THREAT INSIGHT

ActZero

Multi-factor Authentication

Stopping unauthorized access to systems and data

One of the most fundamental cybersecurity practices required by any business is to implement policies and tools that limit access to corporate systems and information - restricting who has access, to what, and by using what means of authentication they'll require. Businesses are frequently turning to multi-factor authentication (MFA) for its added protection over traditional authentication methods.

Multi-factor Authentication adds layers of defense

Traditional user ID and password logins are easily compromised, as they're often stored or saved in an unprotected manner. Additionally, they can be subverted by tools like brute-force attacks, for example, which use automated password cracking tools to guess various combinations of usernames and passwords until they gain access.

The goal of MFA is to harden access by creating a layered defense that makes it more difficult for an unauthorized person to access your endpoints, cloud, network or databases. If one factor is compromised or broken, the adversary still has at least one or more barriers to breach before successfully breaching its target.

For lots of great information on forms of MFA and use cases, check out the Open Web Application Security Project®'s **Multi-Factor Authentication Cheat Sheet**.

What type of MFA do you need?

When it comes down to it, businesses may have to implement more than one type of MFA since many businesses operate in a hybrid environment where some of their stored data and systems, and access to it, is stored locally, and some is hosted in the cloud. For companies using with all systems and data on-site, and using an Active Directory (AD) domain, using digital certificates, like tokens, fobs, or usbs, is an effective way to incorporate MFA. For cloud environments, Out-of-Band (OAB) MFA solutions, like one-time passwords, have to be considered for those environments. A hybrid approach requires both forms.

However, determining MFA technology comes down to two things: 1) knowing **WHAT** your Controlled Unclassified Information (CUI) is; and 2) knowing **WHERE** your CUI is stored, transmitted and processed so you can partition it from non-CUI data, which simplifies compliance scope.

Which applications should have multi-factor authentication?

Below is a sample list of applications that require multi-factor authentication, according to most cybersecurity regulatory frameworks:

- Email accounts
- Any account with access to sensitive information
- Password management tools
- Remote access technologies
- Hosting Services
- Cloud computing management interfaces
- Cloud storage used for sensitive documents

The importance of multi-factor authentication to compliance

Adding MFA mechanism to thwart unauthorized access can aid in organizational compliance with several well-known regulations including: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Cybersecurity Maturity Model Certification (CMMC), the General Data Protection Regulation (GDPR), and other state or local data privacy regulations. In fact, using MFA for compliance reasons is one of the key drivers in current adoption trends.

Below is a small subset of framework that are mandate/recommend MFA to meet compliance.

CMMC	Control #	
	3.1.1	“Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)”.
	3.5.3	“Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts”.
	3.5.7	“Enforce a minimum password complexity and change of characters when new passwords are created”.
	3.7.5	“Require multi-factor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete”.
PCI-DSS	Req. 8.3	“Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted”.
HIPAA	Security rule	The HIPAA security rule is widely understood within the healthcare industry to mean the use of “multi-factor authentication” (MFA) to protect access to medical and patient data. Under the new guidelines, the HIPAA requirements for multi-factor authentication are now being extended to "business associates"
GDPR	Section 4.2: Guideline K.7	“Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.”
GLBA	-	“Single password authentication solutions are not secure enough to comply with the strict internal controls required by SOX and the safeguards required by GLBA”. MFA is therefore recommended
FERPA	34 CFR § 99.30	Under FERPA, "[s]ingle-factor authentication may not be reasonable…for protecting access to highly sensitive information." MFA is therefore required.
FIPPA & PIPEDA	-	In Canada, while no specific mandate exists, both effectively require the use of strong MFA for clear educational data privacy compliance.

Multi-factor authentication isn’t a cure-all

Multi-factor authentication is only component of a successful cybersecurity strategy and implementation. MFA does nothing to detect or prevent Business Email Compromise (BEC), Account Takeover (ATO), social engineering emails attempts impersonating executives, or other methods used to circumvent security measures, such as website phishing tactics. For that, you need an MDR service, like ActZero who can detect, contain and respond to threats across your IT environment.

For those who aren’t yet a customer, learn more about how ActZero can help you understand your security gaps, and identify how and where MFA can help you improve your cybersecurity readiness by contacting us now.