

**DATA SHEET**

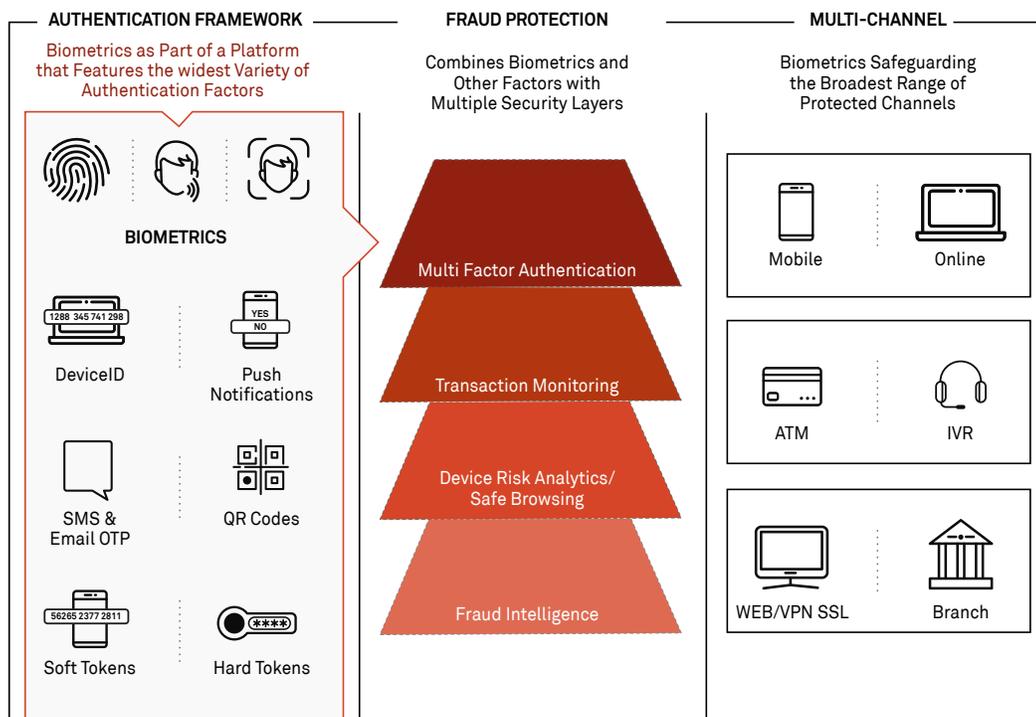
## **BIOMETRIC AUTHENTICATION: More Convenience Less Friction**

State-of-the-art user verification is essential for confirming that users are who they say they are – but too much friction can repel the customers you are trying to protect. Biometric technologies, as part of an adaptive authentication system that combines identity conformation with other risk-based variables, can ensure that only legitimate users access sensitive data and accounts without having to just through all the hoops.



**HIGHLIGHTS:**

- Facial, voice and fingerprint recognition that helps enable simple and safe access.
- Reduce customer friction and reduces the need to memorize passwords or type in security codes.
- Protection in the blink of an eye - SelfID Liveness detection technology monitors an end user’s blinks in the background to prove liveness when autjenticating a transaction, thwarting fraudsters who may attempt to circumvent facial scanners with pictures of end users.
- Part of an authentication framework that offers the most extensive series of different factors across al channels.
- Start trusting mobile with SDKs for biometric security integrated into your application.
- Android and iPhone iOS API support allowing for different phones to add fingerprint validation. Fingerprint readers can be combined with Push notifications for strong, layered user authentication.



## BIOMETRICS AUTHENTICATION FACTORS

### TURN USERS INTO THEIR OWN PASSWORDS

Combine frictionless access with a high level of accuracy to strike the right balance between convenience and security. Your customers become their own passwords by leveraging their unique physical features to protect their accounts and safeguard transactions.



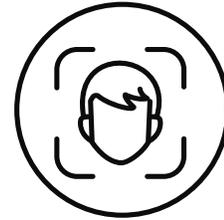
**TOUCH**

Everyone has a unique, unchanging fingerprint. Use this to protect management of your mobile apps.



**VOICE**

The way you speak is as unique as a snowflake. Leverage this on any channel. Just say a simple phrase and you're in!



**FACE**

SelfID Facial Recognition technology measures and records various points on a human face. The user performs a few simple gestures with their mobile camera in order to authenticate access to any channel.

### COMPLEMENTS RISK-BASED AUTHENTICATION

Biometrics can also assist with risk-based authentication. If a transaction falls outside a user's normal habits or comes from a risky device or location, a biometric challenge is sent to the user's device to help verify that it is legitimate. This greatly reduces alert volume and false positives, enhancing accuracy for an optimal user experience with minimal interruption.

### WINK OF THE EYE, WAG OT THE FINGER

Defend against cybercriminals who try to circumvent rudimentary facial scanners by using still photos - with next-generation Liveness Detection and Facial Recognition from SelfID, users are required to move to prove they are a real person. Fingerprint authentication supports all Android OS and iOS phones with built-in fingerprint readers.

### COMPLETE FLOW

APIs for registration, authentication, resets and more are covered by the solution to allow for full customer lifecycle management.

### PART OF THE FRAUD PROTECTION STRATEGY

Appgate's suite of fraud protection products and services can ensure maximum security and complement biometric verification with additional layers of validation, including tokens, device analytics, user profiles and more.

#### AUTHENTICATION - ADDITIONAL FEATURES

Multi-Channel Support: Online, Mobile, ATM/POS, IVR & Branch Offices

Management console for Administration & Auditing

APIs for Integration and Administration through Web Services, RADIUS & SAML

SDKs for Integration of Biometrics into Mobile Apps