e-guide

Multi-Factor Authentication
Importance of MFA in Security Sensitive Industries

A guide to MFA best practices and tailoring MFA to specific user requirements and security levels

SecurEnvoy
A Shearwater Group plc Company

Executive Summary

There is no room to be complacent. With growing cyber security threats everyone in your organisation needs authentication tailored to their specific access needs and the risk profile of their role.

If you think you have implemented MFA already, you may need to think again. Two-factor authentication might not be sufficient across all your business and all users. MFA may have been implemented out-of-the-box for applications such as Microsoft Office 365 or VPN, but does not cover other applications and scenarios. For example, where your employees are accessing commercially sensitive information in an area where mobile phones are not permitted, the mobile authenticator for office or VPN will simply not suffice.

Your employees, partners and contractors may all need different types of MFA (SMS, Yubikey, Smartphone App, etc.) depending on their security and the security of the data they access. To be entirely secure MFA needs to be implemented across the entire organisation and tailored to different scenarios and user access requirements. This is especially crucial in security sensitive industries where the risks are high and a tighter control of data is demanded. .

In this e-guide we look at a variety of user authentication journeys and how MFA might be implemented to meet their individual access needs and the risk profile of the business and role. One size does not fit all, and we look at the different authentication types available to secure your business systems, whether they are on-premise, private cloud or public cloud.

Contents

Importance of MFA in Security Sensitive Industries

What is MFA?

Multi-factor Authentication (MFA) improves security for your business. The use of a single standard username and password to access business systems leaves your business-critical data and assets easy prey for cybercriminals. MFA addresses this weakness by providing additional layers of authentication, known as authentication factors.

Multi-Factor Authentication secures user access by combining two separate factors from the following three categories:

01 **Knowledge Factor** –
Something you know, such as a password, pattern or a PIN.

02 **Possession Factor** –
Something you have, such as a security token, a mobile device, a smartphone app or ID.

03 **Inherence Factor** –
Something you are. MFA can also use biometrics, such as fingerprint and eye scanning, facial or voice recognition to identify the user.

In addition, greater security can also be achieved by utilising other context factors such as **user location/geolocation, login time, device and authentication signals**.

Importance of MFA in Security Sensitive Industries

Security Sensitive Industries

Security-sensitive industries in particular need to ensure that the personal data and assets that they hold are kept safe and protected from threats. If a breach takes place, then cyber criminals could gain access to sensitive personal health information or credit card information and any loss of data may be in breach of data privacy regulations such as GDPR, PCI, HIPAA, etc. and subject to fines. Government departments, local government and public services need to ensure that not only personal data, but also other confidential assets are secured. Mission-critical sectors, such as infrastructure and utilities cannot risk a breach of systems with the potential for a service shutdown.

Examples of industries where security is especially crucial:

Government departments and defence industries where ensuring national security is paramount.

Banks holding personal credit card information.

Sectors such as **healthcare and insurance** holding patient or sensitive personal information need to abide by strict privacy regulations.

Mission-critical industries, who need to guarantee that the **national infrastructure** is kept running and cannot risk downtime, such as rail networks, ports, airports and **utilities**.

Pharmaceutical companies required to ensure their research data is kept secure.

Managed Service Providers and Partners who are providing a service for their customers who have sensitive data.

We will look at some examples of the different authentication journeys employees, partners and customers might have in different scenarios later in this guide.

Reasons for improving security with a fully comprehensive MFA solution

Ensuring your organisation is fully covered by comprehensive MFA is crucial for data security. This means your entire workforce wherever they are located and applications whether they are in the cloud and/or on-premise. We look at the reasons as to why this more important than ever:

Increasing numbers of breaches. The risk landscape is changing constantly and cybercriminals becoming more effective. Cyber risk hit the top of the Allianz Risk Barometer 2022 with increased high-profile ransomware attacks and security problems caused by accelerating digitalisation and remote working. Cyber risk was closely followed by business interruption risks.

With increasing numbers of breaches, organisations cannot remain complacent. Employees using weak passwords which are easy to hack and more and more sophisticated phishing attempts are making it easier for criminals to gather the password data and personal information they need for breaches. Access to personal information and password data can be bought "off-the-shelf" readily available online for cybercriminals to purchase and streamline their breach attempts.

Traditional Two-Factor Authentication (2FA) is no longer good enough. Two-factor authentication can make it more difficult for hackers and many organisations are already using it. 2FA consists of "something you know" with "something you have" e.g. smart tokens or one-time verification codes.

Although a minimum requirement, 2FA can still have vulnerabilities. A process built on password and one-time verification codes sent to a mobile device via SMS or email could be targeted by hackers. For less sensitive information, or information accessed infrequently, SMS may still be sufficient and fairly low risk.

But, with more and more people working remotely since the pandemic, the rise of online transactions, and the need for consumers to authenticate to personal data and banking systems, security might need to be improved with additional factors. Adding fingerprint recognition, which is now more commonly used on smartphones and laptops, or adding geolocation, are a couple of ways security can be enhanced.

Out-of-the-box MFA may not be enough to cover all your security requirements. Even if you have implemented readily available MFA solutions, such as Microsoft MFA, and rolled it out to cover Office365 or VPN, and use the mobile authenticator, you have not covered off all the other internal or bespoke applications you have on-premise which are used by some of your employees.

You indeed may still find that 50% of your workforce is left unprotected, especially if they cannot use a mobile phone and have no authentication option on their laptop. The whole workforce and outside users accessing your systems need to be able to authenticate with MFA in different situations to on-premise as well as cloud applications.

MFA for different security levels and scenarios across your organisation. Across your organisation, you probably have different types of users, customers and partners that require different levels of security depending on the information that they need to access.

Not everyone in your organisation needs access to "top secret", "confidential" or "classified" information, but others may well do. MFA needs to be able to cover the different user scenarios your business or organisation has. In the next section we take a look at the different authentication journeys they might take depending on their roles.

User Authentication Journeys

As mentioned previously, ensuring that you have your whole workforce, contractors, partners and customers covered with MFA in a host of different scenarios is crucial for any security-sensitive organisation or business. To ensure every angle is covered it is worth mapping the authentication journeys for different user profiles.

Matching MFA to security requirements and the needs of your stakeholders

	Office, Branch or On-site Access	Office and On-the-Road Access	Third Party Access
01. Location			
02. Security Level	Access to applications with sensitive personal data subject to regulatory compliance	Access to corporate applications, highly sensitive information	Access to corporate applications, and sensitive information
03. Role & Access Device	Office Teams – Corporate Laptop Call Centre Staff – Shared Desktop Branch Staff – Shared Desktop	Sales Team – Corporate Laptop / Mobile Phone CXO / Senior Mgmt – Corporate Laptop / Mobile Phone CEO – Corporate Laptop / Mobile Phone / BYOD	Outsourced IT Helpdesk – BYOD/3rd Party Laptop Contractors – BYOD
04. Considerations	No access to mobile phone	Laptop and phone while travelling	Via remote access Own device client office
05. MFA Options	Desktop One-Time Passcode Token Voice Yubico Yubikey	Mobile Push Wearables Biometrics Yubico Yubikey	Time-Based One-Time Passcode (TOTP-OTP) SMS One-Time Passcodes Email One-Time Password

Authentication Journey Examples

Here we look at four different users and their authentication journeys. While they have specific job roles, you may find similar profiles in your business or organisation.

#1 Carlos

Carlos frequently travels around the community for onsite visits, working from his corporate laptop to access O365 and a number of thick client applications.

His IT department has recognised that he has sensitive data and has implemented Microsoft MFA Authenticator App for his applications as well as the initial logon to his laptop.

There are occasions when Carlos visits residents who live in rural locations and he is required to work offline. Previously his laptop login would have not been protected, as Microsoft Authenticator does not support desktop logon. Fortunately for Carlos, the windows logon agent implemented by his IT department to secure his laptop logon with MFA, can still provide access and allow a secure logon offline.

#2 Janet

Janet is a lead data operational analyst, regularly working with classified sensitive data. She has security clearance and works onsite using a corporate issued laptop. To access the systems, she authenticates using a Yubikey hardware authentication device. The devices are only issued to authorised employees and contractors of the organisation. The Yubikey provides a one-time password each time she accesses the systems.

For organisations requiring a high level of security, the recognised strength of hardware tokens is essential, and the cost of providing individual hardware is outweighed by the very high security requirement.

#3 Marcus

Marcus is an IT support Engineer. He is working from home using his own personal laptop and needs to support a client, working on their applications via a VPN connection. He accesses the client's site using MFA with a smartphone soft token app with a push notification and additional biometric facial recognition to ensure complete security.

For any company granting access to their applications to third parties in their supply chain, strong authentication is crucial. Even the additional level of security is easy for Marcus given that he didn't have to enroll any additional biometric information as it leveraged the existing biometric authentication provided by his existing phone operating system.

#4 Karen

Karen has been retired for 5 years and receives her private pension. Recently the investment organisation updated its customer portal, which allows clients to review their personal details and accounts. As part of the update, they seamlessly integrated multi-factor authentication via a simple API call, to provide higher levels of customer security and comply with PCI regulations.

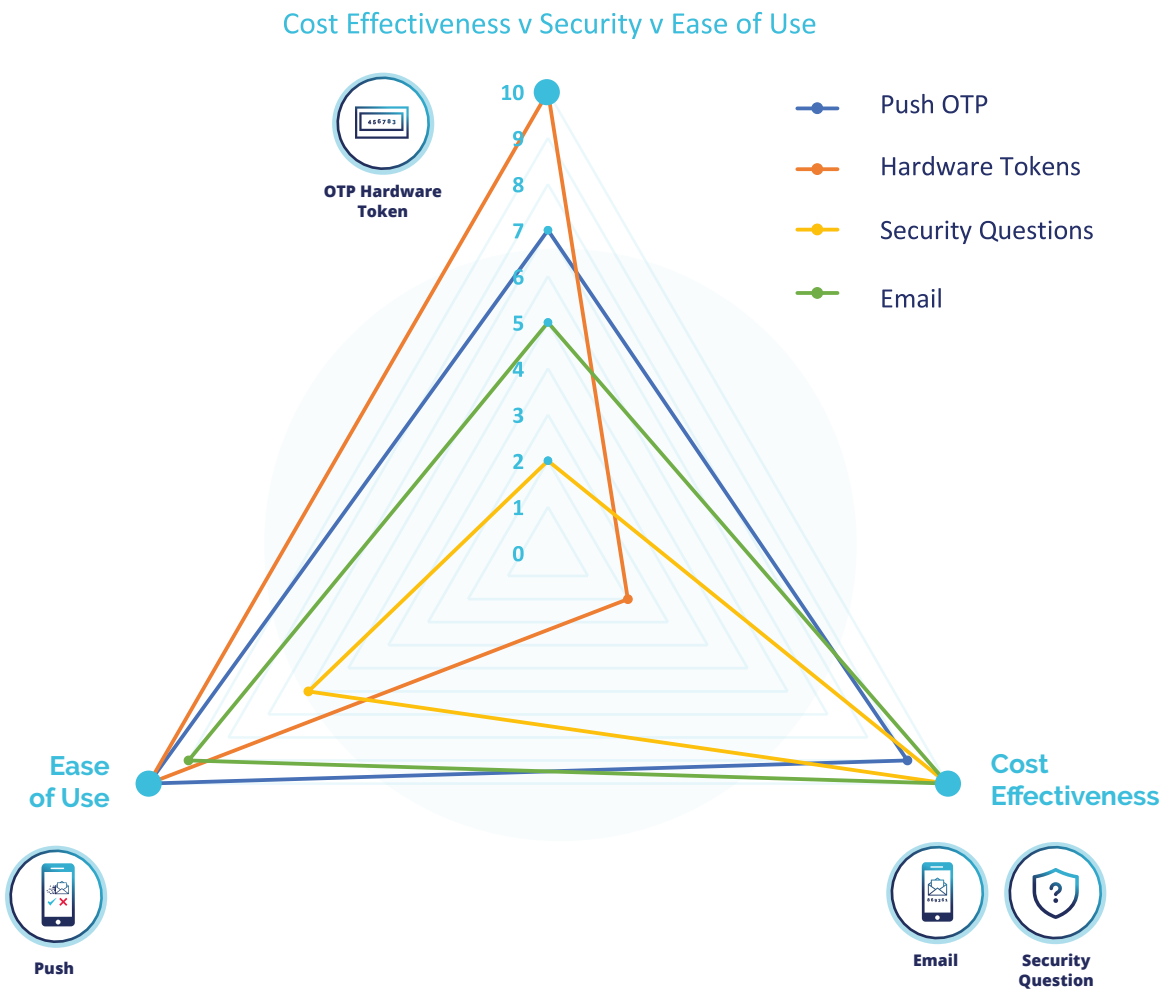
Due to the nature of the account, Karen only ever logs in once or twice a year, so has selected SMS as the mechanism to deliver her one time passcode (OTP). For Karen it is zero footprint, with no app to install and simple to use. As Karen only logs into her account from home, she could also select to have the OTP delivered to her landline.

Picking the right authentication options for your organisation

In some scenarios Yubikey might be the only MFA method, but for organisations, such as banks where there are different levels of security, using a Yubikey might be needed by some employees accessing highly critical applications or carrying out financial transactions, while others in a less sensitive areas, such as in a call centre environment might only be required to authenticate via a smartphone app.

Breadth of authentication methods is important when considering MFA, to ensure you have options for highly secure environments and securing sensitive data, through to giving access to less critical applications. Choosing the right solution for your requirements means evaluating the cost versus security/risk and usability for the employee, customer or partner.

Cost Effectiveness v Security v Ease of Use



MFA Best Practices

In summary, here are some final tips to ensure you make the most of MFA:

01 Deploy MFA across your entire organisation (all applications, on-premise and cloud).

02 Ensure all your workforce is covered – leaving no weak spots.

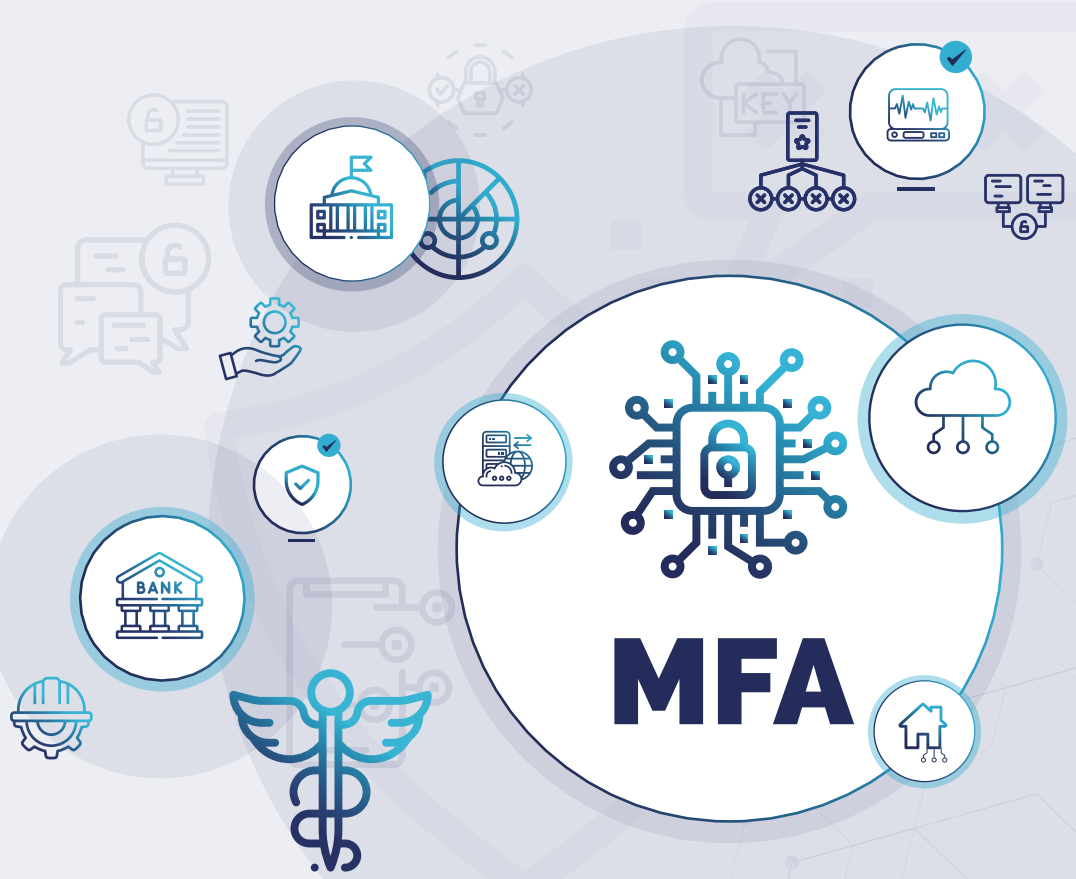
03 Tailor the authentication journey to meet the user needs and align to their risk profile

04 A variety of authentication options are vital for users. A good user experience = good uptake.

05 Combine MFA with complementary identity security tools, such as SSO and User Lifecylce Management.

06 Implementing a standalone MFA tool allows for greater control over MFA processes.

07 Continuously assess to ensure that your MFA solution is meeting the needs of the organisation and all the users.



SecurEnvoy
A Shearwater Group plc Company

The SecurEnvoy Zero Trust Access Solution

The SecurEnvoy Zero Tust Access Solution allows organisations to provide verifiable trust in every action taken.

By providing the identity of the user, the device and the data they are working on you can monitor and prove exactly who is doing what at any time.

Let's Talk

Talk to our experts today for a No-hassle, No Obligation Consultation.

support@securenvoy.com
securenvoy.com
linkedin.com/company/securenvoy
twitter.com/securenvoy