Future of Multi-factor Authentication (MFA)

Purple Team 9

Agenda

- Introduction
- Security Risks without authentication
- Threat Landscape, Risk evaluation
- Brief on MFA
- Need for MFA & Benefits
- Different methods of MFA and their configuration
- WFH situation and MFA impact
- How can MFA be bypassed and Mitigation measures
- Continuous MFA & Use Cases
- Future of authentication
- Summary

Presenters

Harkirat Kaur

Grace Zhou

Jagan

Ashima Dogra

Saswati Prusty

Weiming Luo

Introduction

Purpose - To create ***awareness*** among the audience regarding Multi-Factor Authentication(MFA).

Outcome - Imparting the audience with knowledge of MFA and it’s configuration on devices - for better security, lesser attacks, reduce the overall risk.

Security risks without authentication

Without multi-factor authentication (MFA), cybercriminals easily gain access to an account. Once the username and password are acquired, every transaction will be treated as valid, and basic security measures cannot prevent it.

Phishing is an easy method of stealing user data. Cybercriminals send out fake emails and make phone calls to trick a user into giving up information, including login credentials. These are the most common giveaways of a phishing email:

- The email seems too good to be true
- The email has a sense of urgency
- Suspicious hyperlinks in the email
- Suspicious attachments in the email
- Unusual sender

Other security risks include -

- **Brute Force Attacks** criminals can generate random passwords.
- **Keyloggers** can be used to recode stroke one makes on keyboard
- **Credential Stuffing**
- **Man-in-the-middle (MITM) attacks/Eavesdrop or Impersonation**

Threat landscape within 60-second window

60-second window of malicious activity

Password attacks	34,740 per minute [1]
IoT-based attacks	1,902 per minute [2]
DDoS attacks	1,095 per minute [3]
Phishing attacks	7 per minute [4]
SQL injection attacks	1 every 2 minutes [5]
New threat infrastructure detections	1 every 35 minutes [6]
Supply chain attacks	1 every 44 minutes [7]
Ransomware attacks	1 every 195 minutes [8]

Cost of Cyber crime

Worldwide economic impact of cybercrime	$1,141,553 per minute [15]
Global cybersecurity spend	$285,388 per minute [16]
E-commerce payment fraud losses	$38,052 per minute [17]
Global ransomware damages	$38,051 per minute [18]
Amount lost to cryptocurrency scams	$3,615 per minute [19]
Total cost of a business email compromise	$4,566 per minute [20]
Average cost of a breach	$8 per minute [21]
Average cost of malware attack	$5 per minute [22]

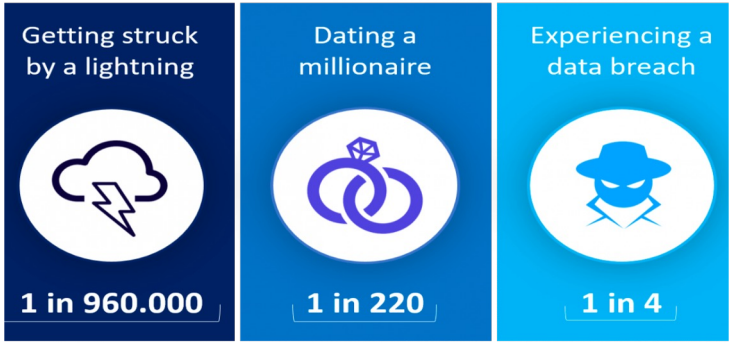
60-second window of expanding internet

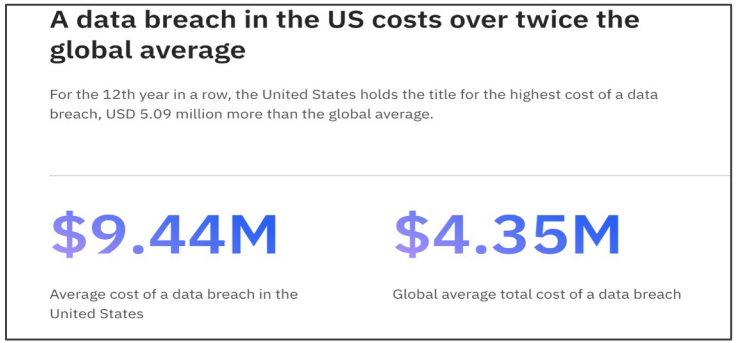
New host	79,861 per minute [23]
New IoT devices	7,620 per minute [24]
New domains	150 per minute [25]
New active LetsEncrypt SSL certificates	53 per minute [26]
New mobile apps created	23 per minute [27]

Source : Microsoft | August , 2022

Risk evaluation without authentication

Likelihood and Impact

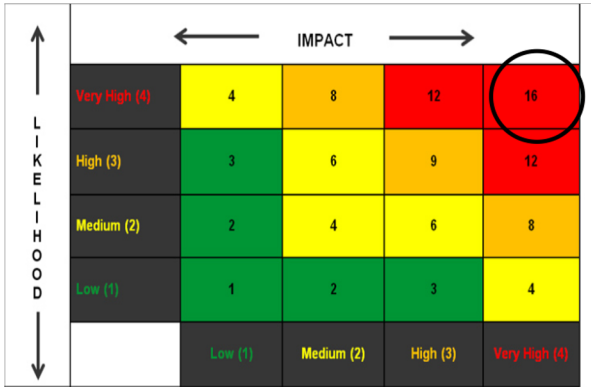




Source : IBM Data Breach Report | 2022

Risk score = Impact (4) * Likelihood (4) = 16

The risk for having cyber security attacks is Very High, given the security measures like MFA are not implemented.



Risk Score	Rating
0 – 3	Low
4 – 6	Medium
6 – 9	High
10 – 16	Very High

User accounts compromised in recent times

- Sony’s PlayStation Attack (2011)
  77 Million accounts hacked
- Adobe Data Breach (2013)
  38 Million accounts hacked
- Yahoo Hacked (2014)
  500 Million accounts hacked
- Under Armour Attack (2018)
  150 Million accounts hacked

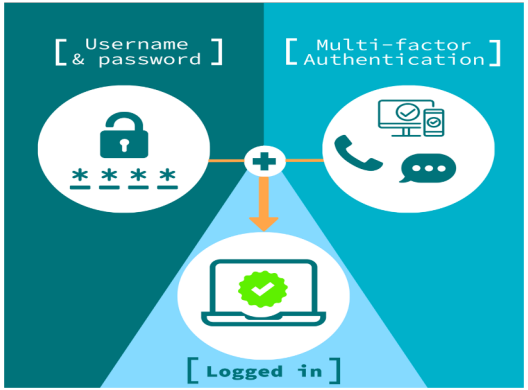
What is Multi-Factor Authentication (MFA)?

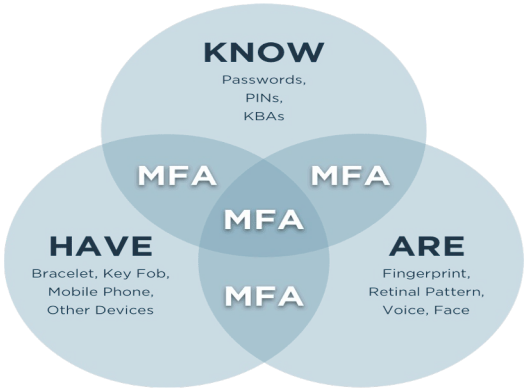
Multi-factor authentication, also referred to as advanced or two-factor authentication, ***provides an additional layer of security when logging in or performing transactions online.***

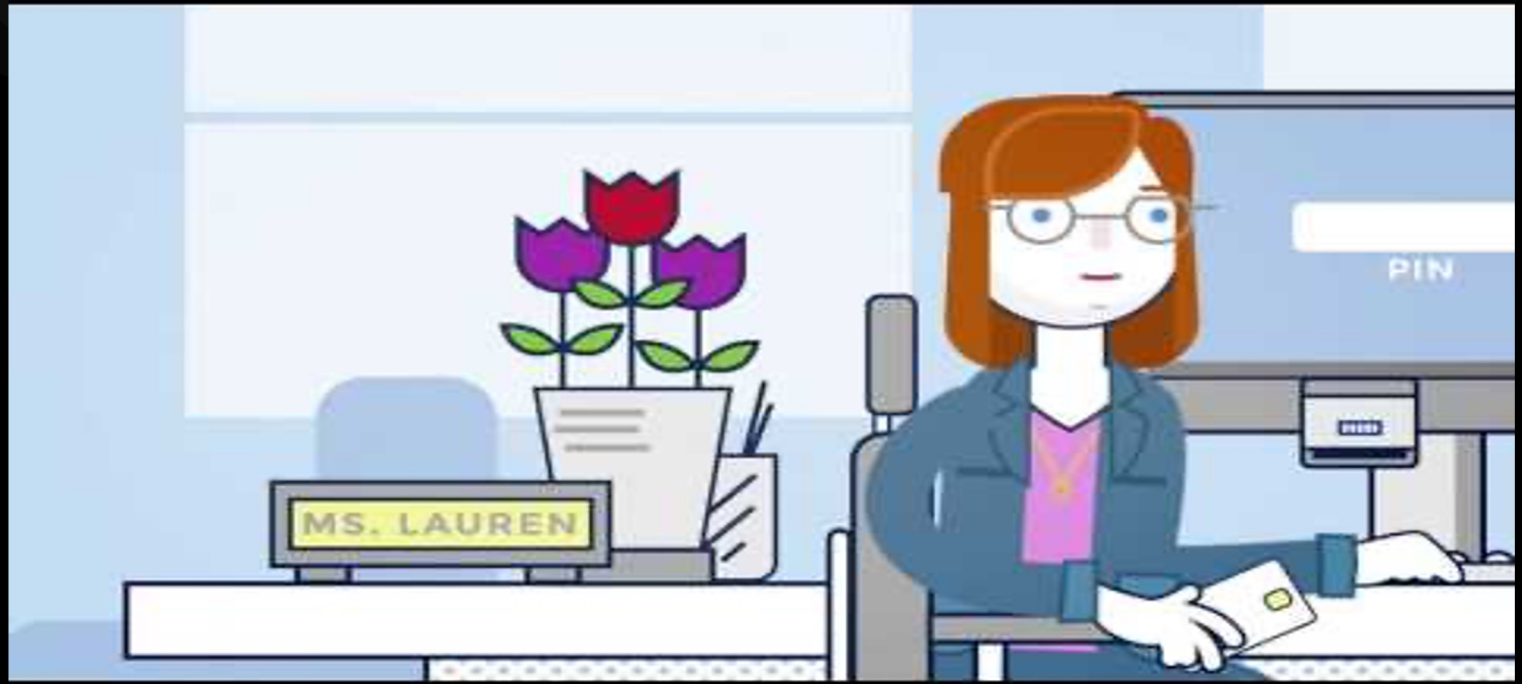
When logging in, a user is required to enter a password and also authenticate using a second factor, typically a phone or hardware token.

Multi-factor authentication verifies the consumer's identity in multiple steps using different methods. It protects accounts by collecting two or more of the credentials below:

- Something you ***know*** (a password or a PIN)
- Something you ***have*** (a mobile phone or a token)
- Something you ***are*** (a fingerprint or other biometric data)






MS. LAUREN
PIN

Why use MFA?

- To prevent unauthorized users
- To protect identity
- To protect data
- To protect money!

98% of the breach can be blocked with multi-factor authentication! (Microsoft)

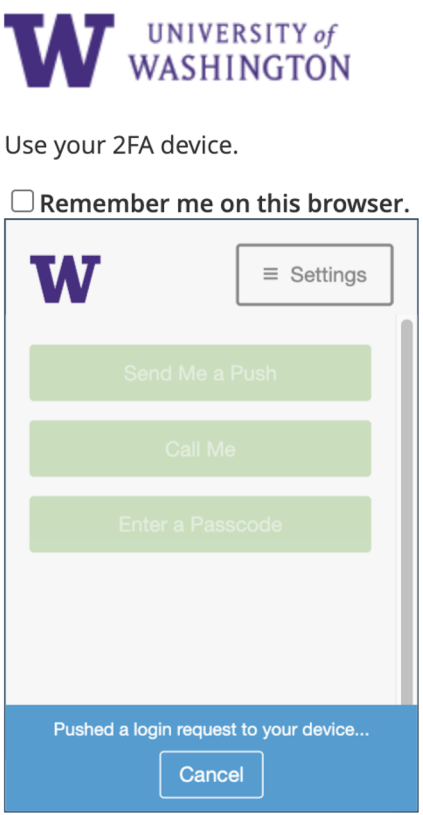
> MFA is strongly recommended for businesses of all sizes. Selecting the right MFA solution is one of the most affordable, effective ways to increase your overall security and protect your business from cyber attacks.

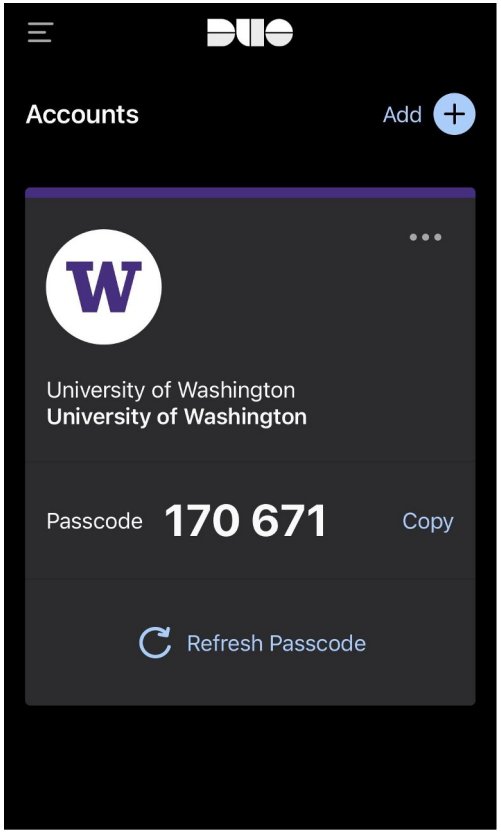
> MFA is a core component of a strong identity and access management (IAM) policy.MFA comes under basic security hygiene which includes other things like patching, zero trust policies etc. These together lead to 98% protection against attacks.

Benefits of MFA

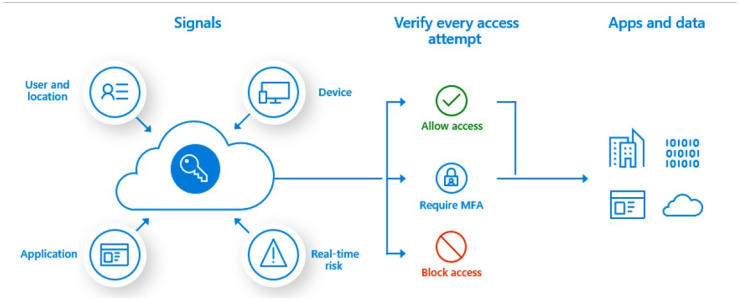
Different Methods of MFA

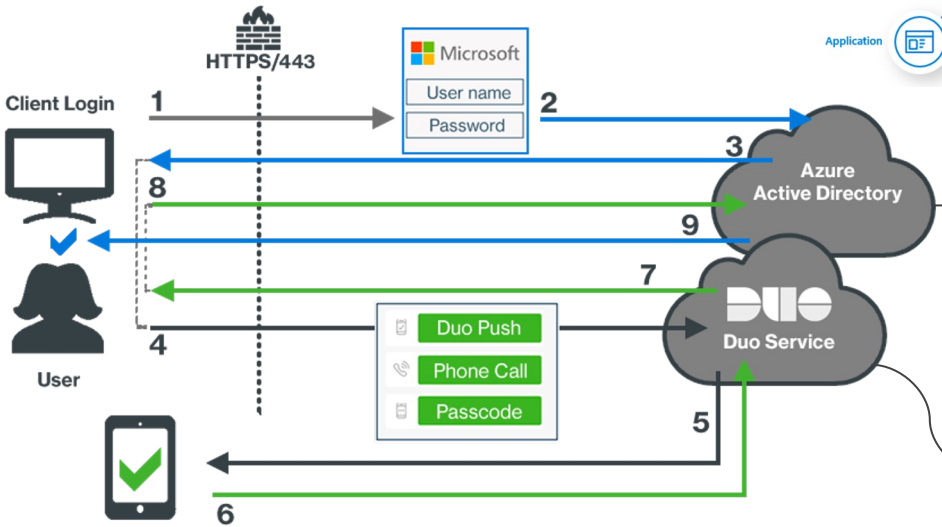
Types of MFA	How it works
SMS, Email and Voice Codes	User receives a code via text, email or phone and inserts it in the app or website to validate credentials.
Hardware Tokens	A physical device that has a pre-configured single use-code that users can connect the devices to be authenticated. Example: RSA physical tokens
Software Tokens	A single-use token is produced out of an algorithm such as OTP, which is shown within a mobile app.
Push Notifications	This allows user to either “Allow” or “Deny” for authentication.
Biometrics	Uses voices, faces, fingerprint to compare two sets of data: the user’s biometrics, and the one saved by the device. If two matches, the user is identified.

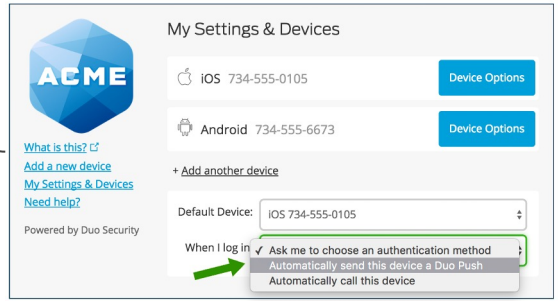

UNIVERSITY of WASHINGTON
Use your 2FA device.
Remember me on this browser.
Settings
Send Me a Push
Call Me
Enter a Passcode
Pushed a login request to your device...
Cancel


Accounts
Add
University of Washington
University of Washington
Passcode 170 671
Copy
Refresh Passcode

How to configure on device?







MFA in WFH situation

- Necessity of MFA in remote workplace
  - Remote workers are more susceptible to cyber threats
- Potential Challenges
  - Inconsistency of available second factors
  - Frustrations rise during initial MFA setup
  - A noisy experience
  - Inability to “Pop Over” for in-person support
- Things to notice when implementing MFA in WFH situation
  - Select the appropriate MFA solution
  - Employee Training
  - Remote IT Support Team

How can MFA be Bypassed ?

Social Engineering Tricking people into revealing **privileged information** through phishing, baiting. • **Likelihood = 4, Impact = 4** • **Risk = 16**	**Consent Phishing** **Open authorization** (OAuth) used to request access to a user's account data e.g. posing as a third party app to gain access to google account. • **Likelihood = 3, Impact = 5** • **Risk = 15**	**Brute Force Attacks** **Cracking password** combinations for hijacking victim **authentication factor**. Special case- **MFA Fatigue -** bombarding an account owner with push notifications until they approve it. • **Likelihood = 4, Impact = 4** • **Risk = 16**	**Exploiting Generated Tokens** Exploiting owner account by accessing the **manual authentication code (Knowledge factor)** • **Likelihood = 3, Impact = 5** • **Risk = 15**	**Session Hijacking/cookie stealing** Cybercriminal **compromises a login session** through man-in-the-middle attack. e.g. cookie stealing. • **Likelihood = 3, Impact = 5** • **Risk = 12**	**SIM Hacking** Hacker gains **unauthorized access victim's SIM card**.to e.g. through SIM swapping. • **Likelihood = 2, Impact = 6** • **Risk = 12**

Mitigation Measures to avoid Bypassing

People

1. Scrutinize all information
2. Using 2 MFA with Biometric as one of the authentication factor
3. Creating complex and updating passwords frequently
4. Avoid SMS based authentication factors, easier to compromise

Process

1. Cybercrime awareness training
2. Establishing security policies and incident response plans.
3. Data security protocols.
4. Check preparedness - Test attacks
5. Monitor attack surface
6. Regular patching and updating devices/apps

Technology

1. Server to restrict number of unsuccessful MFA login attempts that a user can make/lock account
2. Detect data leaks through continuous scanning
3. Anti malware, Firewalls
4. Network segmentation
5. Defense in depth - multiple security layers
6. Encrypting important data

Future of Authentication

“ The Future is Passwordless ”

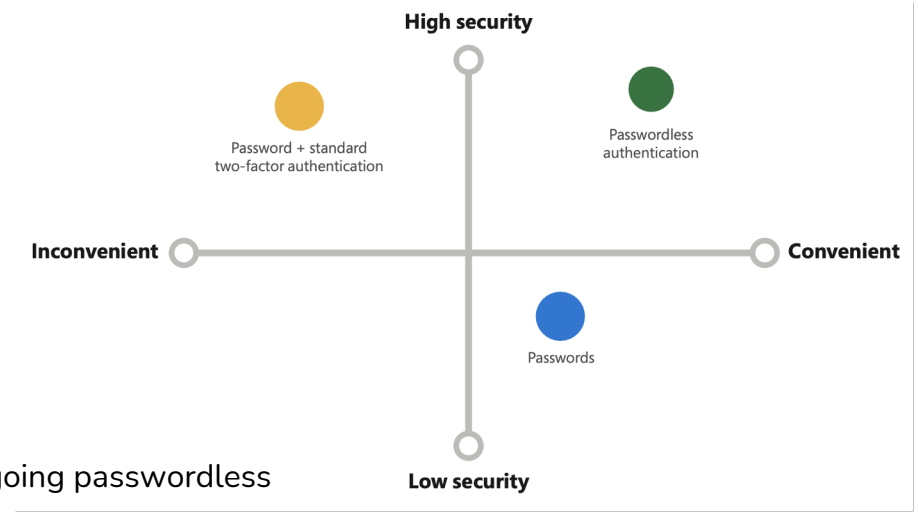
- Customers are 50% more likely to register for an online service if they can sign up with a biometric method.
- About a **third of online purchases are abandoned** at checkout because consumers cannot remember their passwords

**statista.com

Why do we need passwordless authentication?

Password replacement options can help organizations offer **convenience** and ease of use without **high security risks**

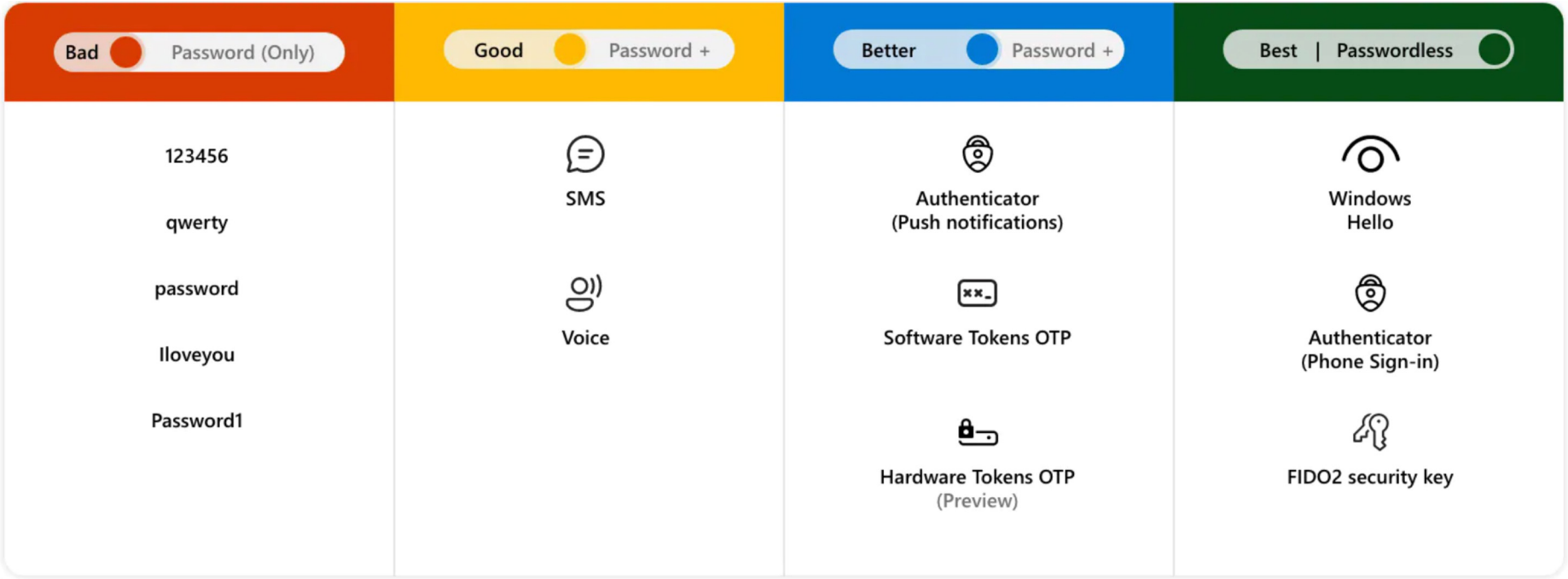
It's imperative for security teams to deliver a **seamless user experience** while balancing security postures.



Deploying **MFA** provides a **solid foundation** for going passwordless

Today, IT security is moving toward passwordless authentication using advanced technologies like biometric verification and public/private key cryptography.

Open standards like W3C WebAuthn and Fast IDentity Online 2 (FIDO2) CTAP2 are enabling passwordless authentication across platforms.



Fast IDentity Online 2 (FIDO2) is an open authentication standard based on public key cryptography

**Microsoft Security

Password replacement technology

Passwordless authentication is a form of MFA used to replace passwords with secure alternatives.

Users have the option to either sign in directly via biometric recognition—such as a fingerprint scan, iris scan, or facial recognition system—or with a PIN that's locked and secured on the device.

- Temporary Access Pins
- Biometrics
- Authenticator apps
- FIDO2 security keys

User and Entity Behavior Analytics (UEBA)

Passwordless authentication systems will monitor people's behavior patterns, taking notice of when, where and how they interact with an app.

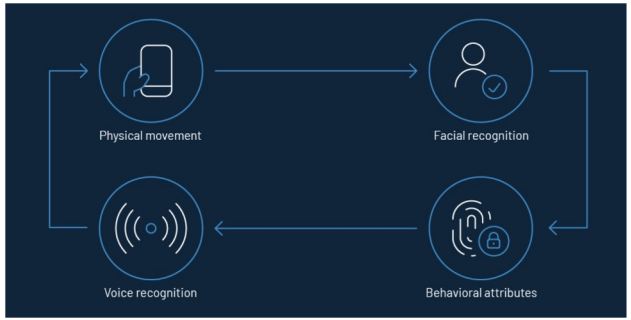
Continuous Authentication

The need for Continuous Authentication

- Password - not enough
- Currently used MFA - static, false sense of security.
- Present solutions are not dynamic - dependent on device being pre-configured.
- Cost of traditional MFA is quickly racking up.

An application with continuous authentication functionality can continually compute an “authentication score” to determine how certain it is that the account owner/authorised user is the one using the device. Depending on the score, the user might be prompted to input additional information such as a password, card or fingerprint.

- Not a lot of attention is paid to a user logging in or out.
- Zero Trust + Zero Touch



Benefits & Drawbacks

How does continuous authentication work?

Constantly collects information about a user's actions and patterns of regular behavior and learns to distinguish between normal and abnormal behavior.

I. Biometrics
II. Leveraging Machine Learning
III. Digital Behavior

- Benefits
  - MFA is dependent on another device which may be prone to issues. Continuous authentication counters this issue.
  - Hard tokens can be exploited.
  - Reinforced learning of behavior - any anomaly will be immediately flagged.
- Drawbacks
  - User acceptance.
  - Invasive.
  - Potential privacy and compliance problems.

Summary

- With a Zero Trust mindset, you must assume a breach could happen.
- However, the adoption of technologies like MFA is one of the best ways for organizations to lower the risk of an identity being compromised.
- Multi factor authentication is the right approach—now and for the future.

Before authentication:
Risk score = Impact (4) * Likelihood (4) = **16**

After MFA:
Residual Risk = Impact (3) * Likelihood (2) = **6**


YOU GET MFA, YOU GET MFA
EVERYONE GET MFA