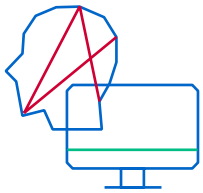
Accelerate Legacy Modernization

- Use ForgeRock Intelligent Access to show immediate value. Add new capabilities using easy-to-design user journeys for modern single sign-on, multi-factor authentication, usernameless and passwordless authentication, and contextual authorization.
- Minimize operational impact by migrating complex legacy IAM deployments in several migration waves over time. ForgeRock makes this process seamless and invisible to end users.
- Automate user migration with ForgeRock's Modernize IAM Accelerators tool kits, while supporting co-existence with the legacy IAM system. Once migration is complete, sunset old systems with no impact to users.



Protect Your Organization

- Build secure user access journeys that consistently apply consistent security policies across all internal, cloud, and edge applications.
- Enforce Zero Trust and Continuous Adaptive Risk and Trust Assessment (CARTA)[5] security models to grant workforce access based on multiple contextual, behavioral, and risk-based signals.
- Continuously assess the risks of users and devices interacting with the organization's digital channels before, during, and after authentication. Enforce fine-grained authorizations based on signals such as device profile, network and geographic context, mouse and keyboard movements, user choice, analytics, and risk profile.



Empower an Efficient Workforce

- Provide secure access for remote workforce users from any location, any time, and on any device, so they can be productive from anywhere.
- Design seamless access journeys with usernameless and passwordless authentication for consistent and frictionless experiences.
- Reduce IT costs and enable regulatory compliance by eliminating manual processes for self-service and password reset.

[5] https://www.gartner.com/en/webinars/3891406/the-7-imperatives-of-continuous-adaptive-risk-and-trust-assessme