WHY MFA?

MFA (multi-factor authentication) is becoming ever-present. If you've been prompted with a push notification on your phone after you've tried logging into a different application, you've experienced it.

MFA requires users to provide an additional factor to verify their identity aside from entering a password — such as a code generated by a hardware token, a one-time email password (OTP), or a biometric identifier (like Apple's Touch ID).

WHAT'S BEHIND THE PERVASIVENESS OF MFA? THERE ARE SEVERAL REASONS FOR MFA'S UBIQUITY IN TODAY'S CORPORATE WORLD.

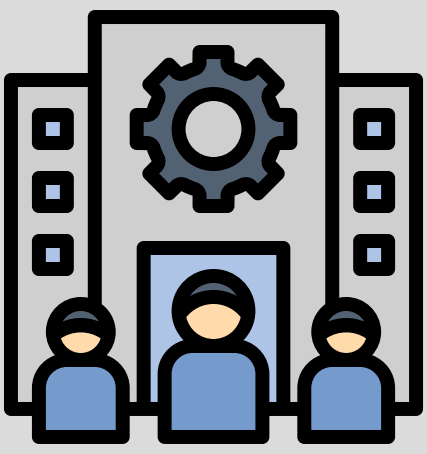
MFA ENABLES STRONGER AUTHENTICATION

Risk reduction is critical for organizations, which is why MFA is growing exponentially. In a world where credential harvesting is a constant threat and over 80% of hacking-related breaches are caused by stolen or weak passwords, this kind of bulletproof authentication solution is essential.

With MFA, it's no longer about granting access based on traditional usernames and passwords; it's about granting access based on multiple weighted factors, reducing the risks of compromised passwords. It adds another layer of protection from the kinds of damaging attacks that cost organizations millions.

This was particularly important for a pharmaceutical company like Allergan, which handles sensitive patient data. When Allergan onboarded both doctors and patients into their system with individual Allergan accounts, they implemented MFA to add another layer of protection. A security breach caused by a weak user password would understandably have huge consequences for both the company and the customers who trust it.

MFA ADAPTS TO THE CHANGING WORKPLACE



As the workplace changes and more employees work outside the office, companies require more advanced MFA solutions to manage more complex access requests. Enter Adaptive MFA. Where multi-factor authentication offers multiple layers of protection, adaptive multi-factor authentication evaluates the risk a user presents whenever he or she requests access to a tool or information, looking at details like the user's device and location for context.

For example, an employee logging in from company premises is in a trusted location and may not be prompted for an additional security factor. But if that same employee logs in from a coffee shop, uses her personal mobile phone to check work emails, or connects over an unsecured WiFi network, she may be prompted to verify an additional factor because she's utilizing an untrusted location, device, or connection.

What's more, adaptive MFA allows for dynamic policy changes and step-up authentication — significant controls in securing critical data. For instance, users may be prompted for a higher assurance second factor (or even a third factor) before obtaining access to deeply sensitive information such as customer data in Salesforce.

MFA OFFERS SECURITY WITHOUT COMPROMISING USER EXPERIENCE

Passwords are a headache to remember — the more users need to remember, the lazier their password habits become. Moreover, it's important to avoid weighing IT teams down with password resets after they've implemented more stringent password policies to protect the company. MFA secures the environment, the people in it, and the devices they're using without requiring cumbersome resets or complicated policies. Organizations can also make it easier for users by providing them with a choice of factors to choose from, or by only requiring additional factors when necessary. And with MFA's simple deployment and management as well as its integration with a broad range of applications, IT teams are freed up and can focus this time on more strategic tasks.

MULTI-FACTOR AUTHENTICATION: A MORE SOPHISTICATED SECURITY LANDSCAPE

Countless organizations have adopted MFA given the realities of today's security landscape and regulations. With compliance standards like GDPR and NIST requiring sophisticated security policies, MFA's presence will only continue to become more widespread. But given its ease of use and the protection it provides, this only stands to benefit employees and IT teams alike.

Davichi