e-guide

Multi-Factor Authentication Buyer's Guide

What to consider when assessing multi-factor authentication solutions

securenvoy.com

SecurEnvoy
A Shearwater Group plc Company

Introduction

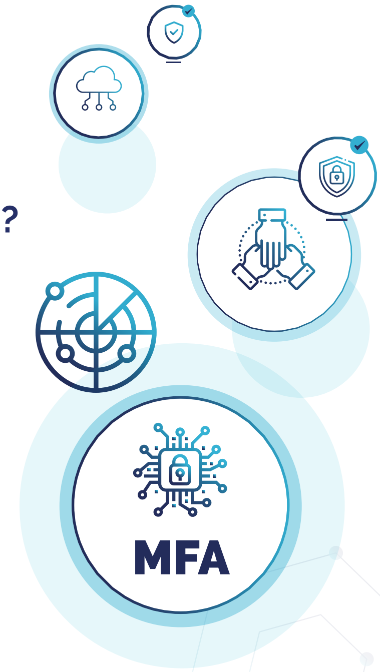
With the increase in phishing and data breaches over the last few years, the chances are that your login credentials (and those of your employees) are out on the dark web somewhere and it is only a matter of time before someone uses them.

Multi-factor authentication is one of the easiest methods to deploy to ensure that your user accounts are safe. It is far more difficult for an unauthorised person to gain access to your network, applications and databases if you have additional authentication methods in place to verify a user's identity when they log in.

However, as IT environments become more complex, with on-premise, hybrid and cloud-based applications, different devices accessing your systems and employees working from home or out in the field, MFA needs to cover a host of different IT and business scenarios and to be easy to use and implement.

In this guide we take an in-depth look at the options and features of multi-factor authentication, including their advantages and disadvantages, and provide recommendations to help you make the most informed choice when buying and implementing MFA solutions.

Contents



e-guide

What is MFA?

MFA or multi-factor authentication is the process of authenticating a user account using both something you know (your password/PIN) and something you own (a device such as a plastic token or mobile phone), or something you are (biometrics). IT security experts universally recommend the implementation of MFA, particularly for public-facing portals, as it reduces the risk of unauthorised access due to threats such as password theft, shoulder surfing and password guessing.

The use of MFA is now widespread. With the low cost of implementing MFA versus the reduction in fraud, it is now hard to find a bank, public-sector organisation, email provider or large online retailer that is not using two-factor or multi-factor authentication. In addition, with MFA being so crucial for business security, insurers are now requiring MFA to be in place as part of cyber security insurance policy conditions.

> "Multifactor authentication is a time-tested approach that has now come of age. Organizations recognize that they face an increasing threat from the compromise of password-based credentials; knowledge-based authentication simply doesn't provide an adequate level of protection against those threats. Push-based authentication using smartphones is both simple for end users and cost-effective for the organization."
>
> **Source: IDC**

What are the Authentication Factors?

Multi-Factor Authentication, as the name suggests, requires two separate factors to ensure authentication:

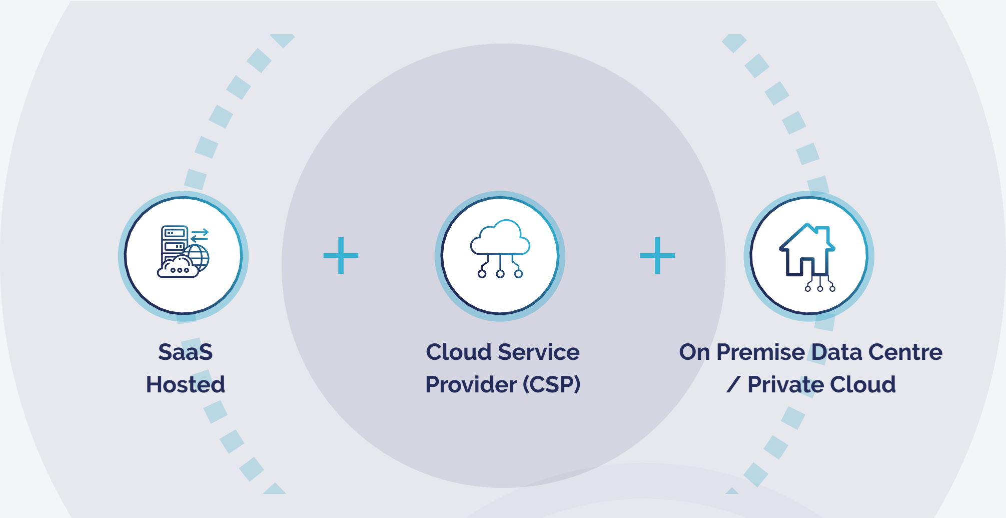
01. A password or PIN which is "**something you know**" (known as the "knowledge factor").

02. "**Something you have**", such as a security token, mobile device or smartphone app to approve authentication requests (known as the "possession factor").

03. Biometrics (known as an "inherence factor" or "**something you are**"), such as fingerprints, facial or voice recognition can also act as a third factor in the authentication process.

Deployment Options

MFA solutions are often available in a variety of architectural formats.


SaaS Hosted
+
Cloud Service Provider (CSP)
+
On Premise Data Centre / Private Cloud

Public Cloud - SaaS

Public cloud based solutions are commonly hosted by the MFA vendor. The maintenance and upgrades to the solution are handled by the vendor, however unlike a dedicated managed service, the ongoing management is made available to you via a web-based portal.

When compared to deploying an on-premise MFA solution, choosing SaaS typically has a lower TCO.

For the security conscious, there are challenges around the ownership of the cryptographic key and how to securely synchronise internal user repositories (for example, Microsoft Active Directory) with the cloud.

On-premise / Private Cloud

An on-premise MFA solution historically required authentication software to be deployed onto a dedicated server, typically a virtual server. More commonly today these types of on-premise deployments are made in dedicated private cloud environments.

On-premise and Private Cloud deployments perhaps tend to be more popular with organisations who are more security conscious and have security concerns regarding the use of multi-tenant style SaaS solutions.

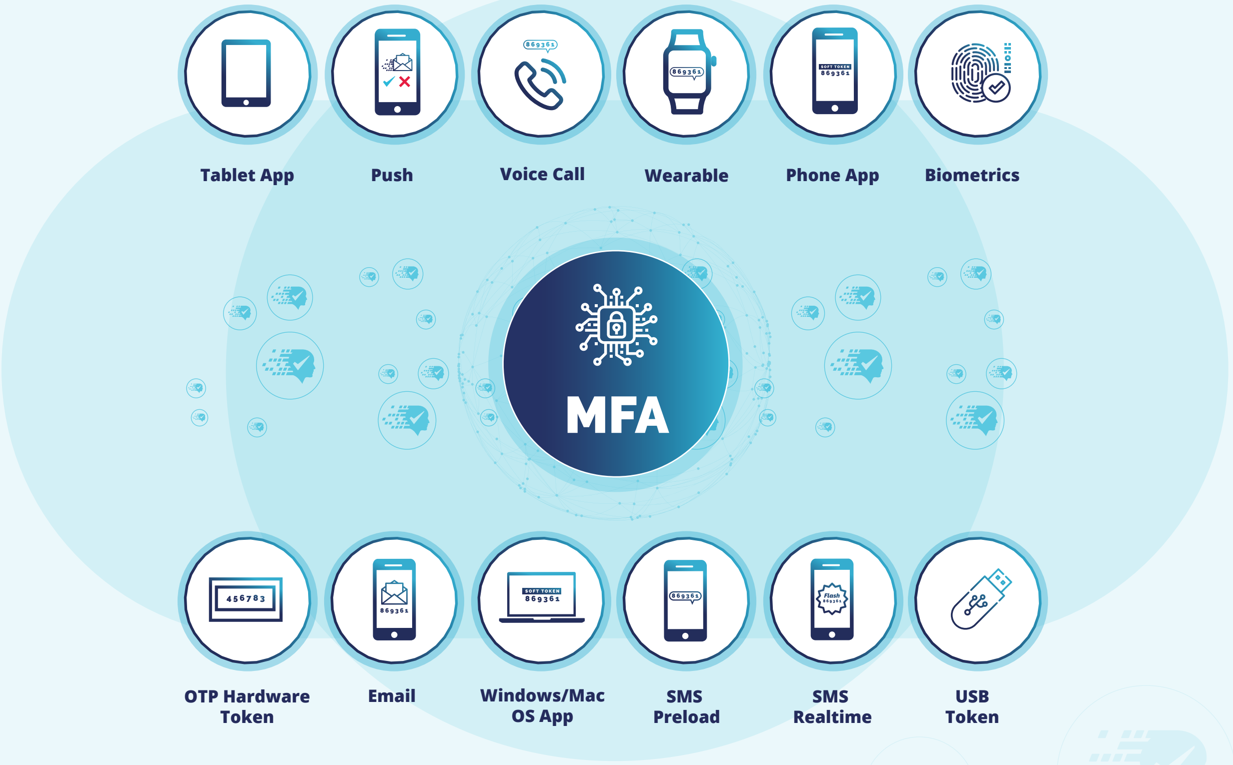
The main drawback to this style of deployment is the administration overhead that comes with keeping an authentication system operational and secure. This drawback can be addressed as part of a dedicated managed service from a reputable Managed Security Service Provider (MSSP).

Consider the Importance of Deployment Flexibility

The MFA industry has seen rapid adoption of SaaS deployments in recent years, with small and medium sized businesses in particular viewing the perceived cost saving opportunities as attractive.

Larger and more heavily regulated organisations have been slower to succumb to change, sometimes unhappy with the additional risk of not hosting the solution themselves. As a recommendation, choosing a vendor who supports both formats and allows you to move easily between them could be key, as today's choices may not reflect tomorrow’s challenges.

Authentication Methods



Since the early days of MFA, where a physical plastic token was issued to the user, the options available have grown significantly, with a range of physical or software-based tokens common place.

Hardware Tokens

Form factors including key fob, credit card and USB tokens are most seen when selecting a physical token for authentication.

Standard OATH compliant TOTP & HOTP tokens are a dedicated authentication device which does not require an external connection to generate a one-time passcode (OTP). Hardware token deployments are often seen either within organisations that are security conscious, such as government and defence and do not allow mobile devices or those where corporate mobile devices have not been issued and users do not consent to the use of their own personal devices for work business.

USB Hardware Tokens, such as the Yubikey from Yubico offer the advantages of the traditional hardware token, but with the added advantage of an improved end user experience, with the OTP being automatically entered at the press of a key on the token, avoiding the requirement for the user to key in the code manually.

As with most things in life there are pros and cons and hardware tokens are no different. Physical devices do require an initial procurement, which can be costly compared to its software counterpart. Once procured, the device must be provisioned to the user, which typically requires physically shipping. Ongoing support for lost and broken tokens must also be factored into any TCO calculation. Another consideration is the carbon footprint of any physical token deployment, with thought being given to both the actual manufacturing and shipping of the device.

Software Tokens

Software tokens are typically available on either smartphone, tablet or laptop. Software authenticators have a much lower total cost of ownership and are quicker to deploy than hardware authenticators. Deployments benefit from the care and personal security afforded to the device by the user. Devices are typically protected by a PIN, password or biometric, meaning if lost it cannot be misused.

Software tokens on mobile devices, also known as soft tokens are an application that is either downloaded by the user from the relevant app store (Android, iOS) or pushed down via a mobile device management system (MDM). The user would then typically enrol the token via scanning a QR code to get the unique seed record onto the device. The soft token generates a 6-8 digit pseudo random number which the user enters during logon in addition to their standard user name and password. More modern soft tokens also support 'push' notifications for user authentication. This involves a notification being sent to the phone following the successful entry of a username and password. The user is then prompted to either accept or deny the authentication to authorise the access. On more secure implementations, the 'push' notification can also be protected by the inbuilt devices' biometric authentication.

Another software token form factor offered by some multi-factor authentication vendors are those deployed directly to a user's laptop (Windows, macOS). Particularly suitable for users without a corporate issued mobile device. The advantage is the requirement not to have an additional device to carry, however conversely from a security standpoint, that advantage also acts as a disadvantage due to the authenticator not being a disparate device. Also, there would be a limitation of where the authenticator could be used, as access to it is post device logon, meaning that it could not be used to enhance the security of the actual device logon itself.

SMS Tokens

Leveraging SMS as the OTP delivery mechanism allows for rapid deployment and a zero-footprint approach, meaning no software or physical device is required to be deployed. Early SMS authentication implementations suffered from native legacy GSM issues such as SMS delays and network coverage issues. Some vendors addressed this issue with the implementation of pre-loaded passcodes, however today GSM coverage is extremely good.

In 2016, NIST (National Institute of Standards and Technology) issued guidance against the use of SMS for delivery of OTPs as it can be intercepted, however following a full risk analysis, many organisations still deploy for low-medium sensitive use cases, particularly with infrequent use situations.

Email Tokens

Delivery of the OTP via email is a rudimentary implementation of multi-factor authentication that organisations may choose for very low value access. The advantage once again is that it is a zero-footprint implementation and doesn't rely on a users' personal device, however the disadvantage is that the email communication channel is unencrypted with the code being delivered in clear text across the network.

Authentication Options Summary

In an ever-changing world, it is important to not only think about today's requirements, but also consider the future. It is recommended to choose a solution which can not only deliver on today's needs, but also be fit for tomorrow's challenges, so select a vendor with a wide range of authentication methods.

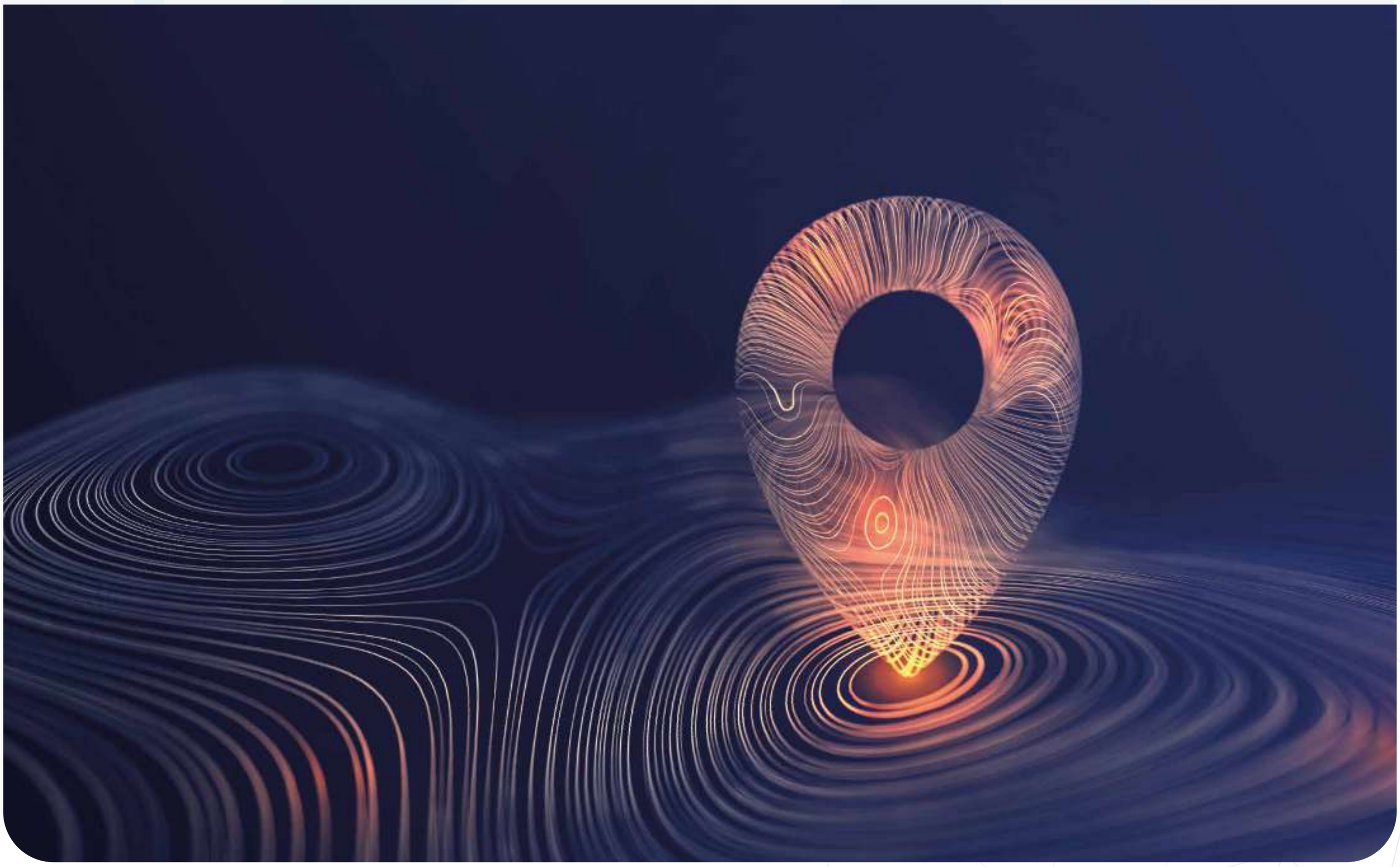
Geo-Location

Building additional trust into the user authentication process can be achieved by adding more context to the interaction. Most commonly this is via the use of geo-location information, traditionally using GeoIP, where the IP address from the user is looked up on a database to see what country or region they are connecting from.

Using a third-party database, you can map an IP address to a location, however accuracy can always be an issue. The main drawback with this approach is that using simple techniques such as proxy, VPN service or browser plugin, the location of the user could very easily be spoofed.

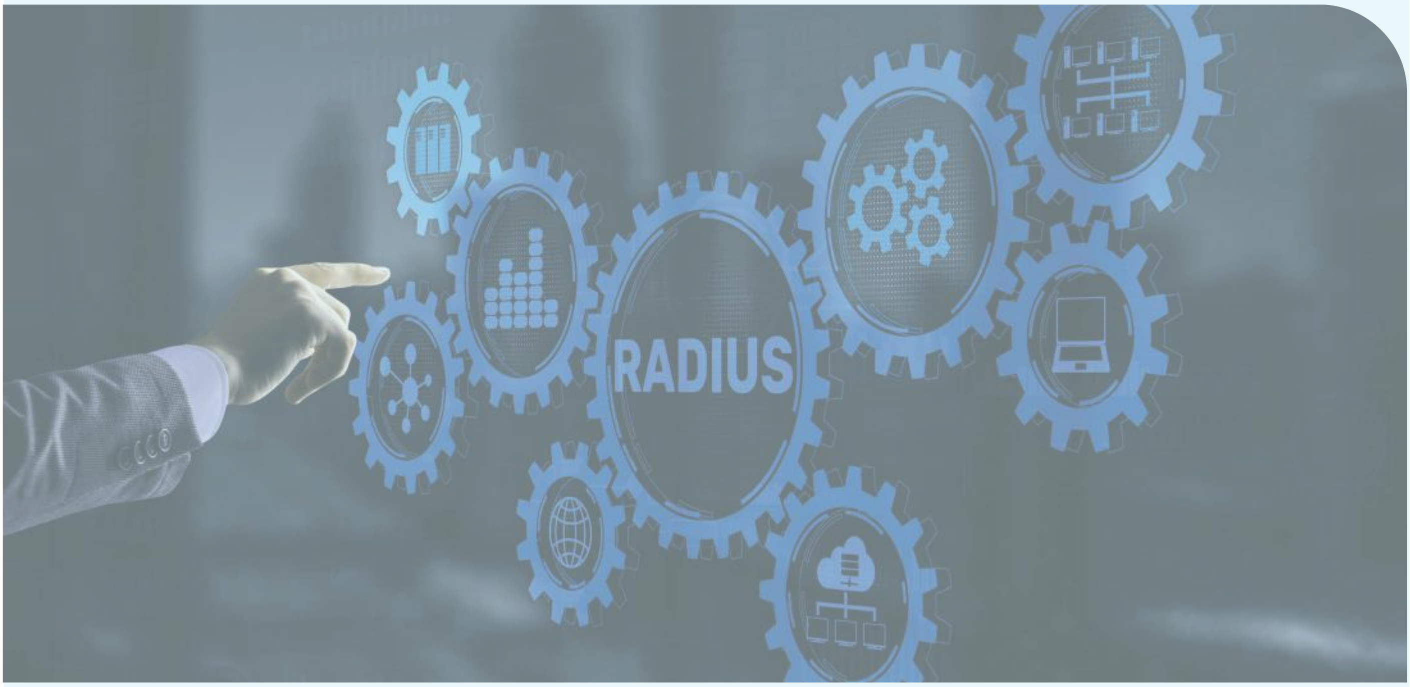
If user location is to form a significant factor in the trust of the user authenticating, you must be able to rely on the accuracy of the location. There are vendors who offer a deeper user location capability, combining additional location metrics such as GPS and GSM cell tower information to provide a true user location. The true location of the user is crucial for a more detailed analysis allowing intelligent decisions to be applied.

With accurate location metrics, you can then configure 'Safe Zones' which can grant access to a user if they are within a certain 'Safe Zone' location. Furthermore, additional security can be added by configuring a maximum distance between where the user request came from and where the authentication response was located.



Integration Areas

It is important to think broadly when it comes to what applications and access need to be protected via multi-factor authentication. It is advised that where a password is used security should be enhanced by adding multi-factor authentication. To achieve this requires a solution that supports a range of authentication standards and has, where required, the appropriate agents..



Remote Authentication Dial-In User Service (RADIUS)

Despite companies beginning to move their IT environments to the cloud, existing on-premise environments are often protected by a VPN or other remote access methods. Predominantly, these methods support the RADIUS protocol.

To support legacy environments and technologies, many vendors offer RADIUS support, however not all offer fully featured RADIUS functionality. Consider the benefits of a vendor that has developed RADIUS capability to offer options such as 'Trusted Networks' and 'Trusted Groups'.

Implementing a 'Trusted Networks' policy, is where users connecting from a specific address or hostname would not get prompted for MFA and could authenticate with just username and password. Secondly 'Blocked Networks' can be added on a similar basis, where authentication attempts from a specified network location(s) will get blocked outright.

'Trusted Groups' can also be configured, whereby users within specified groups will not require MFA when authenticating. For example, users within the 'administrators' group must always provide MFA.

Attributes can be passed back to the RADIUS client, if required. Authentication can only be permitted from specific domains too, which is ideal with Managed Service Providers running multi-tenant environments.

Protecting Desktop Logon & RDP

Securing the logon process for the Windows or macOS with multi-factor authentication is still important today as it protects the device itself, which can be the trusted gateway access to your organisation. There are vendors who offer an agent to be deployed to the device itself via group policy or another orchestration mechanism. The agent could be configured to protect logon and unlock, so if a user manually locks their machine they'll be prompted for MFA on their return.

Users can be enabled for MFA with Group Memberships. For example, only Domain or Local Administrators can be prompted for MFA when RDP'ing into servers, restricting access for users outside of this group – mitigating the risk of credential misuse.

Agents can seamlessly integrate with Microsoft OS or macOS, providing a native workflow for users. Additional features may include emergency access and self-service password reset for users from the endpoint itself.

Web Application Authentication Protocols

With most applications now delivered via the web, it means that authentication technologies need to support a range of web authentication protocols natively.

Security Assertion Markup Language (SAML) is an open standard that is widely employed by both web application providers and single sign-on solutions (SSO) and is the most common authentication protocol in use, particularly when associated with single sign-on for web applications.

OpenID & OAuth are similar to SAML but predominantly used for consumer facing web applications.

Web Services Federation Protocol (WS-Fed) is exclusively used for Microsoft-related products.

The key to a successful authentication deployment is to determine which authentication protocols are in use and work with an identity provider which supports these standards-based authentication protocols, without the need for custom proprietary protocols. A pre-populated catalogue of the most common applications is useful, but the ability to add customer apps dynamically is very important to support your organisations requirements not only today, but in the future.

Self-Service Administration

To optimise end user experience and reduce burdens upon the administration team, it is key to review and implement end user self-service capabilities.

In a recent study, over 50% of users have executed at least five password resets each month on average; spending at least 10 minutes each time doing so*. This can in turn be a large administrative overhead for the IT department if a self-service password reset mechanism is not enabled.

Further to the password, which is the usual first factor in any logon, it is important to cater for users who lose or misplace their token or device.

There are vendors who can use a combination of secret questions, biometrics, passwords, emails or OTPs to resolve lost device issues.

To reduce administrative overheads, investigate authentication vendors options when it comes to user self-service relating to provisioning, lost passwords and devices/tokens.

Licensing

Over the years we have seen an evolution from capital expenditure perpetual licensing models to operational expenditure subscription models dominating the market. Subscriptions periods range anything from monthly to up to five years in advance. If your user base is affected by seasonal fluctuations monthly models may provide the flexibility you require. Alternatively, annual subscriptions can prove to be a more predictable, cost-effective approach.

With regards to varying editions and licensing bundles, it is always worth reviewing what you require from a feature perspective and ensure you are paying for the features you actually need and not over-licensing.

Summary

To summarise, when selecting a new MFA vendor, ensure you consider a solution that is both flexible in its deployment, integration capabilities and authentication methods, as business requirements can evolve quickly. Having a solution that supports new business requirements without the need to change vendors, re-enrol users or redeploy infrastructure is key to success.

SecurEnvoy MFA provides a full range of easy-to-use authentication options, beyond SMS, and is able to scale as your business evolves, seamlessly integrating with your existing user repositories. Fast to deploy – up to 100,000 users per hour – on-premise, private cloud, hosted via AWS or Azure, or as a fully managed cloud service.

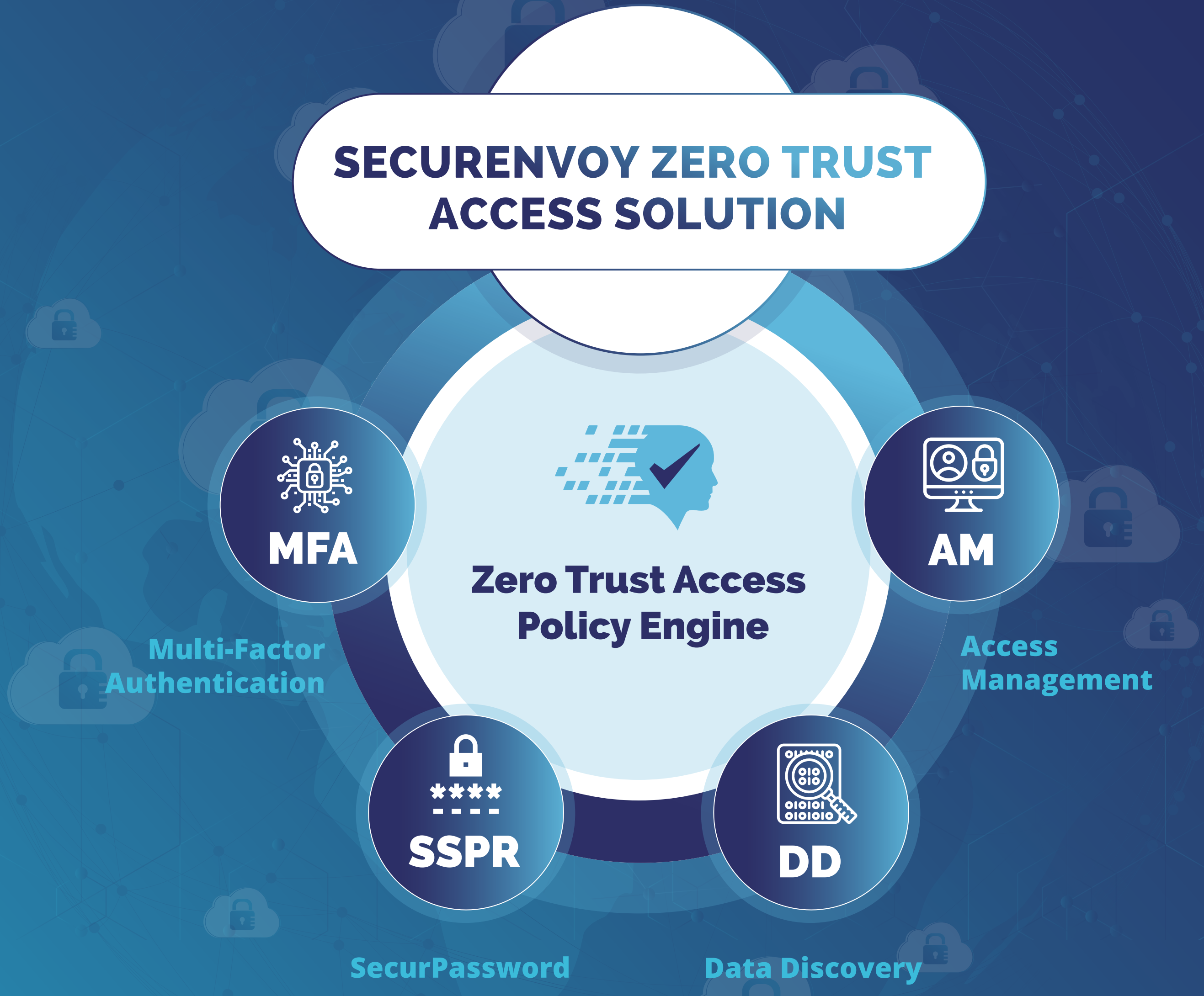
Try free today: securenvoy.com/trial

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.


SECURENVOY ZERO TRUST ACCESS SOLUTION
MFA
Multi-Factor Authentication
Zero Trust Access Policy Engine
AM
Access Management
SSPR
SecurPassword
DD
Data Discovery

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