kuppingercole ANALYSTS

ForgeRock Workforce Identity Governance

Richard Hill

October 10, 2023

EXECUTIVE VIEW

This KuppingerCole Executive View report looks at the ForgeRock Workforce Identity Governance solution, which combines enterprise identity governance with access management to manage the complete identity lifecycle within a single platform.

Content

Figures

Introduction

Integrating security into a company's digital transformation process is often challenging for organizations. If done right, it can ensure that vulnerabilities and risks do not compromise the benefits of the transformation or the company's innovation and technological advancements. Ideally, IT security should be planned early on and maintained throughout the lifecycle of digital transformation initiatives.

Integrating identity and access management (IAM) into the IT security infrastructure is an essential first step. IAM is a framework of policies, processes, technologies, and practices organizations use to manage and secure digital identities and control access to resources. IAM ensures that the right individuals access systems, applications, data, and physical locations appropriately.

Identity Governance and Administration (IGA) is considered a subset of IAM that specifically focuses on managing and governing user identities, access rights, and the associated administrative processes within an organization. It helps organizations reduce security risks, enforce compliance with regulations, streamline administrative processes, and maintain a comprehensive view of user access across the organization's digital resources. IGA is particularly important in complex IT environments with diverse applications, systems, and user roles. Several essential components and practices of IGA include:

- Identity lifecycle management
- Provisioning and deprovisioning of access
- Access request and approval
- Access certification
- Role management
- Segregation of Duties (SoD)
- Audit and compliance

IAM and IGA are interconnected and necessary components for IT security, enabling organizations to navigate the modern digital landscape effectively. However, IGA is sometimes considered later, after IAM implementation, and becomes the last leg of security for the digital transformation journey for organizations.

Regarding IGA solutions, additional capabilities should be considered to improve process efficiencies, alleviate repetitive tasks, and reduce human error. Providing analytics capabilities to IGA can provide insights into access patterns, compliance status, and potential risks. The addition of artificial intelligence (AI), machine learning (ML) can be used to automate complex tasks. Automation within IGA can help with access provisioning when new users join the organization and the deprovisioning process when users leave or change roles. Automating these processes can help minimize the risk of orphaned accounts and unauthorized or overprovisioned access.

Another consideration for organizations is moving IT security services to the cloud and adopting cloud-native approaches to attain cost efficiency, scalability, agility, and innovation capabilities.

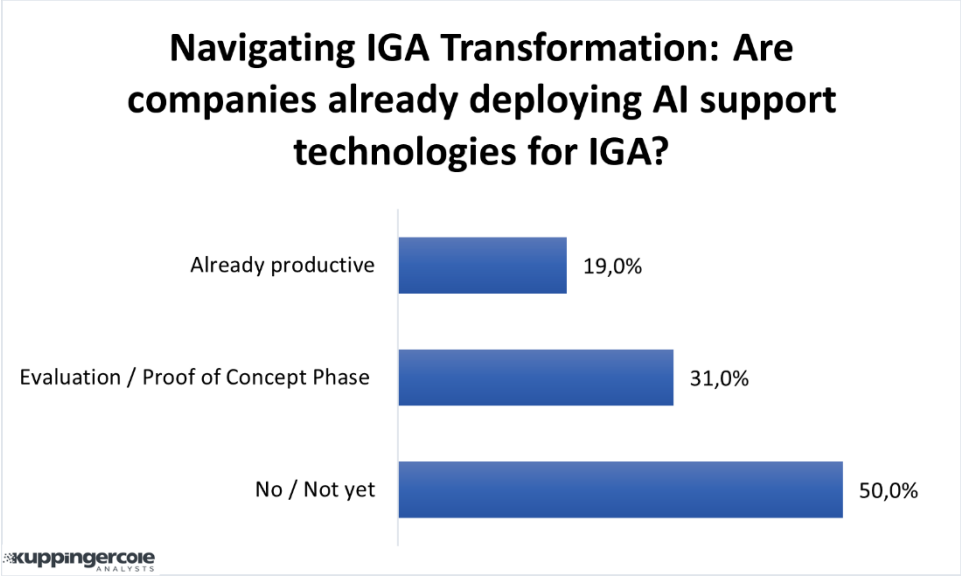

Figure 1: Data from KuppingerCole polling

Product Description

Founded in 2010, ForgeRock is headquartered in San Francisco with offices worldwide. ForgeRock is a well-established, leading-edge vendor in the IAM market, including its Workforce Identity Governance solution.

ForgeRock has been evolving its identity governance capabilities over the last several years. It introduced its IGA offering into the market in 2019 from a self-managed product perspective. ForgeRock's goal was to make it an extension of its existing identity and access management platform, which supports the core workforce, B2B, and customer (CIAM) use cases. ForgeRock's intent is to provide secure access management with the ability to add governance of that access to its overall platform.

Also released in 2019 was ForgeRock’s Autonomous Identity product, which utilizes analytics and AI/ML borne out of a collaboration with the Accenture R&D center. Autonomous Identity automates processes regarding access requests, access certification, and provisioning.

ForgeRock started providing a “lite” version of IGA to some customers early in its identity governance journey, then leveraged its AI and Autonomous Identity capabilities to drive access policy decisions and deliver the full IGA capabilities in line with its customers and market needs. The use of AI allows customers to get to a least-privileged access state quickly, reinforce access certifications and role modeling, and simplify application onboarding. Over the years, ForgeRock has rewritten and effectively built a fully featured IGA solution that is cloud-native, hosted on the Google Cloud Platform (GCP).

The ForgeRock Workforce Identity Governance offering is now part of the ForgeRock Identity Platform. It combines governance, access management, machine learning, and automation, providing security and compliance within one solution built on a cloud-native environment.

ForgeRock Identity Governance focuses on key processes and technologies that manage, control, and monitor user access to various systems, applications, and resources within an organization.

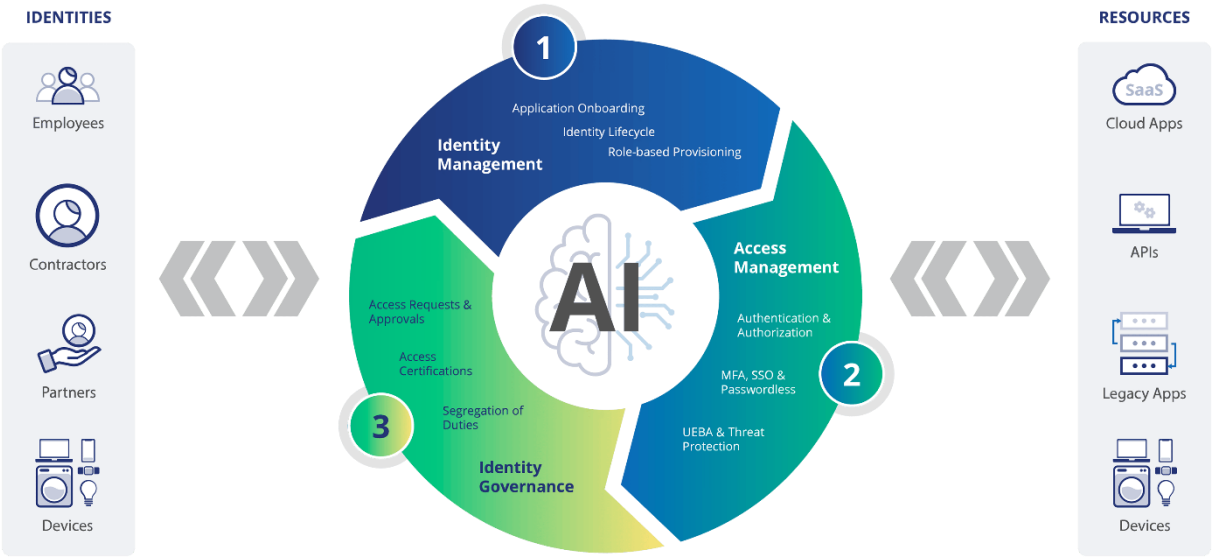

Figure 2 ForgeRock AI Driven Identity, Access Management, and Governance (Source: ForgeRock)

The ForgeRock Identity Platform can integrate with an organization's existing identity infrastructure, whether it's an IAM product from another vendor, Active Directory, an LDAP store, or an SQL database, for example, to provide an aggregated view of the IT user access landscape.

Once the identities of an organization are available to the ForgeRock platform, it can provide the essential components and practices of IGA, such as identity lifecycle management and application onboarding, while allowing mechanisms for users to make access requests, performing access certification campaigns, and enforcing segregation of duties (SoD).

Identity Lifecycle Management

Identity Lifecycle Management is the process of creating, modifying, and deleting user identities and their associated access rights. ForgeRock uses AI/ML to help manage the complete lifecycle of user identities within an organization, from onboarding to offboarding, utilizing automation to manage throughout the joiner, mover, and leaver lifecycle stages.

For on-premises provisioning activities, ForgeRock provides its Remote Connector Server (RCS) as a gateway to the ForgeRock Identity Cloud.

Access Requests

ForgeRock provides users with a 24/7 self-service access request portal. Workflows are provided to walk users through the access request process, and pre-configured workflow templates facilitate the automated application access processing. ForgeRock also provides the ability to automate low-risk access request approvals using its AI/ML capabilities.

Within the end user web portal, pending requests and pending approvals are visible. Users also have the ability to make a request for new items for themselves or others. An Access Catalog is available for applications, entitlements, and roles. Fine-grained attributes can be used to filter within the catalog, as well as enter justification text, and select a high, medium, or low priority to the request. As an approver, a manager is able to see its pending reviews and has the ability to grant or remove applications, entitlements, or roles for their direct reports.

Access Certification

ForgeRock provides an access certification capability for accounts and entitlements. It uses AI in its decision-making to determine access recommendations and confidence scores. In addition, ForgeRock enables automated, periodic low-risk certifications using its AI/ML capabilities. Account and entitlement reviews are easy to navigate within its UI and provide simple approval decision mechanisms.

Segregation of Duties

An IGA system can help prevent conflicts of interest by enforcing the segregation of duties (SoD). This ensures that no single user has access to conflicting functions that could lead to fraud, compliance issues, or security breaches. The ForgeRock platform can enforce SoD policies by proactively scanning user accounts in search of rogue or inappropriate user access. Also, ForgeRock governance analysis helps organizations fully understand user roles and SoD impacts before changes are made to roles and the underlying role model.

Dashboards and Reporting

The ForgeRock Workforce Identity administrative UI provides dashboards that include widgets of graphs and charts of various activities throughout its platform. For example, access certification campaign progress can be shown as the number of active and expiring campaigns, and the number of reviews in individual widgets within the respective screen. A left-hand navigation pane is provided to access the various product capabilities.

ForgeRock's Identity Governance reporting capabilities leverage its data lake of access, identity lifecycle, and governance data, allowing customers to use analytics to build their custom reports. It also provides many IGA reports out-of-the-box, such as accounts not used, passwords not changed, access risk scores, privileged access, roles, new users created in the last 24 hours, users without a manager, user applications, recently disabled users, or users without recent activity, as some examples.

Strengths and Challenges

ForgeRock provides a full workforce solution that combines IAM and governance in a single solution driven by AI. By leveraging AI/ML to automate identity lifecycle management processes, such as role approvals, reviews, and provisioning, ForgeRock can help customers improve process efficiencies, alleviate repetitive tasks, and reduce human error.

ForgeRock Workforce Identity Governance provides many IGA advantages, but a few challenges remain. The ForgeRock's next generation solution offers a SaaS only delivery model, which supports the migration to the cloud, which has become an overwhelming trend in the industry. However, they do offer on-premises only software for limited use cases. The solution's overall UI is simple yet effective, although somewhat basic in its overall look and feel. And although ForgeRock is known for investing heavily in R&D to stay on the cutting edge of IAM, decentralized identities (DI) are not currently supported.

Overall, the ForgeRock Workforce Identity Governance solution is a natural extension for existing customers already using its core IAM platform. It is also a good choice for organizations wishing to integrate an IGA solution with their IT security infrastructure.

Strengths

- Full IGA capabilities
- Good use of AI/ML and analytics
- Automation throughout the product
- Good reporting capabilities
- Cloud-native environment
- Platform integration with other ForgeRock offerings
- Suitable for large enterprises at scale
- Global partner ecosystem

Challenges

- The new governance solution only offers a SaaS delivery option, although an RCS is available for on-premises provisioning activities and older governance product is still offered for customers who want an on-premises version.
- A simple but basic UI look and feel, although effective for accomplishing tasks.
- Decentralized identities (DI) are not supported. However, ForgeRock continues to integrate through partners to enable DID.

Related Research

Executive View: ForgeRock Identity Orchestration
Leadership Compass: Access Management
Leadership Compass: CIAM Platforms
Leadership Compass: Identity Fabrics
Whitepaper: Overcoming Identity Governance Challenges with ForgeRock Autonomous Identity

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.