SecurEnvoy

A Shearwater Group plc Company

Identity Beyond Boundaries

Plataforma de aseguramiento de identidad

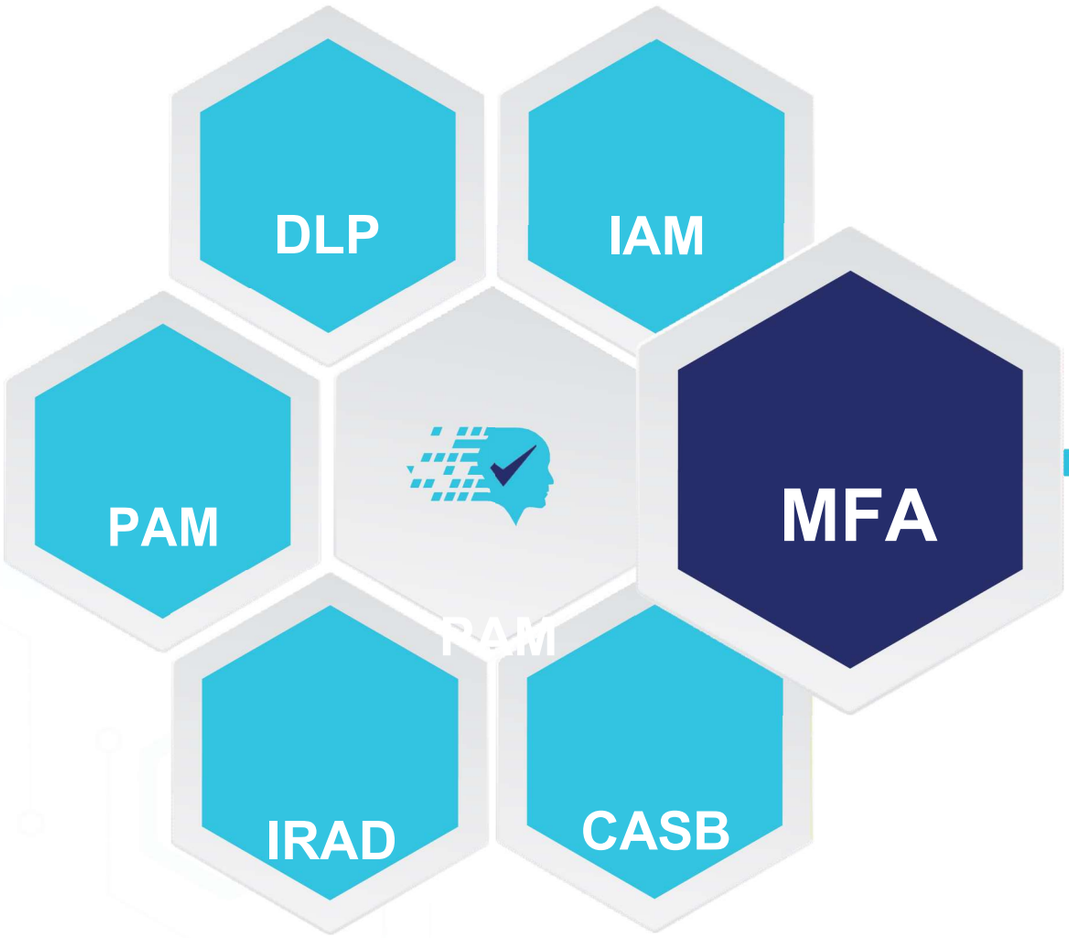
Autenticación multi-factor (MFA)

 versión 1.3

Presentamos la Plataforma SecureIdentity

La plataforma SecureIdentity permite a las organizaciones contar con seguridad confiable en todas las transacciones que realizan. Al proporcionar la identidad del usuario, el dispositivo y los datos con los que trabaja, esta puede conocer exactamente lo que están realizando los usuarios finales o administradores.

Esto garantiza el cumplimiento de las políticas de seguridad corporativa, la reducción del riesgo y de multas o sanciones, así como también, la protección de su propiedad intelectual y activos empresariales esenciales.

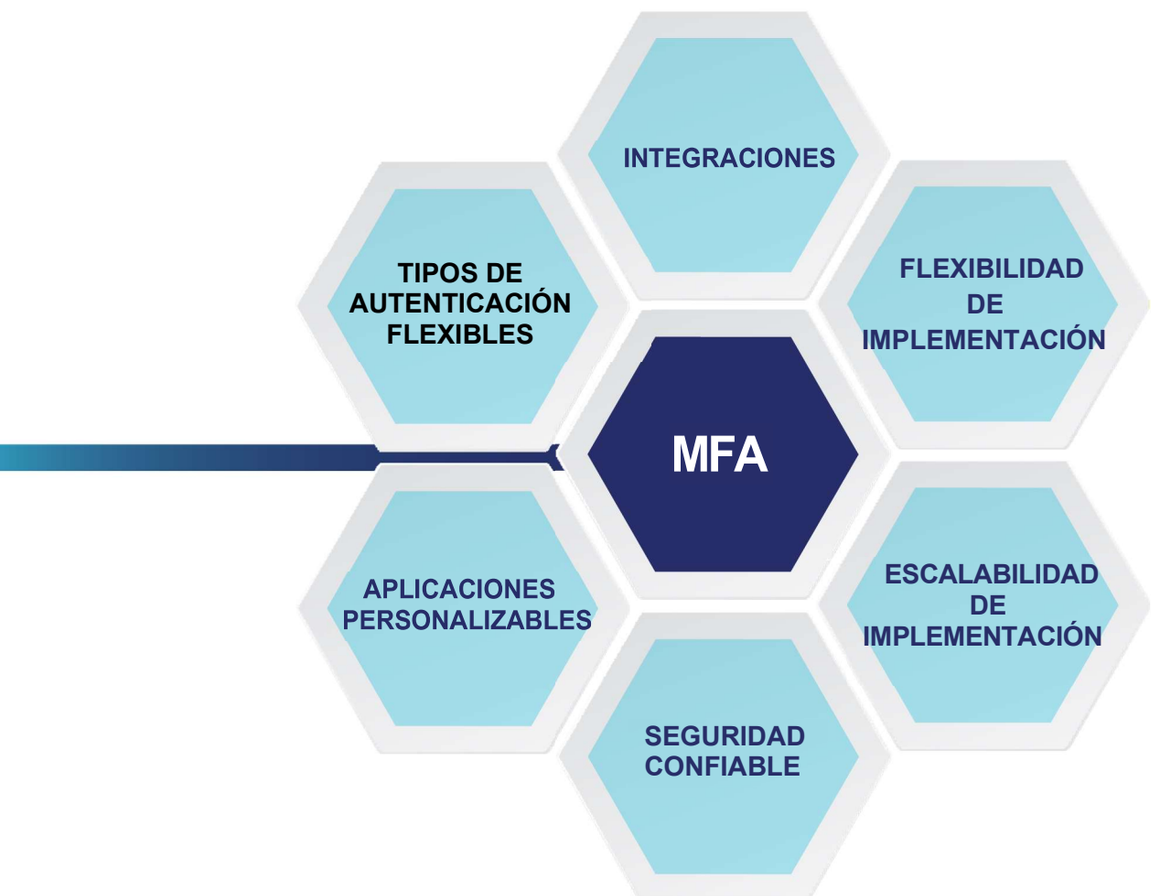


Basándonos en el éxito de nuestra solución líder en el mercado de Multifactor; la visión de SecurEnvoy es llevar al mercado tecnologías de software adicionales que permitan a las empresas conocer la identidad del usuario, del dispositivo y de los datos. Esta inteligencia proporciona un contexto detallado y un análisis del comportamiento del usuario, el dispositivo y los datos con los que interactúa.

Autenticación multifactorial (MFA)

Autenticación multifactor para VPN, SSL, Escritorio remoto, WiFi, portales web, acceso a portátiles y otras soluciones.

Las contraseñas por sí solas no son lo suficientemente seguras para proteger los datos y activos críticos de su empresa. La autenticación multifactor de SecurEnvoy proporciona la seguridad de la identidad del usuario al verificar que una persona es quien dice ser.



Utilizando:
1) Algo que el usuario conoce (Contraseña/PIN)
2) Algo que se tenga (Token de software/hardware)
3) Algo que el usuario es (reconocimiento biométrico/facial).

La solución MFA de SecurEnvoy se integra perfectamente con el Directorio Activo de Microsoft y otras soluciones LDAP, reutilizando la infraestructura de base de datos de autenticación existente en la empresa, evitando la necesidad de rediseñar, desplegar, hacer copias de seguridad y gestionar una base de datos de usuarios secundaria.

Tipos de autenticación

SecurEnvoy considera que los usuarios están en capacidad de poder elegir cualquier dispositivo personal para que sea su token de autenticación, ya sea su teléfono móvil, tableta, ordenador portátil o incluso su teléfono de escritorio. Así como también, el administrador puede limitar el método de autenticación que los usuarios finales pueden utilizar. Los usuarios deberían podrán verificar sin inconvenientes su identidad entre estos dispositivos, sin generar riesgos con tecnologías obsoleta.

Los distintos métodos de autenticación de SecurEnvoy permiten cumplir ampliamente con los requisitos de los diferentes usuarios. Las empresas tienen la posibilidad de controlar los tipos de token que deben utilizar sus empleados, incluida la selección y el control a través del propio portal de inscripción.

Seguridad

Seguridad que le da el control. Las claves criptográficas, llamadas registros semilla son inherentes a la comunicación de cualquier solución MFA, comúnmente generadas y distribuidas por un servidor en la empresa o en la nube al emitir contraseñas de un solo uso (OTP) a los clientes. La solución de SecurEnvoy divide de forma única las claves para almacenar solo una parte en el dispositivo del usuario. La segunda mitad se genera a partir de una huella digital HW cuando se ejecuta la aplicación SecurEnvoy. Este enfoque proporciona protección de copia de seguridad adicional para el registro SEED, ya que se considera que el dispositivo del usuario es un vector de ataque más grande, ya que reside en un entorno más hostil. La solución SecurEnvoy utiliza AES de 256 bits para almacenar de forma segura en el entorno del directorio empresarial.

Implementación de la solución

SecurEnvoy MFA ofrece opciones de implementación para adaptarse a cualquier negocio, con una solución de CSP local, privada o completamente administrada en entornos IaaS independientes o reconocidos por la industria como Amazon AWS y Azure. El desafío de implementar cualquier solución MFA en una comunidad de usuarios es el método en el que los usuarios son notificados e inscritos.
Al aplicar la integración perfecta de SecurEnvoy en el entorno LDAP empresarial, nuestra solución MFA utiliza la "Implementación automática de grupos" para monitorear grupos LDAP seleccionados para cualquier usuario nuevo o eliminado, emitiendo una invitación de inscripción a través del método elegido, es decir, SMS o correo electrónico o colocando al usuario en un estado no administrado cuando se quita del entorno LDAP.
SecurEnvoy puede implementar más de 100.000 usuarios por hora.

Escalabilidad

La solución MFA de SecurEnvoy se integra al instante con el Directorio Activo de Microsoft y otras soluciones LDAP, reutilizando la infraestructura de bases de datos existente en la empresa, evitando la necesidad de rediseñar y gestionar una base de datos de usuarios secundaria.

SecurEnvoy puede utilizar un entorno LDAP mixto (incluye AD LDS), por lo que es compatible con un entorno totalmente heterogéneo que consta de múltiples dominios de autenticación en sitios distribuidos.

Las implementaciones de SecurEnvoy MFA se centran principalmente, en ofrecer una arquitectura de servidor resistente y distribuida con una replicación perfecta de la configuración, ya que todos los datos se almacenan directamente en LDAP.

Integración

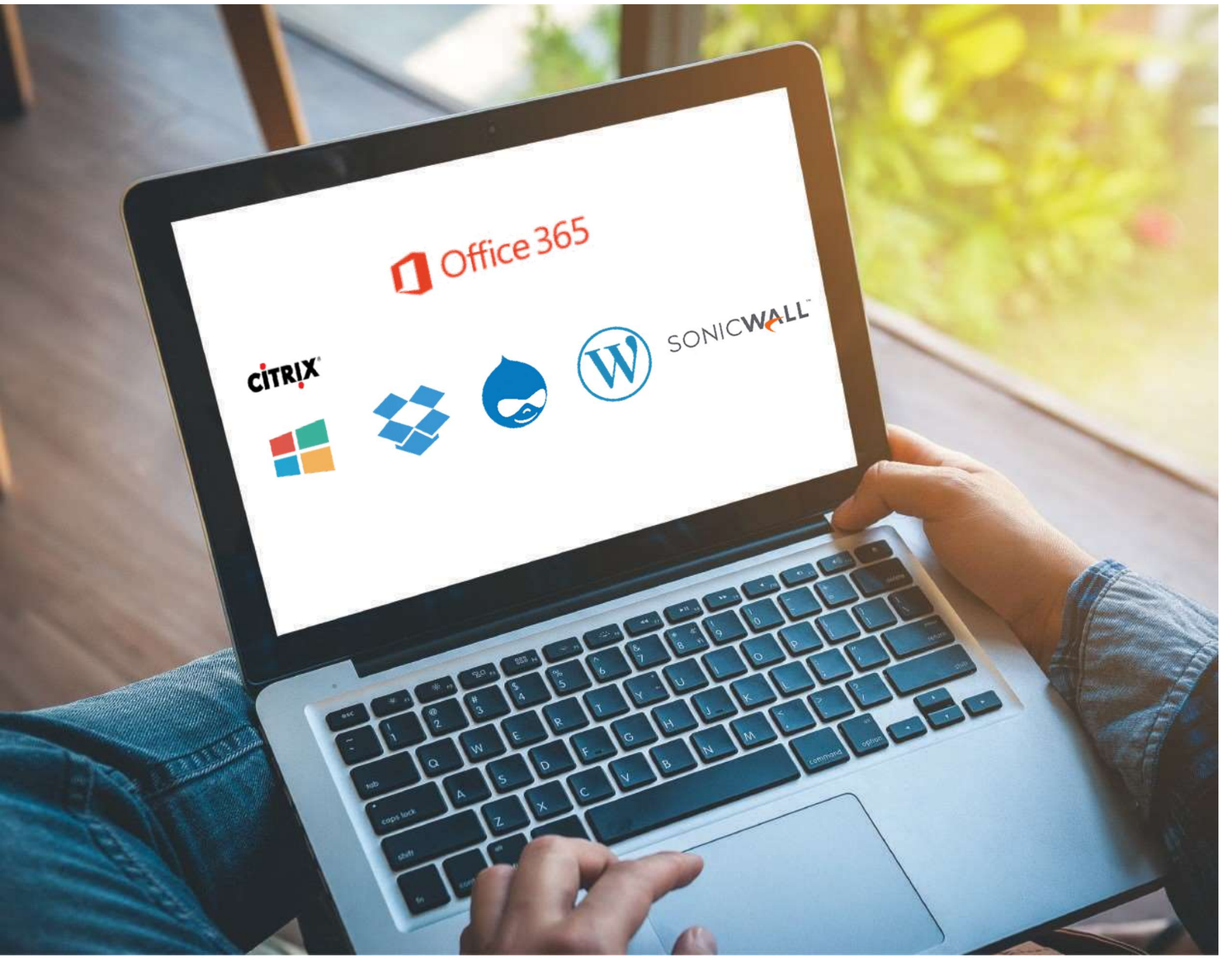
SecurEnvoy *MFA* es compatible con varias interfaces para dar soporte a innumerables aplicaciones SaaS o locales o a la conectividad de la red que requieren protección.

- *Windows Server Agent* ofrece la posibilidad de proteger cualquier sitio web alojado en IIS (por ejemplo, *OWA*, *SharePoint* o la aplicación web del cliente).

- Compatibilidad con *ADFS* para ofrecer *MFA* a aplicaciones públicas basadas en SaaS o SAML.

- El agente de inicio de sesión de Windows extiende la *MFA* a los portátiles unidos al dominio en un en línea o en estado *offline*.

- *RADIUS* con configuración individual para cada cliente permite la integración de los principales dispositivos de seguridad basados en *SSL/IPSEC*.



Migración

La función de migración permite migrar a los usuarios a una solución SecurEnvoy desde una solución de token existente o solo con contraseña. Una vez configurados, los usuarios se pueden migrar en etapas según sea necesario, lo que permite una transición más fluida y un proceso de incorporación.

Personalización

SecurEnvoy ofrece soporte de personalización para cualquier portal de usuario final e interfaz móvil. Esto permite a las corporaciones crear entornos de marca integrados. Elija un color personalizado y agregue su logotipo para una experiencia de cliente consistente.

API

Las API abiertas de SecurEnvoy permiten a los desarrolladores de software el acceso directo a la información y los controles de configuración del entorno MFA. Construido con el marco de Representational State Transfer (REST), las API abiertas de SecurEnvoy le permiten automatizar la creación y modificación de usuarios, incluida la autenticación mediante una llamada web HTTP..

Contactenos.

Distribuidor Latino Americano

Green Light Technology Corp. www.greenlt.com info@greenlt.com

SecurEnvoy
A Shearwater Group plc Company
SecurEnvoy HQ, 1 King William St, London EC4N 7AF
Company No. 04866711 VAT Number GB 862076128

Filiales comerciales

SecurEnvoy Ltd
SecurEnvoy GmbH
SecurEnvoy Inc.