Beyond Identity Secure Customers

BEYOND IDENTITY

Convert and secure customers with cross-platform, zero-friction passwordless authentication.

Eliminate authentication friction and build trusted customer relationships

Customers have rising demands for frictionless experiences while attackers are exploiting the move to digital with increasingly frequent phishing, credential stuffing, and brute force attacks.

The problem is, existing methods of customer authentication don't eliminate the root cause of friction and security issues -- the password.

Beyond Identity Secure Customers delivers the fastest authentication across all your applications with no second devices required and eliminates the password for customers and from your database. 1

Streamline registration, login, and recovery to drive conversions. Secure customers against account takeover fraud by deprecating passwords completely. Precisely control access with adaptive risk-based policies based on granular user and device risk signals captured in real time.

Key Benefits:

- ✓ Completely eliminate account takeover fraud
- ✓ Passwordless MFA with two strong factors in one transaction
- ✓ Privacy-preserving credentials customers own and control
- ✓ Zero-friction with no second devices, OTP, or push notifications

Use Cases

Accelerate customer conversions

Prevent drop-offs by eliminating passwords, one-time codes, push notifications, and second devices on native and web applications.

Eliminate account takeover fraud

Make account takeover impossible by removing passwords from the customer experience and database. Instead, secure accounts with passwordless MFA that validates two strong factors in one transaction.

Modernize your application

Simplify your application stack with a cross-platform authentication product built on proven open standards for extensibility, scalability, and reliability.

Implement adaptive access control

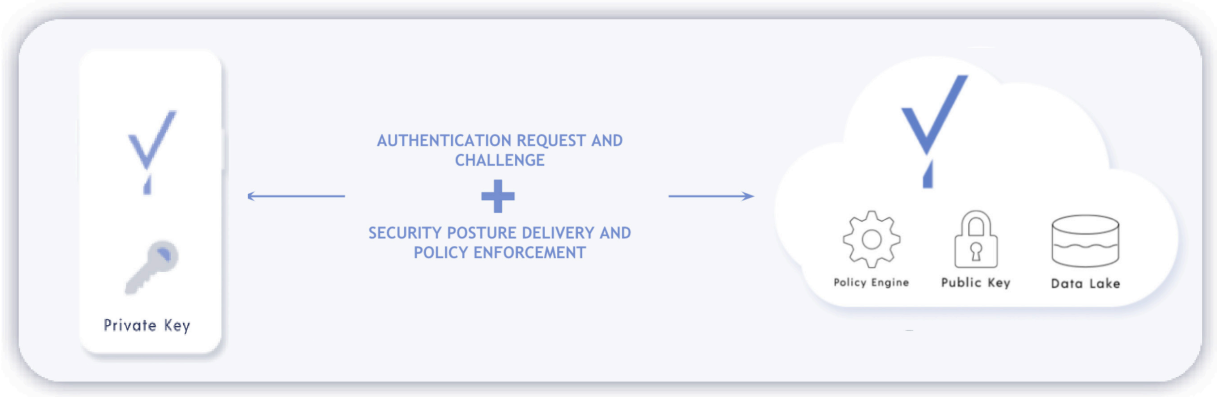
Evaluate user and device risk prior to login and implement dynamic step-up authentication for higher risk behaviors according to your security policies.

How It Works

Beyond Identity leverages an innovative implementation of asymmetric cryptography that underpins TLS to completely eliminate passwords from the customer experience and your database.

Instead of passwords, Beyond Identity authenticates customers with two strong factors -- something you are from the device biometric and something you own from the private key -- without requiring a second device.

During authentication, Beyond Identity issues a challenge signed by the private keys in the device's secure hardware (TPM), evaluates user and device security risk in real-time, and makes a risk-based authentication decision based on your security requirements.



Unique Benefits:

Zero-friction authentication

Drive faster conversions by removing passwords and the need for second devices across native and web apps.

Privacy-preserving credentials

Preserve privacy with tamper-resistant credentials backed by private keys that are only owned by the customer and can't ever leave hardware TPMs.

Cryptographic identity verification

Only allow the right customers to access the right account with immutable, device-bound identity attestation for each access request.

Adaptive access controls

Configure dynamic access policies and step-up authentication using granular user and device risk signals captured in real time.

auth0 KEYCLOAK ForgeRock