Passwords are out, biometrics are in

Passwords have long been the primary way to access and protect digital goods and services. But every day the number and complexity of passwords grows more overwhelming.

This dynamic is changing. Passwordless authentication solutions — especially ones that employ user biometrics — are gaining traction, offering more convenient and secure experiences.

But do consumers feel the same way? We asked consumers to select the identity authentication methods they thought were more secure than a password. More than half of respondents believed biometric solutions are more secure, with 53% selecting fingerprint scans followed by facial recognition (47%). Only 6% of consumers said passwords are the most secure method.

Only 6% of consumers said passwords are the most secure method.

Authentication methods consumers believe are more secure than passwords

Fingerprint scan	**53%**
Facial recognition	**47%**
4- or 6-digit PIN codes	**41%**
SMS one-time passcode	**34%**
Device recognition	**17%**

In addition to security concerns, passwords have grown overly complicated. With more digital services available than ever, consumers struggle to recall an ever-growing inventory of login credentials. **Over half of respondents (51%) reset a password once a month or more frequently because they can't remember it.** Even more alarming, 15% of users do so at least once a week.

Entrust Insight

"Passwords are a necessary evil that is becoming less necessary by the day. Not only are passwords highly susceptible to compromise, but they're inconvenient to keep track of as we access an increasing number of applications and services through digital channels."

Mark Ruchie
Chief Information Security Officer, Entrust