Zero Sign-on : La solution pour une authentification sans mot de passe

Principaux avantages du ZSO

Réduction des risques de fuites de données
En éliminant les mots de passe, le ZSO limite les risques de fuites de données.

Fourniture d'un accès sans friction
Avec le ZSO, les utilisateurs n'ont plus besoin de mémoriser, de saisir ou de réinitialiser des mots de passe complexes, et ils accèdent rapidement et facilement aux applis de Cloud.

Réduction des coûts du centre de support
L'approche sans mot de passe du ZSO évite que le personnel du centre de support perde du temps à réinitialiser des mots de passe ou à déverrouiller des comptes.

Déploiement d'une sécurité de Cloud mobile évolutive
Le ZSO repose sur les normes du secteur, et peut être utilisé dans le Cloud d'entreprise ou pour des services hybrides, sur périphérique géré ou non géré, partout dans le monde.

Il est temps de dire adieu aux mots de passe

Tout le monde déteste les mots de passe. Non seulement ils sont difficiles à mémoriser, longs à saisir et énervants à réinitialiser, mais c'est aussi la principale cause de fuites de données du Cloud d'entreprise.[1] Il n'est donc pas étonnant que 86 % des responsables de sécurité souhaitent se débarrasser des mots de passe, de préférence en utilisant des périphériques mobiles comme ID d'entreprise.[2]

C'est pourquoi Ivanti a mis en place le Zero Sign-On (ZSO), une fonction d'authentification simple qui remplace les mots de passe en utilisant des périphériques mobiles sécurisés comme ID d'utilisateur. Reposant sur notre structure de sécurité Zero Trust, le ZSO permet aux entreprises de l'Everywhere Workplace de :

- Passer à une architecture Zero Trust en remplaçant les mots de passe par des méthodes d'authentification multifacteur (MFA).
- Fournir un accès sans mot passe à toutes les applis et à tous les services de Cloud de l'entreprise, y compris Microsoft Office 365.
- Fournir à l'entreprise une expérience d'authentification semblable à celle des produits grand public, via l'utilisation de mesures biométriques courantes.
- Éliminer le stress et les risques de sécurité des mots de passe.
- Garantir que seuls les utilisateurs, périphériques, applis et réseaux autorisés peuvent accéder aux ressources de l'entreprise.

Notre approche unique

Ivanti ZSO (qui réside sur la plateforme Ivanti Access) remplace les mots de passe par l'utilisation de périphériques mobiles en tant qu'ID d'utilisateur et principal facteur d'authentification. Avec le ZSO, les mots de passe deviennent inutiles. Il utilise de puissants protocoles d'authentification FIDO2.

Ivanti Access est conçu pour l'Everywhere Workplace. Avec comme base la gestion unifiée du poste client (UEM), que ce soit Ivanti UEM ou des systèmes d'UEM tiers comme SCCM et Jamf, Access offre une approche de sécurité Zero Trust qui vérifie chaque utilisateur, périphérique, application et réseau avant d'accorder un accès sécurisé aux ressources de Cloud.

Ivanti Access s'intègre aussi de façon transparente avec Ivanti Mobile Threat Defense (MTD) pour apporter aux entreprises un niveau supplémentaire de sécurité sur les périphériques des utilisateurs, avec accès conditionnel au Cloud en fonction du contexte. MTD peut détecter et éliminer les menaces au niveau du périphérique, de l'appli et du réseau, avant qu'elles ne compromettent les données de l'entreprise.

De plus, Ivanti Access et ZSO s'associent à UEM et MTD pour déterminer l'état de santé du périphérique et s'assurer qu'il est dépourvu de menaces mobiles. Si une menace est détectée, Ivanti Access peut révoquer le jeton de session de l'utilisateur final et bloquer le périphérique pour qu'il ne puisse plus accéder aux ressources de l'entreprise jusqu'à ce qu'il soit redevenu conforme, c'est-à-dire débarrassé de ses menaces mobiles.

Fonctionnalités ZSO

Le périphérique mobile comme ID d'utilisateur
Remplacez les mots de passe par les périphériques mobiles et les mesures biométriques, en tant que principal facteur d'authentification.

Authentification adaptative
Utilisez nos fonctions de MFA (Authentification multifacteur) pour ajouter un niveau supplémentaire de vérification des utilisateurs dans les environnements à fort risque.

Sécuriser tous les périphériques, gérés ou non
Le ZSO fonctionne sur tous les périphériques Android, iOS, macOS, et Windows 10 et 11. Les utilisateurs sont authentifiés à l'aide de références d'authentification à clé publique (certificats) sur les périphériques gérés, qu'ils soient gérés via Ivanti UEM ou des solutions d'UEM tierces comme SCCM et Jamf. Sur les périphériques non gérés, l'authentification passe par des clés de sécurité FIDO ou des codes QR associés à des mesures biométriques.

Sécurité basée sur les normes
Ivanti ZSO prend en charge les protocoles FIDO2 pour l'authentification simple ou avancée pour la connexion sous Windows et Mac, et la connexion SSO transparente via des certificats pour les applications en SaaS et Web.

Prise en charge des applis métiers et IDP courantes
Ivanti Access sécurise tous les services de Cloud ou fédérés, y compris Microsoft 365, Google Workspace et Salesforce. Il s'intègre également à de nombreuses solutions de contrôle de l'identité, y compris celles d'Okta, Ping et Microsoft.

Connexion hors ligne
Les utilisateurs peuvent se connecter à des ordinateurs de bureau ou portables à l'aide de périphériques mobiles lorsqu'ils sont hors ligne, via le ZSO sur Bluetooth.

Moteur de stratégies Zero Trust
Dans une seule console, vous pouvez définir des stratégies pour toutes les applis de Cloud afin de bloquer ou de limiter l'accès des utilisateurs, périphériques et applis non autorisés sur les réseaux non sécurisés, ou lorsqu'une menace est détectée. Les workflows de correction intuitive aident les utilisateurs à autocorriger leurs systèmes.

Rapports en profondeur
Notre tableau de bord d'authentification global fournit une image détaillée des utilisateurs, des applis et des périphériques qui se connectent aux services de l'entreprise, avertit les administrateurs des violations de stratégie, et bien plus encore.

ivanti

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr

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