Auth0

Secure and Seamless User Experience with Auth0's Adaptive MFA

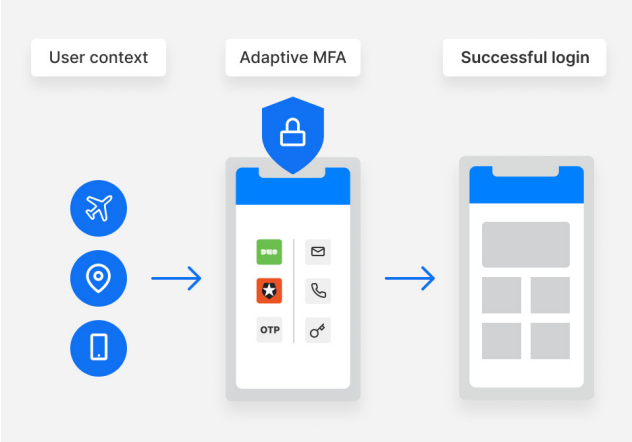
Account hacking is one of the most common security threats that users encounter in cyberspace, with over 80% of data breaches involving the use of lost or stolen credentials, according to Verizon's 2020 Data Breach Investigations Report. However, a 2020 IBM-Poneman report found that multi-factor authentication (MFA), which can block 99.9% of account hacking attacks, was required for only 35% of respondents.

According to the same report, the average cost of a cyberattack for US companies in 2020 is $8.64 million — up from $3.53 million in 2006. This is an increase of 245%. As the world increasingly moves online, these attacks only increase in velocity, intensity, and potential for damage. If MFA is so effective, why is adoption so low?

One oft-cited explanation is that MFA adds friction to the login process. Traditional MFA is incredibly effective in preventing attacks, but it comes with a usability cost, since it requires additional steps that a user must complete in order to continue with the interaction. Auth0's adaptive MFA is only engaged when a user interaction is deemed risky based on behavioral data. This approach preserves the frictionless experience for the majority of users.

How it Works

BAs opposed to traditional MFA, which is triggered by every interaction, adaptive MFA is only activated when behavior indicates that an authentication action does not conform to the typical patterns for a particular user.



An overall risk score is generated by measuring risk in three dimensions:

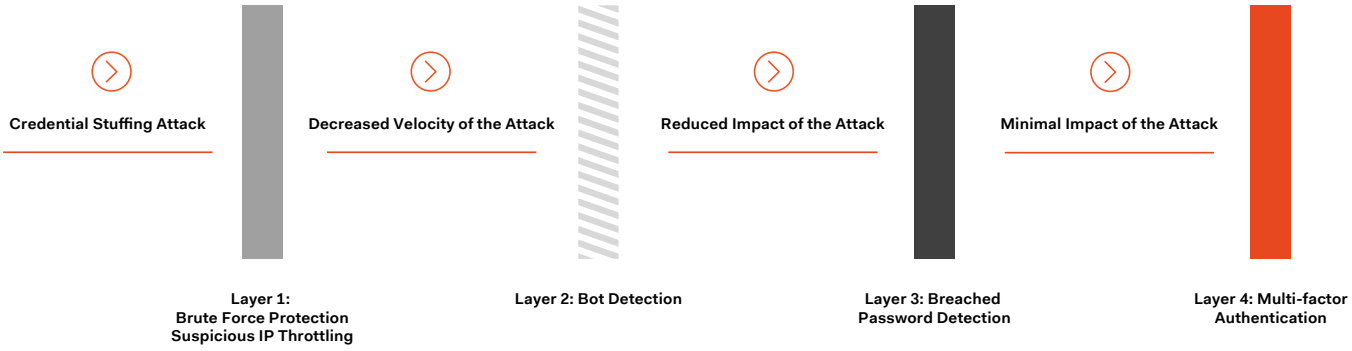
- **Known device:** What type of device is typically used in this interaction?
- **Impossible travel:** Where is this user typically located?
- **IP reputation:** Is the IP address in use associated with past risky behavior?

For example, a user normally signs into their account from Bellevue, Washington, at 9 a.m., from a Windows computer. An adaptive MFA system would only present a second factor challenge to that user when there is a login from outside the vicinity of Bellevue, or at night, or from a Mac computer, depending on how much weight is given to each signal in defining risk.

Layers of Protection

Since automated attacks come in all forms, there is no singularly effective approach to security. This is why Auth0 has developed multiple security controls that are layered together to create a secure framework to combat automated attacks.

Correlating multiple risk signals and layering multiple security controls is an effective way to prevent these bot-driven attacks from wreaking havoc on your business.



Bot Detection

Powered by a collection of risk signals and assessors that identify indications of suspicious activity, Bot Detection comes into play prior to login to identify bad actors before a suspicious login event occurs.

Breached Password Detection

Auth0 maintains a large, continuously growing database of login credentials known to have been compromised in data breaches. Breached Password Detection allows customers to check all their logins against this database and identify users who are logging in with compromised credentials.

Brute Force Protection & Suspicious IP Throttling

Brute Force Protection and Suspicious IP Throttling. defend against velocity attacks in which multiple attempts have been made to access accounts. They are configurable rate-limiting features that are triggered once a particular threshold is reached. efends against velocity attacks in which multiple attempts have been made to access accounts. It is a configurable rate-limiting feature that is triggered once a particular threshold is reached.

Multi-factor Authentication

Multi-factor authentication (MFA) is a method of verifying a user's identity by requiring them to provide more than one piece of identifying information. In order to circumvent MFA, bad actors not only need access to the breached credentials but also the device being used for the second factor. This drastically increases the time and effort needed to hijack accounts and makes account takeover at scale an insurmountable challenge. Adaptive MFA makes your user data more secure without creating friction that could discourage your users from adopting MFA.

A layered approach to authentication is the most effective defense against identity attacks. Auth0's adaptive MFA is a powerful layer of protection that allows you to maintain a strong security posture while still delivering frictionless authentication for most users.

Auth0

auth0.com
sales@auth0.com
+1 (888) 235-2699