ForgeRock

Workforce IAM Evaluation Guide

Table of Contents

In the first half of 2020, the way work gets done around the world dramatically shifted. More employees and contractors are working from home than at any other time in history. Even organizations with a predominantly onsite workforce are increasingly reliant on connected and integrated technologies.

As discussed in the paper *Modernizing Workforce IAM*, 12 workforce trends are actively and interdependently shaping how business and work is done. While addressing these workforce trends with digital transformation initiatives was a priority prior to 2020, recent events have been a force-multiplier. For survival and viability, you must now speed your digital transformation initiatives to meet today's demands by gaining specific capabilities. These capabilities are made possible by modern identity and access management (IAM) platforms.

Required Capabilities to Meet Workforce Demands and Trends

To meet today's workforce demands and trends, you need to be able to support 12 capabilities with modern IAM solutions.

1. Enable remote work with trusted internal apps that can be accessed anywhere.
2. Support a bring-your-own-device (BYOD) model.
3. Deliver secure, frictionless experiences during and after onboarding.
4. Give secure and appropriate levels of access to resources, systems, and apps while constantly verifying that access.
5. Secure digital workplace IoT "things," such as robotics and sensors, as well as their associated data and system integrations.
6. Open externally to third-party systems, apps, and identity-driven API ecosystems.
7. Decrease the strain on IT departments, resources, and administrators.
8. Support rapidly changing business needs with new apps and services while also maintaining business-critical legacy applications.
9. Ensure that security, privacy, and control capabilities meet regulatory mandates and support users' trust.
10. Enable rapid testing and deployment of new solutions easily and securely within the cloud.
11. Support a large seasonal workforce with fast, accurate access and easy de-provisioning.
12. Enable a seamless migration of identities across systems to support evolving needs, such as reorganization or mergers and acquisitions.

How to Evaluate IAM Providers for Today's Workforce Requirements

Unfortunately, meeting the 12 required capabilities presents real challenges to current organizational ecosystems and legacy IAM systems. To gain these capabilities, you need to consider either replacing or modernizing your current IAM systems with a full-service IAM platform designed to address both today and tomorrow's needs. However, not all IAM providers support the 12 required capabilities. This makes the selection process more difficult.

When evaluating IAM providers, we recommend a two-step process organized around basic and strategic components that together support the 12 required capabilities. Basic components cover the most common and simple workforce use cases. Strategic components are those that speed workforce digital transformation; increase efficiency and productivity; improve security, privacy, and compliance; and reduce costs.

This evaluation guide lists key basic and strategic IAM components and provides definitions and request for proposal (RFP) questions for each to help you differentiate solutions during your selection process.

Step One: Evaluate Providers for Basic Workforce IAM Components

For additional RFP questions, ForgeRock's answers, a comparison matrix, and more, request a copy of The Ultimate Workforce IAM RFP Guide.

Behind the scenes, IAM platforms are now the enablers of work and business. Yet, IAM platforms vary in their components and capabilities. The following are the basic workforce IAM components needed to begin addressing today's workforce trends. As a first step in your evaluation process, compare providers for each basic component using the included RFP questions. For ForgeRock's answers to these questions, please contact your representative or stay tuned for the Workforce IAM Comparison Workbook.

Basic Component	Basic Component Description	RFP Questions for Workforce IAM Providers
Single Sign-On (SSO)	SSO is a user authentication service that allows users access to multiple apps, services, and systems with one set of login credentials. Standards used for SSO include SAML, OpenID, and OpenID Connect (OIDC). These standards facilitate the exchange of user authentication and authorization data across secure domains. SSO helps improve security and provides a frictionless user experience, resulting in increased productivity. Learn more about the basics of SSO.	• Does the provider offer single sign-on based on SAML, OpenID, and OIDC?
Federated SSO	Based on trusted relationships between organizations, federated SSO gives users secure access to an organizations' web properties and applications using a single account. In other words, federated SSO enables organizations to conduct business securely with third parties. Federated SSO uses open standards such as OAuth, WS-Federation, WS-Trust, OIDC, and SAML to pass authentication tokens between the organizations' identity providers. Federated SSO helps organizations know who is interacting with them, what they're enabled to do, and trust that the interaction is secure. Learn more about the basics of Federated SSO.	• Does the provider offer federated SSO based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC, and SAML?
Multi-Factor Authentication (MFA)	MFA is a method of validating a user's identity through multiple authentication mechanisms. MFA asks for additional credentials when authentication takes place under centrally defined risky or suspicious conditions. Authentication mechanisms include something the user knows, something the user has, and something the user is. For example, access is only granted after a user enters their password (what the user knows) and a numeric code sent by text to their phone (something the user has). MFA helps organizations know who is interacting with them, what they're enabled to do, and trust that the interaction is secure.	• Does the provider offer MFA? • What MFA mechanisms do they offer?
Authorization	As part of access control within a digital identity solution, authorization is the function of determining if a user has permission to access a specified resource(s), such as a website(s), record(s), document(s), and so on. Authorization helps organizations know who is interacting with them, what they're enabled to do, and trust that the interaction is secure.	• What types of authorization methods and access controls are offered by the provider?

Basic Component	Basic Component Description	RFP Questions for Workforce IAM Providers
Provisioning	A part of authorization, provisioning is the process of managing roles and entitlements that are assigned to specific users, devices, or things based on organizational policy and structure (such as job function, title, and geography), as well as assigning and removing entitlements and resources. Importantly, more sophisticated workforce IAM platforms will offer automated provisioning and workflow-driven provisioning. See the Strategic Components table below for details.	• Does the provider offer provisioning capabilities? • Can the solution manage previously disparate data repositories, network applications, and user data stores anywhere in the infrastructure stack? • Can the solution provision and assign relationships to users, devices, and things? • Does the solution support a 'least privilege' security model by decentralizing control with delegated administration?
Workflow-Driven Provisioning	Workflow-driven provisioning is based on a set of steps within a business process that need to be done during the creation, update, or deletion of a user's account. These workflows could involve simple manager approval to grant new access or a complex multi-step process that involves pulling information from other systems to verify the user and perform multiple levels of approvals. Within workforce IAM, workflows visually organize identity synchronization, reconciliation, and provisioning into repeatable processes with logging and auditing for reporting purposes. This ensures that a standard policy is followed for granting or removing any access to users without having to perform email or paper-based approvals. Importantly, within identity management, workflows are part of the provisioning process. The key to any workforce identity management solution is the ability to provide workflow-driven provisioning activities.	• Does the provider have the ability to integrate simple and complex workflow operations into user provisioning, deprovisioning and access requests? • Does the provider support standards-based workflow engines? • Does the provider incorporate best practices in workflows by offering standard templates? • Does the provider offer the ability to customize the workflows easily to meet business needs?
Governance Administration	Governance administration is the process that allows organizations to monitor and ensure that user access rights are accurate and securely managed. This is typically done by allowing a manager or application owner to review the access of users in the system and then letting them certify that they should continue to have that access or deny that access so it can be immediately removed. This helps ensure that the right people have the right access to the right services at the right time. Many regulations like Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) mandate that such access review be part of the organization's standard security practice.	• Does the provider offer the ability to review and certify user access periodically to ensure that users have the right access? • Does the provider have the capability to perform access reviews on an ad-hoc or event-driven basis, such as when a user changes roles? • Does the provider offer the capability for a multi-step access review process so that more than one reviewer can verify the user access? • Do governance administration capabilities integrate tightly with the provisioning solution so that any access that is denied is immediately revoked?

Basic Component	Basic Component Description	RFP Questions for Workforce IAM Providers
Delegated Administration	Delegated administration allows identity administrators to give selected individuals the capability to create, manage, and delegate the management of employee accounts and access rights, as well as other fine-grained administrative tasks on managed objects. This delegation of administrative duties allows individual lines of business to efficiently manage their own teams without having to depend on the central IT team, significantly improving their agility.	• Does the provider offer delegated administration?
Self-Service	Self-service refers to allowing users to manage their accounts on their own rather than relying on an organization's support staff. Examples of self-service include managing login preferences, password management, updating contact information, searching for and requesting additional access, and so on. Self-service not only reduces support costs, it also improves user experience. Self-service empowers users by giving them more control and choice and reducing their dependency on central IT teams.	• Does the provider offer self-service? • What self-service capabilities does the provider support? • Does the provider allow users to search and request additional access for themselves? • Does the provider allow users to request access on behalf of others?
Identity Store	As part of directory services, an identity store is a repository for identity (user or connected thing) attribution data. Stored identity data should be encrypted both while at rest and in transit. Also, as a best practice, it is good to have an embeddable repository that can easily share real-time employee, device, and user identity data across multiple environments. Additionally, from a hosting perspective, identity stores should include high availability, performance, and security. Importantly, the identity store should be fully compliant with LDAP v3 and should integrate seamlessly with any directory. Having an identity store that is compliant with LDAP v3 and with an embeddable repository allows organizations to easily share real-time employee, device, and user identity data across multiple environments, enabling organizations to integrate that data into their existing application environment securely and easily, allowing for a seamless user experience.	• Does the solution offer fractional and multi-master replication? • Can the identity store scale to support data from hundreds to millions of identities, including devices and things? • Does the solution's identity store comply with LDAP v3 and integrate seamlessly with any directory?
Support for a Single View of Identities	Most employees, contractors, partners, and vendors interact with an organization across many different apps for things like HR, marketing, accounts payable, and so on. There may be user data integration between some apps, but, on the whole, each app and its data about a user is siloed across an organization. This presents difficulties in fully understanding a user from a 360-degree view. This includes knowing all their access rights, preferences, usage, potential risks, and more. In order to gain a complete picture of your users and how they interact with your organization, modern IAM uses identity management and directory services products to synchronize, migrate, and manage identity data across an organization's system environment. With a single view of a user, you can: • Consolidate user identities and increase their security with behavioral, contextual, and risk-based authentication and authorization policies. • Standardize and unify the user experience across the organization on any app and any device (omnichannel). • Conduct analytics on users to better understand their access and associated risks.	• Can the solution integrate with other systems in order to consolidate identity data silos to create a single view of the user organization-wide? • Can the solution provide live bidirectional synchronization and reconciliation of identity attributes between data stores?

Step Two: Evaluate Providers for 20 Strategic Workforce IAM Components

For additional RFP questions, ForgeRock's answers, a comparison matrix, and more, request a copy of The Ultimate Workforce IAM RFP Guide.

IAM platforms should go beyond the basics and incorporate strategic workforce IAM components in order to fully meet today and tomorrow's requirements and to ensure your organization stays relevant into the future. Below are 20 strategic components that modern IAM platforms should offer. The second step in your evaluation process is to compare providers by each strategic component using the included RFP questions. For ForgeRock's answers to these questions, please contact your representative, or stay tuned for the Workforce IAM Comparison Workbook.

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
Availability and Scale	It is important to ensure that a user's access and session remains undisrupted should something happen, such as a server going down. IAM providers should support both 'service availability' and 'session availability'. Service availability ensures that users can access an application when a server goes down. Session availability preserves and keeps a session running if a server goes down. IAM providers should also support a variety of scale scenarios. This includes a shifting number (often millions) of users, devices, and things that need to be stored in a database, as well as changing frequencies and lengths of simultaneous and concurrent sessions. Support for a stateless protocol using JWT session tokens is also advisable. Availability and scale allow organizations to save administrative and IT resource time, resulting in reduced costs.	• Does the solution scale elastically? • For example, does it have the ability to scale the identity synchronization, authentication, and authorization service by many orders of magnitude to respond to predicted peaks, such as during a high-profile event or unpredicted events, such as trending content demand?
Open Standards Support	Open standards are established, uniform technical norms used by developers. Each standard has specified capabilities and functionality. Identity security relies on the OAuth2, OpenID Connect (OIDC), and SAML standards. Going beyond these basic identity standards, leading digital identity providers are integrating standards that are needed to support emerging workforce trends. These include OAuth 2.0 Proof-of-Possession, which ensures that the presenter of a bearer token is the real and original token owner, and OAuth2 Device Flow, which is designed for client devices that have limited user interfaces. Support for both basic and advanced open standards, such as OAuth2, OIDC, SAML, UMA 2.0, OAuth2 Device Flow, and OAuth 2.0 Proof-of-Possession, allows organization to secure data and transactions with outside entities, including third-party APIs, devices, and IoT things. This enables secure business growth and increases competitive advantage.	• Does the solution support both basic and advanced open standards, such as OAuth2, OIDC, SAML, UMA 2.0, OAuth2 Device Flow, and OAuth 2.0 Proof-of-Possession?
Artificial Intelligence (AI) and Machine Learning (ML) Informed Identity Management and Governance Authentication	Many organizations are increasingly supporting an all-remote workforce. This shift is putting pressure on their current employee IAM systems, as well as the IT staff, administrators, and managers who need to ensure that the right people have the right to access the right systems and applications while working from home. Additionally, the risk of breaches, hacks, fraud, and other malicious activity also intensifies with the sudden increase in the number of remote employees. Identity governance and administration (IGA) helps manage and provision user access, as well as reduce the risk that comes with employees having excessive or unnecessary access to applications, systems, and data. AI and ML take IGA to the next level by quickly identifying outliers within a huge volume of data. These technologies also produce confidence scores to assist managers and approvers who conduct access reviews and approvals. All-inclusive modern IAM platforms that offer identity and IGA powered by AI and ML increase efficiency and provide more time for IT staff and access approvers to focus on access rights that have been identified as risky or anomalous. The result is improved security and reduced administrative burden.	• Does the provider offer AI and ML capabilities to extend the governance functionality? • Can the AI engine consume data from other sources? Is it flexible enough to work with other IAM solutions and data sources, or is it limited to the provider's platform only?

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
Automated Provisioning and Deprovisioning	Provisioning is the registration and on-boarding of employees, contractors, partners, or vendors into multiple applications based on specific attributes, such as their title, location, or manager in order to give them access to what they need from day one. Deprovisioning automatically disables or deletes all accounts associated with an identity when employees or partners leave an organization, eliminating so-called zombie accounts. Automating the granting of additional access and the removal of excess and high-risk access with an AI- and ML-powered governance solution saves administrative time, resulting in increased productivity. Automated deprovisioning also improves security hygiene and saves money by removing unneeded accounts from applications and reducing the associated licensing costs.	• Does the solution allow for automated provisioning and deprovisioning of users? • Can the solution integrate with an existing HR system or other sources of truth for user information to onboard, update, or remove users?
Distributed Scope Design with Least Privileged Access	Scopes enable the principle of 'least privileged access', which means only granting access that is essential to perform an intended purpose. For example, employees are only permitted to access the exact information and resources necessary for a particular and legitimate purpose. A first step towards achieving this fine-grained authorization is developing a mechanism to distribute and assign strongly typed scopes to applications, API endpoints, and other protected resources. Scopes must then be coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions should also be applied. Distributed scope design with least privileged access helps organizations prevent fraud and malicious activity resulting in improved security and compliance.	• Can the solution enable least privileged access to only grant access that is essential to perform an intended purpose?
Standards-Based Onboarding for Applications	In the early days of IAM, access management was controlled and administered by central teams. The teams onboarded new applications as point-to-point integrations, which created a bottleneck for organizations that wanted applications integrated with access management. Additionally, the entire process was time-consuming and expensive. Today's modern approach is to publish a set of standards centrally and allow application owners to onboard their own application using an API-driven, standards-based approach. With the standards- and API-based approach, the application owners can integrate their own applications and set access policies without having to depend on an expert who knows how to configure access management. This modern approach is faster, more cost-effective, and more scalable from a roll-out perspective.	• Does the solution provide a full set of standards-based APIs for onboarding applications into the access management framework? • When an application doesn't support modern standards-based API's, can the solution translate legacy API calls into modern standards based API calls?
Zero Trust Security and Continuous Adaptive Risk and Trust Assessment (CARTA)	The Zero Trust Security and CARTA models are based on the idea that no network, individual, thing, or device can be trusted. IAM platforms should be able to determine whether an entity requesting an action is authorized to do so, and if they have proven they are the entity they claim to be with a sufficient level of assurance based on the risk of the specific action. Within a Zero Trust Security and/or CARTA model, every action taken must be properly authenticated and authorized. To do this, authentication and authorization decisions leverage contextual information and become risk-based rather than binary, taking into consideration a rich set of information. Zero Trust and CARTA helps organizations prevent fraud and malicious activity resulting in improved security and compliance.	• Does the solution provide Zero Trust Security and CARTA models of risk and/or value-based authentication (adaptive authentication), enabling people, devices, things, and applications to have different levels of credentials to authenticate against a common identity store?

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
Next-Generation Authentication and Authorization (AuthX)	Traditional authentication and authorization methods include usernames and passwords, as well as third-party validated data elements, such as Social Security numbers and birthdates. However, in a Zero Trust model, it is assumed that these authenticators may be compromised. Therefore, digital identity providers should offer next-generation AuthX, consisting of continuous assessment for authorization and authentication. This includes transactional authorization and authentication, which requires users to perform actions and provide additional factors, often multiple times, for each high-risk transaction within a session. Authentication trees are an integral part of next-generation AuthX. As a visual, drag-and-drop workflow, authentication trees allow administrators to easily configure, measure, and adjust login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. With an intuitive drag-and drop interface, administrators can also quickly consume out-of-the-box authenticators, utilize existing authenticators, and integrate with other cybersecurity solutions. Next-generation AuthX allows organizations to know who is interacting with them, what they're enabled to do, and helps them trust that the interaction is secure. This results in improved security and compliance.	• Can the solution easily configure, measure, and adjust authentication journeys using factors and digital signals (context, risk, behavior, choice, analytics) to not only determine risk, but also to improve the user experience and inform downstream applications of the accumulated knowledge gained during the authentication journey? • Does the solution pre-identify a user's digital signal, such as location, IP address, device type, operating system, browser type, and more, before a username is even collected? • Does the solution provide out-of-band authenticators (OOBA); the ability to custom build authenticators; and rapid integration with third-party authentication, fraud, and risk providers in a centralized location? • Does the solution allow authorization and authentication workflows to be easily viewed, created, and changed with drag-and-drop functionality through workflows and trees? • Does the solution include transactional authorization for high-risk transactions within a session?
Contextual Access	Most identity solutions only protect at the initial authentication. To ensure the authenticity of users, devices, things, and services at all times, and to mitigate risk whenever an anomaly is detected (even during existing sessions), contextual access should be applied. As part of next-generation AuthX and a Zero Trust security model, contextual access builds context-based intelligence into policies to assess risk and protect resources at the time of access as well as at any point during a digital session. Contextual access applies fine-grained authorization policies, adaptive risk, MFA, and push authorization, yet only requires these stronger authentication mechanisms when necessary. This makes it easier for users while maintaining system security, enabling organizations to provide a more frictionless and secure experience for users, resulting in improved competitive advantage.	• Does the solution leverage contextual authentication and authorization factors at any point during a session to assess risk, invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context?

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
Login Analytics and Decision Logic	The only way to continuously improve user experience is to have data-driven insight. As part of next-generation AuthX, user login analytics offer metrics and timers that analyze user interactions and their devices across all channels and lines of business. IAM platforms should be able to monitor the performance of third-party fraud and analysis services that impact login journeys. Platforms should also allow administrators to optimize the employee login experience with contextual and behavioral analytics that investigate what devices and browsers people use, where people log in from, the length of login journeys across the user population, and more. From this, organizations can discover correlations between existing login methods to improve employee, contractor, and partner experiences. Login analytics and decision logic allow organizations to save resources, time, and money, resulting in reduced costs.	• Does the solution assess average time for call-outs to fraud systems? • Does the solution monitor performance of service level agreements (SLAs) that impact login journeys? • Does the solution determine if shorter login journeys result in fewer help desk calls?
System Integrations	As a vital part of the solution ecosystem, identity platforms store identities and perform data collection and analytics. This solution ecosystem includes IAM, mobile device management (MDM) systems, human relationship management (HRM) systems, and enterprise resource planning (ERP) systems, among others. Unfortunately, this broad ecosystem results in fragmented views of users. Advanced IAM platforms have the ability to integrate and connect with these systems to create a single view of the user across the organization. This aggregated data provides a much more robust data set with which to make important workforce and business decisions. System integrations allow organizations to utilize all of their systems and investments, resulting in increased ROI and reduced costs.	• Does the solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of a user across the organization?
Data Residency	Data residency and data sovereignty are related concepts covering the legalities of where user data resides and the legal authority over the data, regardless of where it resides. Generally, data residency requires that a citizen's personal data be collected, stored, and processed only within their country's borders. To address the General Data Protection Regulation (GDPR) concept of data residency, IAM providers should enable privacy-bound user data storage and fractional replication of personal data. This allows the processing of user data that is context-sensitive to a particular jurisdiction. Additionally, enabling privacy-bound user data storage and fractional replication of personal data, as is mandated by GDPR, allows organizations to meet regulatory requirements and reduce the risk of costly fines and penalties.	• Does the solution support data residency by enabling privacy-bound user data storage and fractional replication of personal data?
Data Aggregation of People, Things, and Their Relationships	To create secure, accurate employee access, IAM providers must allow organizations to aggregate relational data between people and their things to create a comprehensive, single view of the employee. This is achieved by meeting several technical requirements, including establishing a common identity data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to user data in an appropriate format. Importantly, with billions of digital relationships to support and manage, the most future-looking digital identity providers are developing identity graph engines. These relationship-focused engines represent and query complex and interconnected webs of identity relationships that cross organizations, systems, people, services, devices, business agreements, and more. Aggregating identity and access data is especially important in mergers and acquisitions, where identity stores and IAM systems from different organizations have to be integrated rapidly, so users can have seamless access to the resources they need to do their work.	• Does the solution include identity relationship modelling at a granular level based on employees and their relationships to applications, locations, policies, and employee devices? • Does it support identity management among those relationships?

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
Identity at the Edge	Unfortunately, most IoT things are not secure. Identity at the edge secures devices and the data they collect with edge controllers and identity message brokers. Edge controllers secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks. Many IoT things use non-secure protocols, such as MQ Telemetry Transport (MQTT), to identify themselves and send and receive information. Identity message brokers secure such protocols by translating MQTT and other protocols to HTTPS and by making authentication and authorization for the devices and data possible. Identity at the edge helps organizations securely leverage IoT things and devices so they can consistently meet demands to grow business and competitive advantage.	• Does the solution use edge controllers to secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems, as well as to prevent man-in-the-middle and other types of attacks?
Application Programming Interface (API) First Model	The API first model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. For ease of use, scalability, and flexibility, IAM providers should apply this API first development model to create one common representational state transfer (REST) API framework across the entire platform to provide a single, common method to invoke any identity service. The result should be a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT. An API first model allows organizations to speed development time for identity, as well as other enterprise applications and services, resulting in increased productivity and a faster time to market for competitive advantage.	• Does the provider use an API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service?
Legacy Application Support	Most organizations support many systems and applications. Many of these store user data and credentials and are critical for business. Yet they have limited or no built-in capabilities for user registration, authentication, authorization, or federation. Therefore, the ability to connect and extend to legacy systems and applications with a contemporary identity system is an important feature of IAM platforms. This is done through an identity gateway, which allows both legacy and contemporary systems and applications to fluidly and securely communicate with each other. Legacy application support allows organizations to extend their current investments, resulting in increased ROI and reduced costs without having to perform a huge rip and replace project.	• Does the solution have the ability to connect and extend to legacy systems and applications through an identity gateway?
DevOps Friendly Architecture and Microservices	DevOps enables software development and deployment to run in a continuous cycle, allowing organizations to roll out new capabilities faster by reducing time to production. IAM providers should provide a DevOps-friendly architecture with the ability to leverage DevOps tools, such as automating and orchestrating push-button deployment and continuous delivery. They should also use containerized images for rapid automation, with Docker and Kubernetes support. DevOps needs an intelligent architecture that separates configuration from binaries to easily leverage version control for DevOps artifacts. Additionally, IAM providers should provide command-line tools for remote configuration. Microservices is another important development method that focuses on building and deploying applications as groups of modular, composable services within an application. The benefit of microservices is the ability to singularly modify a service without impacting the others. The DevOps approach to deployment using containerization and orchestration technologies such as Docker and Kubernetes allows organizations to accelerate projects 3-6 months and save 25% on implementation.	• Does the solution support modern deployment DevOps approaches with containerization and orchestration technologies, such as Docker and Kubernetes? • Is the solution built within a microservices architecture? • Can the solution secure microservices?

Strategic Component	Strategic Component Description	RFP Questions for Workforce IAM Providers
As a Service	Maintaining and upgrading identity solutions is complex and labor intensive. With a true identity platform as a service, organizations can consume a comprehensive identity platform offering without having to be responsible for things such as hosting, maintenance, upgrades, and more. Further, when the as-a-service offering has feature parity with the software version, organizations gain the flexibility to consume and deploy identity solutions throughout the enterprise as they need without risk and at scale. These benefits and more allow IT resources to focus on other important initiatives, such as innovation and modernization.	• Does the provider offer their entire identity platform as a service? • Do the provider's as-a-service and software offerings share feature parity?
Multi-Cloud and Hybrid-Cloud Support	Multi-cloud environments have become a recent trend due to their increased flexibility, availability, and scalability. These environments allow organizations to eliminate vendor lock-in and speed time to market while reducing complexity and saving both time and money. Hybrid environments include both on-premises and cloud environments. Cloud environments support needs at scale, while on-premises environments are a more secure option for storing sensitive data. The advantage of hybrid environments is the flexibility to support any deployment, anywhere, at any time. Support for multi-cloud and hybrid-cloud environments allows organizations to avoid vendor lock-in and reduce costs.	• Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud, within minutes in a highly available and production-ready configuration?
System Auditing and Analytics	System auditing and analytics capabilities are mission-critical functions. IAM platforms must be able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance. They should also support a wide range of monitoring and logging capabilities. Audit logs should gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Additionally, IAM platforms must provide auditing and analytics for the systems they work with, such as partner systems. System auditing and analytics help secure your enterprise, from client-facing applications all the way to the edge, resulting in improved security and compliance.	• Is the solution able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance? • Can the solution also support a wide range of monitoring and logging capabilities?
Strong Partner Ecosystem	To address the 12 workforce trends and more, the strongest IAM solutions are those that work well with a wide variety of other technologies, software, and industry leaders in order to solve the unique goals of each organization. As such, IAM providers must have a strong ecosystem of respected consultancy, technology, and integration partners. Further, this partner ecosystem should be designed to immediately and easily support today's needs, as well as serve as a source of collaboration and innovation for the future. A strong ecosystem of respected consultancy, technology and integration partners enables organizations to easily add the latest capabilities while saving resources, time, and money.	• Does the provider have a strong ecosystem of respected consultancy, technology, and integrations partners? • Does the provider offer out-of-the-box technology partner integrations included with purchase?

Quickly Support Workforce Requirements with ForgeRock

ForgeRock helps people safely and simply access the connected world by enabling exceptional digital experiences, no-compromise security, and comprehensive functionality at any scale. 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 one of the most visionary access management providers by Gartner, the ForgeRock Identity Platform easily supports today's workforce trends, such as remote working, without sacrificing experience and security.

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

KuppingerCole[1]

ForgeRock radically simplifies identity and access management (IAM) with the industry's only full-suite platform, featuring unmatched intelligence capabilities delivered as a modern cloud service or deployable anywhere with the push of a button. Software deployment options include on-premise, or within any cloud environment, including multi-cloud and hybrid-cloud, for millions of identities in minutes using ForgeRock's full DevOps capabilities.

The ForgeRock Identity Platform is both simple-to-use and comprehensive. It can be implemented across an organization for all identities and use cases — consumer, workforce, and things. The ForgeRock Identity Platform is the only full-suite, artificial intelligence (AI) powered IAM solution that consists of identity management, governance and administration, access management, autonomous identity, privacy and consent controls, directory services, edge security, and an identity gateway.

[1] https://www.forgerock.com/resources/analyst-report/kuppingercole-leadership-compass-identity-api-platforms

Meet Modern Identity Demands Without Ripping and Replacing Legacy IAM

Today, time is of the essence when it comes to implementing modern IAM capabilities. Unlike most providers, with ForgeRock you don't need to suffer the pain, risk, and expense of ripping out existing legacy identity solutions to get the features and benefits of IAM modernization needed to support your workforce initiatives at scale.

ForgeRock provides a flexible approach that enables you to augment first, then coexist, so you can consolidate or retire disparate, legacy identity management systems, like CA Single Sign On (SiteMinder), Oracle, IBM, and even homegrown identity systems.

ForgeRock also includes a pre-integrated ecosystem of node partners within Intelligent Access, allowing organizations to add third-party authentication and authorization capabilities, such as biometrics or contextual signal collection, with just a few clicks. This enables low-risk, rapid deployment of the latest innovative technologies at scale and without the risks associated with adopting new technology and working with start-up companies – all while reducing cost and complexity.

Learn More About ForgeRock for Your Organization

ForgeRock is the leading digital identity provider – designed to support workforce trends today and well into the future. As the most flexible, comprehensive digital identity platform on the market, ForgeRock helps organizations grow business and competitive advantage; increase productivity; improve security, privacy, and compliance; and reduce costs.

For additional RFP questions, ForgeRock's answers, a comparison matrix, and more, request a copy of The Ultimate Workforce IAM RFP Guide.

Contact us to learn how ForgeRock can help your organization.