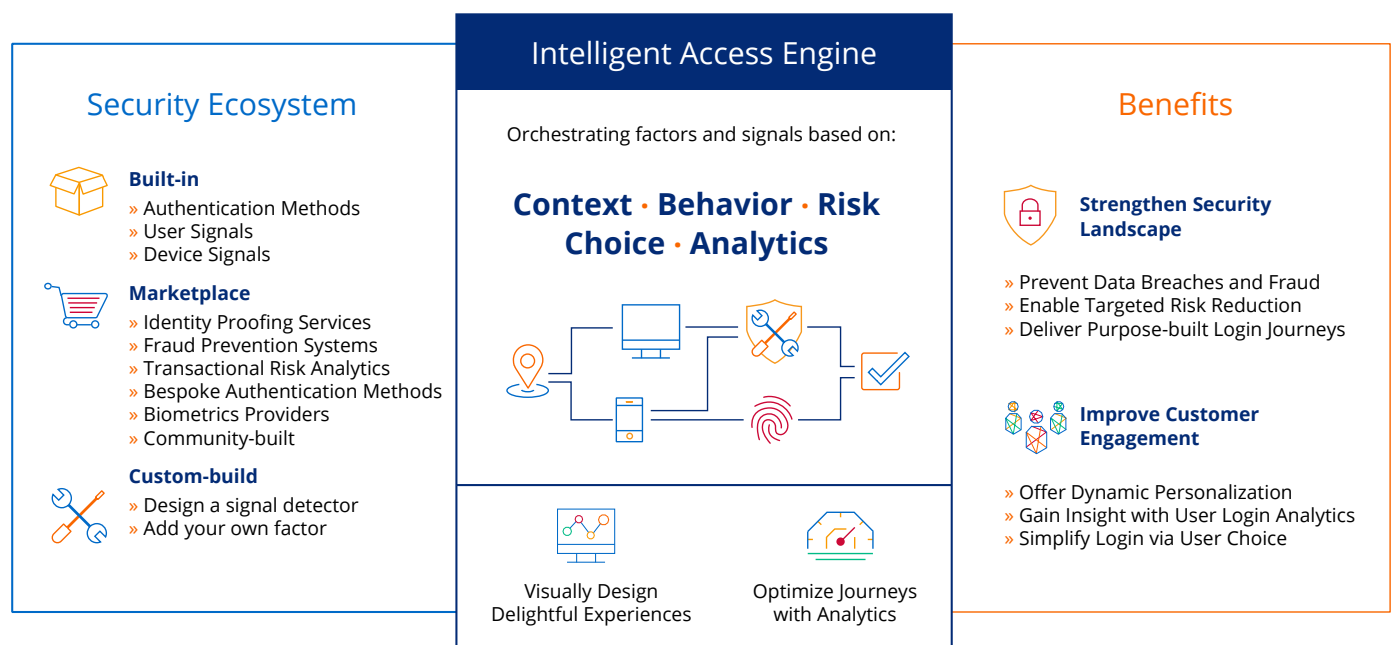**ForgeRock**®

Intelligent Access

A Tough Balancing Act: Customer Experience vs Security

The pressure is on. Customers want easy access to services that cater to personal preferences, while organizations need to protect their assets and customer data from emerging fraud and cyber threats. Access Management solutions such as multi-factor authentication (MFA) are replacing traditional passwords to increase security. But MFA's limitations offer up inconsistent user experiences, often leading to abandonment. Newer capabilities like behavioral biometrics, fraud and risk management, know your customer (KYC), and identity proofing are often handled as security silos and can lead to integration headaches.

You need an easy, secure, and future-proof access orchestration solution that ties together the identities, applications, and services at the center of your business strategy. By leveraging a Zero Trust and Continuous Adaptive Risk and Trust Assessment (CARTA) identity orchestration framework, you can strike a balance between security and user choice, delivering a more secure and meaningful experience across all digital touchpoints for all users, anytime, and anywhere.

Intelligent Access is based on a powerful decision tree framework that enables you to:

› Easily configure, measure, and adjust login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors.

› An intuitive drag-and-drop interface enables you to quickly consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions — all in one place.

› Leverage user login analytics to increase user adoption rates, and improve the customer experience.

› Automatically redirect suspicious users for further monitoring.

Security Ecosystem

Built-in
» Authentication Methods
» User Signals
» Device Signals

Marketplace
» Identity Proofing Services
» Fraud Prevention Systems
» Transactional Risk Analytics
» Bespoke Authentication Methods
» Biometrics Providers
» Community-built

Custom-build
» Design a signal detector
» Add your own factor

Intelligent Access Engine

Orchestrating factors and signals based on:

Context · Behavior · Risk Choice · Analytics

Visually Design Delightful Experiences

Optimize Journeys with Analytics

Benefits

Strengthen Security Landscape

» Prevent Data Breaches and Fraud
» Enable Targeted Risk Reduction
» Deliver Purpose-built Login Journeys

Improve Customer Engagement

» Offer Dynamic Personalization
» Gain Insight with User Login Analytics
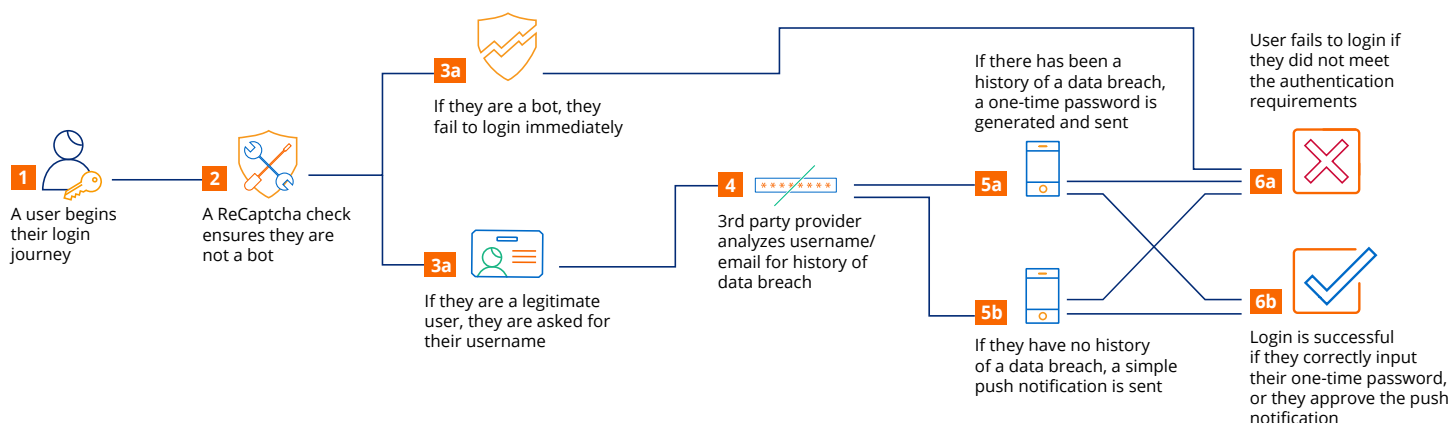» Simplify Login via User Choice

Strengthen Your Zero Trust and CARTA Security Landscape

Improve the security posture of your business by designing purpose-built journeys. Digital signals, factors, and third party integrations for risk, fraud and malware can be interconnected to establish your required level of trust. Intelligent Access enables you to secure the login experience, audit all login events, and minimize risks of DDoS attacks and data breaches.

› Pre-identify a user's digital signals such as location, IP address, device type, operating system, browser type, and more before a username is even collected

› Intelligently adjust login journeys to identify legitimate and suspicious users

› Uncover threats by isolating and monitoring malicious activity using honeypots.
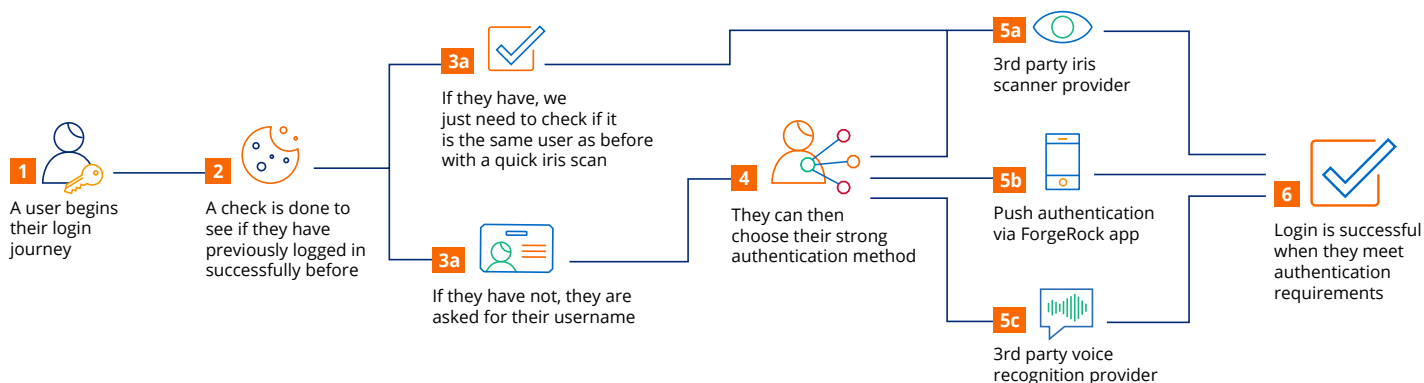
Improve Customer Engagement

People crave a simple and flexible omnichannel login journey. Intelligent Access enables you to continually assess and improve their experience across digital touchpoints. Make login effortless by offering dynamic login choices. Frictionless, passwordless login methods such as push notifications makes life easier for users — and requires extra steps in the login journey only when necessary.

1 A user begins their login journey

2 A ReCaptcha check ensures they are not a bot

3a If they are a bot, they fail to login immediately

3a If they are a legitimate user, they are asked for their username

4 3rd party provider analyzes username/email for history of data breach

If there has been a history of a data breach, a one-time password is generated and sent

5a

If they have no history of a data breach, a simple push notification is sent

5b

User fails to login if they did not meet the authentication requirements

6a

6b Login is successful if they correctly input their one-time password, or they approve the push notification
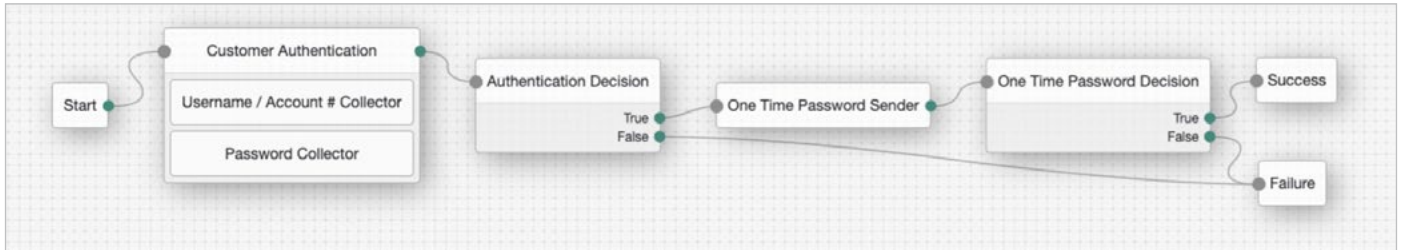
Deliver Dynamic Personalization

Irrelevant content can frustrate consumers. Intelligent Access helps you deliver dynamic content by using context to drive personalization. Digital signals like user device, location, and time can be leveraged in real-time to build dynamic web personalization content. This informs downstream applications, and ultimately helps you to develop offers aligned with customer expectations.

1 A user begins their login journey

2 A check is done to see if they have previously logged in successfully before

3a If they have, we just need to check if it is the same user as before with a quick iris scan

3a If they have not, they are asked for their username

4 They can then choose their strong authentication method

5a 3rd party iris scanner provider

5b Push authentication via ForgeRock app

5c 3rd party voice recognition provider

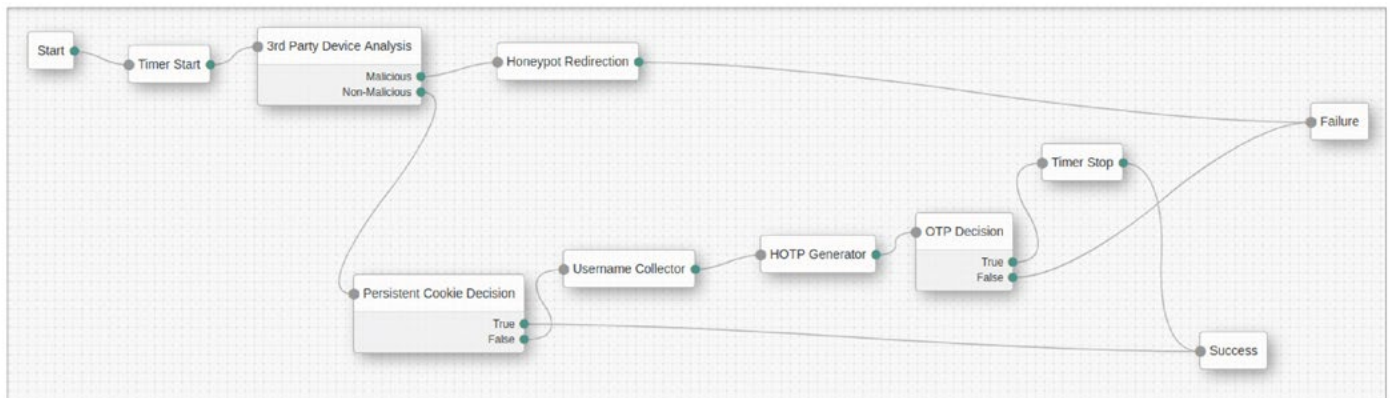**6** Login is successful when they meet authentication requirements

Visually Design Delightful Experiences

Visually map login journeys before implementing them with an interface that supports agility and rapid integration. Intelligent Access provides a drag-and-drop interface where you can easily design and adjust journeys that satisfy user populations across your digital channels.

Harness Analytics to Optimize Customer Journeys

Data-driven insight helps you to continuously improve and secure the customer journey. User Login Analytics, built into Intelligent Access, offers metrics and timers that measure user interactions as well as their devices across services and applications. With User Login Analytics you can: