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.

Organizations need 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 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 heuristics (advanced pattern matching).

AI-enabled Users Journeys

Eliminate unnecessary friction and orchestrate seamless experiences with no-code configuration and AI-powered digital customer journeys.

AI-driven Anomaly Detection

Quickly flag emerging threats with layered AI evaluation of user and entity behavior analytics (UEBA), behavioral AI, and other AI models.

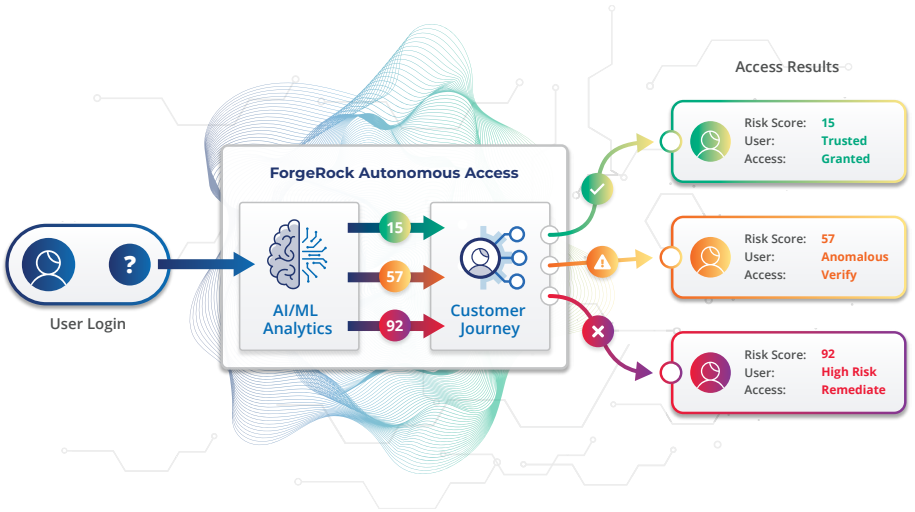
Enterprise-wide Threat Visibility

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

Access Decisions are 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 user who logs in at the same time and location using the same device. This user sails through login without friction.
2. **Anomalous Behavior** - A familiar user who may be logging in on a new device or at an unusual time or location. User receives a step-up challenge.
3. **Known Threat** - This high-risk attempt is almost certainly malicious, having tried multiple automated logins. Login requests can be remediated or fully blocked.



Differentiators

Layered Intelligence

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

Limitless User Journeys

Built into ForgeRock Intelligent Access Trees to remove unwanted friction for trusted users. AI-powered customer journeys improve the digital experience by providing adaptive security choices when step-up challenges are required.

No Code Orchestration

Autonomous Access provides no-code access orchestration to help determine the right user journey at the right time. Delivered from the ForgeRock Identity Cloud, your data is protected by a unique security and privacy model based on full tenant isolation.

To learn more:
https://www.forgerock.com/platform/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
- And more...

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.

- Individual User
- City and Country
- Day of Week and Time of Day
- Operating System and Version*
- Device Model and Type*
- Jailbreak/Root Detection*
- Fingerprint Authentication*
- Browser Profile
- And more...

**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 1300 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