CAPACITY ENHANCEMENT GUIDE: IMPLEMENTING STRONG AUTHENTICATION

AUDIENCE

Weak authentication is a common vulnerability for information systems—it is consistently one of CISA's top five, most frequent findings for Federal High Value Asset systems. Furthermore the 2019 Verizon Data Breach Investigations Report states that compromised passwords remain "prominent fixtures" of breaches.[1] Implementing strong authentication methods across an organization can dramatically improve resilience against common cybersecurity threats such as phishing attacks and compromised credentials.

Although this guide references federal standards and publications, it is not mapped to nor directly associated with any agency. These recommendations are applicable to any organization seeking to better their authentication process.

PURPOSE

The purpose of this guide is to lay out the concept of authentication, recommend related security enhancements, and provide guidance to help plan and implement a strong authentication solution. Strong authentication is one of many pillars of a defense-in-depth cybersecurity strategy, but it is not the only solution to cybersecurity issues.

THE CONCEPT

Authentication is the process of verifying that a user's identity is genuine. Most systems require a user to be authenticated prior to granting access to the system. The user does this by entering a password, inserting a smart card and entering the associated personal identification number (PIN), providing a biometric (e.g., fingerprint, voice pattern sample, retinal scan)—or a combination of these things—to prove they are who they claim to be. The credentials provided are compared to those that have previously been associated with the user. The credential match may be performed within the system being accessed or via a trusted external source. If the credentials match, the system authenticates the identity and grants access (see figure 1).

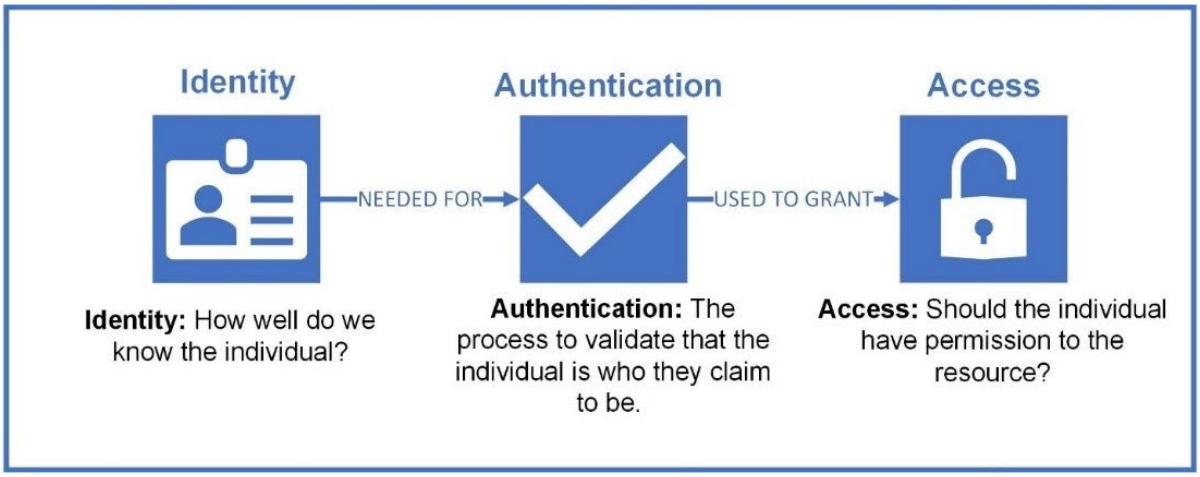

Figure 1: Relationship between identity, authentication, and access

[1] 2019 Verizon Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir/2019/.

Authentication Methods

Different systems may use different authentication methods to validate the user's identity. Authentication methods can be grouped into three **factors**:

- Something you know (knowledge)
    - Examples include password, passphrase, or PIN
- Something you have (possession)
    - Examples include smart card, token, look-up secrets, one-time password devices, or cryptographic devices
- Something you are (inheritance/physical traits)
    - Examples include fingerprints, iris, facial characteristics, voice pattern, or gait

Single-Factor Authentication is a common, low security method of authentication. It only requires one factor, such as a username and password, to gain access to a system. (Although it includes two pieces of information, a username and password combined is still a single factor because they both come from the same category.)

Multi-Factor Authentication (MFA) is a strong authentication method. It requires two or more factors to gain access to the system. Each factor must come from a different category above (e.g., something you know and something you have). MFA may be referred to as two-factor authentication, or 2FA, when two factors are used.

A study conducted by Google, New York University, and University of California San Diego demonstrates the significant improvement implementing MFA has on an organization's resistance to malicious attacks. The study found that using MFA blocked 100 percent of automated bots, 99 percent of bulk phishing attacks, and 66 percent of targeted attacks on users' Google accounts.[2]

Assurance Levels

Different authentication methods have different assurance levels based on the robustness of the process and the confidence that the identity is who they claim to be. Organizations may determine that it is not worth the cost of implementing higher assurance levels for systems that do not contain sensitive information and are not connected to the same network as those that contain sensitive information. For more information on assurance levels, refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 Digital Identity Guidelines[3] and associated standards,[4] which describe authentication assurance levels and provide a risk-based approach for selecting the strength of authentication appropriate for a given system.

THE PROBLEM

Single-Factor Authentication—Everybody Uses Passwords. Are They Really That Bad?

Single-factor authentication, which usually means a username and password, provides attackers an easy way to gain

[2] New research: How effective is basic account hygiene at preventing hijacking, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[3] https://pages.nist.gov/800-63-3/

[4] Other digital identity standards include ISO/IEC 29115:2013 and the European Union's eIDAS regulation, as well as efforts to apply digital identity to emerging needs such as ePassports (ICAO's Digital Travel Credentials Sub-Group) and digital driver's licenses (ISO 18013 standards). Other examples can be found through The World Bank's ID4D Identification for Development resources at https://id4d.worldbank.org/.

access to the system.[5] Since passwords are just data, attackers have many different techniques they can use to steal a password without being physically present, including:

- Brute-force attacks
- Plaintext password storage
- Phishing
- Credential dumping
- Keylogging
- Network sniffing
- Social engineering
- Malware

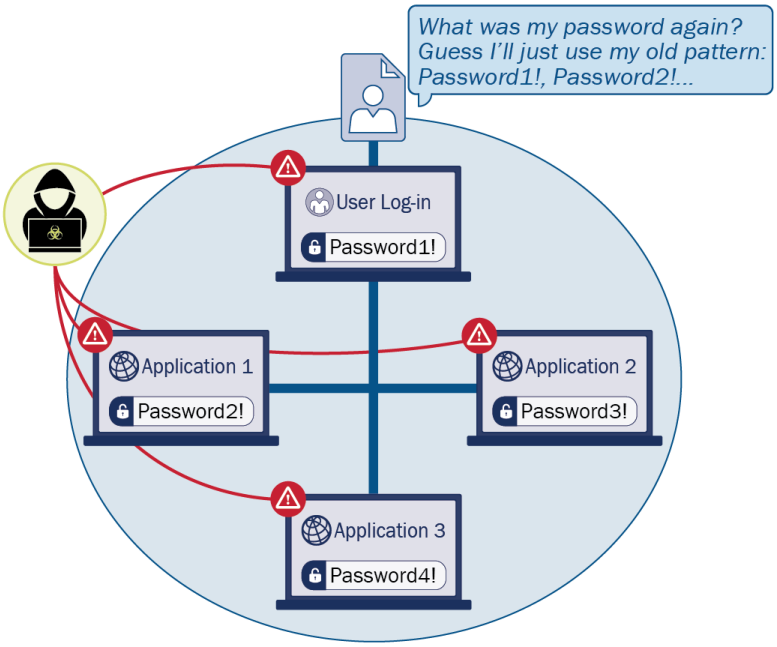

Figure 2: Example of password pattern use

Weak passwords (e.g., the manufacturer's default password or passwords that follow a pattern [see figure 2]) make it easier for an attacker to compromise a password. Other unsecure practices may compound the impact a compromised password can have on the organization.

- Password reuse allows an attacker who has compromised a password to access multiple systems, networks, or data sets. Organizations can discourage password reuse, but there is no technical control that can prevent a user from reusing a password across multiple systems. The inability to prevent password reuse leaves a compromised password available for attackers to use to gain access to other systems.
- Admin password sharing makes it more likely that a privileged (administrative) account with elevated access can be compromised; an administrative password is often written down, located in a place where multiple people have access to it, simplified to make it easier to remember, and not changed frequently—even after people leave the organization. Once it has been compromised, an administrative password grants the attacker elevated access across the network and/or across multiple systems.

Adding another authentication factor (i.e., something you have or something you are) dramatically increases the difficulty

[5] NISTIR 7983, Report: Authentication Diary Study, surveys user behaviors for coping with the friction and burden imposed by managing their portfolios of user IDs and passwords (https://csrc.nist.gov/publications/detail/nistir/7983/final).

of compromising an account, because a compromise now requires either the physical presence of the user or possession of a physical object such as a smart card.[6]

An asset with the weakest method of authentication becomes a potential path to bypass stronger authentication for a system that it is connected to. A concrete and steel building with reinforced doors and sophisticated locks can still easily be entered by intruders if there are large open windows.

To receive the full benefit of an MFA capability, organizations should be sure to implement it across all systems, applications, and resources. Requiring multi-factor authentication to gain initial access to an organization's network (usually the user's workstation) is a good first step; however, this provides only limited protection to other systems and data within the organization that are protected with only single-factor authentication. Threat actors may seek to exploit the less protected systems and then move to other systems and continue their malicious actions.[7] Network segmentation may also reduce the attacker's ability to move throughout the network, but accounts relying on single factor authentication are still susceptible to compromise and represent the weakest link.

WHAT CAN YOU DO?

Planning Phase

Strategic Planning

Implementing MFA on all systems, applications, and resources can be challenging and expensive; when approached individually each requires its own, specific method of verifying a user's identity (e.g., multiple credentials must be issued, managed, and revoked). For this reason, organizations will be most effective in implementing authentication by taking an organization-wide approach and implementing the solution as an enterprise service for systems and applications across the entire organization instead of trying to implement redundant, isolated authentication solutions for each application.

An organization-wide strategy allows standardization of authentication policies and practices, including the issuance and management of necessary credentials, and reduces the cost of each application acquiring or building its own authentication solution. Organizations should examine their existing capabilities to determine if they already have a viable solution to provide MFA across the organization. Federal agencies, for example, have Personal Identity Verification (PIV)-based authentication for users. An organization whose user accounts are managed through large commercial providers may be able to leverage the MFA capabilities already available from their service provider. Organizations with no MFA capabilities currently available should procure or design an MFA solution.

When deciding on an MFA solution, organizations should consider the following.

- Initial authentication of a user to the network or system
- Additional authentication as users access other systems, applications, or new segments of infrastructure
- Authentication to externally hosted resources
- Authentication to internal resources by external entities

Once an organization decides on an enterprise MFA solution, authentication capabilities can be expanded through single sign-on (SSO) and identity federation services. SSO and identity federation securely shares authentication and identity information across organizations, systems, applications, and resources without requiring individual implementations of

[6] While there are types of attacks that can compromise MFA, particularly for "something you have" authenticators, they require deceiving the user to take an affirmative act to allow access to the account and are thus not easily automated or commonly used.
[7] A dramatically improved approach to address these issues underlies the concept of a zero-trust architecture, which does not implicitly trust anyone but enforces continuous authentication. NIST SP 800-207 Zero Trust Architecture (https://csrc.nist.gov/pubs/sp/800/207/final) goes into more detail on the concept of zero trust.

the MFA capability on each system. Many systems come with connectors for SSO already in place. SSO and identity federation enhance security to the organization by putting control of access to resources in the hands of a central identity management administrator, which allows the organization to rapidly and comprehensively revoke access across all its resources when the user leaves or should the account ever be compromised. These steps simplify the management of the identity lifecycle—including various credentials issued to the user—and help ensure that access across the organization is promptly revoked when a user leaves.

An additional benefit is simplifying the user experience—users no longer must keep track of dozens of credentials—while simultaneously reducing the organization's vulnerability to weaknesses in how the users manage multiple credentials.

Single Sign-On

SSO is an authentication method where a user authenticates once—typically using the strong MFA authentication solution selected by the organization—to the centralized SSO solution. Other systems and applications are configured to trust the centralized SSO solution to authenticate the user with no further interaction required (see figure 3). This reduces the need to repeatedly authenticate to multiple systems and services. Most importantly, when a user moves from their initial authentication to other systems through SSO, the user's credentials for the initial system are not shared with the other system. Once a user authenticates, the SSO solution transparently and securely completes the process for all systems involved without further exposing the initial system credential. In addition, each application is not required to manage its own identity credential store but leverages a centralized store across the organization.

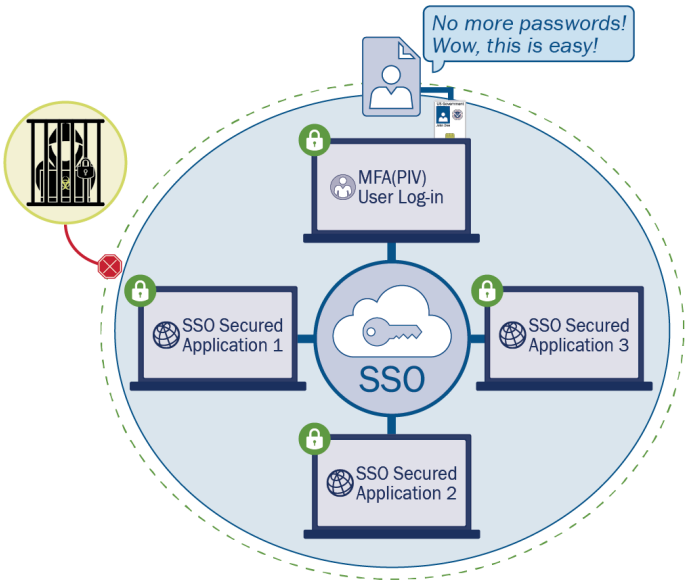

Figure 3: A central organization-wide identity provisioned with access through an SSO solution preserves the security of the MFA network login across internal and external resources.

Note: some SSO providers may still authenticate to other systems with a username/password for that system; organizations should ensure their SSO solution is set up with strong, non-password-based protocols at each step of connecting to a resource.[8] Multiple technical options for incorporating SSO capabilities in an organization's infrastructure exist. When selecting an SSO solution, organizations should consider single sign-off capabilities—which terminate all open and active sessions when a user logs out—to minimize the risk of session hijacking.

Identity Federation

Although identity federation is not, in and of itself, a solution to weak authentication; it can provide substantial indirect support for improving authentication. Identity federation refers to the establishment of a trusted relationship between more than one organization that manage their own users, identities, and authentication, in order to accept each other's users. Organizations should only federate with other organizations whose identity vetting and authentication processes they trust. Such as, two organizations manage their own users, identities, and authentication and then establish connections between their systems, to reduce the points of weak authentication for external users that expose an organization to attacks. For example, imagine that Acme Anvil Co., and Coyote Missile Co., have an overlapping mission

[8] Open ID Connect, OAuth 2.0, Kerberos, and SAML 2.0 are examples of protocols that use secure, non-password-based connections for SSO. Many social media-based SSO services that consumers use are based on Open ID Connect, allowing even consumers to use SSO while focusing on strong authentication for their primary login provider.

that requires Acme Anvil to share information with Coyote Missile, but each organization already manages the identities of their employees in their own identity store. Instead of using resources to perform a new background check on the Coyote Missile employees who need access to the information, Acme Anvil could choose to establish a trusted relationship with Coyote Missiles identity store to authorize access to the Acme Anvil system, knowing that Coyote Missile has already conducted a background check on the individual and established their identity (see figure 4).

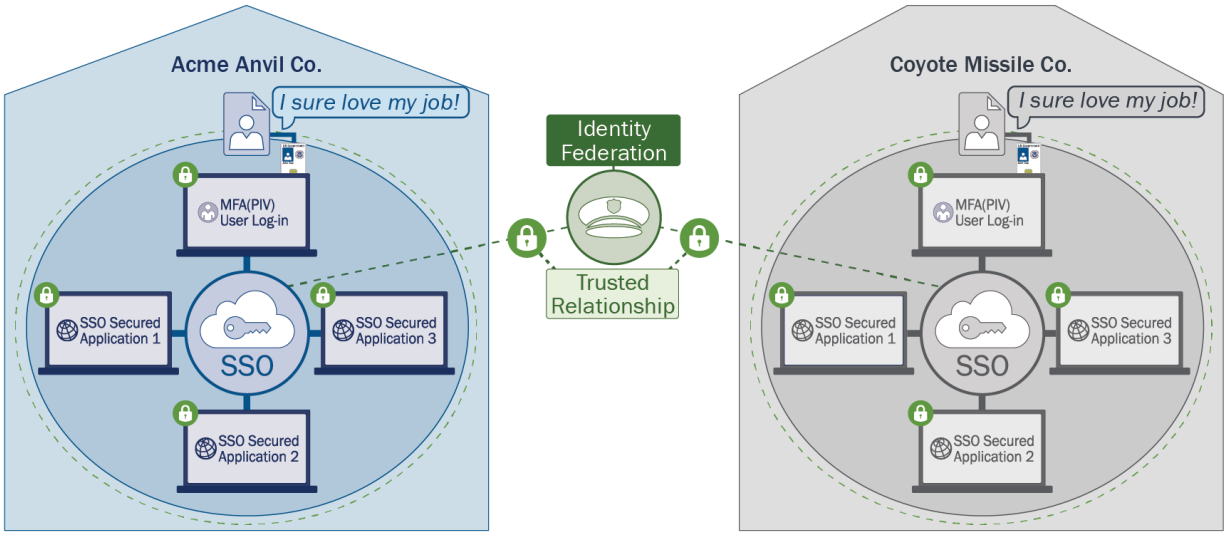

Figure 4: A user at Acme Anvil can securely log in to her company workstation with MFA and access an application hosted by her vendor, Coyote Missile, through a secure identity federation without needing a login or password.

Identity federation thus can expand an organization's strong authentication and SSO capabilities even further to systems owned by trusted organizations that its users access and vice versa. Organizations that need to share resources with another organization's users can use the trusted, federated user identities without duplicating the identity-proofing or identity management for those users. Without identity federation, the authentication and identity store for any resource that is shared with another organization must be configured and managed separately from its primary identity store, which increases complexity.

Know When to Move On

An organization may identify resources for which incorporating strong authentication will prove too expensive or technically complicated. If this occurs, the organization must decide between 1) remaining with the current system and implementing compensating controls to address the risk to the organization; or 2) migrating to a new, modernized system that allows integration with the strong authentication solution. The organization should weigh the cost and risks of each option.[9]

Note: although outside the scope of this document, the organization should consider the performance and security benefits in addition to strong authentication that migration to updated technology will provide when making their decision.

Other Strategic Considerations

Especially for large organizations, non-technical considerations regarding binding policies, responsibilities, and budgets are likely to be relevant. If information systems are not managed and controlled by a central office or chief information officer (CIO), additional engagement and coordination will be necessary with the different offices that own the systems to

[9] The calculation of the cost of such compensating controls should incorporate the cost of technical implementation of compensating controls, the cost of time and organizational complexity for administering those compensating controls, and the risk introduced by relying on additional controls and security measures to support those controls.

align with the organization's overall strategy. Similarly, if an organization's information technology (IT) budget is not centrally managed, then the organization may need to consider how the cost of implementing and operating components of strong authentication, SSO, or identity federation can be recovered from each element of the organization.[10]

While automated system-to-system connections are not strictly within the scope of this guidance (and MFA is not an option for a server credential), they still leave an avenue of attack open by providing a "non-person account" to access a system. As mentioned previously, when any form of weak authentication is combined with a lack of effective network segmentation this weakness can be further exploited to move around a network, thus defeating the benefits of strong authentication implemented elsewhere. Organizations can remove this path for attackers to bypass the strong user authentication to systems by securing these connections with strong credentials (Secure Socket Layer [SSL] certificates), encrypted communications, and application-specific or IP address allowlisting.

Tactical Planning

Tactical planning involves discovery of the current state environment, determining the to-be state, and developing a transition plan to execute cost effective methods to migrate to the target state.

To address weak authentication, there must be 1) knowledge of the "as-is" state, 2) available capabilities, and 3) understanding of what is needed to achieve the desired state. It is essential to avoid analysis paralysis when planning and undertaking these enterprise improvement efforts. Seeking 100 percent knowledge or assurance (perfection), whether for current or future state, inhibits incremental improvements based on available (good enough) information.

Understand the "as-is" State

1. Catalog current applications and systems.
2. Identify users and user groups that have access to the system or application, including partners and external stakeholders with whom you share data.
3. Catalog the nature of the data shared with partners, as the need to safeguard sensitive data can drive protocol and architectural considerations. Where sensitive data is being exchanged, more detailed information about users may be necessary to enforce least-privileged access. This is particularly true for systems where sensitive data is only a subset of the data in the system (and the organization does not want to incur the financial or efficiency cost of extra security on non-sensitive data).
4. Identify the authentication method for each user to each application or system.
5. Identify authentication protocols that each system or application supports.
6. Identify supporting elements of the architecture—such as automatic system-to-system connections that will also need to be secured—to ensure configuration of secondary elements does not introduce vulnerabilities.

Identify Current Capabilities

1. Identify existing MFA capabilities, such as PIV card authentication, within the organization.
2. Evaluate the acquisition or budget options for executing an initiative to strengthen authentication, incorporating the strategy for recovering costs that aligns with the strategy of broad adoption of strong authentication.
3. Identify existing assets or licenses for applications that could provide MFA capabilities.

[10] Consider the incentives that the cost recovery model creates. Any pass-through of costs to business units for adoption of the organization's authentication can be counterproductive to improving security if the business unit's cost increases incrementally for each user or application which it transitions to the strong authentication solution.

4. Evaluate licensing agreements for systems or applications to be integrated with the strong authentication solution. Support for methods of strong authentication or strong SSO/federation protocols may require additional licenses or a different type of license from the application to be secured; those licenses are separate from the cost of the strong authentication solution or SSO/federation solution itself. Understanding the end-to-end cost of implementation will inform total cost of ownership and support decision-making about cost-effective risk-management.
5. Identify current personnel with experience in implementing MFA capabilities.

Understand the "to-be" State

1. Select the strong authentication solution that best fits your environment and regulatory requirements (e.g., certain authentication solutions may work for an on-premise architecture but may not work well for a cloud architecture).
2. Define how users will authenticate to the network, to each subsequent system and application, and to externally hosted resources; define how external users will authenticate to internal resources.
3. Determine which systems and applications will be integrated into an SSO solution.
4. Determine which organizations with which to establish a trusted identity federation.
5. Set boundaries for systems that have different strengths of authentication and ensure that connections from weaker authenticated systems or users do not allow for weakly authenticated access to a system that is secured with stronger authentication. Pay attention to system-to-system connections crossing a boundary from a less secure environment to a system in a more secure environment.
6. Design the target architecture upon full deployment of the planned strong authentication solution. Include where the authentication solution will support other organizational security practices such as network segmentation.

Transition Plan

1. Develop a transition plan and schedule to get from the "as-is" state to the defined "to-be" state.
    a. Use a risk management strategy to prioritize users and applications for onboarding to the solution.
    b. Users with elevated privileges in a system or application are most critical for onboarding, as are those systems or applications that are critical to delivering the business mission, for core organizational functionality, or that contain sensitive data.
    c. Prioritize the organization's most critical systems and assets that have the weakest authentication.
2. If a trusted identity federation with another organization will be used, determine how these users will be transitioned without negatively impacting their current accesses.
3. Test the migration plan against representative systems.

EXECUTION PHASE

In this phase, your organization executes strong authentication using the artifacts obtained during the planning phase. During execution, schedules and other artifacts may need to adjust to "conditions on the ground" and lessons learned. As such, adjustments under consideration should undergo the same level of rigor given to the artifacts during the planning phase. The notional timelines below can be adjusted based on the size and scope of the effort.

Short-Term Actions

1. Procure or design the strong authentication solution based on the organization's architectural analysis and risk management determination.
2. Acquire hardware, software, and licenses, including the SSO solution, necessary to implement the transition plan defined during the planning phase.
3. Identify and catalog business processes for managing users from a centralized identity governance administration point.
4. Begin implementing strong authentication for the organization's privileged users and its highest value systems and assets as defined in the transition plan.
5. Incorporate criteria for evaluation of a system's authentication compatibility with the organization's solution into the organization's review of proposed acquisitions or new systems.

Medium-Term Actions

1. Continue migrating systems to the strong authentication system.
2. Leverage the initial implementation of the strong authentication solution to connect to an SSO solution.
3. Transition authentication from existing systems and applications to the SSO solution.
4. Evaluate new acquisitions or proposed systems to determine compatibility with the organization's strong authentication solution prior to procuring those systems.

Long-Term Actions

1. Continue migrating systems to the strong authentication system.
2. Establish trust relationships with other organizations for identity federation.
3. Onboard non-person entities such as service accounts.
4. Enable continuous improvement through regular review and updates to requirements, policy, and reference architecture.

SUMMARY

Strong authentication via MFA is a critical and sometimes expensive investment, but should be implemented across all networks, systems, applications, and resources to adequately protect the organization. For this reason, an organization-wide approach is recommended. One method of expanding MFA capabilities across an organization is through an SSO solution. In addition to providing better security for an organization's resources, an SSO solution improves the user experience because it removes the need to remember passwords or manage multiple credentials such as RSA tokens for each system and application. An SSO solution implemented at an enterprise level may also eliminate the need for system owners to expend resources managing their own authentication solutions. Once an SSO solution is in place, organizations can further expand strong authentication capabilities through identity federation with other organizations. By incorporating these concepts and other strategic considerations into the evaluation of their "as-is" state, an organization can define their desired "to-be" state and create a plan to get there.

CONTACT INFO

For questions about this guidance and other CISA services available to federal agencies, please contact cyberliaison@cisa.dhs.gov.