

Transcending passwords: Emerging trends in authentication

Leading IT analyst research firm Enterprise Management Associates (EMA) conducted research into enterprise and end user requirements, perceptions, and outcomes in the usage of password and passwordless authentication technologies. The results present a clear snapshot of where the identity management market is today and the direction it is heading. Here are a few of the key findings.

End users

Security is not the only issue that employers face—employee satisfaction, retention and recruitment are also affected.

Enterprise

Security breaches drive significant business consequences including employee satisfaction.

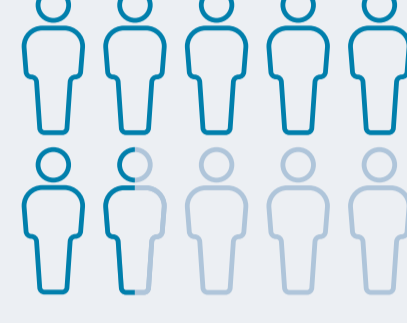
Employee satisfaction



78%
of respondents

indicated they would be **attracted to a new employer** that offers easy-to-use authentication processes.

65%
of respondents



indicated they would be motivated to **change employers** if presented with high-friction authentication processes.



97%
of organizations

that have adopted passwordless authentication reported achieving **quantifiable business improvements**, most notably for increasing security effectiveness and **employee satisfaction**.

Authentication



91%
of business workers

continue to rely on passwords as a primary form of authentication.

93%
of businesses



reported employees had **violated password policies** in the last year, including using the same password for multiple accounts and physically writing down passwords.

10x
each day



on average, **business users authenticate** to access the business applications, data, and IT services they require to perform job tasks.



82%
of surveyed businesses

reported **IT security breaches occurred** in their organizations in the last year, including compromised credentials and successful phishing attacks.



32^{sec}
to authenticate

with a traditional password and an OTP verifier. This equates to **22 hours of work** per user each year.

72%
of businesses



that experienced security violations in the last year **reported significant consequences** to the business, including unexpected IT service failures, damage to company reputation, and a failure to meet regulatory compliance.

8^{sec}
or less
to authenticate



when users employ FIDO-base authenticators (mobile or security key), which is **roughly 5.5 hours of work time** per user each year.



19%
of workers

were reported to have been targets of phishing attack attempts in the last year **with 6% being successful**.

Passwords



87%
of respondents

recognize passwordless authentication solutions **as secure as, or more secure**, than traditional passwords.



81%
of surveyed IT managers

perceive **passwordless authentication technologies as higher level security** than traditional passwords.

86%
of business users

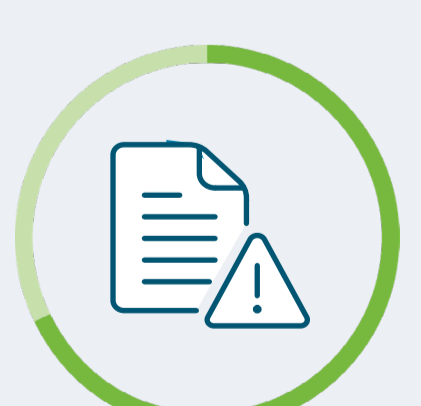


find it **disruptive to their work productivity** to perform a password reset.

The majority
of surveyed IT managers



recognize that the adoption of passwordless authentication will **prevent most, or all, security breaches**.



68%
of respondents

admitted to **violating their business' password policies** by using the same password for multiple accounts, physically writing down a password, and/or resetting a password to one that was previously used.



[Read the report](#)

Learn more about the HYPR | Yubico passwordless authentication solution

yubi.co/HYPR
hypr.com/integrations/yubikey