10 Reasons Why You Need Adaptive Authentication Over 2FA

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

Ten reasons adaptive authentication is a smart solution:

#1 User experience is everything
Employees expect simple user experience in every aspect of business, even access. Granular control should be a user experience to everyone. Too much technical jargon leads to frustration.

#2 Push notifications aren’t enough
Cybersecurity is increasing in sophistication, and therefore security must, too. Organizations need multifactor authentication strategies to include push codes – too many errors in a push notification could provide a path for a hacker.

#3 Flexibility is crucial
There isn’t a one-size-fits-all approach to security. Authentication solutions must meet your needs. Without context, you have no control.

#4 User experience 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.

#5 Without granular control, you have no control
Authentication solutions must enable you to control access and ensure only the right users have the right access. Without granular control, you have no control.

#6 Biometrics can’t be replicated
No two humans have the same fingerprints, iris or facial feature. If biometrics are replicated, they can’t be leveraged to authenticate users to sensitive resources.

#7 Context drives authentication
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.

#8 2FA doesn’t offer enough insight
While 2FA can provide two-factor authentication, it doesn’t go far enough. A one-size-fits-all 2FA solution isn’t sufficient. It’s too basic to detect advanced threats.

#9 2FA can’t adapt with your users
No two users are the same. That’s why authentication needs to adapt with the context of the request to offer the appropriate authentication, without adding any complexity.

#10 A one-size-fits-all authentication doesn’t work anymore
Intelligent authentication doesn’t need to be complex. With adaptive authentication, you can automatically change the level of authentication based on the needs of the situation and user context.

Learn more about adaptive authentication: www.lastpass.com/solutions/authentication