Acceptto®
INTELLIGENT MFA™

Quick Guide to MFA

What is MFA, and why do I need it?

Factors are typically categorized as one of the following: something you know, something you have, or something you are. Traditional authentication takes a look at one factor to verify your identity- this is usually a password. But one factor isn't enough to stop malicious actors. Multi-factor authentication (MFA) uses two or more unique factors to verify your identity, providing an essential barrier against threat actors hacking into accounts, breaching systems, and generally causing severe damage to your enterprise.

What are challenges that come with MFA?

The first potential challenge of MFA is that it's more costly to implement in enterprise than just a simple one-factor authentication method. In the long run, however, the value of the security it provides far outweighs deployment and maintenance costs.

The second MFA challenge is that it requires additional user effort and time. This kind of repeated effort to login can rapidly go from a minor nuisance to exhausting, dissuading users from valuing MFA. This phenomenon is referred to as "**MFA fatigue**," and the irritating effort that it takes to achieve MFA is called "**friction**." It's undeniable that you need more than one factor to get all your data secured- because that's precisely what keeps the threat actors at bay. Solving the authentication challenge requires balancing an easy experience for legitimate users, while still making it very difficult for attackers to abuse and misuse the system.

How do MFA factors stack up?

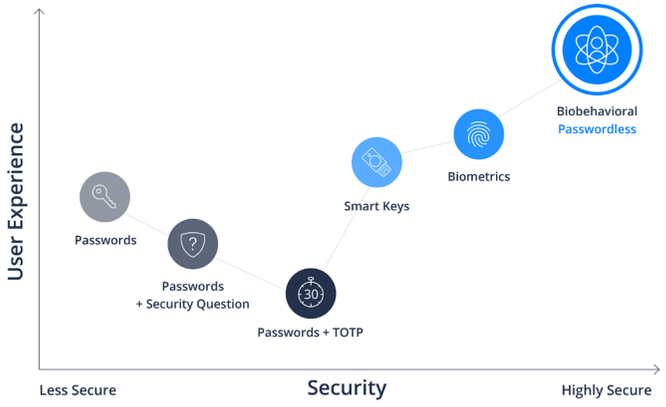
MFA methods all have different trade-offs. Each enterprise MFA option will score differently across these areas:

- **Level of Security**
- **User Experience**
- **Cost of Deployment**
- **Dependence on Phone**
- **Cost of Maintenance**
- **Compliance**
- **Adaptability**
- **Interoperability**

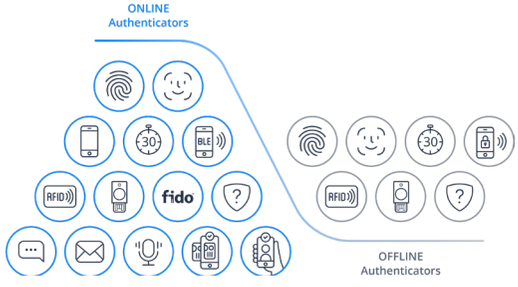
Some methods, like security keys, are not much safer than passwords on their own. Others, like smart keys, or biometrics, provide a more secure and convenient experience at a cost. Time-based one-time passwords (TOTPs) sit somewhere in the middle, depending on the method of delivery; SMS TOTPs are vulnerable to SIM-swapping, while quickly-expiring QR codes can generate a secure and passwordless experience. In our MFA eBook, we evaluate these methods in depth.

75%-81% OF DATA BREACHES OVER THE LAST 5 YEARS ARE DUE TO VULNERABILITIES OF BINARY AUTHENTICATION SUCH AS PASSWORDS AND WEAK 2FAS.1

Acceptto has pioneered an MFA solution that uses a novel type of biometric authentication: your digital behavior. Replicating your long-term pattern of logins and post-login digital maneuvering is a far more difficult breach method than lifting a fingerprint or password. Taking into account the discrete habits, devices and significant events of users, we model their behavior while also continuously monitoring the surrounding environment.



Accordingly, we have coined this idea biobehavioral®. We create a unique representation of the human user for precise identification, which is nearly impossible for attackers to mimic or to cover their tracks by interfering with legitimate data. Our patented biobehavioral approach still allows for the use of the many MFA methods listed below, meaning that it can accommodate user preferences.



This solution generates minimal friction and fatigue, as it doesn't ask users to do anything except act like themselves. It eschews the need for passwords or the "something you know" factor by making "something you have" and "something you are" the two factors of choice, integrated into one seamless user experience. By doing so, we maintain superior security because the factors cannot be easily replicated or seized by attackers. The high security of biobehavioral authentication combined with the ability to personalize configuration enables this method to meet many compliance standards, and quickly adapt for the future.

Case Studies

Healthcare

Acceptto helps healthcare organizations secure patient data by protecting EHR systems and healthcare software.

Protect EHR Applications

Acceptto's highly interoperable solution works with your electronic health record (EHR) systems in order to protect access to patient data and streamline authentication for healthcare professionals.

Safeguard Patient Health Information

Acceptto's Intelligent MFA mitigates risk by delivering a continuous, risk-based step-up authentication that meets Health Insurance Portability and Accountability Act (HIPAA) guidelines associated with remote access to systems containing patient data.

Before Acceptto

Challenges

- Past MFA solution was **not being adopted** due to number of times a day the users needed to authenticate with it (approximately **8 times/day**)
- Changing and remembering 15-character password every 90 days caused **productivity issues for end-users**, since they kept getting locked out and couldn't do their job

Costs

- **$700K a year increase in helpdesk cost** due to current MFA issues
- **35% increase in helpdesk** calls for locked accounts and password related inquiries
- **15% reduction in productivity** of knowledge workers due to increase in friction

With Acceptto

Solution

- Implemented Acceptto's Passwordless technology for laptop/desktop users to **eliminate the need for 15-character passwords**
- Deployed Acceptto's Intelligent MFA with risk engine to provide continuous authentication that requires **authentication once a day, with no password**

Benefit

- **Saving $700K in helpdesk cost** since implementing frictionless MFA
- Helpdesk calls related to password and lock accounts **reduced from 35% to 3%**
- Resources allocated to helpdesk was **transferred to more mission critical projects** within IT

Financial Services

Acceptto verifies and secures user identities, checks device health, and continuously authenticates users throughout all online transactions to keep financial data safe.

Multi-Factor Authentication

Acceptto's Intelligent MFA delivers maximum security and a frictionless user experience by offering a multitude of login options via our mobile app, It'sMe™. Plus, Acceptto also supports offline users integrating apps to protect hybrid environments, remote access VPNs, SSO and more.

Risk-based Step-up Authentication

Acceptto's solution lets you set policies to block access attempts based on an individual or group, geolocation, network type and device security. Enforce stricter login controls for unmanaged, personally-owned devices used by third-party service providers. Require encryption or enabled passcodes, and block access by devices without enabled security controls.

Device Visibility & Policies

To support BYOD (Bring Your Own Device) systems, Acceptto provides greater device insight without an intrusive agent. Gain visibility into all user devices, including corporate and personal devices. Detect devices running out-of-date software, and identify endpoints that are jailbroken, unencrypted and more with our real-time reports and analytics.

Before Acceptto

Challenges

- **30% increase in end-point attacks** in stealing password credential using spear-phishing tactics
- 15-character strong password implementation **too difficult for users** to manage
- Adding MFA to fix password issue forced users to authenticate about **7-10x/day**

Costs

- **$500K a year** in additional costs to fix/recover users credential stuffing attacks
- **$1M a year** in helpdesk support to handle password/lock account issues
- **20% additional yearly operation and infrastructure cost** to manage multiple MFA solutions

With Acceptto

Solution

- Leveraging Acceptto's on-boarding and account creation **reduced user registration process from 15 steps to 3**
- **Eliminated the need for lengthy passwords** by implementing Acceptto's Passwordless technology with existing mobile app
- Implemented Acceptto's risk engine, **reducing ATO to .02%**

Benefit

- Reduced credential stuffing from 30% to 1% that resulted in **$450K a year in saving.**
- **$1M in annual saving** due to eliminating helpdesk call for locked accounts and password reset
- Consolidated all MFA/password siloed solution into one platform, **reducing operation cost by 15%.**

20M+
Users

20
Patents

98%+
Eliminated Account Takeovers

3M+
Daily Secured Authentications

Acceptto Solutions

Intelligent Multi-Factor Authentication
Employees hate using passwords as much as you hate managing password vulnerabilities. More passwords and tokens lead to greater security risk, fatigue, and cost. It's time to get rid of them for good.

Zero Trust Identity (CIAM)
You need to know that your customers are who they say they are; customers do not want to jump through hoops to prove it and they want you to keep their credentials safe.

Device Trust
Acceptto Device Trust solution enables passwordless Desktop SSO for Windows and Mac workstations and measures the security hygiene of devices, tracks who is accessing which company applications, and eliminates costly helpdesk support calls.

FIDO Solution
FIDO Certified program provides assurance of product compliance to roll out FIDO Authentication using Acceptto's enterprise identity authentication security solution.

Why Acceptto

Enable Frictionless Productivity
By using context and behavior-aware risk-based analysis, Acceptto facilitates a frictionless and secure authentication experience for legitimate users and a step-up authentication for suspicious login attempts. We proactively eliminate fatigue while meeting the objectives of IT Operation and Risk Mitigation.

Correlate Audit Logs & Threat Intel in Real-time
Acceptto eliminates the reliance on weak and outdated controls by incorporating multi-modal telemetry into our solution. We utilize contextual, behavior-based credentials that are virtually impossible to replicate, tamper with, or spoof.

Eliminate Account Takeover (ATO)
Acceptto renders credential stuffing benign using passwordless risk-based authentication. Our services drastically reduce the attack surface and eliminate ATO.

Dramatically Reduce Cost of Operations
By eliminating the need for passwords, we significantly reduce help-desk costs, like password resets, governance and compliance, audits, and password tool managers.

Orchestrate Dynamic Authentication
Acceptto offers a powerful but simple set of configurable policies that drive dynamic risk-based scoring of authentication requirements. This, in turn, adapts to user behavior, attributes, and the ecosystem of associated devices and resources.

Integrate and Scale Efficiently
Acceptto provides an out-of-the-box solution for all enterprise cloud or on-premise applications, certified WebAuthn FIDO servers, Mobile SDKs, and REST APIs for scale, extensibility, and visibility into the IT ecosystem. We integrate across web, mobile, cloud, or IoT applications.

About Acceptto

Acceptto secures all your devices, enterprise applications, and credentials, to you.

We are the winner of a number of awards including the **4 Cybersecurity Excellence Awards 2020** and prestigious 2019 SINET 16 Innovator Award. Our expertise and trailblazing perspectives on cybersecurity have been featured in publications like TechRadar, Security Magazine, and digimonica.

Headquartered in Portland, USA with offices in Lisbon, Portugal, and Vancouver, Canada, serving global active customers in healthcare, education, and financial services.

www.Acceptto.com Sales@Acceptto.com @AcceptoCorp Acceptto Corporation