10 Reasons Why You Need Adaptive Authentication Over 2FA

passwords cause 80 percent of data breaches, it's clear that passwords alone won't protect your business.

When poor

access and attributes.

Two-factor authentication (2FA) is a great starting point, but a one-size-fits-all approach doesn't work when users have different behavior, devices, levels of

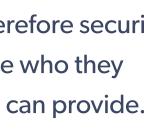


is everything Employees need a simple user experience to access work. Otherwise they'll lose productivity. 2FA provides the same experience to everyone – both legitimate and fraudulent requests.



User experience

Push notifications aren't enough Cyberthreats are increasing in sophistication, and therefore security must, too. Organizations need full assurance users are who they claim to be – more assurance than a push notification can provide.



43 Authentication solutions must integrate

There are a variety of apps, users and devices in use throughout the business. Authentication solutions need to integrate with all of them, so you have streamlined visibility into user activity and logins.

#4 Flexibility is crucial

The more authentication factors you have – from standard push to

biometrics – the more flexibility you have to manage authentication



in the way that suits your business the best.



granular control,

you have no control

Authentication works to ensure users are who

they say they are. You need to be able to

manage who is authenticated, from where

and when, at the organization, group

and individual level.

Without

2FA doesn't offer enough insight 2FA provides a second factor, but you need to know exactly who is accessing what

users have the right access.



H7 Biometrics can't be replicated What better way to ensure users are who they are than by leveraging what they are? 2FA factors such as a TOTP can be replicated, whereas a fingerprint, voice or face is unique to the individual alone.

To be fully certain of a user's legitimacy, you need more context than a username and password. Location, IP address and device are all critical components in ensuring the validity of a request.

Context drivesauthentication



adapt with the context of the request to offer the appropriate authentication, without adding any complexity.

#9 2FA can't adapt with your users

No two users are the same. That's why authentication needs to

#10 A one-size-fits-all authentication doesn't work anymore

factors, without increasing the friction of the login experience.

www.lastpass.com/solutions/authentication

Intelligent authentication doesn't need to be complex. With adaptive

authentication, you can prove a user's identity with a combination of

Learn more about adaptive authentication:

©2019 LogMeIn, Inc. All rights reserved.