Acceptto

Multi-Factor Authentication Beyond Binary Authentication

– by Shahrokh Shahidzadeh, CEO, Acceptto –

It is beyond imagination to understand that we are still having discussions about passwords and their implicit vulnerabilities in 2019. With over 2 billion identified as having passwords stolen out of the 4.2 billion people globally with access to the internet, it boggles the mind that people still use simple passwords like "password" and expect to be secure.

CISOs and CSOs can no longer rely on traditional identity authentication processes to protect their companies or employees. Unfortunately, not all identity authentication processes are built the same and most suffer from one chronic pain point and that is the reliance on binary authentication. For example, two-factor security is temporal, causes high friction and can be easily intercepted during transmission. Current multi-factor authentication (MFA) security lacks context and relies on too few attributes. And, there are few, if any, solutions that continuously validate your identity post-authentication.

Multi-factor authentication is just what it sounds like. Unfortunately, MFA solutions impose significant friction through a variety of temporal (e.g., OTP, captchas, reset links) and other binary controls that have all still proven ineffective safeguards against techniques such as credential stuffing, SIM swap, and identity spoofing. There has to be a better way to authenticate based on individual characteristics that cannot be easily imitated.

The way forward? Continuous authentication based on artificial intelligence, machine learning and behavior modeling. With this type of technology layered on to an existing MFA, the authentication factor becomes extremely secure. And it's so easy that it gets rid of the hassle often associated with MFA.

Here is quick checklist:

Copyright © 2019 Acceptto Corporation. All rights reserved.

1. Understand Your Requirements for Next 3 Years

Ensure that you understand the technical and business needs of your organizations and its users for today up to 3 years from now. Is it an IAM or CIAM or both that you need a fix for? Do you need an MFA for cloud apps, local on-premise line of business apps, are workstations in the play, do you care about compliance, etc. are all questions you need to ask, tabulate and score when you start on your journey to select your Next Generation Authentication solution.

2. Execute for now and plan for flexibility in the future

Key in selecting the right solution is not to be too tactical and short-sighted when selecting your MFA solution. If it was just doing what everyone does and search for top mainstream solutions that probably got developed a decade ago or more then you need to ask if these solutions are effective and have, they prevented the billions of breached records.

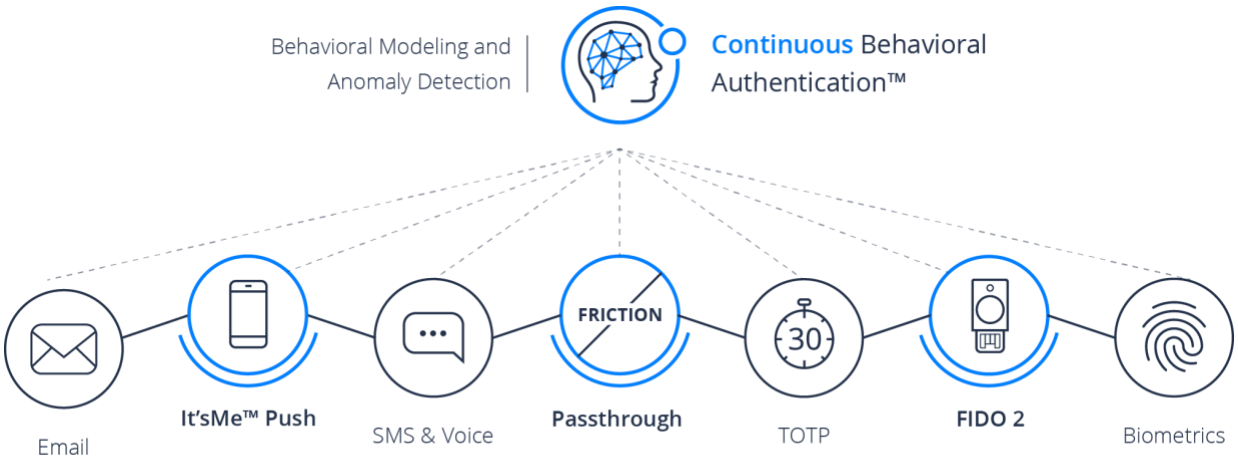
Your selection should address immediate needs, but more importantly needs to include paths to modern modular technologies that will support all your future needs. This means a solution that supports a) IAM and CIAM needs b) If offered On-premise, Cloud or Hybrid c) Cover all three vectors of mobile, web and workstations d) Allows for interoperability.

Copyright © 2019 Acceptto Corporation. All rights reserved.

3. Configurable Smart Out of Band Delivery

It is key to recognize that the delivery method of Out of Band (OOB) is safe for the login/transaction of interest. You all know that even NIST has called SMS as not safe but yet majority use SMS for a convenient 2FA. Well, the key here is can your MFA engine detect when one method of OOB (e.g. SMS) is safe and when it is not use alternatives to secure the access.

Most MFA solutions rely on an integrated or discrete mobile app authentication method. The options of Push, QR, One Time Passwords like SMS or Voice or email token, or time-based one-time password (TOTP), Hardware based tokens, FIDO, etc, are all great and have what might fit your needs but remember that your authentication needs may change. Look for the solution that covers all channels and is configurable based on policy all the way at the individual user level. There will be always a user who does not want to use their phone…

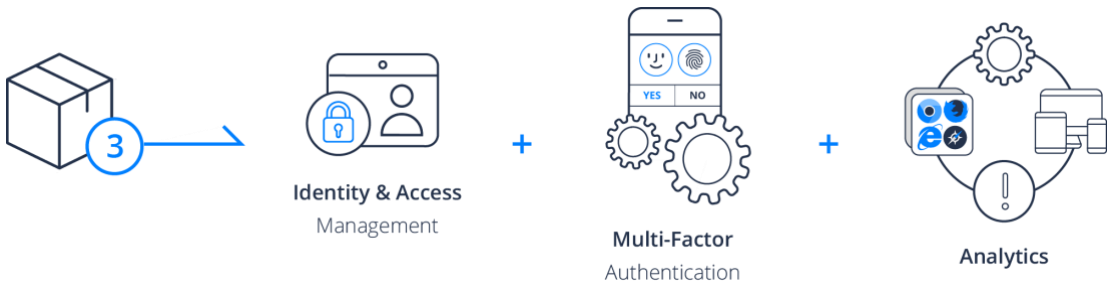


Configurable Smart Out Of Band Delivery

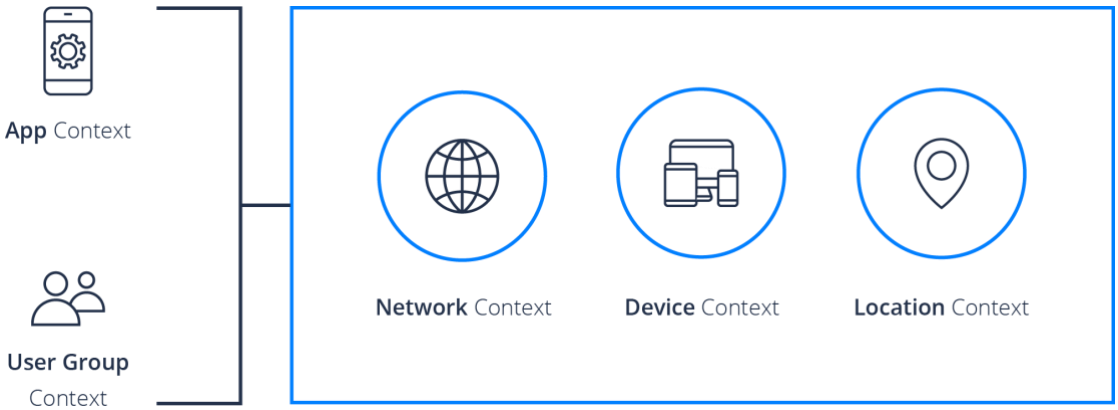
Copyright © 2019 Acceptto Corporation. All rights reserved.

Multi-Factor Authentication Beyond Binary Authentication

4. Three in a box IAM + MFA + Analytics vs. discrete solutions



You need to make one final decision and that is if your strategy on how to integrate it all. Ideally you want an IAM solution that offers state of the art MFA and delivers Analytics and Compliance, all tied together under one console. Pick vendors that offer a modular stack, an IAM solution that includes integrated MFA and options for analytics and compliance management that is bolted-on or can be integrated using 3rd party solutions. This simplifies managing IAM, MFA, Analytics and Compliance all from one console/viewpoint.

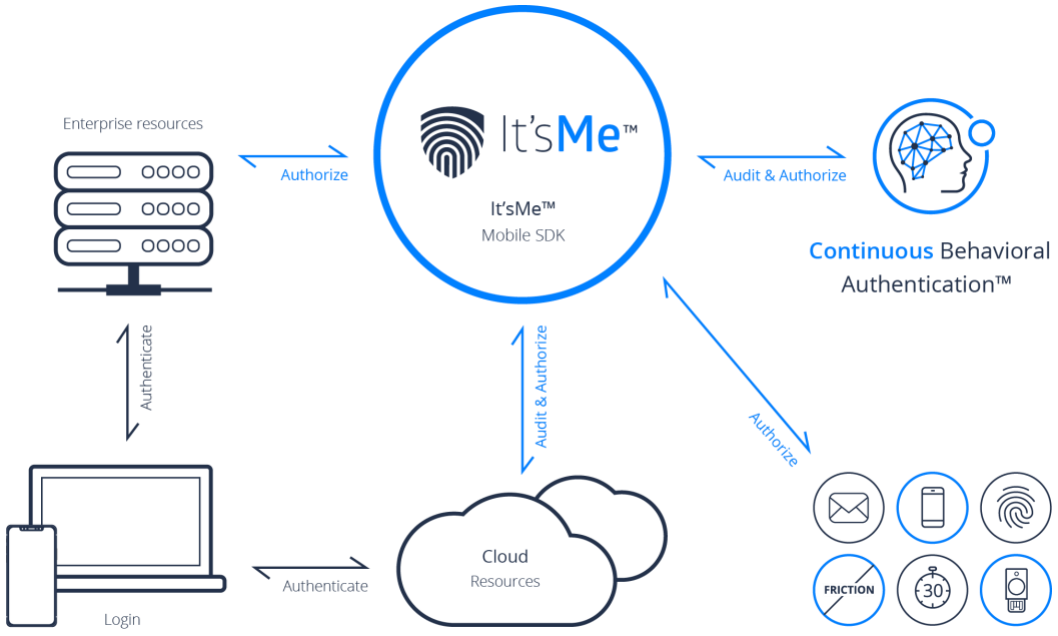


Copyright © 2019 Acceptto Corporation. All rights reserved.

Multi-Factor Authentication Beyond Binary Authentication

5. Consider Next Generation Authentication: Continuous Behavioral Authentication

Investing in a continuous authentication technique is the way forward. Companies and end-users that are relying solely on binary authentication tactics such as two-factor authentication (2FA) or (MFA) need to understand that these solutions are static and stored somewhere, waiting to be compromised time and time again. The best way to avoid a syndicated cyberattack or breach is to assume all credentials, even those yet to be created, have been compromised. Then, it is important to proactively instill a technology solution that continuously monitors authentication and employs modern artificial intelligence and machine learning techniques, along with behavioral modeling. By doing so, cyber attackers do not stand a chance because nobody can mimic your innate behaviors, thus making your identity immutable, and data inaccessible.



Ready to get started with next generation authentication?

Email us for a free consultation and demo: info@acceptto.com or learn more at www.Acceptto.com

Copyright © 2019 Acceptto Corporation. All rights reserved.