SOLUTION BRIEF

# ForgeRock Autonomous Access

## Orchestrate Secure and Personalized Experiences with AI-Driven Threat Protection

ForgeRock Autonomous Access is an AI-powered threat protection solution that helps organizations prevent account takeover and fraud at the identity perimeter.

Over the past decade, the number, size, and velocity of data breaches have accelerated. In the past, a breach that compromised the data of a few hundred thousand people would have been big news. Now, breaches are measured in the hundreds of millions or even billions of records impacted. Breaches containing usernames and passwords increased 450 percent in 2020, totaling 1.48 billion compromised records.[1]

Cybercriminals are targeting global organizations through a wide variety of attack methods, including bots, credential stuffing, phishing, malware, brute-force, and many more. While these bad actors are increasing the risk of breaches from the outside, organizations are also combating a rise in internal risks. Insider threats, such as employee data exfiltration, third-party credential theft, and unauthorized employee access, among others, are very much on the radar of security and IT teams.

These threats, combined with the aggressive growth in fraud, challenges around the hybrid/remote workforce, and the need to address poor customer experiences, are overwhelming security and IT teams.

1 ForgeRock Consumer Identity Breach Report

# Today's Identity Perimeter Dilemma

Security and IT teams have seen the pace of change accelerate significantly in the IT environment. With consumers, remote workers, partners, mobile, and cloud deployments, the classic organizational perimeter no longer exists. Instead, the fundamental means of access in most cases is digital identity.

In the past few years, consumers have spent more time making online purchases — and their digital expectations have increased. They expect an "Amazon-like" experience and strong security for their personal data.

With the acceleration in digital spending, there's been an increase in related cyberthreats, like account takeover. Account takeover (ATO) occurs when a bad actor gains unauthorized access to a user's digital identity account. ATO is often the source of data breaches, theft, and other fraudulent activities.

In breach after breach, the cyberattack cycle starts with identity. Bad actors seek to gain unauthorized access to a user's digital identity account. From there, they pivot between resources, discovering more credentials and other identities to get greater access to the valuable data they're after. This ability to exploit one account as a means of entry is the reason account takeover attacks increased 307 percent from 2019 to 2020.[2]

To address the issues of user experience and security, your organization needs a sophisticated solution that removes unwanted friction while strengthening security.

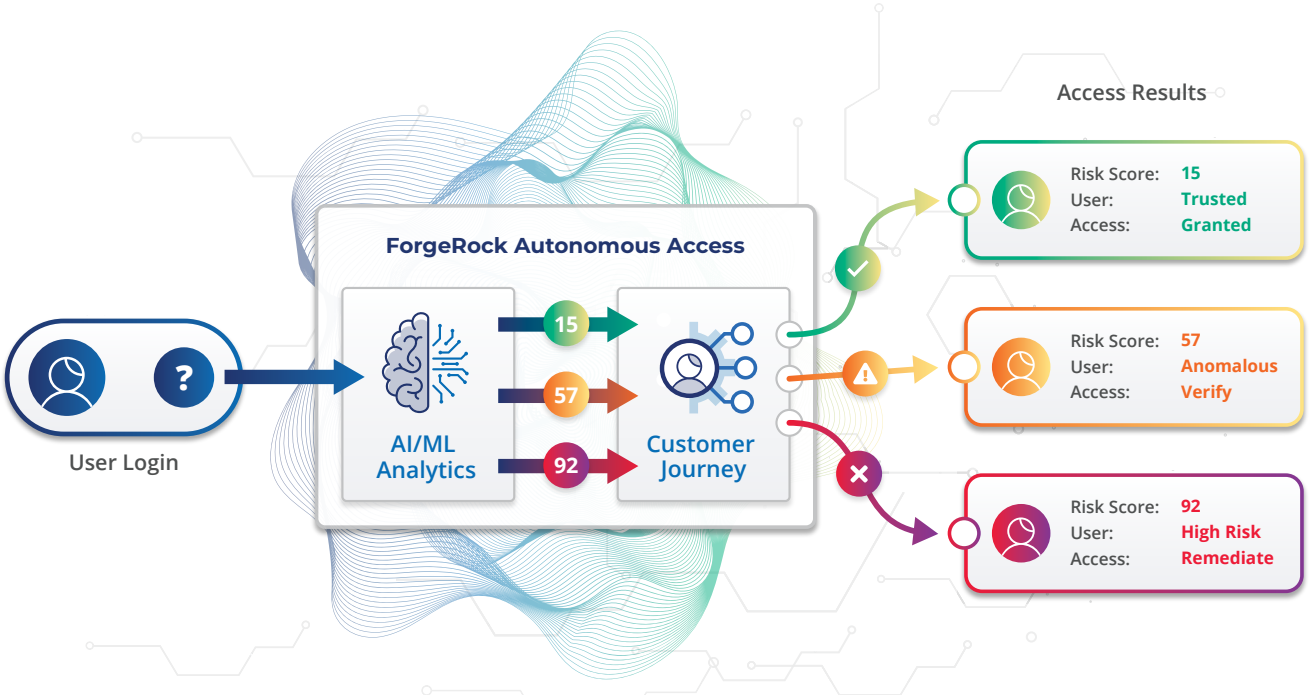
# ForgeRock's AI-Driven Approach

ForgeRock Autonomous Access leverages artificial intelligence (AI) and machine learning (ML) techniques to analyze threat signals and anomalous behavior patterns. It speeds and simplifies access decisions, enabling your organization to block threats and deliver personalized journeys that enhance the digital experience of legitimate users.

### Better Protection is as Easy as 1-2-3

With Autonomous Access, you can treat each login request differently based on its risk score, so you can fast-track trusted users with options like passwordless authentication while stopping attackers.

1. **Trusted User** – A low-risk user who logs in at the same time and location using the same device. User sails through login without friction.
2. **Anomalous Behavior** – A familiar user who may be using a new device or logging in at an unusual time or location. User receives a step-up challenge.
3. **Known Threat** – A high-risk user that is almost certainly malicious, possibly a bot, having failed multiple automated login attempts. Requests can be remediated or fully blocked.




2 Sift, Digital Trust & Safety Index Report: Account Takeover Fraud and the Growing Burden on Business

# ForgeRock Autonomous Access Benefits, Differentiators, and Features

## Benefits

### Better Protection

Protect your customers and your organization from damaging and costly breaches. Block threats, such as account takeover and fraud, before they occur, thereby driving down the cost of mitigation.

### More Customer Engagement

Removing unneeded friction for legitimate users improves the customer experience, leading to better engagement, stronger retention, and ultimately more revenue. It's easy with unlimited, personalized journeys.

### Faster Time-to-Value

Fully integrated from the start, Autonomous Access eliminates the need to integrate disparate point solutions. Combined with no-code access orchestration, you can save time and resources, while creating the right journey for each user.

## Differentiators

### Layered Intelligence

ForgeRock Autonomous Access leverages a unique combination of AI, machine learning, advanced pattern recognition, and big data to provide risk scores to help stop known bad actors, flag anomalous behavior, and learn about new and emerging cyberthreats. The solution provides organizations with real-time threat protection during user authentication.

### No-code Access Orchestration

Built into ForgeRock's industry-leading Intelligent Access solution, Autonomous Access includes drag-and-drop configuration, making it easy for your teams to create any number of personalized user access journeys based on identified risk scores.

### Built for the Enterprise

Delivered from the ForgeRock Identity Cloud, Autonomous Access is purpose-built to meet the security, scale, and resiliency needs of large, complex enterprises. It's easily activated with the touch of a button, eliminating costly deployment and integration of disparate point solutions.

# Features

## Threat Prevention

With Autonomous Access, you can stop known bad actors by preventing bot attacks, credential stuffing, suspicious IP, and other forms of cyberattacks. By leveraging real-time advanced pattern recognition, Autonomous Access stops known threats before they can infiltrate and cause damage to your organization.

## AI-driven Anomaly Detection

You can quickly flag emerging threats with the solution's layered AI, including user and entity behavior analytics (UEBA), that continuously gets smarter at identifying the difference between normal behaviors and emerging threat patterns.

## Personalized Customer Journeys

Unlike other "bolt-on" or "point" solutions, Autonomous Access does not require time-consuming and costly custom integrations. Autonomous Access is built into and administered from ForgeRock Intelligent Access, which empowers IT administrators to design tailored experiences for every login attempt based on the level of risk — all with simple drag-and-drop configuration.

## Enterprise-wide Threat Visibility

Because Autonomous Access provides the ability to identify threat signals and anomalous behavior patterns in real time, your security and IT teams can quickly distinguish attempted account takeovers, fraud, and other cyberattacks. Using contextual risk scores, explainable AI, and fraud analyst dashboards, your organization can proactively address enterprise-wide threats.

## Threat and Risk Signals

### Threat Prevention

Block threats before they occur, thereby reducing business risk and driving down the cost of mitigation.

- Credential Stuffing
- Suspicious IP
- Impossible Traveler
- Brute Force
- Bot Detection

### Anomaly Detection

Detect anomalies for frequent, first-time, and infrequent users. All anomalous results are fed into the machine learning engine at the end of each login journey.

- User, City, and Country
- Day of Week
- Time of Day
- Operating System and Version
- Device Model and Type
- Browser
- Jailbreak/ Root Detection*
- Fingerprint Authentication*

**SDK-enabled features*

**About ForgeRock**

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that delivers modern and comprehensive identity and access management solutions for consumers, employees, and things to simply and safely access the connected world. Using ForgeRock, more than 1,300 global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data — consumable in any cloud or hybrid environment. The company is headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com**.

**Follow Us**

ForgeRock

Copyright © 2022 ForgeRock, All Rights Reserved.