Single Sign-On vs. MFA: Do You Know The Difference?

By Fortified Health Security June 2, 2020

Usernames and passwords are the foundation of user authentication, but these factors are enough to prevent data exposure. As cyber threats become more complex, com through single sign-on and multi-factor authentication. These solutions can strengthen yo

cybersecurity framework without hindering user experience.

What Is Single Sign-On?

Single-sign on (SSO) is a login method in which users have one set of credentials to acces applications. The main benefit of SSO is the streamlined approach. Users can access multi without pausing to enter new credentials.

A common example of SSO is Google's set of applications. With one login, users can acce inbox, calendar, documents, photos, and videos. They can organize a video call and even s through one central login.

There are a few main benefits of SSO. This approach can improve user experience when u and boost workflow when used internally. It's also convenient when users are accessing a multiple devices.

SSO is more centralized, so it can also make it easier for IT departments to monitor user a centralization may also cut down on the number of weak passwords in the network. Hack fewer potential entry points, and the IT team can stop attacks more quickly.

When implementing SSO in your cybersecurity framework, it's important to keep some po in mind. Widespread access through one entry point is one of the main risks of this approa gains entry into an SSO system, they'll have access to all of the applications tied to that log the system is compromised, users won't be able to access any of the associated applicatic accounts to remember and also maintain, it is often a good idea for an organization using strengthen the authentication controls by increasing the number of characters required fo password, increasing complexity requirements, account lockout policies and password reu

This is where multi-factor authentication comes in.

What Is Multi-Factor Authentication?

Since password guessing and login access are among the top causes of cyber at

protection are essential. Multi-factor authentication (MFA) requires users to enter two or m identification factors to access an application. These pieces of information are unique to th challenging to guess or replicate. The MFA approach makes it more difficult for hackers or parties to access sensitive data.

Security experts typically separate MFA credentials into three main categories:

- Something You Know: Factors that a user *knows* can include passwords, security quest numbers. These are private login credentials that are difficult for others to guess, espec they're simply memorized and not stored in an external location.
- Something You Have: This type of factor involves another device or object, like a smart verifying a user. As an example, a user might need to enter a code that they receive as a following their password. Other factors that users might *have* include security badges, apps, or security tokens.
- Something You Are: This group of factors generally includes biometrics. Fingerprints, fa recognition, and voice recognition are common sources of verification. Retina scans ar this group. These factors are often part of high-level security requirements.

When implementing MFA, organizations typically choose two of the above factors. So, a u to enter a password and a Short Message Service (SMS) code. The system might require M login or only when users login on a new device. By doing so, users verify their identity and access the applications. These authentication layers also make it more challenging for hac applications and networks.

SMS codes, security questions, and pin numbers are the most common types of authentic However, these factors can become more complex when users need more security cleara organization might have data that only upper management can access. You might add mo login factors like security tokens and voice recognition to prevent unauthorized access. Bi verification factors go even further, creating exclusive access. It's important that chooses appropriate authentication factors based on the data at risk.

Which Is Best For Cyber Security?

Single sign-on and multi-factor authentication aren't mutually exclusive. In fact, organizat benefit from implementing both at the same time. Doing so improves both user experienc while making it easier to monitor network activity.

These security layers together can stop hackers in their tracks. If a hacker or malicious par gains access to a user's password, this won't be enough to access your system. Chances a have the answers to a user's security questions as well. It's even less likely that they can ac text messages to enter the verification code. This keeps the hacker away from all applicati authorized users can still enjoy the streamlined experience.

When implementing SSO and MFA, it's important to do so in a way that meets your organi cyber security needs. A cyber security consulting firm can work with you to effectively adc loss prevention solutions into your framework. An expert can assess whether SSO makes s users and when MFA is necessary. With the right approach, your organization can balance security and user experience.

Ready to strengthen your cybersecurity framework through MFA and SSO? The team at Fc Security, based in Franklin, TN, offers comprehensive security solutions. With services like testing, vulnerability threat management, data loss prevention, and managed solutions, ou specialists can put together a security strategy based on your organization's needs. We spe healthcare industry, offering HIPAA compliance and medical device solutions as well. Con get started.

CAUSES OF CYBER ATTACKS, CYBER THREATS, CYBERSECURITY FRAMEWORK, DATA EXPOSURE, DATA LOS SOLUTIONS, NETWORK SECURITY

PREVIOUS
Kwampirs Trojan Targets Healthcare Industry

Compliance Scanning – are you overlooking a big part of

HEALTH SECURITY

Fortified Health Security is healthcare's recognized leader in cybersecurity – protecting patient data and reducing ecosystem.

Follow Us

QUICK LINKS

SERVICES

RESOURCES

NEWS & EVENTS

ABOUT

CONTACT

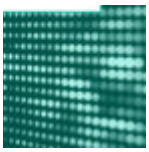
COMPANY ADDRESS

2550 MERIDIAN BLVD., SUITE 190
FRANKLIN, TN 37067

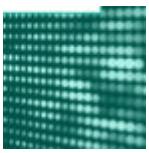
CONNECT@FORTIFIEDHEALTHSECURITY.COM

615-600-4002

LATEST FEATURED NEWS



FORTIFIED HEALTH SECURITY RELEASES 2021 MID-YEAR HORIZON REPORT



MORE LESSONS IN RISK ANALYSIS, HIPAA SECURITY COMPLIANCE IN LATEST...