KuppingerCole Report

WHITEPAPER

by Martin Kuppinger | January 2021

Overcoming Identity Governance Challenges with ForgeRock Autonomous Identity

Most organizations see the value of identity governance and administration (IGA). However, they recognize that it has its challenges in practice, with certain tasks being complex and cumbersome. As a result, existing IGA solutions are faltering. Dynamic businesses require new approaches with a high degree of automation. Artificial intelligence (AI) and machine learning (ML) bear the promise of delivering such automation to complex tasks. ForgeRock Autonomous Identity implements such capabilities for ForgeRock and third-party IGA platforms, ensuring that more organizations can use them effectively and gain maximum benefit from them.

by **Martin Kuppinger**

mk@kuppingercole.com

January 2021

Commissioned by ForgeRock

Content

Table of Figures

Related Research

Executive View: ForgeRock Access Management – 80319

Leadership Compass: Consumer Authentication – 80061

Leadership Compass: Identity API Platforms – 79012

Whitepaper: ForgeRock Identity Platform for PSD2 and API Security – 80049

Leadership Compass: Access Management and Federation – 71147

Leadership Brief: Status and Advantages of Small Data Machine Learning Paradigms – 80364

1 Introduction

IGA is one of the core components of identity and access management (IAM). While IGA is a well-established technology, it remains challenging for both businesses and the users that are involved with IGA tasks. There are various reasons for these IGA business challenges:

- Identity silos are hard to manage. It is difficult to understand where access takes place and hard to deliver consistent experiences for managing access entitlements, such as roles and groups, for requesting access, and for doing access reviews and analytics across the silos.
- Operational inefficiencies are related to the complexity of many tasks for users, such as access recertification, which frequently leads to rubber stamping. Inefficiencies are also caused by the complexity of administration and operation, including creating and maintaining role models or manual fulfillments.
- Many activities are also made more challenging by a lack of context, including why an entitlement has been granted, whether it is used, or how it relates to other entitlements.

This results in a range of challenges for businesses, including over-privileged access and excessive permissions, orphaned accounts that are no longer required or used, and a lack of visibility and accountability. Despite enormous time and effort dedicated to implementing and running IGA, many organizations don't see great results because of these challenges.

Conceptual approaches, such as role mining and engineering, have proven to be insufficient to address these challenges. Many of these can be addressed with automation, more advanced solutions, and approaches that assist users in executing many IGA-related tasks. AI and ML technologies can do many of these things.

Enhanced by AI and ML, IGA solutions are better suited to deal with regulatory compliance and security risks – such as data breaches, privacy violations, or fraud – and to provide more agility and ensure a better customer experience. In light of the COVID-19 pandemic, businesses have had to become more agile, support different work models, implement new types of collaborative solutions, and even change their business models entirely. To support these requirements, IGA must not be an inhibitor for change. Instead, it must deliver the flexibility required by dynamic businesses and changing access requirements.

AI can support many areas of IGA. It can be used to analyze common patterns of entitlements and identify outliers, as well as standard entitlements for certain groups of users. This can help to create roles or other groupings of entitlements. AI can propose entitlements to users that are most likely to be requested, simplifying the search amongst the sheer mass of available entitlements. AI can also make recommendations for access review processes regarding approvals and revocations.

Augmenting traditional IGA with AI and ML, is an obvious measure as long as solutions are well thought out. When they are, they can help overcome many of the challenges users face with their existing IGA solution.

ForgeRock's AI-driven solution, ForgeRock Autonomous Identity, focuses on understanding who or what should have access to what – with sufficient confidence for supporting and automating approvals – provisioning, and reviews.

The specific strengths of ForgeRock Autonomous Identity are its data agnostic approach (the use of a large amount of data beyond data kept by the ForgeRock Identity Platform) and the ability to operate with other third-party IGA solutions. The latter is enabled by a comprehensive set of application programming interfaces (APIs) for integration with other solutions. With these capabilities, ForgeRock Autonomous Identity leverages existing identity investments and overcomes the challenges introduced by multiple identity silos.

We are convinced that we will see a strong uptake of AI-based solutions in IGA and overall IAM, such as ForgeRock Autonomous Identity. However, it is essential to understand that technology will not solve all challenges, and to be aware that we are still at the beginning stages of an evolution in this area.

2 Highlights

- Where and why IGA is faltering today
- Business requirements for more agile, highly automated IGA
- Areas for improving the IGA tool landscape with automation and augmentation and how to leverage existing investments
- Use cases for AI and ML in IGA
- Requirements for efficient implementations of AI and ML in IGA
- How ForgeRock Autonomous Identity solution augments IGA with AI and ML
- Eight steps for successfully implementing AI and ML solutions for IGA

3 The Need to Augment IGA: Better Support for Businesses and Users

There is a need to augment IGA with new technology. Agile businesses can't rely on static entitlements with complex management. Users need to understand what they do and why. They need context and support. The inherent complexities of IGA, including the large lists of entitlements, requires tools and approaches that provide more efficiency and automation for IGA tasks.

IGA encompasses two major areas:

- Identity lifecycle management or provisioning, which support the life cycle processes of users joining, moving, or leaving, by creating and deleting accounts.
- Access governance, access request management, access reviews, and access intelligence include workflows for requesting and approving access, access review processes, and analytics that provide insight into the state of access. They also cover managing the entitlement models, such as roles or groups.

Access request management has been considered a part of identity lifecycle management for a long time. Today it is commonly viewed as an element of access governance. This distinction is not critical for integrated IGA solutions, which most offerings in the market provide.

The challenge for IGA today is that tasks are complex, without context, and highly manual. This does not address today's business requirements.

While IGA is a well-established technology, it is perceived as cumbersome. Most IGA implementations fail in delivering on critical business needs:

- Overprivileged access is the norm, not the exception. This is because it is hard to understand which access to request, and to decide which access is still required during access reviews. The lack of context, growing complexity, and static data is difficult to understand makes users feel overwhelmed
- Excessive permissions violate regulatory compliance requirements. They also pose cyber risk, increasing the chances of data breaches or fraud.
- Orphaned accounts are a common risk, because static data doesn't indicate which accounts are or are not in use.
- The overall lack of visibility and accountability contributes to a risk of failing with regulatory compliance mandates. It also leads to high efforts in auditing and increases audit risks.

Today's IGA solutions commonly struggle with delivering on their main task – , managing user access to the applications and services they need. Granting the required entitlements (and only these) when users need them (and only then) is rarely done well. Users struggle with getting access on time, and frequently suffer from poor user experience. And access is far too often left in place when it isn't required anymore, posing an ongoing security risk.

This makes it difficult to support changing businesses requirements. As the pandemic introduced new remote work models and collaboration tools, corresponding user entitlement changes were required. The shift to the cloud requires managing access to new types of services. Business agility requires an IGA that can rapidly adapt to changes, instead of first requiring lengthy and complex changes to overly complex role models.

Today's IGA is not built to rapidly adapt to changes, such as the shift to the cloud or new remote work models in the COVID-19 pandemic.

To meet these challenges, there is an urgent need to automate tasks and deliver integrated insight and context. However, manual involvement of users will not fully disappear. Augmenting user purview and understanding is also essential for modern IGA. Unfortunately, user involvement frequently brings complexity, such as:

- **Entitlements that are hard to understand:** In many implementations, the names displayed to users do not easily indicate the purpose of entitlements. Users may struggle to understand what to request, and managers may struggle to make the correct decisions during approvals and reviews.

- **Complex and/or inconsistent entitlement models**: Entitlements are commonly too complex. Multi-level role models require very strict rules and stringent implementation to work. Not following these rules leads to inconsistencies, making it even harder to determine which entitlements are needed.

- **Too many entitlements are granted**: Another common challenge results from the sheer number of entitlements. Many users struggle to identify the entitlements they should request for a particular business activity.

- **Time-consuming processes**: Access reviews are commonly perceived as being too time-consuming. Combined with the perception that access review is not the primary task of managers, delays or imperfect access reviews can result.

These challenges are further complicated by the fact that many of these tasks are not part of the daily routine for many teams. Users request new access only occasionally, and managers perform access reviews every few months. This results in an inconsistent experience and execution of these tasks. While there are various approaches for overcoming some of these challenges, automation makes a big difference in executing these tasks accurately. This is where AI comes into play, helping to address the new requirements such as cloud migrations, machine identities, agile application development, and organizational changes.

4 Common Challenges and Pitfalls in Today's IGA Solutions and How to Address Them

Many of the areas in IGA which are perceived as being overly complex are related to well-known and common challenges. Several of them can be successfully improved by applying AL and ML technologies.

IGA is complex. There is a gap between what businesses really require and how IGA is done today. Understanding the common challenges and the best practices on how to address them is the key to maximizing IGA investments.

Business View on Entitlements

Many organizations lack a business view of entitlements and context, resulting in difficult to understand entitlements. This can be caused by overly technical entitlement models and a lack of business involvement in IGA. Entitlements that are visible to the business users must be translated for recipients, so they can describe the entitlement from their perspective. They must provide details on how they relate to other entitlements and why they have been granted.

Entitlement Management and Role Management

Translating entitlements into business-level language straightforward. But it must be done correctly. To accomplish this, organizations must face the challenge of complex entitlements and role models. Many role models fail or deliver poorly to expectations. This is due to a lack of stringent rules, enforcement, and overly complex models.

Access reviews are commonly perceived as being time-consuming, hard to understand, and cumbersome. The right technology can help simplify access reviews.

One solution is the simplification of such models by having fewer levels of roles. Another solution is to identify common groups of entitlements and automatically propose them without the effort of manually maintaining a complex model. Using AI to implement automation helps organizations adapt to changes more rapidly, including incorporating new applications.

AI can also augment the process of reviewing and automatically granting entitlements requested by users. Searching for the "needle in the haystack" is a task well suited for AI.

Complexity of Access Reviews

Another critical issue is the perception of access reviews as being time-consuming, hard to understand, and cumbersome. There are ways to simplify access reviews, including moving away from regular recertification campaigns with complex matrices of users and their entitlements, to recertification focusing on critical entitlements or on recent changes, or building on other criteria. This leaves only a few entitlements to be manually reviewed. However, most of these approaches don't solve the core complexity problem. AI can help organizations focus on what is most critical and relevant instead of treating every entitlement the same by providing context and automation.

Lack of Automation

Many IGA solutions also lack automation and require many manual tasks. Teams must manually select access entitlements (which, alternatively, might be assigned via policies or proposed by the system) or de-provision entitlements and accounts that are never used. For example, AI and ML can automate these tasks, by identifying entitlements and accounts that are never used.

Lack of Flexibility and Scalability

Dealing with an increasing number of identities and new use cases requires agile solutions with a high degree of automation. Machine identities and the identities of things in IoT, agile development and DevOps environments, dealing with partner and customer identities, and the overall increase in business agility in digital transformation will not work when still building on complex, manual approaches in IGA.

There are three essential areas to address:

- **Automation**: This includes providing the context for decision making across all environments and identities, identifying excessive entitlements, delivering confidence scores, and automatically identifying entitlements that must be reviewed for "micro certifications."
- **Intelligence**: Delivering insights into every part of IGA, such as the most likely entitlements for access requests, context and risks for approvals and reviews, and the logical combinations of entitlements for role and entitlement engineering.
- **Collection and normalization of all identity data:** This needs to be done across all identity resources. The analysis of that data provides context, risk and confidence scores, and other information. Identity and access related data is held in a range of resources beyond IGA. This includes the Microsoft Active Directory and Azure Ad, Databases, Privileged Access Management solutions, HR systems, Cloud services, ERP solutions, and many more.

These common challenges require new and better solutions. AI and ML provide the potential to elevate IGA to a new level, without losing existing investments.

5 Improving IGA with AI: What to Consider and How to do It Right

AI and ML can deliver significant value to IGA. It is essential to understand where AI can help and how this fits into an existing IAM landscape.

Recently, a growing number of vendors started to deliver new solutions that complement traditional IGA tools by making use of advanced technologies like AI and ML. To help determine when a technology is truly AI, think about this rule of thumb: if it augments decision-making, it can be categorized as AI.

In addition to chatbots and user behavior analytic (UBA) to analyze anomalies in user behavior, an increasing number of IGA use cases can benefit from AI. This is not surprising, given the fact that users struggle with executing IGA tasks. The automation enabled by AI delivers significant advantages.

IGA use cases have moved to the center of attention and innovation for AI and ML in IAM. These technologies deliver significant benefits to organizations using IGA solutions.

AI can support many areas of IGA by analyzing common patterns of entitlements and identifying outliers as well as standard entitlements for certain groups of users. This helps to create roles or other groupings of entitlements. AI can propose entitlements to users that are most likely to be requested, simplifying the search among the mass of available entitlements. AI can also make recommendations for access review approval and revocation processes.

However, to make AI and ML successful in IGA, some key requirements should be kept in mind:

- **AI requires focus**: AI must not lead to information overload. It must deliver focused recommendations to reduce complexity. For example, an AI-driven solution should deliver

recommendations about the most likely entitlements to request or indicate the most critical entitlements.

- **AI requires accuracy**: AI must deliver valid recommendations. Proposed entitlements must be the right ones for that particular user instead of a copy or superset of peer entitlements . Either of these could lead to potentially excessive entitlements.
- **AI requires data**: Related to these requirements is the need for data, as ML builds on and learns from large data sets. If there are only a few thousand users for a small number of systems, the volume of data will be low, making it challenging for AI to deliver the correct results for decision making. Manual training is a possible workaround, but for the best results, more data is better. This includes data from all target systems as well as the IGA repository, and usage data as well as static entitlements.
- **AI must be predictable and reproducible**: One of the challenges with many AI solutions is that they don't explain the rationale behind their results or proposed recommendations. AI must explain the key indicators as to why it is proposing these recommendations. This helps to explain to the administrator or business line manager why the recommendation is being proposed. AI must be predictable and deliver the same results on the same set of data. It must also be reproducible so users can understand where decisions or recommendations come from.

Successful AI solutions must deliver predictable and reproducible results.

Augmenting traditional IGA with AI and ML, is a given. Solutions need to be well considered to help overcome the challenges users face when working with an IGA solution.

AI solutions for IGA should:

- Work with existing IGA and IAM solutions, as well as their respective data sources to deliver a comprehensive view of users as well as other identities and their access
- Work with current data sets to analyze huge volumes of data quickly and deliver recommendations, predictions, and risk/confidence scores based on that data
- Provide scalable, context-based risk insights for security and risk professionals,
- Provide bias-free insights derived from artifacts, such as roles, while building on raw data and organizational data to develop analysis and derive recommendations
- Allow users to fully comprehend how risk and confidence scores are built, visualize and deliver detailed drill-down capabilities
- Act upon information. For example, push remediation recommendations, access predictions, or role proposals.

This actionable intelligence approach enables security and risk professionals to take immediate action and to accelerate decision making while improving operational efficiencies across the entire organization.

6 ForgeRock's Modern Approach - AI-Driven Identity Analytics

ForgeRock Autonomous Identity is an innovative solution utilizing AI and ML to provide predictions and recommendations that help security and risk professionals and other users with IGA tasks, including identifying appropriate access entitlements or performing access reviews.

ForgeRock is an established, leading-edge vendor in IAM, delivering a strong IGA solution. ForgeRock IGA covers all major areas of IGA, including

- Identity Lifecycle Management
- Policies, Role and Entitlement Management
- Access Requests and Approvals
- Workflow Capabilities
- Access Reviews
- Auditing and Reporting
- Identity and Access Analytics

ForgeRock Autonomous Identity is an AI-driven identity analytics solution that allows organizations to accelerate secure access, achieve regulatory compliance, mitigate risks, and reduce costs. The solution enables organizations to understand who or what should have access to what, with sufficient confidence to support and automate approvals, provisioning, and reviews. ForgeRock Autonomous Identity leverages ML to collect and analyze all identity data. In contrast to some other solutions, ForgeRock Autonomous Identity consumes data from a variety of sources, including ForgeRock's own Identity Platform and third-party IGA solutions.

That data is collected, analyzed, and modeled across all connected systems. Based on that model, confidence scores for user access levels are calculated so that predictions and recommendations can be made, and tasks automated, given sufficient confidence.
With these capabilities, ForgeRock Autonomous Identity provides real-time, continuous, enterprise-wide insight into user access entitlements and allows for control and remediation. It works using AI and ML techniques for collecting and analyzing all identity data from "raw" entitlements derived from a wide range of systems to accounts, roles, assignments, and other information, to identify access-related security risks and blind spots.

By overlaying with third-party IGA and IAM solutions, ForgeRock Autonomous Identity increases the business value of existing identity investments.

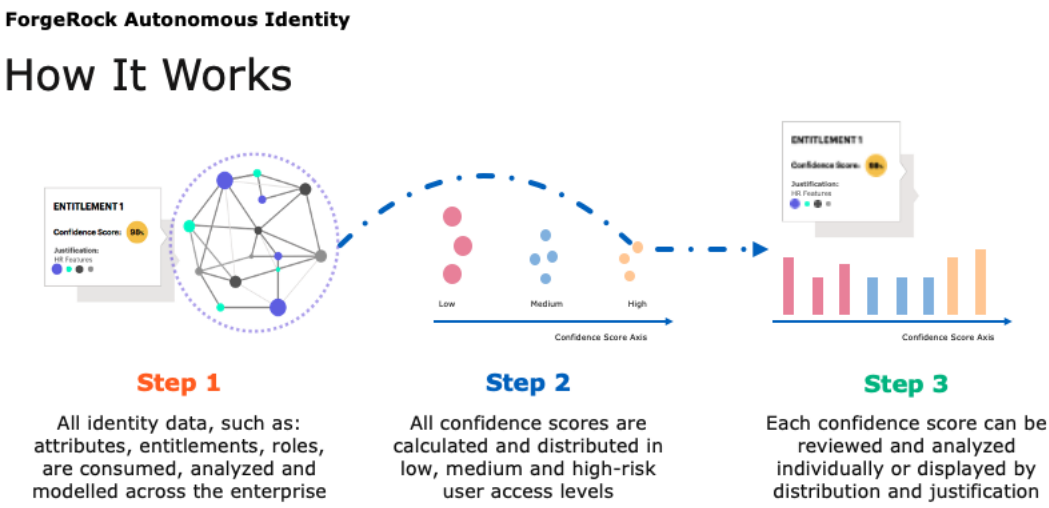

Figure 1: How ForgeRock Autonomous Identity works [Source: ForgeRock]

In the first step, ForgeRock Autonomous Identity ingests user data from multiple sources, such as IAM systems, HR applications, directory services, and other applications. This data is aggregated across sources. ForgeRock Autonomous Identity builds a history of such data for understanding how and why access changes over time.

The AI/ML algorithms are then applied to the aggregated identity data in order to predict and propose entitlements for users, and to explain these predictions in three ways:

- **Confidence score:** This score delivers information on the degree of confidence in whether a user or other identity should have access or not.
- **Justification**: This delivers insight into how the prediction reached that outcome.
- **Recommendations**: These are the concrete entitlements ForgeRock Autonomous Identity suggests.

Based on these capabilities and a modern, intuitive user interface (UI), risk and security professionals can review predictions and take actions, such as certifying access entitlements. Most importantly, ForgeRock Autonomous Identity supports explanations for predictions and recommendations. This transparency is essential for modern AI solutions.

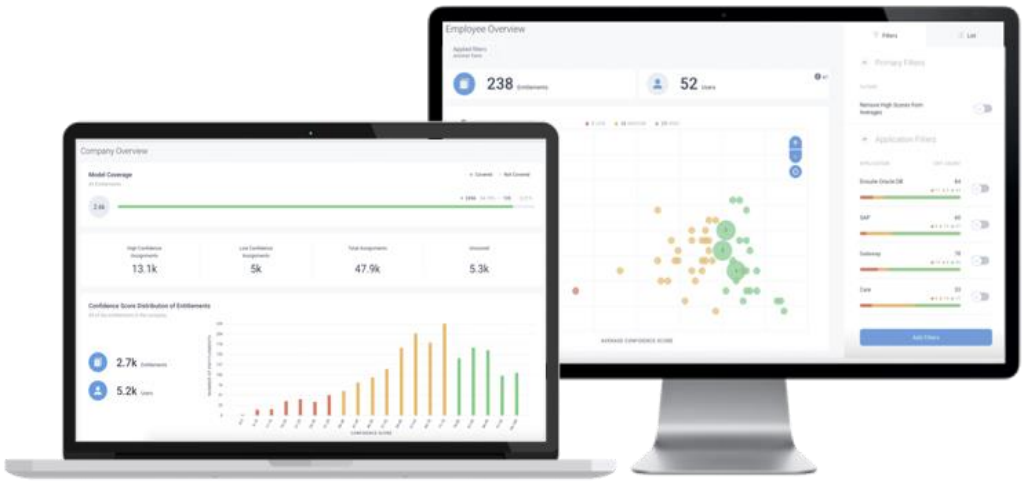

Figure 2: ForgeRock Autonomous Identity integrates with the Common UI [Source: ForgeRock]

ForgeRock Autonomous Identity features a modern UI that integrates with the standard ForgeRock Identity Platform UI, seamlessly augmenting the user experience.

ForgeRock Autonomous Identity features a modern UI that integrates into the standard ForgeRock Identity Platform UI, seamlessly augmenting the user experience.

ForgeRock Autonomous Identity AI-driven actions include:

- Push remediation recommendations
- Push access predictions
- Push access provisioning
- Push access deprovisioning
- Push role definitions

Specific strengths of ForgeRock Autonomous Identity are its data-agnostic approach – the use of a large amount of data, beyond data kept by the ForgeRock Identity Platform and the ability to operate with other third-party IGA solutions. The latter is enabled by a comprehensive set of APIs for integration into other solutions. With these strengths, ForgeRock Autonomous Identity differs from other identity analytics solutions in several ways, including:

- **Global visibility**: Building on a vast volume of identity-related data across the organization.
- **Data agnostic**: Includes data outside ForgeRock Autonomous Identity and agnostic to data structure. Data models do not need to be built before using ForgeRock Autonomous Identity. It can integrate quickly with data sources and consume data, regardless of data structure.
- **Transparent AI**: Recommendations and predictions are explained.

- **No data bias**: Because decisions and recommendations are based on raw data – and just not on artifacts, such as static roles and rules created by humans – results are free of data bias

ForgeRock Autonomous Identity is not just an add-on to existing IGA solutions. It can be used as an overlay for the entire IAM landscape, independent of components and vendors already in place.

7 Action Plan for Leveraging AI-Based Solutions in IGA

Before making a jump-start with AI- and ML-based solutions for IGA, it is essential to understand current challenges and their respective root causes. A mix of technology and conceptual work that leverages IGA implementations will most commonly take AI-based solutions to the next level.

Many vendors use terms like AI and ML in marketing materials, but their solutions are not always underpinned by real AI and ML capabilities. There is understandably some reluctance on the part of organizations to adopt such technology despite awareness of the significant potential to augment existing solutions with such technologies. In areas of IGA that are complex and used seldomly, such augmentation is essential and can help in overcoming the challenges faced in IGA today.

Solutions should build on all identity data available. They should leverage existing IAM and IGA investments, and not replace them. They must provide confidence and explanations. And they must simplify work with recommendations and opportunities to drill down into the details.

To successfully implement such solutions, we recommend you consider the following steps:

1. **Understand your IAM**: This is the first step is toward understanding where you are with your current IAM solution. It also includes understanding which data might be consumed by a solution such as ForgeRock Autonomous Identity.
2. **Understand IAM challenges**: To understand the potential benefit of implementing such a solution, the challenges and deficits in the current IGA solution must be well understood.
3. **Understand the root cause and fix it**: While technology might help address challenges, not everything is a technical challenge. Some challenges stem from organizational or conceptual difficulties, including overly complex entitlement models or a lack of proper process definitions and documentations. Don't put all your eggs in the AI basket, but also solve the conceptual issues.
4. **Understand the capabilities of an AI solution**: It's important to understand and not overestimate the capabilities of an AI solution. Promises that can't be kept will not help in delivering a successful project. AI that explains outcomes and provides confidence is essential for success.
5. **Map capabilities to root cause and understand how they will help**: Part of that exercise is mapping the capabilities to the root cause for current challenges, to understand how AI for IGA can best help and to ensure that such a solution doesn't build on potentially biased data such as static roles and rules only but provides comprehensive analysis across all relevant data points.

6. **Implement AI**: Once it is understood that an AI-based solution for IGA will deliver a benefit, implement it. Focus on well-integrated UIs and on reducing complexity. Well-integrated and concrete recommendations for standard tasks such as access requests, approvals, and reviews will deliver the bigger benefit.
7. **Educate users**: Ensure that your users understand what is changing, what predictions and recommendations will be delivered, what functionalities the solution will deliver, and how to work with that information. Help them understand both the value and the limitations of the AI solution.

We are sure we'll see a strong uptake in AI-based IGA and IAM solutions such as ForgeRock Autonomous Identity. ForgeRock enables organizations to accelerate secure access, achieve regulatory compliance, mitigate risks, and reduce costs. However, it is essential to understand that technology will not solve all business challenges, and that we are at the beginning of a new evolution in the identity governance market.

8 Copyright

KuppingerCole supports 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 back 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 and 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**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Deutschland

Telefon +49 (211) 23 70 77 - 0
Fax+49 (211) 23 70 77 - 11
www.kuppingercole.com