ForgeRock

DATASHEET

# ForgeRock Autonomous Access

*Orchestrate secure and personalized experiences with AI-driven threat protection*

Over the past few years, consumers have spent less time shopping in stores and more time making online purchases. With the heightened risks that come with increased online activity, consumers' digital expectations have also increased. They expect an "Amazon-like" personalized experience and strong security for their personal data.

With the acceleration in digital spending, there's been an increase in related cyberthreats, such as 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 that lead to lost revenue, damaged brand reputation, and significant mitigation costs.

Your enterprise needs a modern security solution that removes unwanted friction while strengthening security. ForgeRock Autonomous Access is an AI-powered threat protection solution that helps to prevent account takeover and fraud at the identity perimeter.

## Key Benefits

### Better Protection

With a unique combination of AI, machine learning, and advanced pattern recognition, you can block threats 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 and, ultimately, more revenue.

### Faster Time-to-Value

Full ForgeRock Identity Cloud integration 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.

## Features

### Threat Prevention

Stop known bad actors by preventing bot attacks, credential stuffing, suspicious IP, and other forms of cyberattacks with advanced pattern recognition.

### Personalized Customer Journeys

Empower IT administrators to design tailored experiences for every login attempt based on the level of risk — all with simple drag-and-drop configuration.

### AI-driven Anomaly Detection

Quickly flag suspicious behavior with layered AI, including UEBA, that continuously gets smarter at identifying the difference between normal behaviors and emerging threat patterns.

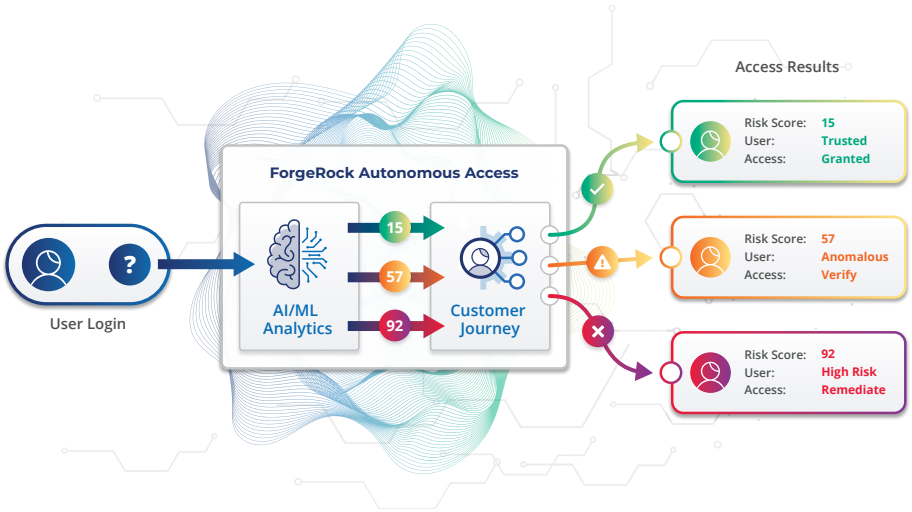
### Enterprise-wide Threat Visibility

Identify attacks and anomalies across the entire organization with contextual risk scores, explainable AI, and dash-boards for admins and fraud analysts.

## 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.




## Differentiators

### Layered Intelligence

A unique combination of AI, machine learning, and advanced pattern recognition provide risk scores to help stop known bad actors, flag anomalous behavior, and learn about new and emerging cyberthreats.

### 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 the identified risk score.

### 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.

**To learn more:**
[forgerock.com/autonomous-access](forgerock.com/autonomous-access)

## 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