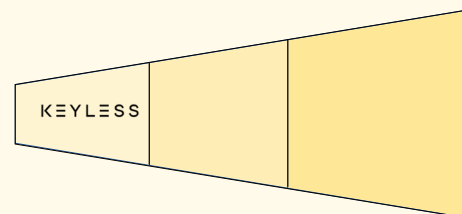
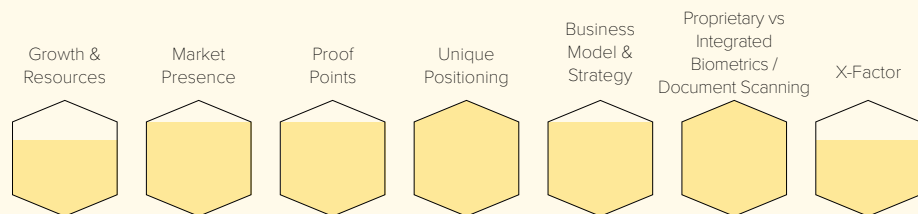


BEAM: Biometric ID Platform / CLASSIFICATION: Luminary



Keyless is carrying the torch for platform-based biometric digital identity. This Prism Luminary extends the traditional security perimeter to include the end user with its proprietary cryptography and face biometrics technology. Frictionless experiences, strong security, regulatory compliance, and rapid ROI are major selling points for Keyless' biometric authentication platform—offered through flexible deployment models, including cloud-native, hybrid, and on-prem—and the company prides itself on meeting all global compliance and data sovereignty requirements, including GDPR and CCPA, and regulatory requirements such as PSD2 SCA, with certifications pertaining to FIDO Biometrics, FIDO2, information security management, quality management, and more. This all adds up to a strong biometric authentication platform ready to move organizations—particularly those in the financial sector—into an era that relies less on traditional (and phishable) keys like passwords, tokens, and magic links.

Leveraging True User Identity with Zero-Knowledge Biometrics

Keyless is not simply replacing passwords with biometrics—its MFA-by-design solution positions true user identity as the primary credential for all transactions. Capturing two authentication factors in one look, Keyless defends against deepfakes and spoof attacks. It's great for user experience, too. With a single selfie upon enrollment, a user can continue to authenticate and assert their identity through every interaction on a Keyless-protected service, across any device. This is all facilitated through the company's trademark Zero-Knowledge Biometrics, a unique zero knowledge cloud computing model designed for privacy and compliance. With Keyless, biometrics are stored neither on devices nor in the cloud, simplifying compliance with data privacy regulations. Our researchers see this as a realization of a core concept of the Prism: that biometrics are not analogous to passwords.

Account Recovery in the Age of Automation

A persistent challenge for all post-password authentication systems is the account recovery step. When a user loses access to strong credentials, a system's weakness is revealed: many biometric authentication systems revert to a password or magic link for account recovery, making them as vulnerable as legacy systems, while solid device-based authenticator apps demand lengthy and costly call center processes that can take days. With Keyless, account recovery is a simple process that can get a verified user back on the platform as quickly as taking a selfie. As automated account recovery becomes an increasing priority for the identity ecosystem, Keyless is among the handful of vendors leading the way.

Fulfilling the Promise of Full-Lifecycle ID

User experience is a priority of Keyless, and that is on display with its various controls to reduce friction, even beyond the enrollment and login steps. Modeled after the mainstream IAM single sign-on experience, the company has integrated with risk platforms to enable step-up authentication when it is needed based on the weight of the transaction. In taking this approach, Keyless helps its partners move beyond a defensive stance that treats every user like a potential liability, enabling them to operate from a position of active customer satisfaction.