TARPON HEALTH

Multi-factor Authentication

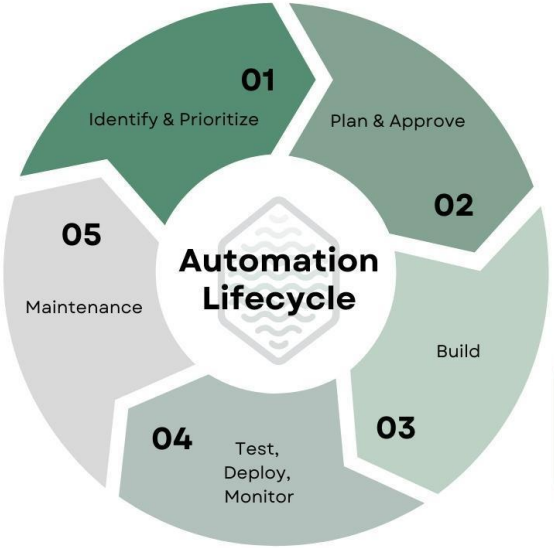
Agenda

- Overview
- Avoiding multi-factor authentication
- Viable approaches
- Getting an approach approved

Today's goals:

- Define MFA and the best way to avoid it
- Articulate viable integration solutions
- Share best practices on getting an approach approved

The Tarpon Health Automation Lifecycle



01

- Create a pipeline of ideas by functional area
- Establish estimated ROI, volume, and complexity
- Prioritize ideas for impact

02

- Review the foundational process to be automated and identify process improvement opportunities
- Build the Process Definition Document (PDD)
- Review automation with finance and compliance
- Approve build

03

- Optimize upstream processes
- Standardize data inputs
- Code development
- Manage engineering build, including exceptions, risks, and issues that arise

04

- Manage automation through four phases of testing: QA, Integration, User Acceptance, End-to-End
- Deploy to production
- Monitor post go-live and adjust code as needed

05

- Define analytics to measure automation efficacy
- Integrate automation into ticketing and support process
- Establish quality assurance reviews

Background

Data breaches are costly, especially in healthcare.

Per IBM's Cost of a Data Breach Report, the cost of a breach in the healthcare industry went up 42% since 2020. For the 12th year in a row, healthcare had the highest average data breach cost of any industry.

$10.1 Million - Average total cost of a breach in the healthcare industry.

Biggest factor - Stolen or compromised credentials. More than Phishing, business email compromise, 3rd party software vulnerabilities and malicious insiders.

Why MFA?

Passwords alone are not good enough.

Why the proliferation of MFA?

Healthcare has been steadily moving workflows and data into a digital format. This has sparked an increase in user account creation. All of these accounts must be secured.

A common point of failure in digital security is the password. Passwords are frequently forgotten, shared, and stolen for malevolent reasons. Many organizations deploy multi-factor authentication (MFA) for identity and access management as an additional layer of security.

Key Statistic

A 2018 report to congress on the Federal Information Security Management act revealed that up to **65%** of cybersecurity incidents were preventable with strong multi-factor authentication.

Authentication basics

There are three types of authentication. Any combination is what we mean by “MFA”.

Category	Example
Something you know	Passwords
Something you have	A device, such as a phone
Something you are	Biometrics, such as facial recognition

MFA = when 2 or more of these approaches are used to verify identify.

Most commonly its a password plus something you have.

Common forms we see in healthcare applications include:

- **One-time passwords (OTP):** Codes that come via email, text, or app
- **Time-based one-time passwords (TOTP):** Codes that constantly update (e.g. every 30 seconds) and must be retrieved from an app

Prevention is the best medicine

TARPON HEALTH

Incorporating MFA into an automation can be challenging. It is best to avoid MFA altogether where possible. Below are 4 tactics you can use.

Tactics	Description
Service accounts	A special type of account for applications, not people that typically limits access to other applications. Advanced password schemes ensure secure access.
Single Sign On (SSO)	SSO allows users to log in once and access multiple applications without having to enter their credentials for each one separately. It uses a central identity provider (IDP) to authenticate users and provide them with access to the applications they are authorized to use.
Open - Authentication	OAuth can only be used if your automation platform is 'On Premise' (not cloud based). OAuth provides an application with secure delegated access to server resources without providing credentials.
MFA Alternatives	Similar to disabling MFA altogether, some applications offer an MFA alternative, such as an advanced password scheme. For example, a password that has 72 characters. Selecting this security feature is preferable to MFA because the automation can store the username and password in its credentialing management system.

Best options for integrating with RPA

Third party organizations own the MFA approach, but often there are options from which to choose.

TOTP via desktop or browser extension

Why:

- Contains the least number of steps
- There is no send/receive delay
- No manual intervention is needed

Applications we endorse

- Authy
- Google Authenticator

Other viable options

Use one time passwords (OTP) if TOTP is not available. Commonly this involves using an email or a phone.

OTP via desktop or browser extension

Why:

- Integration is easy despite more steps and some delay
- Easy to track success

Drawbacks:

- More steps
- Send / receive delay
- More credentials (for email or phone)

Applications we endorse

- Email
- Dialpad

Most difficult

Any MFA solution that requires an external device (e.g. not a desktop application), biometrics, or manual action creates large challenges.

External devices

Drawbacks:

- Relying on two devices makes integration nearly impossible
- Manual intervention is required, reducing the effectiveness of the automation

Discussion

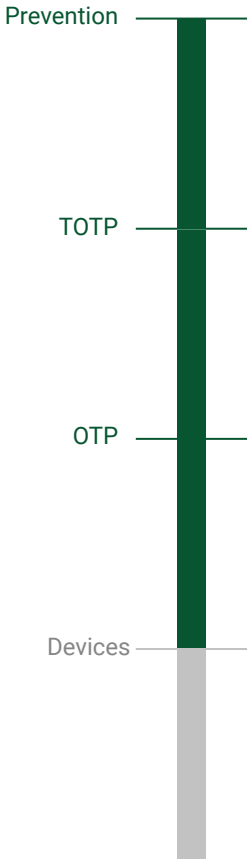
- Has anyone had to stop building an automation?

Hierarchy

Here is a framework you can follow when evaluating how to integrate MFA into your automation.

Discussion

- How do teams evaluate MFA today?
- How early in the process should you be looking at MFA?



Avoid MFA Where Possible

Evaluate the use of service accounts, SSO, OAuth, and the use of strong passwords. Likely, this is most applicable in enterprise software systems.

TOTP via desktop or browser extension

Time based one time passwords delivered via desktop or browser extension are best for integration. Try Authy or google authenticator.

OTP via desktop or browser extension

One time passwords delivered via desktop or browser extension will work well, but expect some issues due to built in delays and more steps. Email or dialpad have proved reliable.

Devices and biometrics

Any MFA solution that cannot be accessed via desktop or browser extension will be difficult for integration.

Working with IT

Even with preferences, your IT team will have a big say on what approach gets approved.

How does your organization work with IT on these issues?

- Who does your organization work with on these questions: security, compliance, etc.?
- Does your organization have guidelines around selection?
- What factors does your IT team care about the most?
- Any useful lessons that can be shared with the group?

Tell us how we did

1 - Least valuable

10 - Most valuable

We value your feedback!


TARPON
HEALTH