SEGMENTACIÓN DEL MERCADO

Principalmente, nuestro producto se enfoca a:

- Pymes que no quieran preocuparse por las contraseñas de sus empleados.
- Grandes empresas que tengan que administrar una gran cantidad de usuarios accediendo a la red corporativa o a los equipos de la empresa (puestos de trabajo)
- Particulares que prefieran una solución de este tipo, en vez de recordar todas sus contraseñas.

Hoy en día, cada vez más empresas buscan soluciones de autenticación robusta y seguridad, para permitir y controlar los accesos a los diferentes usuarios. Como, por ejemplo: el control de acceso a una red corporativa, acceso remoto a través de VPN o SSLVPN, gestión de datos sensibles, firma de correo, protección en el intercambio de informaciones sensibles, soluciones de Single-Sign-On, etc.

El requerimiento trasciende la frontera de un sistema operativo en particular, muchas veces buscan soluciones a una diversidad de equipos o topología. Por estos motivos, desde AllInKey proveemos diferentes soluciones de autenticación a través de dispositivos USB.

Nuestra competencia se forma en, productos de llavero de contraseña de escritorio, llavero de contraseñas en la nube y segundo factor de autentificación en USB.

Como principal competencia de segundo factor de autentificación en USB tendríamos a Yubico, que nos ofrece dos productos principales:

El YubiKey 4:

- Conexión USB A
- 40€
- Serviría como autenticación en dos pasos para PC
-

El YubiKey 4 NEO:

Conexión USB A

- 50€
- NFC
- Autenticación en dos pasos para PC y dispositivos móviles con NFC

Sus productos simplemente nos permiten que aplicaciones que tenemos registradas con su segundo factor de autentificación no nos permita ingresar si no detecta el usb conectado al ordenador, o en productos de mayor coste si no está

validado vía NFC. No nos permite almacenar contraseñas, siempre deberemos recordar la contraseña, tiene un coste alto.

En los últimos años se ha impuesto en el mercado los llaveros de contraseñas online, aun con varios casos de robos de contraseñas sigue siendo el método más usado tras la contraseña tradicional.

Estas herramientas almacenan nuestras contraseñas en la nube, lo cual puede ser potencialmente peligroso si nos entra un virus en el ordenador, o la empresa de almacenamiento sufre un ataque y les roban nuestras contraseñas, por lo que son poco recomendables.

Como ejemplos tenemos LastPass.

También existen llaveros de contraseñas locales como Keepass que nos permite almacenar una BD de con las mismas de una manera segura, aunque también se han conocido de casos que han sido sustraídas y con fuerza bruta (Probar miles de contraseñas, se consigue la master pass).

	Precio	*Usuarios*	*Características*	*Seguridad*
LastPass	2$/mes Mínimo	1 usuario	Generador de contraseñas, 1GB de almacenamiento	Controlada por el servidor
1Password	2,99$/mes Mínimo	1 usuario	Soporte por email, 1GB de almacenamiento	Media y con fallos de seguridad
AllInKey	Desde 44€		Soporte para Móvil, Tablet o PC Incluye almacenamiento local ...	Alta, biométrica y encriptación.
YubiKey	Desde 40€	1 usuario	Soporte PC	Baja, se compone de un solo método