SANS

Analyst Program

Survey

SANS 2021 Password Management and Two-Factor Authentication Methods Survey

Written by **Chris Dale**

May 2021

yubico

Executive Summary

Using passwords for authentication has been a scourge in the security industry for a long time. Assuredly when passwords were first birthed, they were adequate to secure systems, but with the rapid movement and growth within IT, they have long since been considered inadequate. We developed this SANS survey—the first of its kind—to explore how many passwords users and admins in today's organizations must use to accomplish their work as well as how organizations are managing passwords across users, apps, and devices. As it turns out, many organizations' systems still rely on passwords as the primary method of securing unauthorized access and misuse. In the survey, 38% of respondents indicated that they do not yet use password managers, while 27% have not yet implemented multifactor authentication (MFA). This indicates a growing maturity in organizations' implementation of security controls as it pertains to using passwords to fight cyber threats.

Security controls do not come without sacrifice, and it is imperative for users to understand them and gain user buy-in. In helping users develop safer IT behaviors, executives should be the first ones to implement and convince users that the security controls are necessary and can be used efficiently, rather than slow down current practices. Survey data indicates that 38% of respondents said MFA makes life too difficult for users, 25% believe it's too difficult to implement, and 13% consider it too expensive. If organizations can help users understand the security threats and controls to mitigate them, there is a much higher likelihood of success. When users see the benefits of security controls, and when those controls are practical to use, we can expect more successful outcomes at our organizations.

Here are some of the key findings from the survey:

- **69% of respondents are using MFA, compared with 55% using a password manager**
- **92% of respondents require their password manager to support MFA technologies such as one-time password (OTP) or hardware security key**
- **38% of respondents identified "makes things too difficult for users" as the primary reason organizations either do not use or do not plan to use MFA**
- **33% of respondents chose "negative impact on user productivity/user-friendliness" as the key barriers to using a password manager**

Awareness training will naturally help users prevent compromise of their accounts, but compromise is inevitable. Opportunities for tricking, exploiting, and otherwise getting a user's password will always exist. MFA serves to mitigate this, even if an attacker can compromise the user (via a phishing attack, for example). We raise the bar of thwarting attacks by making applications ask users to present something they have (e.g., a token or access to their smartphone). MFA is not perfect, but it does add more barriers for attackers: 63% of respondents said that they had not experienced a breach on accounts that were protected by MFA.

Vendors and organizations should work together to find easy-to-use solutions that are increasingly difficult for attackers to overcome. Moreover, organizations should consider different measures for different solutions. Systems that are more sensitive could be protected by stricter controls, while less-sensitive systems could benefit from laxer controls. Preferably, organizations should accomplish this without implementing numerous different solutions that require individualized, solution-specific governance and management. Instead, organizations should strive to find a vendor that can meet their requirements with as much ease as possible. Our survey results show that 44% of respondents have implemented discretionary access controls, which we see as an attempt at finding a middle ground between usability and security.

Misuse of passwords can be monitored, detected, and responded to if effective security controls fail. Applications logs should be monitored, allowing for multiple ways to look for breaches. Monitoring, however, is often laborious, because logs must be forwarded and they arrive in a variety of formats, all of which require understanding from the receiving solution. Implementing password and MFA solutions governing an organization's various solutions can help greatly with detecting and responding to account compromises.

Figure 1 provides a snapshot of the demographics for the respondents to the 2021 survey.

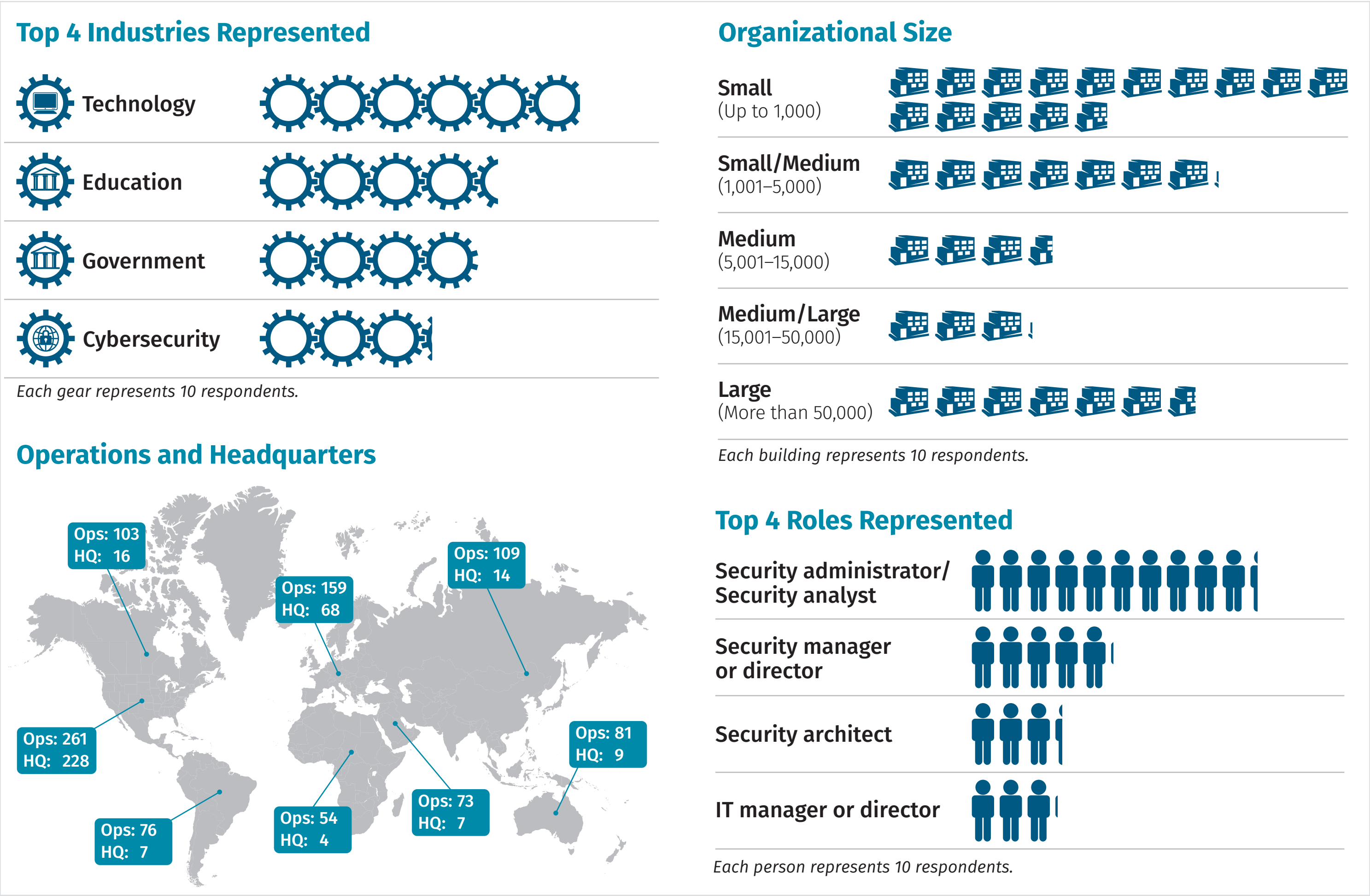

Figure 1. Demographics of SANS 2021 Password Security Survey

Password Managers or MFA?

Passwords are often reused, easily guessed, or otherwise vulnerable to attackers' efforts. Furthermore, users are challenged with creating longer and more complex passwords to remain safe. Password managers make life easier and provide more security. But can organizations (and users) be convinced of such, and can providers prove the return on investment?

With password managers, attackers can still compromise and misuse a password. When single sign-on (SSO) is implemented, one password gives access to even more services that attackers can abuse. MFA helps prevent this, but is it user-friendly enough for users and easy enough to implement at scale?

That begs the question, “Do you choose between a password manager or MFA?” Is it one or the other? The answer is a definitive no! Both security controls strongly support each other while mitigating threats in different areas. Password managers enable users to securely store passwords and keep them unique across services, but passwords could still be compromised in different ways, such as phishing attacks. MFA would help mitigate these types of attack and protect “the keys to the kingdom,” so to speak. In return, password managers would help mitigate attacks where MFA might be compromised. For example, the use of legacy MFA methods, such as SMS or mobile MFA, can be phishable. In this instance, it is harder for attackers to obtain a unique password stored in a password manager, thus protecting the user even when using an MFA solution. However, modern MFA using hardware security keys based on modern authentication protocols are known to be far more secure compared with legacy MFA methods.

Best practices include using both a password manager and MFA to protect services. Organizations must ensure that they do not impose too much on users' ease of use and accessibility of services. Find the best threshold between security and usability, ensuring you let your users know why the measures are in place, so they understand why they are important.

Password Managers: A Safe Instead of “Money in Your Mattress”

More than 39% of the 353 survey respondents characterized their organizations' password solutions being stored without any hashing, thus making them easily readable. Close to half (48%) responded that they do not know of such systems in their organization, while 13% do not know. Overall, this is a chilling result, indicating a lack of auditing, governance, and awareness regarding the storing of passwords.

Respondents indicated that the password manager features that provide them the most security are:

- Unique passwords across different systems (34%)
- Flexible and easy access to passwords (30%)

At SANS, penetration testers come across many organizations using inadequate algorithms for storing passwords. From time to time, we see plain-text passwords being stored (luckily, less frequently than in the past), but very often we see systems not implementing password-storing algorithms and instead using simple, easy-to-crack hashing algorithms.

To make IT services secure and easy to use, a password manager is recommended for most users. The implementation rate of password managers will ensure that organizations give employees the tools and capabilities not only to change their passwords in a quick and efficient manner, but also ensure that the compromise of one service does not automatically compromise other services where the same password is used (in cases where the password manager enforces unique passwords). The survey shows great progress in this field: 55% of respondents indicated that their organization is currently using a password manager to help solve this challenge, with another 22% currently implementing or planning to implement such a solution for their organization. Unfortunately, 23% of respondents currently have no such plans or are unaware of such plans.

The survey also explored how organizations are using password managers. Ensuring unique passwords across applications took the lead (34%), with flexible, easy access coming in second (30%), followed by organizational governance over passwords (23%). Provisioning and deprovisioning access to assets (7%) rounded out the top four closed responses. See Figure 2.

The practice of using shared accounts is frowned upon, because it makes it hard for security teams to determine which users performed what actions. The same concept applies to an organization's governance of its password manager. We must recognize that users cherish ease of use and preferably would use one—and only one—password manager for both enterprise and private accounts. Organizations should try to resist the urge of governing too much and realize the positive effect of a higher adoption rate of password managers. Policies that are too restrictive don't encourage widespread adoption.

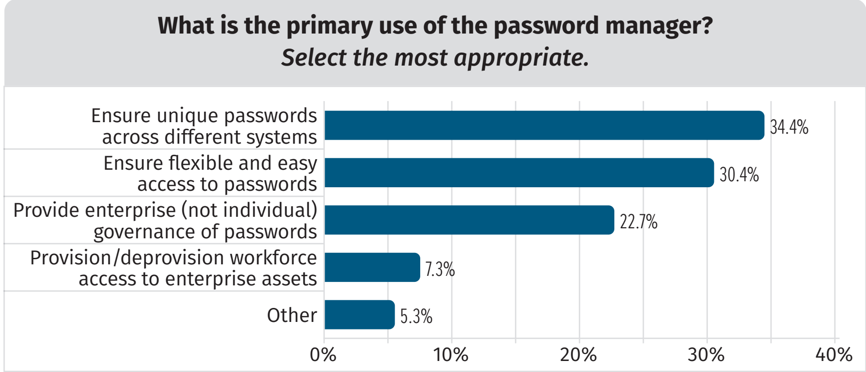
What is the primary use of the password manager?
Select the most appropriate.

Figure 2. Primary Use of Password Manager

In addition to governance, 7% of respondents reported other barriers, including cost and enforcing user adoption/compliance. Use cases and blog posts could undoubtedly alleviate some key adoption barriers, while demonstrating improvements in security, workflows, and efficiency could help justify costs.

Table 1. Barriers to Use

Negative impact on user productivity/user-friendliness	Difficult to manage	Difficult to implement	Costly encryption
32.9%	30.0%	25.8%	13.9%

Unfortunately, users may have a perception that a password manager is an extra hassle and difficult to use. In fact, users might require convincing that having a single place for all passwords is safe. Respondents shared key barriers for not implementing a password manager (see Table 1).

Users demand easy access to applications and services. However, a lost credential on one service should automatically cause other services to be compromised. The concept of SSO shows how these two factors are diametrically opposed. On one hand, SSO enables users to easily reuse credentials across many applications, while on the other hand, it allows attackers to ride on this convenience to exploit multiple services. Every organization must find its threshold of acceptable ease of use and security.

Most respondents (59%) indicated that their password manager limits the need of shared credentials across the enterprise, while 26% indicated that it does not, and another 15% do not know. These numbers lead us to believe that those who cannot limit shared credentials likely have an inherent issue where applications cannot support individual logins from users. See Figure 3.

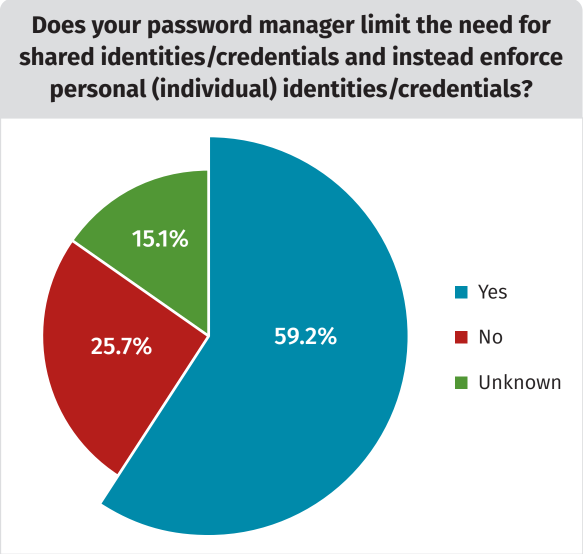
Does your password manager limit the need for shared identities/credentials and instead enforce personal (individual) identities/credentials?

Figure 3. Shared vs. Personal Identities/Credentials

Respondents indicated that user-friendliness is important (30%). So how accessible should the password manager be?

In terms of accessibility, the password manager can be implemented in different ways. Eighteen percent responded that their password manager is integrated into the browser only. This effectively limits applications that are not hosted on a web technology being supported by the web application, but in return greatly supports usability. As a surprise, however, 42% said that they have their password manager as a standalone application, and 41% have it both integrated into their browser and as a standalone application.

Where the password manager should be stored is also a concern addressed in the survey. Nearly half of respondents (49%) indicated that passwords should be highly accessible (that is, available locally and through a cloud solution). This makes passwords highly accessible, but does not necessarily distinguish the difference in the sensitivity of passwords. Some organizations make the password manager accessible only beyond a second barrier, such as a VPN, and not always accessible unless the user wants them to be. In respect to storing passwords in the cloud vs. locally, 28% responded as having local storage only, while 21% indicated cloud storage is acceptable.

Centralizing password management is something that most organizations (62%) are looking to enforce, although 26% indicate this is not a requirement. The remaining 12% are unaware if it is a requirement. Yes, centralization is an important factor, but we must be careful not to make centralization a barrier that discourages users from using password managers for home and private use.

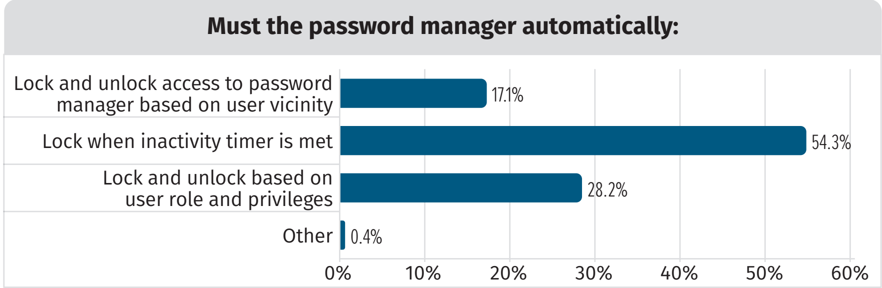

Figure 4. Password Functionality

The password manager exposes a new risk, previously contained by the user's memory and ability to create robust passwords. What if the password manager is compromised? More than half (54%) of respondents require their password manager to automatically lock itself and prevent access after an inactivity timer has been met, while 28% require passwords to automatically unlock based on user roles and privileges, and 17% require the password manager to unlock and provide passwords based on vicinity. See Figure 4.

Access based on vicinity is typically required by users who visit many different systems (e.g., workstations) in a short time and provide the password to unlock automatically. For example, this could be a doctor who visits different patient rooms, where each room has a workstation that must be unlocked. Manually typing in passwords would be cumbersome, while an automatic solution based on proximity/vicinity would potentially make the solution safe enough and user-friendly.

Securing password managers is typically done via yet another password. By far, the majority (92%) of respondents want the password manager to support MFA for added security. Another 6% want biometrics, while another 3% chose "other."

If MFA should be enforced on the password manager, how should users provide their token? The results shown in Figure 5 provide valuable insight.

When asked about their desired state of the password manager, 85% of respondents chose an authentication application to be used before allowing access. This is great in terms of security. With discretionary access controls, the password manager can adequately protect (via MFA), while usability and ease of use is preserved.

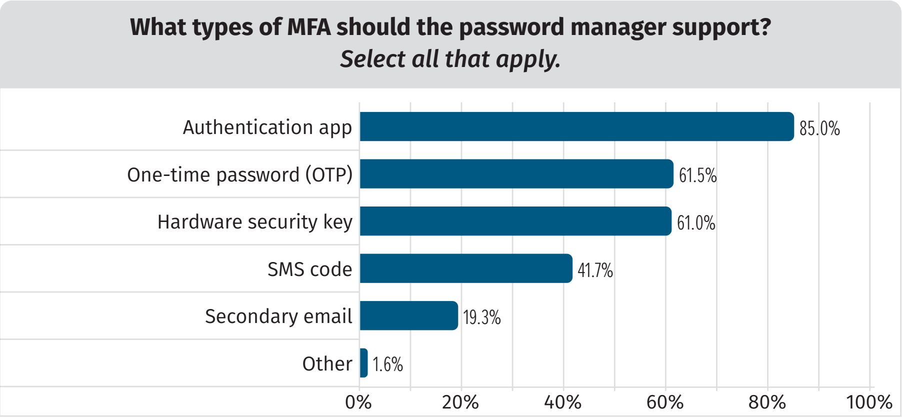

Figure 5. Types of MFA Supported

There is an even distribution on which platforms the password manager should run. Most organizations and users today employ a healthy mix of platforms. Our respondents do not prefer one platform over another when it comes to Android vs. iOS or Microsoft vs. Linux.

The majority (93%) of respondents believe a password manager should support auto-generation of passwords. So what are the requirements for generating strong and unique passwords? Most (78%) indicated that a password should be of a certain length and completely random. This makes for strong, hard-to-crack passwords that will work in scenarios where users aren't required to type passwords manually. If users must type a password, an auto-generation algorithm that creates passwords based on a wordlist would be a better option (only 5% prefer this option). Other options include password generation based on patterns (3%) or custom algorithms (12%) or passwords derived from previous passwords (1%)—where the latter almost feels like a trick question.

Respondents value vendor reputation, with 87% indicating that the reputation of a password manager vendor is important to their organizations. Only 33% of respondents believe it is important that their password manager of choice is open source.

Users will not automatically see the benefits of a password manager. Training and education is necessary. Follow these best practices to ensure that users see the immediate benefits from a password manager:

- **Make online life easier and more accessible.**
- **Avoid requiring users to remember passwords.**
- **Make it easy to generate new and secure passwords.**
- **Mitigate identity theft by ensuring that one password does not automatically provide access to everything else.**

A great way to ensure adoption is to start with the management team. Get them on board by proving the value of the system. Next, let management be the champions in campaigns that promote employee adoption of the password manager. Also, make training videos and materials easily accessible, and train your support staff to assist the organization.

MFA and Passwordless: "You Do Not Have to Rename Your Dog"

MFA refers to multi-factor authentication, where users are asked to provide two or more factors to verify their identity. With the security vulnerabilities and costs associated with passwords, in recent years one aspect of modern MFA has been the idea of doing away with passwords altogether. Not only would that eliminate the costly overhead of implementing password management best practices, such as choosing complex passwords or changing passwords every 90 days, but also it would make the organization more secure and efficient. Users can be absolved of administering their own passwords across tens if not hundreds of services and can instead be helped by using secure passwordless solutions that offer stronger security and enable productivity.

While passwordless solutions might be the future, we asked respondents what *passwordless* means to them. The term seems to be ambiguous, meaning different things to different respondents, based on individual interpretation. Needless to say, this can cause some confusion. Let's look at an example. An application that enables creation of accounts with a password but then does not ask for it again is typically just an application in which a session does not time out by itself. Facebook is such an application, but we would not define it as passwordless. Instead, true passwordless solutions enable users to authenticate via means other than a password (e.g., a smartcard, USB or Near-Field Communication [NFC] security key, or biometrics). Figure 6 presents the various meanings of *passwordless* according to survey respondents.

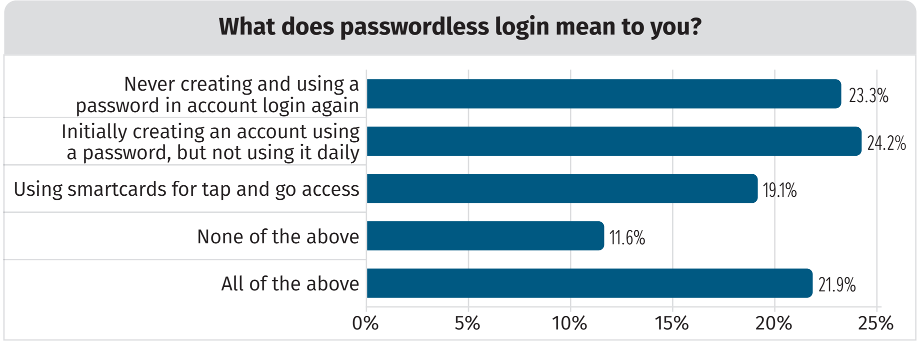

Figure 6. Defining "Passwordless"

Hackers can attest to how MFA has the potential to ruin their day—and that is the defender's goal, is it not? MFA helps prevent a compromised password from being used without the owner of the credentials supplying a second form of authentication, such as a token, cellphone, or code. A total of 69% of respondents are using MFA currently, while 14% are implementing it, and another 11% are planning to do so. That makes for a whopping 93% making headway with MFA implementation. See Figure 7.

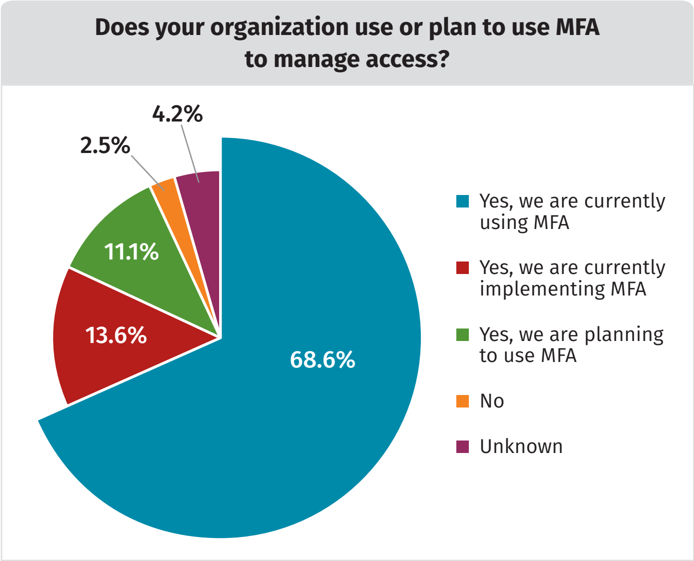

Figure 7. MFA Usage

MFA can support different ways for users to provide additional factors for authentication. The choice of solution depends on the required level of security relative to how user-friendly and accessible the token should be. Figure 8 shows the types of MFA respondents' organizations are using currently.

SMS is leveraged by 39% of respondents as their current method of providing tokens. While it is great for communication, SMS is not purpose-built for security. Therefore, it is often criticized because the transport medium is inherently unsecure and can be intercepted via multiple means. Conversely, SMS is an easy-to-understand and well-supported way of providing authentication codes to users. Smartphones are now widely adopted and can provide similar ease of use as SMS, but can also ensure safe delivery of MFA tokens to users. A majority (58%) of respondents indicated that authenticator applications are used to allow users to get codes, likely because of their immediate convenience and familiarity.

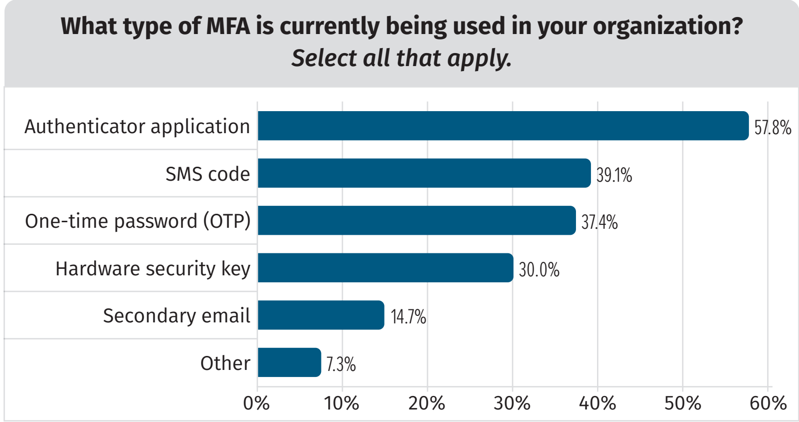

Figure 8. MFA Types in Use

SMS and OTP tokens are legacy forms of MFA and easily phishable. A hardware security key, where the secrets reside on the key itself and therefore cannot be exfiltrated or fall victim to a remote attack, can offer a balance of intuitive user convenience and strong security to users. Some security keys support authentication via proximity using NFC, reducing the efforts needed to plug in the key for authentication. Inconveniences in terms of managing lost and stolen security keys can happen, but can be remediated easily via management solutions. Several respondents also noted that they use phone calls to provide the MFA codes.

In high-security areas, users are accustomed to having barriers as well as interfaces that are not especially user-friendly. However, for noncritical applications, it can quickly become frustrating if too many barriers are in place. Discretionary access control means that barriers are in place only when the system can no longer recognize a user or device. For example, if a user changes to a different web browser and/or is accessing the system from a new location, this would warrant the system to challenge the user with an MFA request. Conversely, a user leveraging the same software from a familiar location would simply accept a password without MFA. The survey showed a relatively close split of 44% implementing discretionary access control, while 47% do not. Ten percent responded that they do not know if their organization supports discretionary access control.

As previously discussed, SSO may provide opportunities for attackers to use a single password across multiple services, thereby making it not only easier for users to access applications but also attackers. One password provides access to multiple services, while if we did not have SSO, a password manager could ensure unique passwords across the different services. MFA can be implemented across SSO to help combat this challenge, perhaps with discretionary access control turned on. In the survey, 38% indicated that they have MFA enabled for SSO, while 35% do not, and 27% do not know. Allowing both SSO and MFA is a good idea, because it may allow organizations to fine-tune their balance between security and user-friendliness across the multiple applications. However, this approach requires more effort in terms of complexity and architecture. See Figure 9.

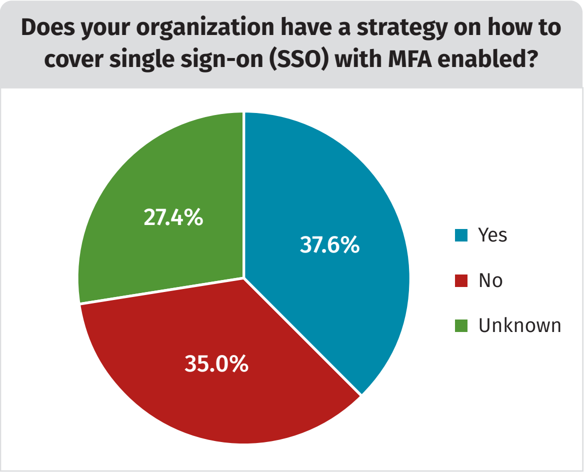
Does your organization have a strategy on how to cover single sign-on (SSO) with MFA enabled?

Figure 9. MFA-Enabled SSO Strategy

Is MFA perfect? Of course not. There are no perfect solutions. Instead, organizations should focus on ways to improve security enough to make most attackers fail, allowing only the most lucky or persistent attackers to get through. MFA can have vulnerabilities in its implementation or configuration to allow it to be bypassed. For example, one might not have rate-limiting of how many codes can be tried before blocking the user and requiring that a new token be issued. Attackers could then abuse this weakness to guess hundreds of thousands of codes after a successful password has been entered. Although there are many attacks against MFA, its use raises the bar, often leaving attackers with non-ideal options such as trying to social engineer MFA codes from victims. Nevertheless, 63% of respondents said that they have not experienced breaches involving accounts behind MFA, while 13% have experienced breaches, and 25% do not know.

How hackers will bypass MFA defenses depends on which MFA solution is in place. Some solutions are easier to bypass, while others are harder. A hardware security key is the hardest control for attackers to bypass, because it is based on modern security protocols such as FIDO/WebAuthn. Only 10% of respondents had a breach of account behind this solution. While SMS is heavily debated and criticized for its weaknesses, only 13% of respondents had breaches behind this solution. See Figure 10.

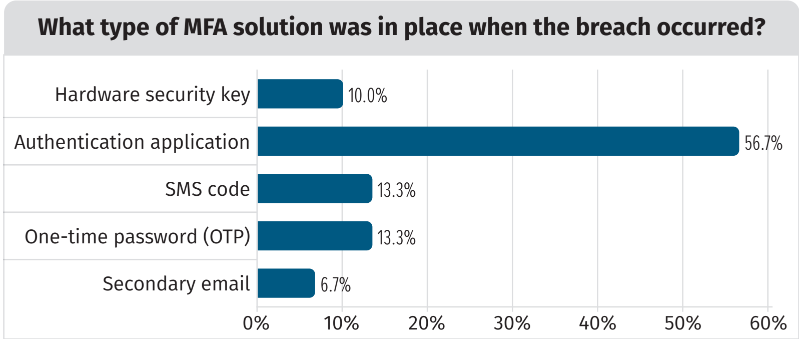

Figure 10. MFA in Place When Breach Occurred

The big outlier in breaches behind MFA is authentication applications, where 57% of breaches were reported. The reason for this could naturally be the higher adoption rate of authentication applications, but also implementations such as push notifications from them. Some authentication applications allow users to simply tap *Yes* on a pop-up on their smartphone to authenticate a request. With a well-timed attack, perhaps in the morning while the user is logging onto systems and expecting to see MFA pop-ups on their smartphone, the attacker could very well be lucky—the user simply taps Yes, allowing attackers access to the system.

MFA can be a daunting challenge for many organizations. How do they implement it? Does it require development efforts? Is implementation expensive? A strategy should be considered on how solutions could be effectively covered behind MFA. Instead of considering how to implement MFA on a single-solution basis, a strategy should be implemented in how new and existing solutions could more easily be supporting an MFA scheme. Such solutions exist, but perhaps implemented in ways that do not conform to traditional design of authentication, where the application itself implements the MFA. Instead, consider an SSO strategy where MFA is implemented and only when authenticated via the SSO will you be able to access and provide authentication to a specific service. This concept is often referred to as *secure access service edge (SASE)* and covered in many zero-trust architecture schemes.

Conclusion

No security control is perfect, of course, and there is always a trade-off between how little friction users experience to get work done—and how well the company's data is protected. However, organizations and users seem to be maturing to the point where adoption of both password managers and MFA is reaching healthier numbers.

In terms of adoption rate, most of our survey respondents are leveraging easy-to-use, application-based MFA solutions to ensure the security of their users. This is not surprising, because organizations have likely come to realize that security controls are not effective unless their users buy into them. Organizations have potential here with password managers and should consider allowing employees to use both private and enterprise passwords in the same solution. Adoption rates for password managers must increase before we can enforce harder and stricter controls; thus, a compromise in security might be in order.

We realize password managers add their own inherent risk to the organization. However, organizations must carefully consider which of the following battles they want to fight:

- Users trusted to keep track of passwords in their own unreliable ways
- Password managers that make life easier and more secure—but when compromised possibly reveal all the secrets

The latter is the consensus as the most viable solution.

To stay ahead of the game and give us a fighting chance against the cyber threats of tomorrow, users must start documenting their passwords in their password managers and become used to MFA (preferably with discretionary MFA controls), and the industry should shift toward hardware-based authentication controls.

Users must realize the internet is not a happy playground where they can carelessly navigate in their naive ways, but rather embrace security controls that offer a user-friendly and accessible way to innovate, explore, and benefit from the full potential of the internet and related IT solutions.

About the Author

SANS instructor **Chris Dale** teaches SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling. As head of the penetration testing and incident handling groups at Netsecurity, a company based in Norway, Chris brings significant security expertise and a background in system development, IT operations and security management. He is passionate about security, and he regularly gives presentations and teaches at conferences and workshops. Chris holds the GCIH, GPEN, GSLC, GDAT and GMOB certifications and participates in panel debates and government-related working groups to recommend and improve security in the Norwegian private and public sectors.

Sponsor

SANS would like to thank this paper's sponsor:

yubico