

Inicio de sesión cero: la solución para la autenticación sin contraseña

Beneficios clave de ZSO

Reduzca el riesgo de filtraciones de datos

Al eliminar las contraseñas, ZSO reduce el riesgo de filtraciones de datos

Proporcione un acceso sin fricciones

ZSO elimina la necesidad de que los usuarios memoricen, introduzcan o restablezcan complejas contraseñas y les permite acceder a las aplicaciones basadas en la nube de forma rápida y sencilla.

Reducir los costes del servicio de asistencia técnica

El enfoque sin contraseñas de ZSO implica que no se gasten recursos del servicio de asistencia técnica en el restablecimiento de contraseñas y el bloqueo de cuentas.

Implantar una seguridad escalable en la nube móvil

ZSO se basa en los estándares del sector y puede utilizarse para servicios empresariales en la nube o híbridos en cualquier dispositivo gestionado o no gestionado, en cualquier parte del mundo.

Es hora de decir adiós a las contraseñas

Todo el mundo odia las contraseñas. No solo son difíciles de recordar, requieren mucho tiempo para ingresar y son molestos para restablecer, sino que también son una de las principales fuentes de violaciones de datos en la nube empresarial.¹ No sorprende que el 86% de los líderes de seguridad quieran deshacerse de las contraseñas, preferiblemente por usando dispositivos móviles como ID de la empresa.²

Por eso Ivanti ha introducido el zero sign-on (ZSO), una sencilla capacidad de autenticación que sustituye las contraseñas por dispositivos móviles seguros como identificación del usuario. Al aprovechar nuestro marco de seguridad de confianza cero, ZSO permite a las organizaciones en el lugar de trabajo en “cualquier parte”:

- La transición hacia una infraestructura de confianza cero mediante la sustitución de las contraseñas por métodos de autenticación multifactoriales (MFA).
- Ofrecer acceso sin contraseña a cualquier aplicación empresarial o servicio en la nube -incluido Microsoft Office 365- mediante un marco de confianza cero.
- Ofrecer a la empresa una experiencia de autenticación similar a la del consumidor mediante el uso de la biometría común.
- Eliminar las molestias y los riesgos de seguridad de las contraseñas.
- Garantizar que solo los usuarios, dispositivos, aplicaciones y redes verificadas puedan acceder a los recursos empresariales.

Nuestro enfoque único

Ivanti ZSO -que reside en la plataforma Ivanti Access- sustituye las contraseñas por dispositivos móviles como identidad del usuario y factor principal de autenticación. ZSO elimina la necesidad de contraseñas mediante el uso de protocolos de autenticación FIDO2.

Ivanti Access se ha creado para el Everywhere Workplace, aprovechando la gestión unificada de puntos finales (UEM) como base -ya sea Ivanti UEM o sistemas UEM de terceros como SCCM y Jamf- para ofrecer un enfoque de seguridad de confianza cero que verifica cada usuario, dispositivo, aplicación y red antes de conceder un acceso seguro a los recursos de la nube.

Ivanti Access también se integra perfectamente con Ivanti Mobile Threat Defense (MTD) para ofrecer a las empresas una capa adicional de seguridad en los dispositivos de los usuarios, junto con un acceso condicional y consciente del contexto para la nube. MTD puede detectar y remediar las amenazas a los dispositivos, las aplicaciones y la red antes de que puedan poner en peligro los datos de la empresa.

Además, Ivanti Access y ZSO trabajan con UEM y MTD para determinar la salud de un dispositivo y si está libre de amenazas móviles. Si se detecta una amenaza, Ivanti Access puede revocar el token de sesión del usuario final y bloquear el dispositivo para que no pueda acceder a los recursos corporativos hasta que vuelva a estar en estado de conformidad, de nuevo libre de amenazas móviles.

Capacidades ZSO

Identidad de dispositivos móviles

Reemplace las contraseñas con dispositivos móviles seguros y biometría como factor principal para la autenticación del usuario.

Autenticación adaptativa

Utilice nuestras capacidades de MFA para proporcionar una capa adicional de verificación de usuarios para entornos de alto riesgo.

Asegure cualquier dispositivo, administrado o no

ZSO funciona en todos los dispositivos Android, iOS, macOS y Windows 10 y 11. Los usuarios se autentican mediante credenciales de clave pública (certificados) en dispositivos administrados, ya sea que se administren a través de Ivanti UEM o soluciones de UEM de terceros, como SCCM y Jamf, y con claves de seguridad FIDO o códigos QR combinados con datos biométricos en dispositivos no administrados.

Seguridad basada en estándares

Ivanti ZSO es compatible con los protocolos FIDO2 para una autenticación simple para el inicio de sesión de escritorio de Windows e Mac y SSO sin inconvenientes a través de certificados basados en cloud en la web.

Soporte para aplicaciones empresariales e IDPs comunes

Ivanti Access asegura cualquier servicio en la nube o federado, incluyendo Microsoft 365, Google Workspace y Salesforce. También se integra con muchas soluciones de identidad, incluidas las de Okta, Ping y Microsoft.

Acceso offline

Los usuarios pueden iniciar sesión en ordenadores de sobremesa y portátiles con dispositivos móviles cuando están desconectados utilizando ZSO a través de Bluetooth.

Motor de política de confianza cero

Mediante una única consola, puede definir políticas para todas las aplicaciones en la nube que bloqueen o limiten el acceso a usuarios, dispositivos y aplicaciones no autorizados a través de redes no seguras o cuando se detecten amenazas. Los flujos de trabajo de corrección intuitivos ayudan a los usuarios a autorremediarse.

Informes detallado

Nuestro panel de autenticación global proporciona una vista detallada de los usuarios, las aplicaciones y los dispositivos que se conectan a los servicios comerciales, alerta a los administradores sobre las infracciones de las políticas y mucho más.

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.es](https://www.ivanti.es)

+34 91 049 66 76

contact@ivanti.es

1. Verizon, "2019 Data Breach Investigations Report." www.verizon.com/business/resources/reports/dbir/2019
2. IDG Research, "Say Goodbye to Passwords," April 2019. www.mobileiron.com/sites/default/files/Whitepapers/Say-Goodbye-to-Passwords/Say-Goodbye-to-Passwords.pdf