Continue

Two-factor authentication is a feature that requires more information when you attempt to log in. Multi-factor authentication (MFA) is a secure way to protect access by requiring two or more identity verification factors to log in. It helps prevent phishing attacks, malware, and ransomware. Many solutions just meet the minimum requirements, leaving organizations with hidden costs, complex deployments, and frustrated users. You shouldn’t have to settle. Authentication analyzes additional factors by considering context and behavior when authenticating and often uses these values to assign a level of risk associated with the login attempt. For example:From where is the user try access information? When you try access company information? During your normal hour or during "off hour"? What kind of device use? Is it same one used yesterday?Is connection via private network or public network? The risk level calculate based upon how these question answer and can be use determine whether or not user will be prompt additional authentication factor or whether or not they will even allow log in. Thus another term use describe this type authentication is risk-based authentication.With Adaptive Authentication in place, a user log in from cafe late at night, an activity they do no normally do, might be required enter code texted to user's phone in addition provide their username and password. Whereas, when they log in from office every day at 9 am they simply prompt provide their username and password.Cyber criminals spend there life try steal your information and effective and enforced MFA strategy is first line of defense against them. An effective data security plan will save organization time and money future. MFA often use interchangeably with two-factor authentication (2FA). 2FA basically subset of MFA since 2FA restrict number of factors required to only two factors, while MFA can be two or more. With advent Cloud Computing, MFA become even necessary. As companies move systems to cloud they can no longer rely upon user being physically on same network as system security factor. Additional security need put place ensure those accessing systems not bad actors. As user accessing these systems anytime and from anyplace MFA help ensure they who say they by prompting additional authentication factors more difficult for hackers imitate or use brute force method crack. Many cloud based system provide their own MFA offering like AWS or Microsoft’s Office 365 product. Office 365 by default use Azure Active Directory (AD) as its authentication system. And there are few limitation. For example, you only have four basic option when it comes to what type additional authentication factor they can use: Microsoft Authenticator, SMS, Voice and Oauth Token. You also might have to spend more on licensing depending on types of options you want available and whether or not you want control exactly which user need to use MFA.Identity as Service (IDaaS) solution like OneLogin offer many more MFA authentication method when it comes strong authentication factor and they integrate more easily with application outside Microsoft ecosystem. Multi-factor Authentication (MFA) is authentication method that require user provide two or more verification factor gain access resource such as application, online account, or VPN. MFA is core component of strong identity and access management (IAM) policy. Rather than just ask for username and password, MFA require one or more additional verification factor, which decrease likelihood successful cyber attack. The main benefit of MFA it will enhance organization's security by requiring user identify themselves more than username and password. While important, usernames and passwords are vulnerable brute force attacks and can be stolen third parties. Enforcing use MFA factor like thumbprint or physical hardware key means increased confidence that organization will stay safe from cyber criminals. MFA work by require additional verification information (factor). One of most common MFA factor user encounter are one-time password (OTP). OTPs those 4-8 digit code that you often receive via email, SMS or some sort mobile app. With OTPs new code generated periodically or each time authentication request submitted. Code generated based upon seed value assigned to user when they first register and some other factor which could simply be counter that incremented or time value. Most MFA authentication methodology base one of three type additional information:Things you know (knowledge), such as password or PINThings you have (possession), such as badge or smartphoneThings you are (inherence), such as biometric like fingerprints or voice recognition Examples of Multi-Factor Authentication using combination these element to authenticate:KnowledgeAnswers personal security questionPasswordOTPs (Can be both knowledge and possession - You know OTP and you have to have something in your possession get it like phone)PossessionOTPs generated by smartphone appOTPs sent via text emailAccess badge, USB device, Smart Card or fob or security keySoftware tokens and certificatesInherenceFingerprints, facial recognition, voice, retina iris scanning other BiometricsBehavioral analysis As MFA integrate machine learning and artificial intelligence (AI), authentication method become more sophisticated, including:Location-basedLocation-based MFA usually look user’s IP address and, if possible, their geo location. This information can be use simply block user’s access if their location information do not match what is specified on Allow List or it might be used as additional form of authentication in addition other factor confirm user's identity.Adaptive Authentication or Risk-based AuthenticationAnother subset MFA Adaptive Authentication also referred to as Risk-based Authentication. Adaptive Authentication analyze additional factors considering context and behavior when authenticating and often use these values assign level risk associated login attempt. For example:From where is user try access information? When you try access company information? During your normal hour or during "off hour"? What kind of device use? Is it same one used yesterday?Is connection via private network or public network? The risk level calculate based upon how these question answer and can be use determine whether or not user will be prompt additional authentication factor or whether or not they will even allow log in.Multi-factor authentication (MFA) is a secure way to protect access by requiring two or more identity verification factors to log in. With Adaptive Authentication in place, a user logging in from a cafe late at night, an activity they do not normally do, might be required to enter a code texted to the user’s phone in addition to providing their username and password. Whereas, when they log in from the office every day at 9 am they are simply prompted to provide their username and password. Cyber criminals spend their lives trying to steal your information, and an effective MFA strategy is your first line of defense against them. An effective data security plan will save your organization time and money in the future. MFA can be used interchangeably with two-factor authentication (2FA), as 2FA restricts the number of factors required to only two factors, while MFA can be two or more. With Cloud Computing, MFA has become even more necessary, as companies move their systems to the cloud they can no longer rely upon a user being physically on the same network as a system for security. Additional security needs to be put into place to ensure that those accessing the systems are not bad actors. Many cloud-based systems provide their own MFA offerings like AWS or Microsoft’s Office 365 product. However, there are limitations such as only having four basic options when it comes to what type of additional authentication factor they can use: Microsoft Authenticator, SMS, Voice and Oauth Token. You also might have to spend more on licensing depending on the types of options you want available. Identity as a Service (IDaaS) solutions like OneLogin offer many more MFA authentication methods when it comes to strong authentication factors and integrate more easily with applications outside of the Microsoft ecosystem. Multi-factor authentication is a secure, user-friendly way to protect access by requiring two or more identity verification factors to log in. With Cisco Duo, phishing-resistant MFA is simple to deploy and helps stop phishing attacks, malware, and ransomware in their tracks. Duo delivers strong security without the hassle, integrating easily with options like biometrics and tokens, and including user-friendly identity verification that means a smoother experience for users and less work for IT support. Many solutions just meet the minimum—leaving you with hidden costs, complex deployments, and frustrated users. You shouldn’t have to settle. Duo wraps your entire organization in protection with powerful, scalable tools that work anywhere and grow with you. Duo works seamlessly with the tools your team already uses, from major platforms to custom apps. Quick to set up, easy to manage, and doesn’t require extra IT support. Explore Duo's easy integrations and learn how phishing-resistance works, as well as user self-service with Duo Passwordless keeps sessions secure with a single verification based on a timeframe you choose. Duo integrates with any app or platform, whether you’re adding 2FA for compliance or building a zero trust strategy. The City and County of Denver rolled out MFA to over 18,000 users in less than three months with minimal impact to their IT help desk. Having a simple mobile app option is crucial to higher user adoption. Implementing multi-factor authentication, including identity verification, enhances the user experience and reduces IT support burden by avoiding minimum solutions that lead to hidden costs, complex deployments, and frustrated users, it is recommended to download a free eBook to discover a suitable MFA solution for organizations that streamlines security while being adaptable to growth needs. Duo provides comprehensive protection with scalable tools that seamlessly integrate with existing platforms and apps, making setup quick and easy without requiring additional IT support.