



SecurEnvoy

A Shearwater Group plc Company

Identity Beyond Boundaries

The SecurIdentity™ Platform

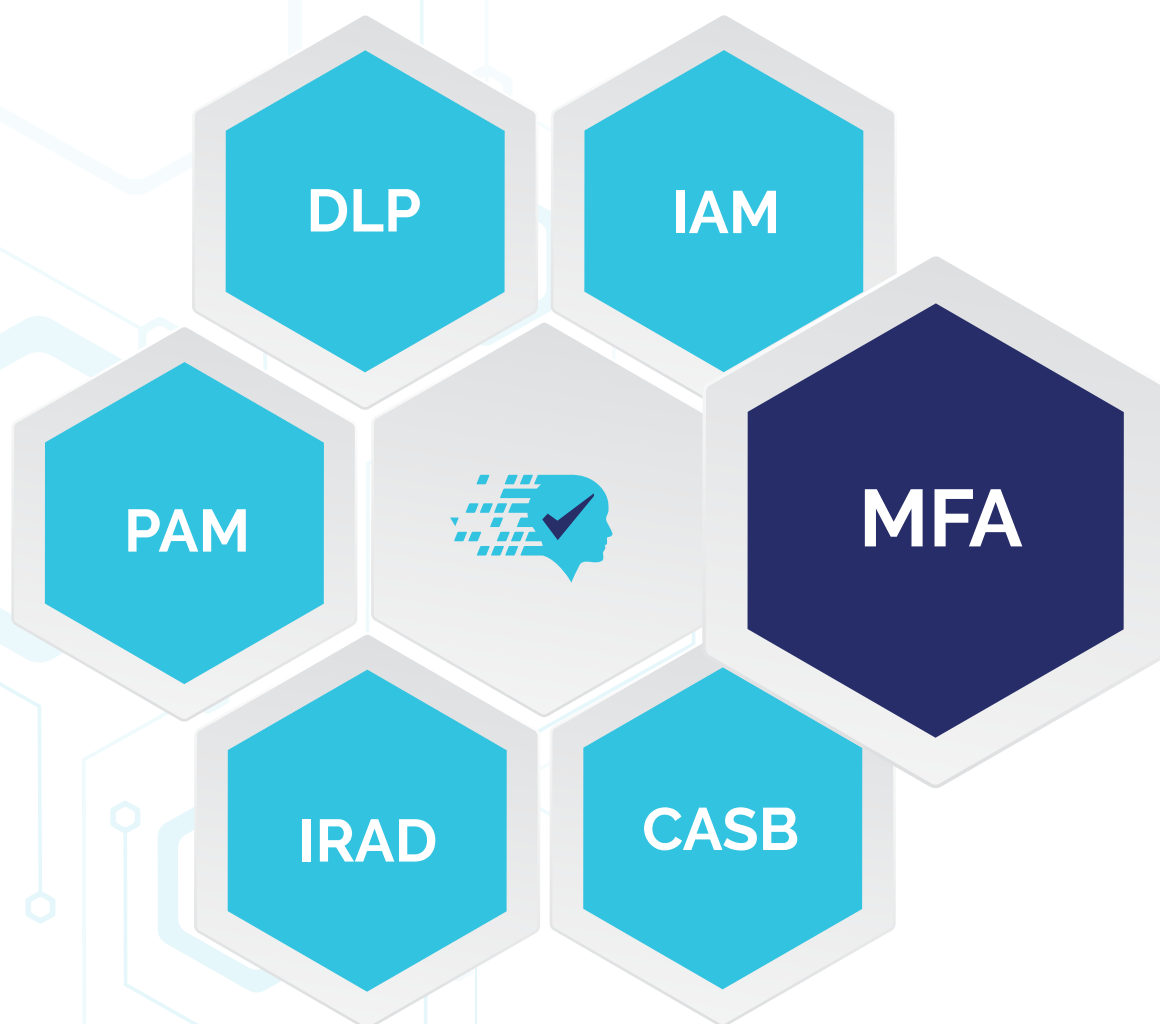
Multi-Factor Authentication (MFA)



Introducing the SecurIdentity™ Platform

The SecurIdentity™ Platform allows organisations to provide verifiable trust in every transaction they perform. By providing the identity of the user, the device and the data they are working on you can prove exactly who is doing what at any time.

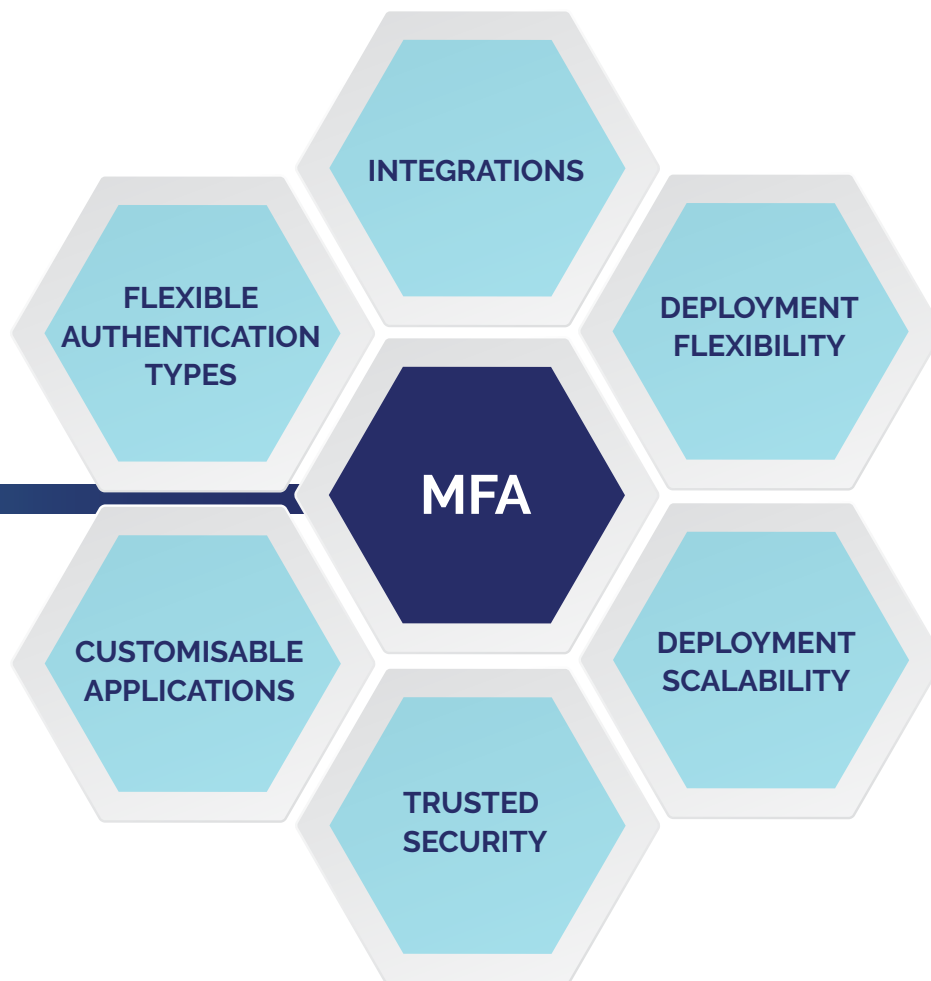
This ensures compliance within the corporate policy, reduction of risk of fines and protection of your vital intellectual property and business assets



Building upon our success of a leading on-premise MFA solution, SecurEnvoy's vision is to bring additional software technologies to market, allow corporations to understand the identity of the user, identity of the device and identity of the data. The intelligence will provide detailed context and behavioural analysis of the user, the device and the data they interact with.

Multi-Factor Authentication (MFA)

Tokenless® Two Factor Authentication for VPN, SSL, Remote Desktop, WiFi, Web portals, laptop access and other solutions.



Passwords alone are not strong enough to protect your business-critical data and assets. SecurEnvoy Multi-factor authentication provides the security of user identity by verifying that a person is who they claim to be. Utilising something the user knows (Password/PIN), something they have (Software/Hardware Token) and in some instances, something they are (Biometric/ Facial Recognition).

SecurEnvoy's MFA solution integrates seamlessly with Microsoft's Active Directory and other LDAP solutions, reutilising the enterprises existing authentication database infrastructure, avoiding the need to re-architect, deploy, backup and manage a secondary user database.

Authentication Types

SecurEnvoy believe users should be able to choose any personal device to be their authentication token, whether it is their mobile phone, tablet, laptop or even their desk phone. Users should be able to seamlessly move their single identity between these devices without leaving their identity behind on obsolete technology.



SecurEnvoy's various authentication methods allow for a comprehensive fulfilment of different users requirements. Companies have the ability to control what token types should be used by their employees, including selection and control via brandable self-enrolment portal.

Security

Security that puts you in control. Cryptographic keys, called seed records are inherent in the communication of any MFA solution, commonly generated and distributed by a server in the enterprise or cloud when issuing one-time passwords (OTP's) to clients. SecurEnvoy's solution uniquely splits the keys as to only store one part on the user device. The second half is generated from a HW fingerprint when the SecurEnvoy application is run. This approach provides additional security copy protection for the SEED record, as the user device is deemed to be a larger attack vector, as it resides in a more hostile environment. The SecurEnvoy solution uses AES 256-bit to store securely within the enterprise directory environment.

Solution Deployment

SecurEnvoy MFA offers deployment options to suit any business, with an On-Premise, Private Cloud or fully managed CSP solution in either independent or industry recognised IaaS environments like Amazon AWS and Azure.

The challenge of deploying any MFA solution to a user community is the method in which users are notified and enrolled.

Applying SecurEnvoy's seamless integration into the Enterprise LDAP environment, our MFA solution utilises "Automatic Group Deployment" to monitor selected LDAP groups for any new or removed users, issuing an enrolment invite via the chosen method i.e. SMS or Email or placing user into an unmanaged state when removed from LDAP environment. SecurEnvoy can deploy more than 100k users per hour.

Scalability

SecurEnvoy's MFA solution integrates seamlessly with Microsoft's Active Directory and other LDAP solutions, reutilising the enterprises existing database infrastructure, avoiding the need to re-architect and manage a secondary user database.

SecurEnvoy is able to use a mixed LDAP environment (includes AD LDS), thereby supporting a fully heterogeneous environment consisting of multiple authentication domains across distributed sites.

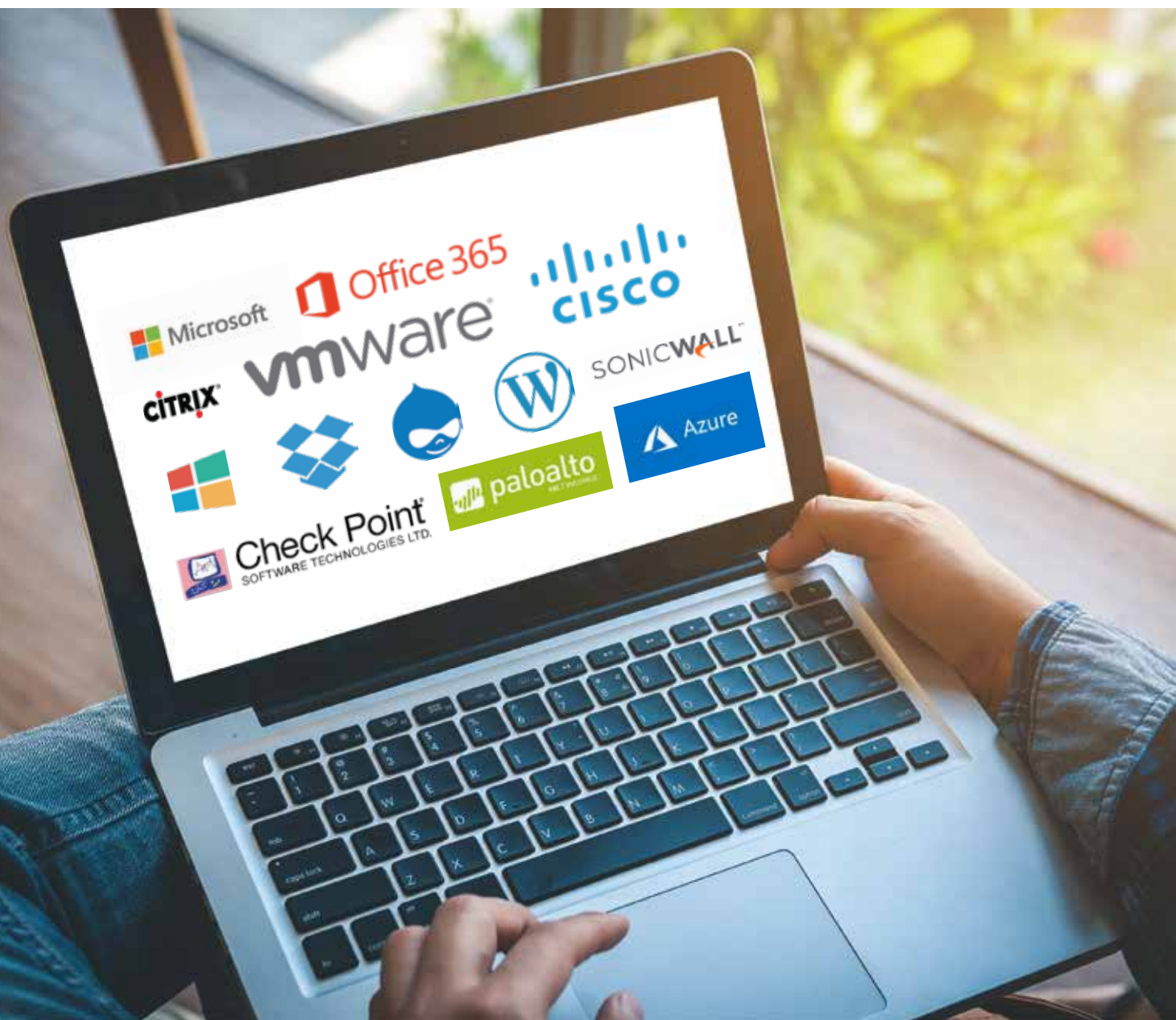
SecurEnvoy MFA deployments are focused primarily at delivering a resilient and distributed server architecture with seamless replication of configuration as all data is stored directly in LDAP.



Integration

SecurEnvoy MFA supports various interfaces to support countless SaaS or on-premise applications or network connectivity that require securing.

- ✓ Windows Server Agent offers the ability to secure any IIS hosted websites (e.g. OWA, SharePoint or customer web application).
- ✓ Support for ADFS in delivering MFA authentication to public SaaS or SAML authentication-based applications.
- ✓ Windows Logon Agent extends MFA authentication to domain joined laptops in an online or offline state.
- ✓ RADIUS with individual configuration for each client allows integration for all major SSL/IPSEC based security appliances.



Migration

The Migration feature allows users to be migrated to a SecurEnvoy solution from a password-only or an existing token solution. Once configured, users can be migrated in stages as required, allowing a smoother transition and onboarding process.

Customisation

SecurEnvoy offer customisation support to any end user portals and mobile interfaces. This allows corporations to create seamless, branded environments. Choose a custom colour and add your logo for a consistent customer experience.

API

SecurEnvoy's Open APIs allow software developers direct access to information and configuration controls of the MFA environment. Built using the Representational State Transfer (REST) framework, SecurEnvoy's Open APIs enables you to automate the creation and modification of users, including the authentication via a HTTP web call.





Global Impact & Innovation.

Let's Talk.

Global Hubs

LONDON

MUNICH

NORTH SYDNEY

CHICAGO

NEW YORK

BASINGSTOKE

SALES

sales@securenvoy.com

TECHNICAL SUPPORT

support@securenvoy.com



SecurEnvoy

A Shearwater Group plc Company

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010
Company No. 04866711 VAT Number GB 862076128

[SecurEnvoy.com](https://www.securenvoy.com)



SecurEnvoy

A Shearwater Group plc Company

Identity Beyond Boundaries

The SecurIdentity™ Platform

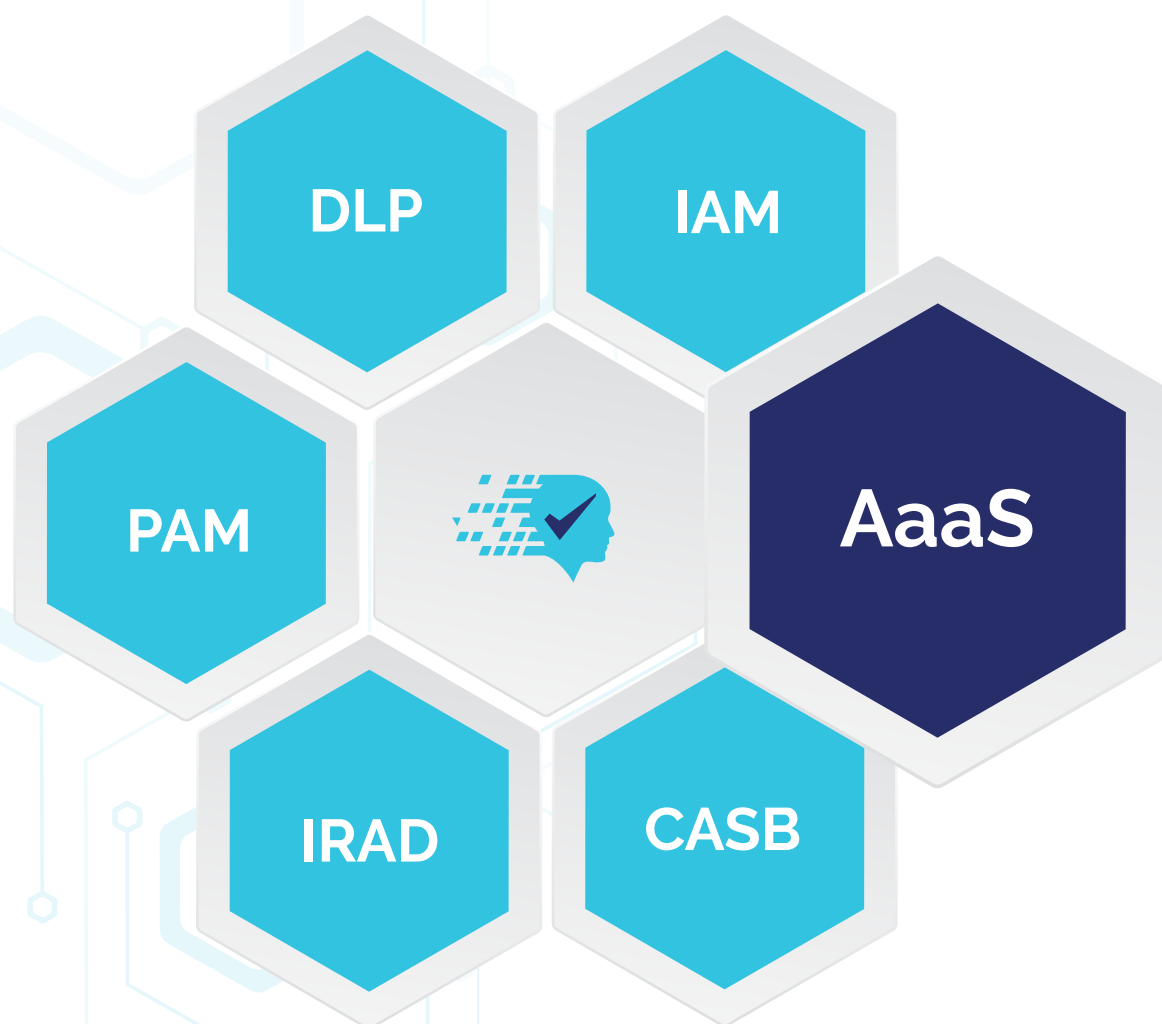
Authentication as a Service (AaaS)



Introducing the SecurIdentity™ Platform

The SecurIdentity™ Platform allows organisations to provide verifiable trust in every transaction they perform. By providing the identity of the user, the device and the data they are working on you can prove exactly who is doing what at any time.

This ensures compliance within the corporate policy, reduction of risk of fines and protection of your vital intellectual property and business assets



Building upon our success of a leading on-premise MFA solution, SecurEnvoy's vision is to bring additional software technologies to market, allow corporations to understand the identity of the user, identity of the device and identity of the data. The intelligence will provide detailed context and behavioural analysis of the user, the device and the data they interact with.

Authentication as a Service (AaaS)

Our release of Authentication as a Service extends the current capability of our successful MFA solution for cloud-based applications. With companies having a cloud first strategy, they can now embrace a SecurEnvoy MFA solution as part of their digital transformation to a more cloud centric model.



SecurEnvoy Authentication as a Service provides secure, reliable and easy to use MFA to cloud-based applications, such as Microsoft Office 365. It also eliminates the overhead of infrastructure management and operational uptime. Companies can now concentrate on business needs, without the burden of administrating Application and Operating system software and security updates.

AaaS Core Features

USE EXISTING DIRECTORY SERVERS

Through our Cloud connector agent, companies still have control of all user data that exists in their own environment. The Cloud connector agent allows direct interaction over a secure tunnel for user authentication of cloud-based applications, with the additional benefit, that user accounts are not replicated outside of the company's network.

LEGACY TRANSITION SUPPORT

The Cloud connector agent provides extra functionality to support Legacy Radius based environments. Companies can now work on their transition plans to migrate from a remote access strategy to a cloud first strategy without service interruption.

SINGLE SIGN-ON

SecurEnvoy Authentication as a Service provides federated access into public cloud-based applications. We provide users with a seamless secure logon experience, utilising our trusted MFA solution, with a breadth of supported authenticator types.

RAPID USER DEPLOYMENT

Deploy SecurEnvoy Authentication as a Service at speed with simple integration options and onboard and enable users with our pre-built Group Deployment. Leveraging Microsoft Active Directory Groups can automatically enable users.

DEPLOYMENT SCALABILITY

Our MFA solution is designed to scale as your business grows, utilising existing authentication database infrastructure, avoiding the need to re-architect, deploy, backup and manage a secondary user database. Whether you have one or thousands of users, our module deployment can scale in minutes.

TRUSTED EXPERTISE & SUPPORT

Our customers recognise our stellar support team and response rate for any issues that may arise. We offer direct user portal access, temporary access codes and many automated features to securely assist any business in reducing overhead and costs.

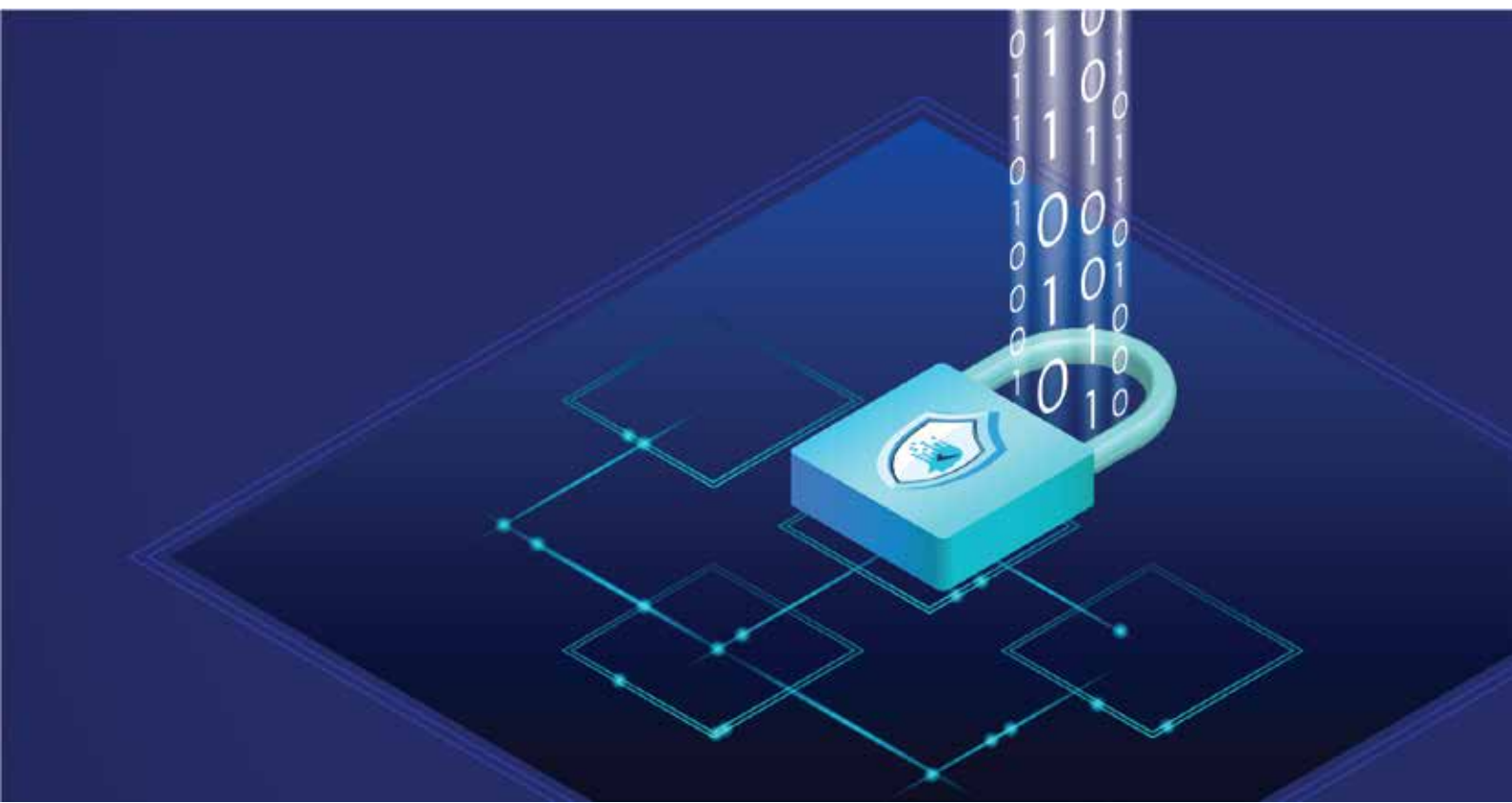
Key Solution Benefits

Authentication as a Service Security

Security that puts you in control. Cryptographic keys, called seed records are inherent in the communication of any MFA solution, commonly generated and distributed by a server in the enterprise or cloud when issuing one-time passwords (OTP's) to clients. SecurEnvoy's solution uniquely splits the keys so that on the user device only one part is stored. The second half is generated from a HW fingerprint when the SecurEnvoy application is run. This approach provides additional security copy protection for the SEED record, as the user device is deemed to be a larger attack vector, as it resides in a more hostile environment. The SecurEnvoy solution uses AES 256-bit to store securely within the enterprise directory environment.

Solution Architecture

SecurEnvoy Authentication as a Service is deployed in Amazon AWS across multiple regions and availability zones. Amazon AWS provides fault tolerance as each region has multiple availability zones and data centres. SecurEnvoy have multiple servers per region to facilitate seamless scale and resilience. SecurEnvoy provide an industry standard of 99.99% operational up time, so corporations can work effectively without having to worry about any service interruption.



AWS Security

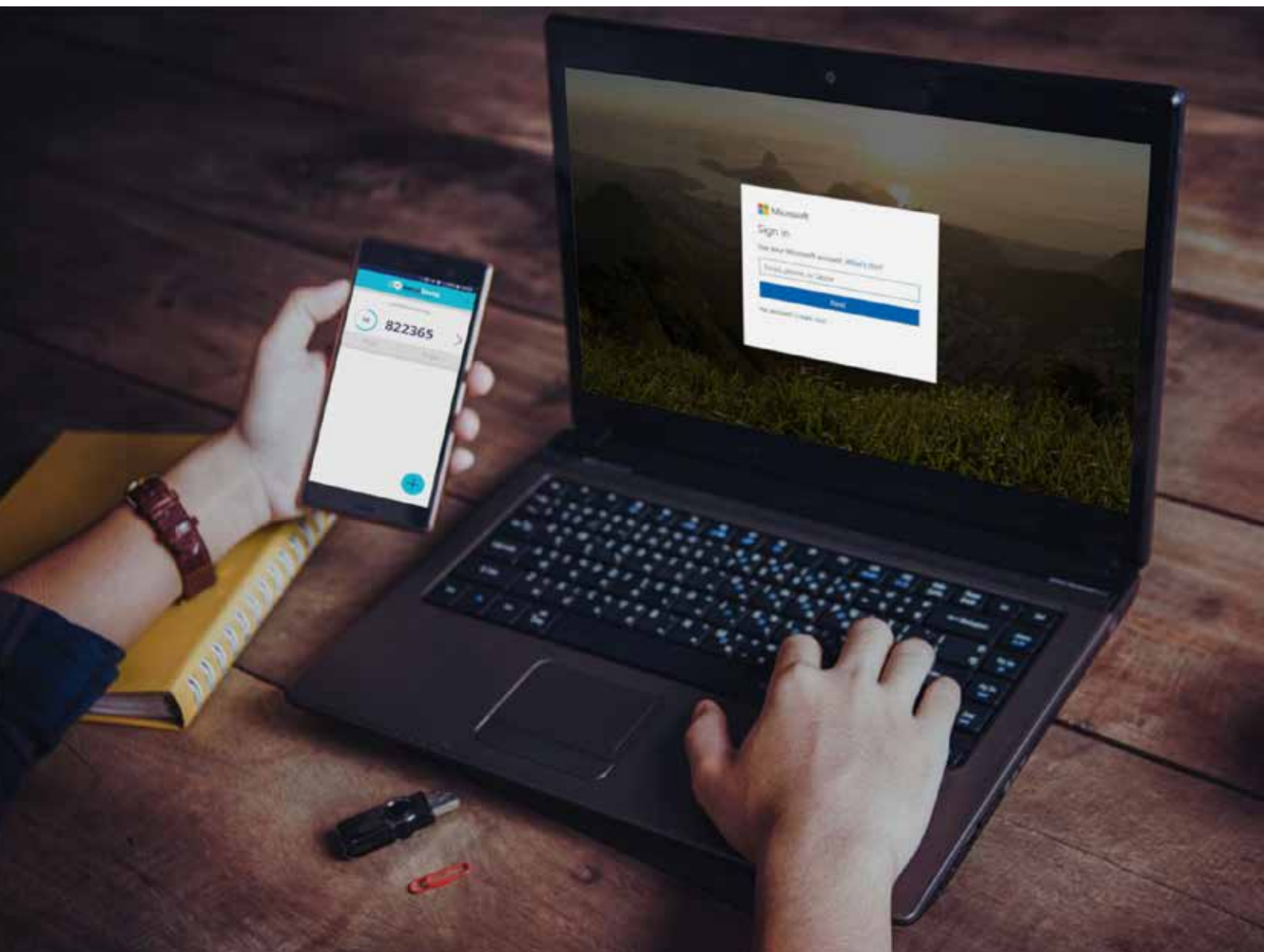
AWS has the following security capabilities and services to increase privacy and control network access:

Network firewalls built into Amazon VPC and web application firewall capabilities in AWS WAF let you control access to the Securenvoy Authentication as a service instances and application. Customer-controlled encryption in transit with TLS across all services.

DDoS mitigation. Availability is of paramount importance in the cloud. AWS provide the benefit of automatic protection of AWS Shield. AWS Shield defends against most common, frequently occurring network and transport layer DDoS attacks.

Office 365 Support

SecurEnvoy Authentication as a Service offers multi-factor authentication out of the box for Microsoft Office 365. Including full support of both web and thick client (Modern Authentication) based access provides users secure application access to continue in their day to day business activities without any interruption.



Migration

For customer's already utilising an existing "on-premise" SecurEnvoy MFA solution, migrating to the cloud is even simpler. As the same user data repository and encryption is used, customers can progress to a Cloud service with minimal configuration changes and little to no impact on users.

Ease of Use

End User ease of use is instrumental in the successful adoption of any authentication solution. Whether a simple to use push notification via a smartphone application or a zero footprint SMS OTP, SecurEnvoy is simple and straightforward for all users, irrelevant of their technical aptitude.





Global Impact & Innovation.

Let's Talk.

Global Hubs

LONDON MUNICH NORTH SYDNEY
CHICAGO NEW YORK BASINGSTOKE

SALES

sales@securenvoy.com

TECHNICAL SUPPORT

support@securenvoy.com



SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@securenvoy.com T: 44 (0) 845 2600010
Company No. 04866711 VAT Number GB 862076128

[SecurEnvoy.com](https://www.securenvoy.com)