Multi-Factor Authentication

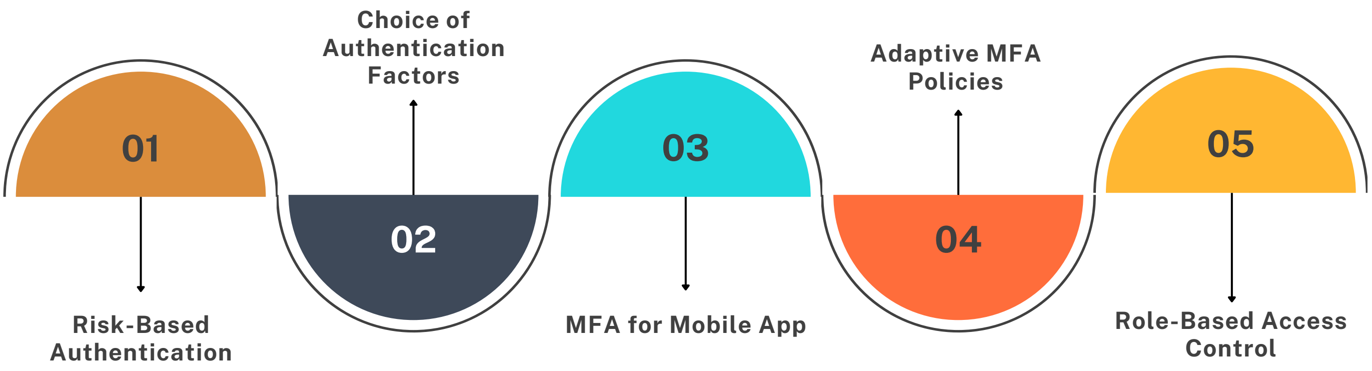
Why MFA?

In 2020, cybercrime cost the world over $1 trillion, 37% of organizations were affected by ransomware attacks, and 61% were affected by malware attacks.

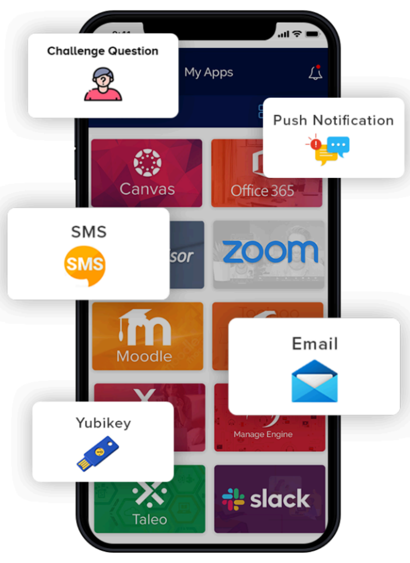
What is MFA?

Multi-Factor authentication (MFA) is a security mechanism that requires users to provide two or more forms of identification before granting access to a system or application. MFA is a more secure authentication method than traditional username and password because it adds an extra layer of security to verify the identity of the user.

QuickLaunch MFA Capabilities



01
Risk-Based Authentication
02
Choice of Authentication Factors
03
MFA for Mobile App
04
Adaptive MFA Policies
05
Role-Based Access Control



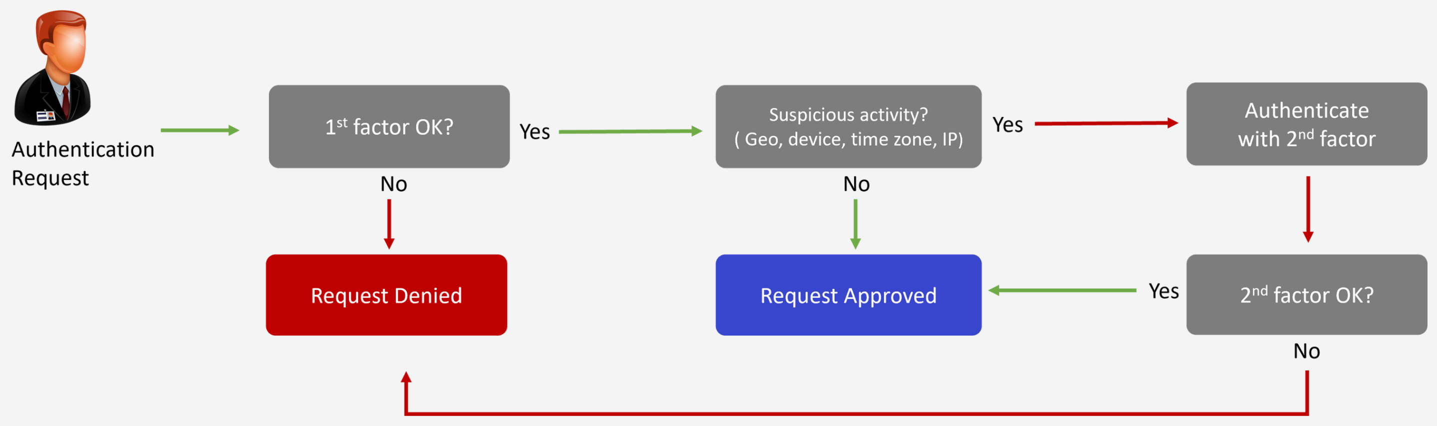
Multiple Authentication Factors

With support for various authentication factors, QuickLaunch provides both businesses and users with the flexibility to choose the authentication method that suits their needs best.

Types of Authentication factors:

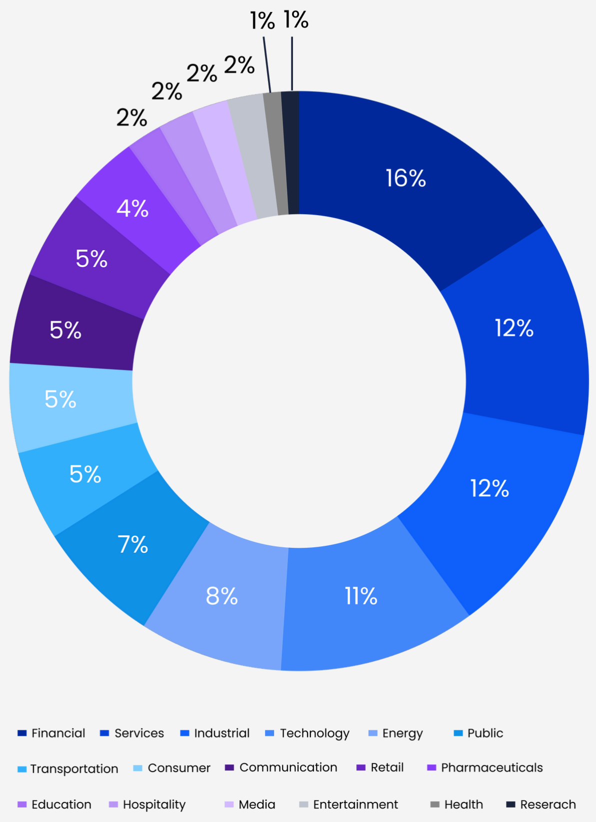
- ✓ Security Questions
- ✓ Email OTP
- ✓ Phone OTP
- ✓ Google Authenticator
- ✓ Yubikey
- ✓ Mobile Push
- ✓ Microsoft Authenticator
- ✓ Face ID/Touch ID

How Risk-Based MFA Works?

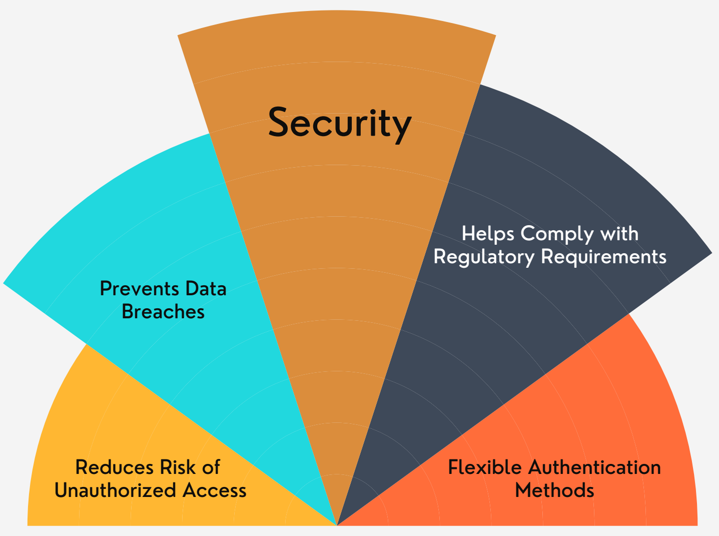


Industry-Wise Cost of Data Breaches

Distribution of Sample by Industry



WITH MFA RESULTS



Security
Helps Comply with Regulatory Requirements
Prevents Data Breaches
Reduces Risk of Unauthorized Access
Flexible Authentication Methods

Quicklaunch™
identity & integration

WWW.QUICKLAUNCH.IO