e-guide

Multi-Factor Authentication

Guide to On-Premise MFA

What to consider when you need the security of an on-premise or private cloud deployment of MFA

securenvoy.com

SecurEnvoy
A Shearwater Group plc Company

Executive Summary

Despite the advantages of moving to the cloud and in spite of security assurances, there are still organisations that are reliant on on-premise applications and data storage.

For those companies seeking more control of their data and security, mission-critical organisations who are unable to countenance even an hour's downtime, or those taking a phased approach to cloud migration, the on-premise environment is still very much part of the picture and likely to remain so.

Whether you are a company that is likely to continue with on-premise implementations or planning a phased migration to private cloud, public cloud or a hybrid model, the challenge is how to manage secure access for users across all these platforms effectively.

Multi-factor authentication is crucial, but how can you ensure that you have an MFA solution that is fit for on-premise, cloud and a wide range of business and user scenarios?

Read on to find out more about the challenges and options available.

Contents

On-Premise

What is “on-premise”?

First of all, let’s look at what we mean by “on-premise”. The definition has definitely moved on from meaning just “a server in the computer room”.

“On-premise” still means exactly that, i.e. where technology is located within the physical confines of an enterprise, often in the company’s data centre, as opposed to being remote on hosted servers or in the cloud. But it could also extend to a private cloud within a data centre controlled by the company.

The need to implement MFA on-premise vs in the cloud

While the cloud might be the obvious choice for many companies looking to reduce the cost of managing applications, there are a few fundamental reasons why some are opting out of public cloud and sticking to on-premise and private cloud for close control of their data.

Regulatory compliance

For any customer-facing company or public sector organisation operating today, ensuring data privacy and complying with data protection regulations is a prime concern.

Safeguarding personal information Many organisations dealing with sensitive personal data need to ensure that they have particularly tight procedures in place to protect them from a potential leak and ensure they meet regulations such as GDPR, PCI DSS or HIPAA. Moving data to the cloud means that you are reliant on the security and access controls provided by the cloud supplier. Often, organisations prefer to keep data on-premise or in a private cloud where they have sole access and control.

Data Residency/Sovereignty

Data privacy legislation in different countries can lead to differing data protection requirements, with the need to keep the data in the country of residence.

Managing international data protection policies For companies with a multi-country presence, variations in regulations in different countries can lead to the requirements for how and where data is stored to differ from place to place. There is often a need to keep certain data on-premise to ensure that it does not exit the country of residence In addition to data privacy regulations, other laws may be in place on the collection of data, for example, in the US where the Patriot Act enables the government to view data when deemed necessary.

Back up of data to countries outside the country of residence Data hosted in the public cloud is often backed up to a different country. Choosing a resident account (say, in the UK or US) with the hosting company can combat this, but can this be trusted? Some cloud applications, like Office 365, may transfer data abroad, and Microsoft Azure AD, for example, backs up to datacentres in the US and Finland. If your Zero Trust policy does not allow data to be transferred, this is yet another reason to retain applications and keep data on-premise.

Resilience and Business Continuity

How resilient is the cloud? No cloud supplier offers 100% availability. Though some offer 99.9% uptime guarantees, that might not be enough for some businesses, where even 0.01% can mean an outage of critical services for nearly an hour.

Is the cloud safe enough for your data? Cloud hosting companies provide a lot of functionality, but often the security they provide is for their platform and it might not be best suited for your data. The recommendation from the UK NCSC in their Cloud Security Shared Responsibility Model is to always have responsibility for making sure that 1) the service can meet your security needs, and 2) that the services you use are securely configured, alongside deciding which data to store in their services.

Risk of security breaches. The last point, but certainly not the least important. Does the cloud have the level of trust needed? With the number of breaches of cloud-based solutions increasing (e.g. Okta, Entrust, Azure), companies are cautious about multi-tenanted cloud and the risk of password reset mechanisms in the cloud. Instead, they are looking for more "security with obscurity".

What type of organisations need on-premise MFA?

Security Sensitive Industries

There are obvious industry sectors where additional data security is key and where there is often a requirement for data to be kept on-premise or in a private cloud for tighter security. Government departments and defence, for example, where national security is paramount.

Other sectors such as pharmaceuticals, healthcare and insurance, where data on research or patient and sensitive personal data is held, are other examples.

National infrastructure, including rail networks, ports and airports, along with mission-critical utility companies, all need to ensure that their services are kept running and secure, without the risk of downtime.

These organisations have one, or more, of the following challenges and demand tighter control of their data:

- Heavily regulated environments
- Large amounts of private or sensitive data which cannot be compromised
- Need to ensure that data stays within a specific region
- Cloud downtime is not an option
- Cannot risk security in any way

Migrating to the cloud in a phased approach

Not all companies staying with on-premise applications and data are as security conscious as the defence industry, for example. Deciding to remain on-premise might well be required as you move to the cloud in a staged approach, or adopt a hybrid model of cloud and on-premise/private cloud. Or, you might need to consider more secure authentication requirements for some users and departments across your organisation.

Whatever the reason you choose to have some, or all of your applications and data on-premise, there is still a need to ensure that access for users and customers via multi-factor authentication, is available in whichever environment

When is an MFA solution really “on-premise”?

The lion’s share of new vendors in the MFA market provide software-as-a-service implementations of MFA – which means that the only option is to have a cloud solution, with the security and data control risks that poses.

Some MFA vendors do offer both, but they have two separate code bases for on-premise and cloud, or they may be in the process of transitioning to a cloud code base.

This can result in some features only being available in the cloud, while other features are only available in the on-premise version. This can limit the capabilities available if you are only looking at on-premise and limit the ability to cater for different scenarios and locations where you would still like the same features on-premise and in the cloud.

What to consider when implementing MFA on-premise

Authentication is an important consideration when deploying a complete on-premise solution. Many forms of MFA require the internet for connection in order to send a request to a mobile phone, whether it is for SMS or Push OTP. For a full on-premise solution, consider using an OTP app on phone and hardware tokens.

Enrolment page for new users. When implementing MFA securely, you might also want to consider using internal enrolment for new users on the local area network, rather than public-facing enrolment or choose the one most suited for the security levels needed.

Flexible Multi-Factor Authentication - On-Premise or however you need it

SecurEnvoy MFA offers a solution to help customers who are looking for an on-premise deployment, but which also provides future-proofing to ensure that your MFA keeps up with the changing demands of the organisation. This MFA offering provides flexible options to suit the business and its users. Let's take a look at some of the advantages.

Future Proofed MFA

On-premise now – with the option for cloud in the future. SecurEnvoy MFA enables you to have an on-premise only solution and move to cloud for some applications or move to the cloud in the future, all using the same technology from start to finish.

Adopt a hybrid architecture. SecurEnvoy MFA gives you the option to support a hybrid architecture with some data residing on-premise and some in the cloud.

The same features - on-premise, in private or public cloud. SecurEnvoy MFA has been developed as one code-base – one solution whether you are implementing on-premise, in your private cloud or in the public cloud. With one code-base all the same MFA functions are available, whichever environment you choose, and you are sure to get all the latest and greatest features whether you are implementing on-premise or in the cloud.

Adaptable to changing risks and regulations. SecurEnvoy MFA provides a migration path to go to the cloud (or back) if your security posture changes or regulatory compliance rules change.

Adaptable to local requirements – SecurEnvoy MFA gives different departments and countries the ability to choose the environment which is most suited to their local data control requirements.

Flexible MFA on-premise, in the cloud or hybrid environment

On-premise -Server room

Public cloud

Cloud Services:
Box, Dropbox, Hosted Exchange, Azure, Office 365, Sharepoint, OneDrive, Google Drive

On-premise - In private hosted data centre

Private cloud with country-specific mode

Flexible MFA Options

Easily deployed in different environments – With SecurEnvoy MFA you have the option of deploying MFA in a range of different environments:

- Server in the computer room
- In private hosted data centre
- In the public cloud
- On-premise + public cloud

Meeting the needs of different users and regional differences

Role-based access control is not what it used to be – i.e. *"one size fits all"*. The needs of different parts of the business and users, some wanting to use personal phones, others needing higher levels of security clearance, means that authentication needs to be tailored to the user and security requirements. There may also be global and regional differences in the type of authentication needed.

With SecurEnvoy MFA you get a wide range of modern authentication options to meet the needs of different users and business requirements and you can read more about the options available for different scenarios in the following section.

Easy administration through your own directory services and fast deployment

With SecurEnvoy MFA there is no need to learn another tool for administration, you can use your own directory services and it is easy to deploy in a matter of minutes.

Security with obscurity

If your organisation needs to be ultra-cautious enrollment for employees and administration staff can be carried out on-premise, reducing risk of a breach via web-based enrollment.

Security with confidence

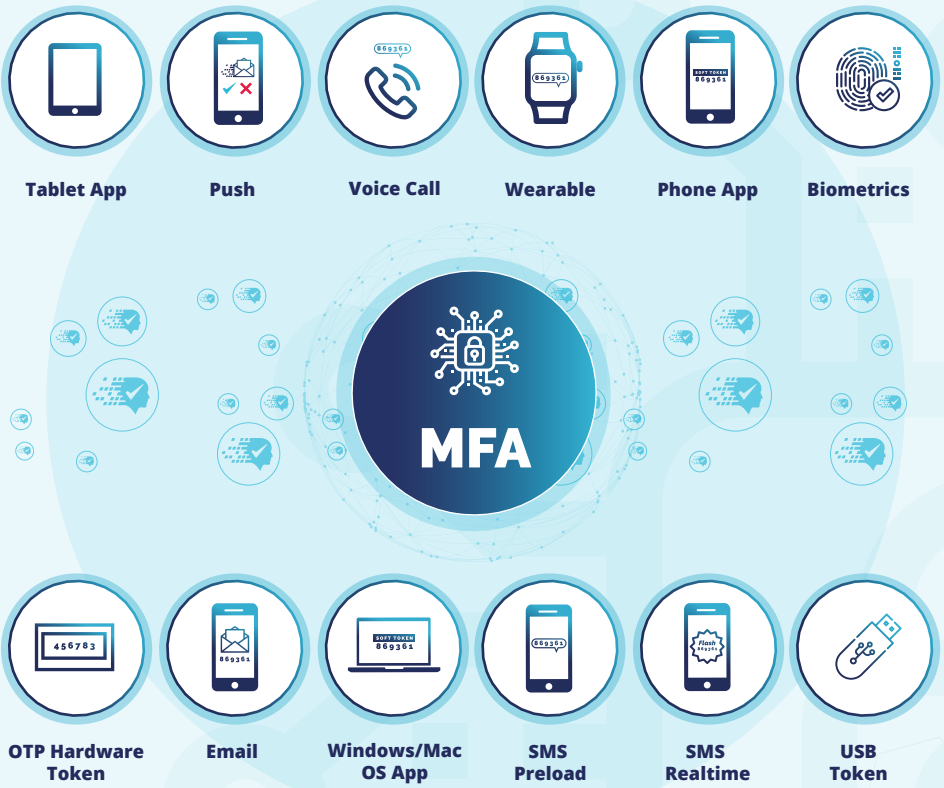
SecurEnvoy MFA has a clean bill of health in all pen tests that have been conducted.

SecurEnvoy MFA – Modern Authentication

What is Modern Authentication? - Modern authentication is more than just traditional multi-factor authentication and uses similar techniques to those used in complicated Access Management products. For example, Modern Authentication takes all the different signals used during an authentication attempt, such as the location, network, time of day, browser etc. to determine whether a user should have access – regardless of whether a user has correctly verified themself.

SecurEnvoy MFA has the ability to enable a range of authentication methods which means that organisations can select the most appropriate authentication technology to address different use cases and take different levels of security into account.

In addition to identifying different signals during the authentication process, SecurEnvoy MFA provides all the authentication methods below whether on-premise, or in a private or public cloud.



Find out more about SecurEnvoy MFA Authentication Methods >

Flexible Multi-Factor Authentication

Conclusion

If an on-premise only MFA solution is required, make sure that it is truly on-premise in all aspects, or that you understand the potential limitations.

If you have some cloud applications but also need to keep other applications on-premise for security reasons, or need to facilitate the requirements of different departments and country offices, then a flexible solution is required that provides all the features you need across on-premise, private and public cloud.

SecurEnvoy MFA overcomes these challenges and can ensure that your environment is secured for the future.

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