Zero Sign-on:
Die Lösung für passwortlose Authentifizierung

Die wichtigsten Vorteile von ZSO

Reduzieren Sie das Risiko von Datenverletzungen
Durch die Eliminierung von Passwörtern reduziert ZSO das Risiko von Datenverletzungen.

Reibungslosen Zugang bieten
Mit ZSO müssen sich Nutzerinnen und Nutzer keine komplexen Passwörter mehr merken, eingeben oder zurücksetzen und können schnell und einfach auf cloudbasierte Anwendungen zugreifen.

Senkung der Helpdesk-Kosten
Der passwortlose Ansatz von ZSO bedeutet, dass keine Helpdesk-Ressourcen für das Zurücksetzen von Passwörtern und das Sperren von Konten aufgewendet werden müssen.

Skalierbare Mobile-Cloud-Sicherheit bereitstellen
ZSO basiert auf Industriestandards und kann für Enterprise Cloud- oder Hybrid-Services auf jedem verwalteten oder nicht verwalteten Gerät überall auf der Welt eingesetzt werden.

Es ist an der Zeit, sich von Passwörtern zu verabschieden

Jeder hasst Passwörter. Sie sind nicht nur schwer zu merken, zeitaufwändig einzugeben und lästig zurückzusetzen, sie sind auch eine der Hauptquellen für Datenschutzverletzungen in der Unternehmens-Cloud. Es ist keine Überraschung, dass 86 % der Sicherheitsverantwortlichen Passwörter abschaffen wollen, vorzugsweise durch die Verwendung von mobilen Geräten als Unternehmens-ID.

Aus diesem Grund hat Ivanti Zero Sign-On (ZSO) eingeführt, eine einfache Authentifizierungsfunktion, die Passwörter durch sichere mobile Geräte als Benutzeridentität ersetzt. Durch die Nutzung unseres Zero-Trust-Sicherheits-Frameworks ermöglicht ZSO Organisationen im Everywhere Workplace Folgendes:

- Übergang zu einer Zero-Trust-Architektur, indem Passwörter durch Multi-Faktor-Authentifizierungsmethoden (MFA) ersetzt werden.
- Bieten Sie passwortlosen Zugriff auf jede Business-App oder jeden Cloud-Dienst – einschließlich Microsoft Office 365 – durch ein Zero-Trust-Framework.
- Bieten Sie dem Unternehmen ein verbraucherfreundliches Authentifizierungserlebnis durch den Einsatz gängiger biometrischer Verfahren.
- Eliminieren Sie den Ärger und die Sicherheitsrisiken von Passwörtern.
- Stellen Sie sicher, dass nur verifizierte Benutzer, Geräte, Apps und Netzwerke auf Unternehmensressourcen zugreifen können.

Unser einzigartiger Ansatz

Ivanti ZSO – das auf der Ivanti Access Plattform basiert – ersetzt Passwörter durch mobile Geräte als Benutzeridentität und primären Faktor für die Authentifizierung. ZSO macht Passwörter überflüssig, da es die starken FIDO2-Authentifizierungsprotokolle nutzt.

Ivanti Access ist für den Everywhere Workplace konzipiert. Es nutzt Unified Endpoint Management (UEM) als Grundlage – sei es Ivanti UEM oder UEM-Systeme von Drittanbietern wie SCCM und Jamf – um einen Zero-Trust-Sicherheitsansatz zu bieten, der jeden Benutzer, jedes Gerät, jede Anwendung und jedes Netzwerk überprüft, bevor er sicheren Zugriff auf Cloud-Ressourcen gewährt.

Ivanti Access lässt sich außerdem nahtlos in Ivanti Mobile Threat Defense (MTD) integrieren, um Unternehmen eine zusätzliche Sicherheitsebene für Benutzergeräte und einen kontextabhängigen, bedingten Zugriff auf die Cloud zu bieten. MTD kann Bedrohungen auf Geräten, in Apps und im Netzwerk erkennen und beseitigen, bevor sie die Unternehmensdaten gefährden können.

Außerdem arbeiten Ivanti Access und ZSO mit UEM und MTD zusammen, um den Zustand eines Geräts zu ermitteln und festzustellen, ob es frei von mobilen Bedrohungen ist.Wird eine Bedrohung festgestellt, kann Ivanti Access das Sitzungs-Token des Endnutzers sperren und den Zugriff auf Unternehmensressourcen blockieren, bis das Gerät wieder einen konformen Zustand erreicht hat und frei von mobilen Bedrohungen ist.

ZSO-Fähigkeiten

Mobiles Gerät als Benutzeridentität
Ersetzen Sie Passwörter durch sichere mobile Geräte und Biometrie als primären Faktor für die Benutzerauthentifizierung.

Adaptive Authentifizierung
Nutzen Sie unsere MFA-Funktionen, um eine zusätzliche Ebene der Benutzerverifizierung für Umgebungen mit hohem Risiko bereitzustellen.

Sichern Sie jedes Gerät – ob von Ihnen verwaltet oder nicht
ZSO funktioniert auf allen Android-, iOS-, macOS- und Windows 10- und 11-Geräten. Benutzer werden mit Identitätszertifikaten und öffentlichen Schlüsseln (Zertifikaten) auf verwalteten Geräten authentifiziert – unabhängig davon, ob diese über Ivanti UEM oder UEM-Lösungen von Drittanbietern wie SCCM und Jamf verwaltet – und mit FIDO-Sicherheitsschlüsseln oder QR-Codes in Verbindung mit biometrischen Daten auf nicht-verwalteten Geräten.

Auf Standards basierte Sicherheit
Ivanti ZSO unterstützt FIDO2-Protokolle für eine einfache und starke Authentifizierung bei der Anmeldung an Windows- und Mac-Desktops sowie nahtlose SSO über Zertifikate für SaaS- und webbasierte Anwendungen.

Unterstützung für gängige Geschäftsanwendungen und IDPs

Ivanti Access sichert jeden Cloud- oder föderierten Dienst, einschließlich Microsoft 365, Google Workspace und Salesforce. Es lässt sich auch mit vielen Identitätslösungen integrieren, darunter die von Okta, Ping und Microsoft.

Offline-Anmeldung

Benutzer können sich mit mobilen Geräten bei Desktops und Laptops anmelden, wenn sie offline sind, indem sie ZSO über Bluetooth verwenden.

Zero trust policy engine

Über eine einzige Konsole können Sie Richtlinien für alle Cloud-Apps definieren, die den Zugriff auf nicht autorisierte Benutzer, Geräte und Apps über unsichere Netzwerke oder bei Erkennung von Bedrohungen entweder blockieren oder einschränken. Intuitive Workflows helfen Anwendern bei der Selbstreparatur.

Ausführliches Reporting

Unser globales Authentifizierungs-Dashboard bietet einen detaillierten Überblick über Benutzer, Apps und Geräte, die sich mit Unternehmensdiensten verbinden, alarmiert Administratoren über Richtlinienverstöße und vieles mehr.

ivanti

ivanti.de
+49 (0)69 66 77 80 134
contact@ivanti.de