kuppingercole ANALYSTS

81333 Executive View ForgeRock Identity Orchestration

Deshpande, Nitish

March 01, 2023

Identity and access management (IAM) systems represent the front door to every digital organization. They can provide a welcoming experience, or they can make it difficult to get in. They can provide security, ensuring that those entering can see what they're authorized to see and nothing else. If they know you, they can wave you in. If they don't, they can ask for proof of identity. In the digital world, all of these experiences, and many more, are made possible by identity orchestration.

Orchestration is a critical function for digital businesses because it makes it possible to create differentiated, personalized experiences for customers, provide the workforce with fast access to the right resources, and protect data and assets by blocking suspicious access attempts. This paper analyzes the ForgeRock Identity Platform's built-in orchestration capabilities, which include a visual designer and drag-and-drop nodes for mapping out journeys based on the context of the access request.

Content

Figures

Introduction

Identity and access management (IAM) is a core component of the enterprise IT infrastructure and central to protecting digital corporate assets. By enabling enterprises to manage and govern identities and the assets they are authorized to access, IAM can ensure that the right entities — including people, applications/workloads, and devices — can access the right resources at the right time, while preventing unauthorized access, a leading cause of data breaches.

IAM plays a key role in the enterprise security ecosystem and can help organizations move towards "least-privileged" access, a core principle of the Zero Trust security framework. A well-constructed identity orchestration tool in IAM can help organizations gain end-to-end visibility of all identities and entitlements. It can consolidate identity silos to remove gaps between controls for the cloud and those for legacy on-prem systems. And it can govern access controls for all, automate routine workflow tasks, and dramatically reduce risk.

Most organizations operate in a hybrid environment with a combination of legacy systems and apps that coexist with cloud services. Enabling easy, consistent access to applications is business-critical no matter where those applications are hosted. A unified IAM platform can make your workforce more efficient and productive, with single sign-on (SSO) and other tools that work across on-prem and multi-cloud environments. For your customers, it can create frictionless, targeted experiences that lead to greater satisfaction and loyalty.

Organizations are under intense pressure to differentiate themselves by delivering new digital initiatives and innovative services without disruption. At the same time, they have to protect their digital assets, systems, and data, while maintaining regulatory compliance, all in an increasingly complex IT environment amid a sophisticated threat landscape.

An integrated IAM platform can help organizations modernize IT and achieve their goals for workforce productivity, customer satisfaction, stronger security, greater agility, and faster innovation.

The Essence of IAM: Identity Orchestration

Identity orchestration is at the heart of delivering frictionless user experiences. It facilitates the creation of digital identity journeys that deliver security and the right level of friction for end users, whether they are employees or customers. Homegrown IAM solutions used by many enterprises are doing a suboptimal job of addressing modern threats or the rising user expectations for excellent digital experiences.

Orchestration for the workforce

Orchestration plays a vital role in business enablement when it comes to the needs of employees, contractors, business partners, and customers to access specific applications, systems, and data.

While access in the workplace was once far simpler, and could be handled through onboarding, today's environment is far too complex, with far too many identities, to be handled manually. People are constantly moving, changing roles, and leaving companies, which leads to the risk of over-provisioned access. Identity orchestration can help ensure that user journeys are fulfilled or denied as appropriate, permissions are granted or revoked, and that accounts are deleted or deactivated once they are no longer required.

Orchestration for customers

In today's hyper-competitive business environment, delivering differentiated customer experiences has become a strategic priority for corporations. The digital experience served can mean the difference between customer acquisition and conversion or a lost opportunity and shopping cart abandonment. Organizations are looking to drive better and faster engagement that keeps customers on the site longer and brings them back again and again.

But just as the need for hyper-personalization intensifies, so does the need for customer data security and privacy. Businesses are losing millions of dollars annually to online fraud, such as account takeover, through malicious actors.

In this executive view, we discuss ForgeRock's next-generation identity orchestration features that deliver superior digital identity experiences, block fraudulent activities, and reduce complexity.

Product Description

ForgeRock was founded in 2010 with its headquarters in San Francisco, U.S., and has many offices around the world. The ForgeRock Identity Platform unifies the various IAM solutions provided by ForgeRock, including Access Management, Identity Management, IoT/Edge Security, Identity Gateway, Identity Governance, Privacy & Consent Management, and other components, including Directory Services.

ForgeRock's strong and expanding partner ecosystem, the ForgeRock Trust Network, is a technology alliance program and partner channel that consists of approximately 150 partner companies. These partners build, test, and integrate various capabilities, including strong authentication, biometric ID, risk and fraud mitigation, and identity proofing into the ForgeRock Identity Platform.

The ForgeRock platform serves B2B, B2E, B2C, and B2B2C markets, and primarily targets customer identity and access management (CIAM) and workforce use cases for large enterprise customers.

ForgeRock Intelligent Access

ForgeRock Intelligent Access is the company's next-generation identity orchestration solution, colloquially known as "Trees." Intelligent Access can enable organizations to deliver great user experiences to their customers and workforce with minimal effort.

Intelligent Access allows organizations to finely orchestrate every aspect of the user journey, from registration to login to authentication and ongoing authorization, and it features self-service capabilities for password management, privacy settings, and more. Newly introduced capabilities make it easier to define, build, test, deploy, and measure user identity journeys.

Intelligent Access is natively built into the ForgeRock Identity Platform, so there are no connectors or integrations needed to orchestrate across the entire identity lifecycle.

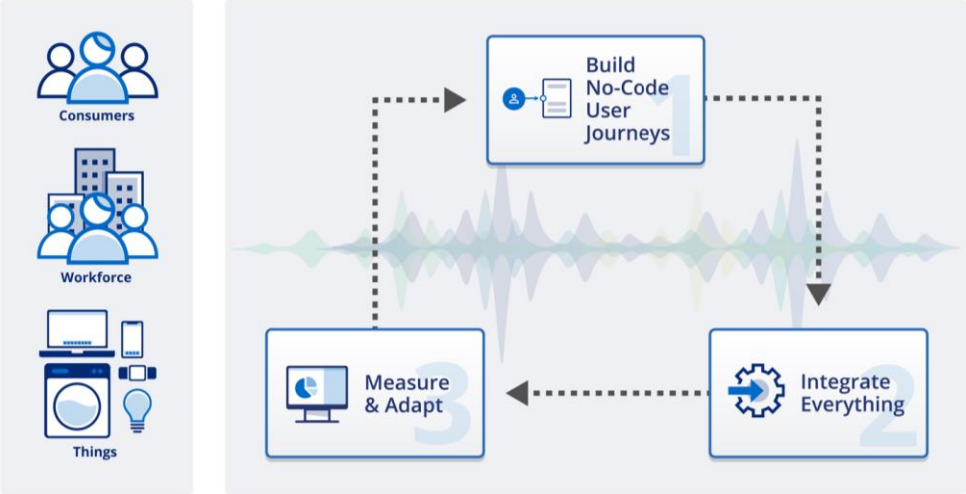

Figure 1: ForgeRock Identity Orchestration: Creating User Journeys

ForgeRock Intelligent Access supports a library of hundreds of pre-built out-of-the-box (OOTB) nodes that span a wide variety of use cases, from strong authentication, risk and fraud management, behavioral biometrics, and identity proofing and enrichment to self-service, social registration, and more. OOTB nodes make it easier to build and manage user journeys for complex use cases using a simple drag-and-drop method that can save developer time and resources. Extensibility is made easy with inline scripting. Once a journey has been built, the solution has additional OOTB nodes for debugging, impact assessment with A/B testing, fine-tuning, and removing friction.

No-code orchestration accelerates journey development and time to market. Because it is native to the platform, orchestration enables dynamic and contextual journeys based on real-time intelligence gathered about the user. In addition to ForgeRock nodes, customers can choose from more than 150 pre-built partner integrations through the ForgeRock Trust Network at no additional cost. All of these pre-built capabilities add up to faster OOTB use case solutions with the potential to reduce development and maintenance costs. Additionally, ForgeRock offers out-of-the-box SDKs that integrate into applications. Developers can dynamically change user access behavior with drag-and-drop journeys without having to recode or redeploy apps.

ForgeRock offers an AI-powered threat protection solution that is integrated into the drag-and-drop orchestration engine. ForgeRock Autonomous Access applies artificial intelligence, machine learning, and advanced pattern recognition in real time during authentication to minimize friction and improve the overall experience for trusted users, while blocking malicious attempts and adding authentication steps when it detects anomalous behavior.

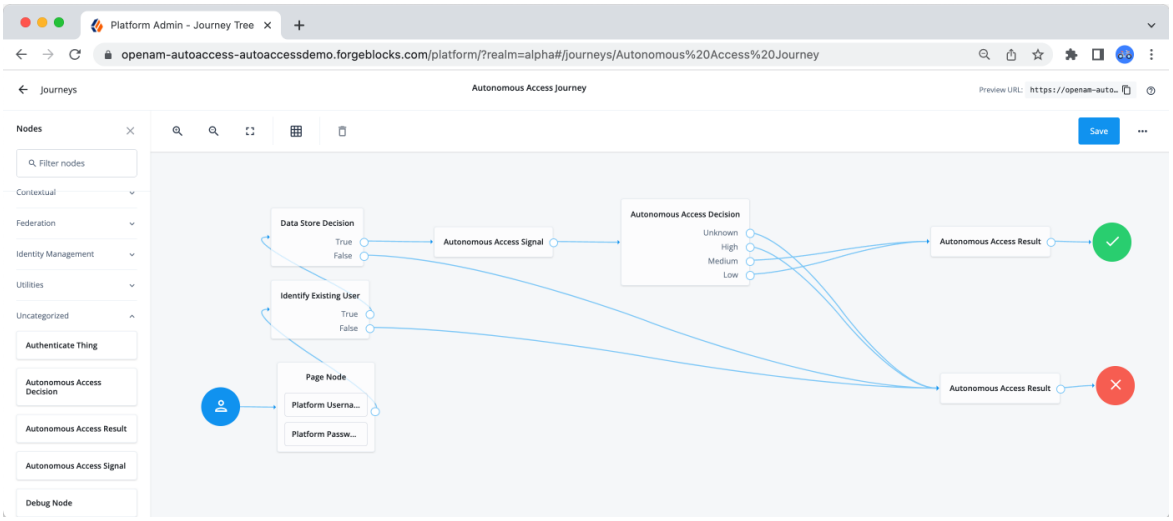

Figure 2: Autonomous Access integrated with Intelligent Access for continuous authentication

ForgeRock's built-in support for passwordless authentication and passkeys is a key component of its orchestration solution. It provides the ability to create a personalized journey based on customer choice and allows admins to register FIDO2 authenticators to a user's account as part of the authentication journey. Three WebAuthn nodes are included in the platform: one for creating credentials, one for using those credentials, and one for adding information about the FIDO2 device to a user's profile for later authentication. WebAuthn nodes support Windows Hello, Touch ID, and any FIDO or U2F security keys such as YubiKeys, Feitian, and Titan, among others.

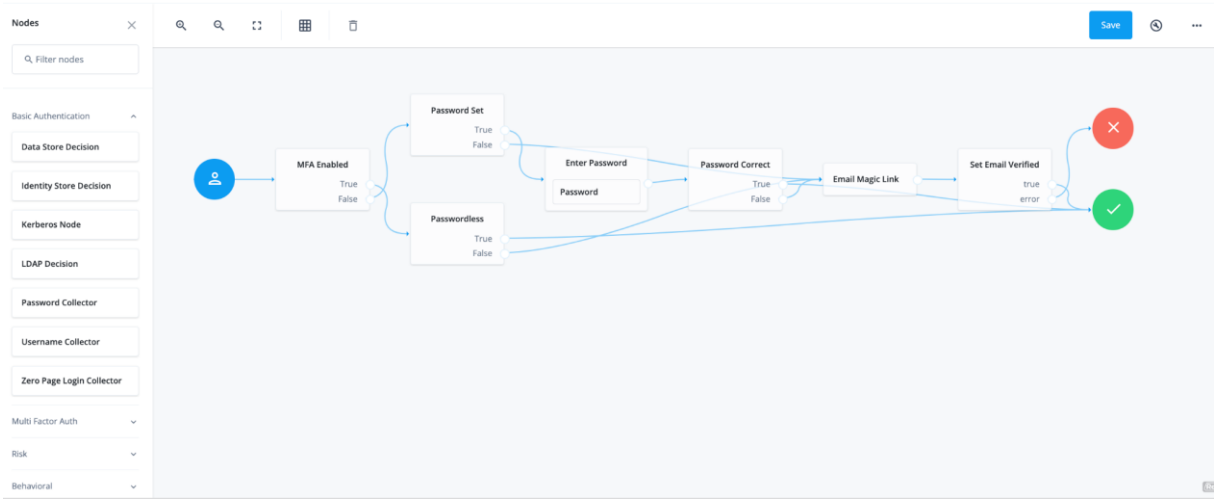

Figure 3: ForgeRock Passwordless Journey

ForgeRock Intelligent Access helps organizations provide hyper-personalized experiences based on user preferences, real-time context, and many other variables. Custom UI theming and localization features are available OOTB and allow organizations to personalize the experience based on the user's region, location, organization and other contextual information. Everything from a user's language, email templates, to terms and conditions can

be localized and personalized. This localization capability can help improve customer satisfaction, reduce drop-off and churn rates, and potentially amplify the brand experience in a particular region.

ForgeRock's progressive profile capability in identity orchestration simplifies registration and removes the potential for "form fatigue" by collecting a minimum of information at registration and requesting a little more information in subsequent logins. This incremental approach allows customers to build their user profile over time. The orchestration engine also allows you to nest one journey within another, to increase reuse of common journeys and reduce administrative time. The user has full control to manage their account profile, preferences, credentials, and more, without the need to open a support ticket, as the self-serve account management can be easily enabled within the user journey.

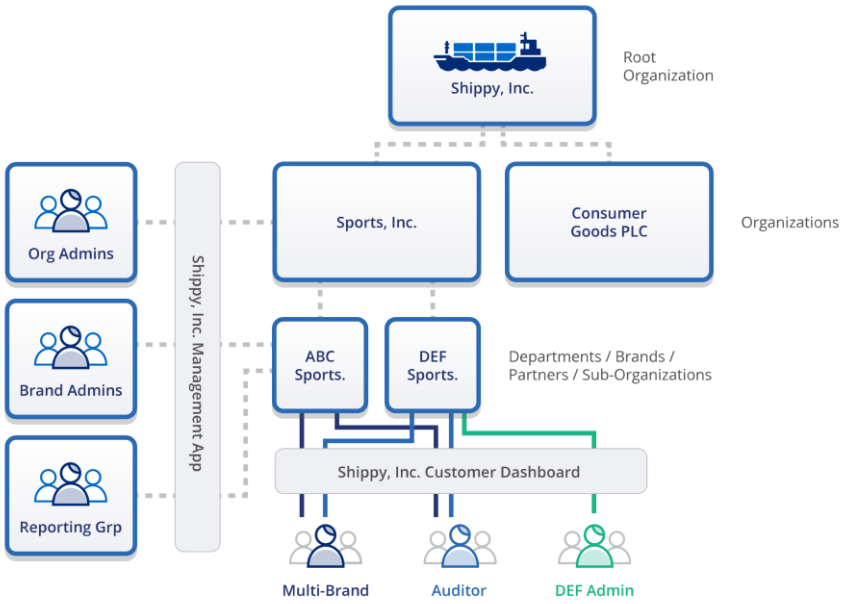

Figure 4: ForgeRock Multi-Brand Framework

Intelligent Access has a unique Organizations capability that allows for simplified identity management in complex, hierarchical environments. An organization can define a hierarchy of organizations and sub-organizations that can be flexibly grouped by area, such as brands, supplier groups, vendors, and other identities. This feature dynamically matches a user's brand and channel preferences within a single journey, thereby delivering customer experiences tailored to individual brand preferences.

Intelligent Access provides a comprehensive user journey analytics tool. The tool uses a centralized dashboard for viewing counts of existing users and applications, along with the ability to get granular data on user journeys and compare success and failure rates of journeys. The insights from these analytics could be used by business decision-makers to understand user journeys and implement changes as needed to improve business outcomes.

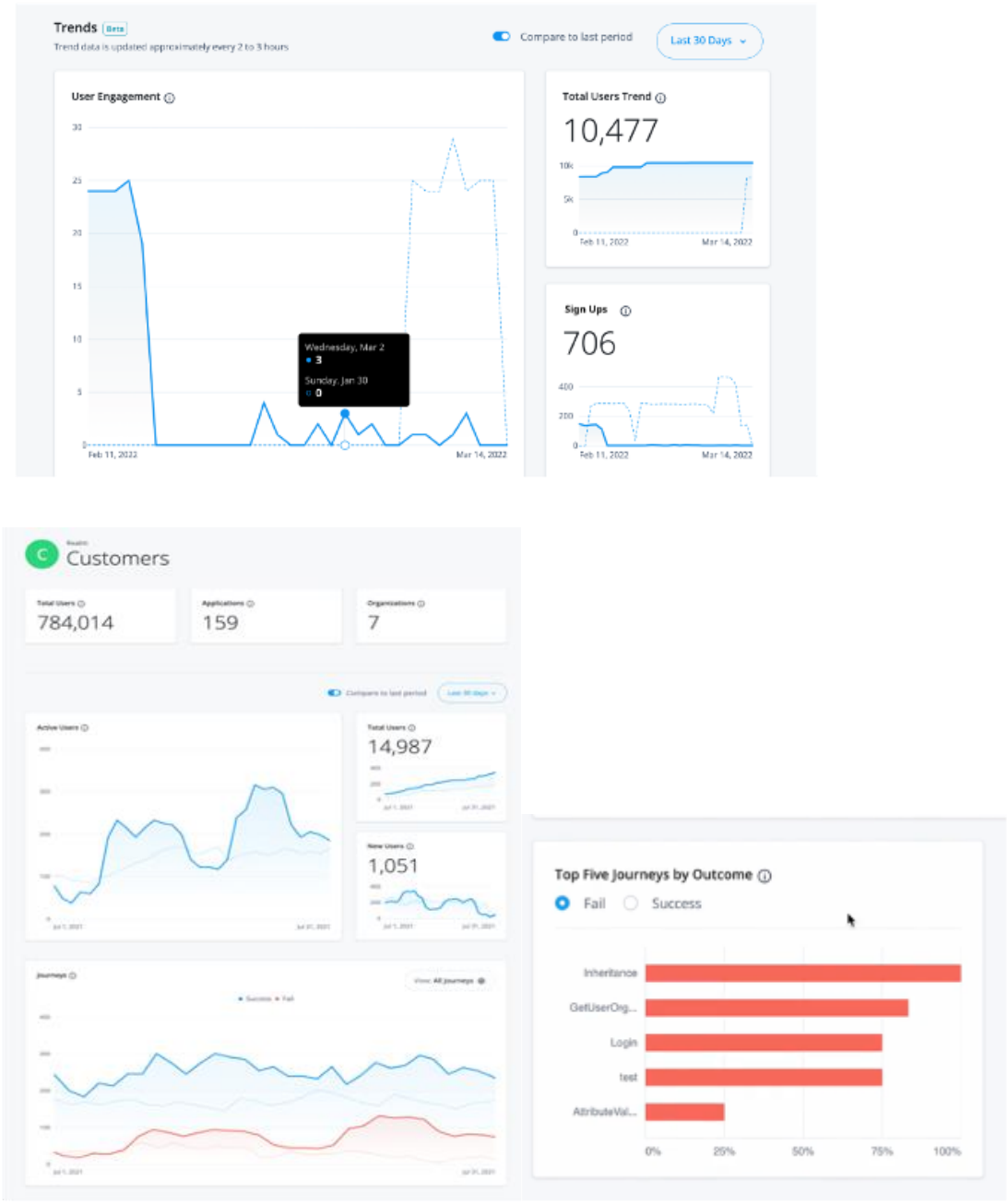

Figure 5, 6 and 7:Journey Analytics dashboard to view market trends and conduct deeper journey analysis

ForgeRock supports an as-a-service consumption model for organizations that want a cloud IAM service. On-premises deployment of the solution is also available for use cases that require some or all of the solution to be run on-premises or in a public cloud. Integrations for migrating to the cloud without disruption are also available in the form of just-in-time migration and pass-through authentication to legacy systems. Intelligent Access is integrated in ForgeRock's unified identity platform, so every customer has access to the company's identity orchestration services no matter their deployment choice.

Strengths and Challenges

ForgeRock Intelligent Access is a comprehensive identity orchestration solution offering a breadth of use case support, with new-generation capabilities such as AI-driven threat protection and an industry-first journey analytics dashboard.

The no-code drag-and-drop approach allows quick and secure management and personalization of user journeys. Intelligent Access is highly performant and resilient as it is well integrated into the ForgeRock Identity Platform. It does not require any connectors or integrations for communicating between different services in the platform.

However, the product also faces a few challenges for being integrated into the unified identity platform. Being a part of the ForgeRock Identity Platform components, it has some Java runtime dependencies. Intelligent Access is missing capabilities around concurrent versioning systems (CVS); therefore, it lacks the ability to rewind and rework on earlier versions of journeys today. However, this capability is on the company's current product roadmap and expected to be available later this year. A stage-based approach for managing rollout of capabilities including approval of changes is also missing.

ForgeRock supports cloud-based SaaS deployment as well as self-managed software, showing strong flexibility in orchestrating identity journeys from any environment. ForgeRock has an extensive global partner ecosystem, and Intelligent Access has the benefit of being a part of a unified identity platform that allows all components to be deployed on-premises or as a cloud-delivered service. The on-premises deployment of the ForgeRock Identity Platform requires more expertise and attention than other solutions in this market, but the SaaS version is easier to implement.

Strengths

- Very strong number of OOTB nodes (native and third-party) as well as a large number of pre-built user journeys
- No-code drag-and-drop approach for managing user journeys
- Passwordless innovation with built-in support for passkeys and pre-coded workflows
- UI can be customized based on regional requirements
- Artificial intelligence and machine learning (AI/ML)-driven threat protection including evaluating risk signals
- Very strong analytics dashboard providing in-depth details about user journeys
- Global partner ecosystem

Challenges

- ForgeRock Identity Platform components have Java runtime dependencies, although the SaaS delivery option is fully turnkey
- Ability to rework back to earlier versions for journeys is missing today
- Stage-based approach for managing rollout of new journeys is missing

Related Research

Leadership Compass: Identity Fabrics
Leadership Compass: Access Management
Leadership Compass: CIAM Platforms
Leadership Compass: CIEM & Dynamic Resource Entitlement & Access Management (DREAM) platforms

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.