

The Future of Authentication

Paving the path to continuous authentication

Authentication is evolving and it doesn't take a crystal ball to see where it's headed. We're moving from static, password-based authentication to intelligent, continuous authentication.



NOW ENTERING STATIC AUTHENTICATION

The original authentication method

WHAT YOU KNOW

The first method of securing authentication consisted primarily of usernames and passwords.

AUTHENTICATED UPON ENTRY

 Passwords

EXAMPLE

2-factor authentication

WHAT YOU KNOW

+

WHAT YOU HAVE

As cybercrime grew and hackers captured passwords, organizations began to require an additional authentication factor like One Time Passwords and smartcards.

AUTHENTICATED UPON ENTRY

NEW

Security question



Passwords

NEW

Phones

NEW

Smart cards

Multi-factor authentication

WHAT YOU
KNOW

+/-

WHAT YOU
HAVE

+/-

WHO YOU
ARE

Physical items can be stolen or lost. And they aren't the best user experience. So factors like biometrics were added for authentication.

AUTHENTICATED UPON ENTRY

? Security question

(***) Passwords

NEW Iris scans

Phones

NEW Facial recognition

NEW Fingerprints

Smart cards

WELCOME TO INTELLIGENT AUTHENTICATION

Contextual authentication



Even biometrics can be hacked. Cutting-edge MFA uses AI to understand a person's normal login patterns and flag unusual behavior. It prompts for more or less information based on that behavior.

AUTHENTICATED UPON ENTRY



WE ARE HERE



Phones



Facial recognition

NEW

Login locations

NEW

Time of day

NEW

Device used

NEW

IP address



Passwords



Iris scans



Smart cards

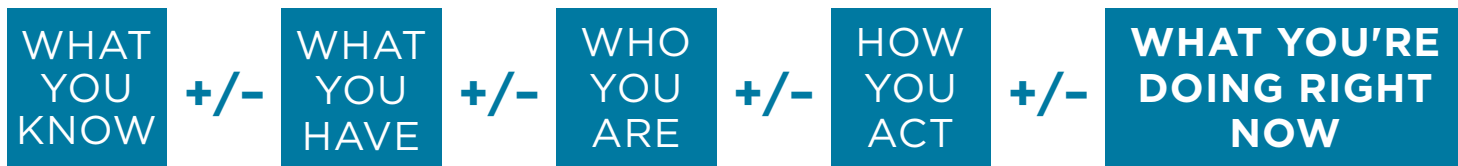


Fingerprints



Security question

Contextual, continuous authentication



It's not enough to check user authenticity once, at login. Soon, MFA will monitor user actions throughout a session to identify anomalous behavior and respond to it in real-time.

AUTHENTICATED UPON ENTRY

CONTINUOUSLY



 Passwords

 Phones

 Fingerprints

 Time of day

 Smart cards

NEW Application accessed

 IP address

 Iris scans

NEW Data accessed

NEW Change in physical location

 Device used

 Login locations

 Facial recognition

 Security question

About OneLogin

OneLogin is the identity platform for secure, scalable, and smart experiences that connect people to technology. With the OneLogin Trusted Experience Platform, customers can connect all of their applications, identify potential threats, and act quickly. Headquartered in San Francisco, CA, OneLogin secures over 2,500 customers worldwide, including Airbus, Stitch Fix, and AAA. To learn more visit www.onelogin.com.

[WATCH DEMO](#)