# Introduction to ZTrust

## SECURE ANY APP & ANY DEVICE ON CLOUD

# Contents

# Executive Summary

## WHY IS SSO NEEDED

SSO simplifies access to multiple apps with one login, reducing password hassle. It can include MFA for added security, offering multiple benefits.

## WORKING OF SSO

SSO verifies users across applications. Once logged in, users gain access to other apps without re-authenticating.

## FEATURES OF SSO SYSTEM

An effective SSO should prioritize key feature such as security, integration, scalability, customization, and convenience.

## WHY ZTRUST

ZTrust by Prodevans provides seamless and secure Single Sign-On, enhancing user experience and application security.

## FEATURES OF ZTRUST

ZTrust offers robust security features like Multi-Factor Authentication, Advanced Password Management, Brute Force Detection, and Role-Based Access Control.

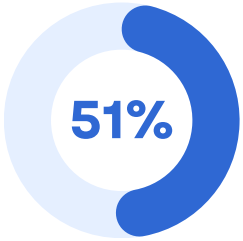
## PROBLEMS FACED AND SOLUTIONS PROVIDED BY ZTRUST

This section addresses common user challenges and the corresponding solutions offered by ZTrust.

# Why is SSO needed

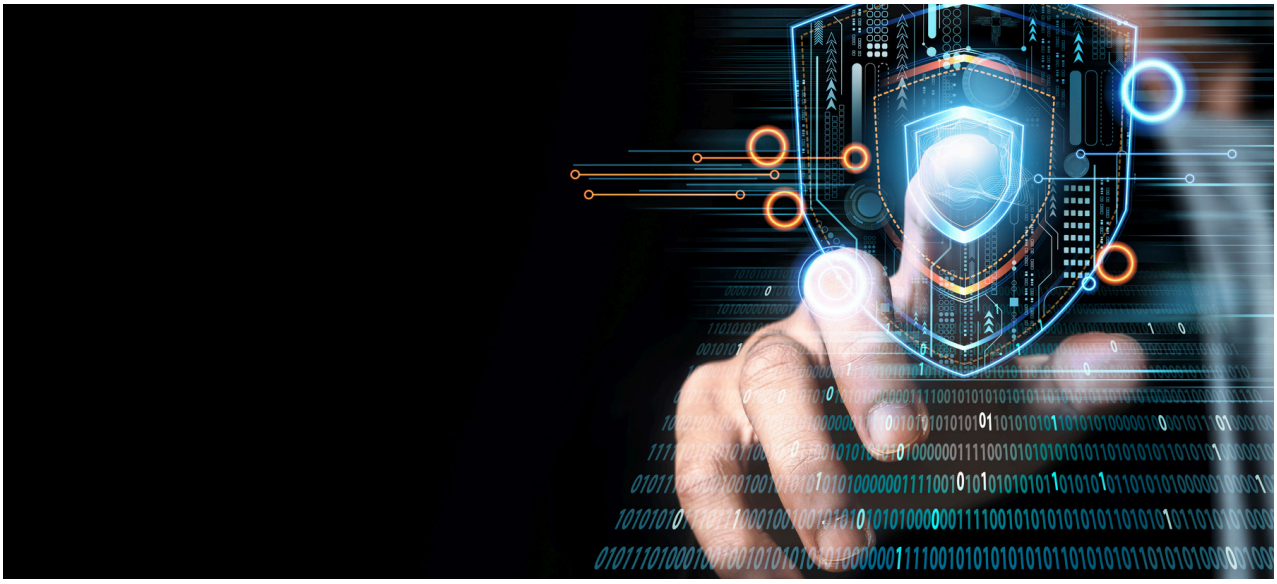

**According to a Yubico Survey, 39% of the respondents accepted that they use the same passwords for multiple accounts.**

**According to another survey, nearly half of the respondents, specifically 49%, reported not utilizing Multi-Factor Authentication (MFA) or or lack complete awareness of MFA.**


**An Entrust study found that 51% of respondents confessed to resetting their password monthly due to difficulty remembering it.**

Single Sign-On (SSO) enables users to access multiple applications with a single set of credentials, eliminating the requirement to remember multiple passwords or log in separately to each application.
Additionally, SSO can incorporate Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA), thereby enhancing system security.



It offers several other advantages such as -

**Increased productivity**

In the case of a company, employees often require to login to multiple applications for their day-to-day work. Without the convenience of Single Sign-On (SSO), employees are burdened with the task of remembering numerous sets of credentials. They also have to spend around 15-30 seconds logging into each of these applications. For instance, if they need to access four different applications, this login process could consume approximately 60-120 seconds of their time.


However, SSO simplifies this process significantly. By requiring employees to remember only one set of credentials, they can log in to the SSO platform and gain access to all authorized applications. This streamlined approach saves employees considerable time, which can then be allocated to completing other essential tasks. As a result, this would increase their productivity levels. It also enables them to remain actively involved and inspired while transitioning between different tools.

**Security**

In the absence of Single Sign-On (SSO), employees are tasked with remembering multiple sets of credentials to access various applications that they are authorized to use. This often leads them to resort to using similar, easy-to-recall passwords, as managing numerous strong passwords becomes challenging. This practice may compromise the security of their accounts, making unauthorized access easier.

However, with Single Sign-On (SSO), users only need to manage one set of credentials, which enables them to utilize stronger passwords. Additionally, Multi-factor Authentication (MFA) or Two-factor Authentication (2FA) can also be implemented along with SSO, which adds an extra layer of security. After entering the credentials, users have to undergo further verification steps. Upon successful verification, they gain access to the applications. Furthermore, the SSO portal also allows administrators to enforce customized password policies aligned with their particular organizational standards across the entire user base.

It also enables swift identification of malicious activities, and as a result prompt response is also possible, thereby improving the overall security.

### Convenience

When dealing with numerous applications, users typically must log in separately to each one. However, Single Sign-On (SSO) minimizes the need for multiple logins, simplifying access and improving user experience. With just one set of credentials, users can access multiple applications simultaneously, eliminating the need to remember numerous sets of login information and reducing "Password fatigue". Consequently, there's a decrease in helpdesk calls related to password-related issues.

With Single Sign-On (SSO), accessing various applications becomes as simple as a single click, thereby increasing convenience.

### Cost-Savings


Managing multiple passwords can be challenging for users, especially in cases where organizations enforce complex password policies. Remembering the numerous passwords becomes cumbersome, leading to difficulties in password retrieval. In situations where users forget their passwords, they have to get in touch with the IT team for assistance, resulting in costly password reset procedures.

Moreover, if an employee gets locked out of a specific application, it can cause a loss of productivity and potential revenue that could otherwise have been generated.

Single Sign-On (SSO) offers a solution by reducing costs associated with password management, including creation, storage, encryption, and synchronization.

**Regulatory Compliance**

Single Sign-On (SSO) helps maintain compliance with regulations such as HIPAA, which mandates companies to document their implemented IT procedures for safeguarding customer data and privacy, including automatic logoff protocols. Non-compliance may result in substantial fines or damage to trust among partners, clients, or employees.

SSO helps to comply with the laid-out regulations.

# Working of SSO

- After a user logs into any service using Single Sign-On (SSO), an authentication token containing user information is generated by the SSO solution.
- This token is stored either in the user's web browser or within the SSO system, and it indicates that the user has been verified.
- When the user attempts to access another application or service (referred to as the Service Provider), the Service Provider checks with the SSO system.
- If the user is already authenticated, the SSO system validates the user and grants access to the Service Provider application.
- If the user has not yet logged in, they will be prompted to do so by providing the necessary credentials to the SSO system.

# Features of SSO System

Any modern SSO should provide the following key features -

### Security

It is one of the most important features of any SSO. It should support Multi-factor Authentication (MFA) or Two-Factor Authentication (2FA) to provide one additional layer of security.

### Scale

The SSO should be able to integrate with already existing common Identity Providers and other Social login providers enabling seamless connection.

### Integrations

This feature is very crucial. The system should be able to accommodate user numbers ranging from hundreds to millions, scaling up as needed.

### Customizations

Customization options are important, allowing the solution to be tailored to match the client's brand identity and themes.

### Convenience

The SSO system should be user-friendly across various systems and channels, including web and mobile platforms.

# Why Ztrust

Today, everyone prefers a smooth login experience across all interactions and access points, regardless of time or location. Implementing Single Sign-On (SSO) is essential to meet this demand, as managing multiple sign-ins can be difficult and time-consuming. Failure to properly implement SSO may lead to a loss of customer trust or expose the company to security vulnerabilities.

This is where ZTrust, a Single Sign-On solution by Prodevans, can make all the difference.

Powered by Keycloak, this Single Sign-on solution streamlines Omnichannel Identity and Access Management, simplifying the user login and onboarding process while ensuring ease and security. ZTrust helps secure the applications and enables access to multiple applications with just one click. It also enhances the user experience without compromising on security.

# Features of ZTrust

ZTrust provides the following key features -

## ROLE BASED ACCESS CONTROL

ZTrust implements Role-Based Access Control (RBAC) to ensure the appropriate delegation of tasks among users. This system safeguards sensitive data by granting different levels of access based on user roles and responsibilities.

## MULTI-FACTOR AUTHENTICATION

ZTrust incorporates Multi-Factor Authentication (MFA), which requires users to successfully pass through two or more authentication factors. It provides a range of authentication methods including Push Notification-based authentication, Biometric Authentication (utilizing FaceID and Fingerprint recognition), ReCAPTCHA on both Registration and Login pages, OTP and QR Code-based login, as well as NFC and MPIN-based login.

## ADVANCED PASSWORD MANAGEMENT

ZTrust provides password synchronization, facilitating seamless access across platforms with synchronized passwords. It offers self-service password reset feature, which enables users to reset their own passwords. It includes Multi-Factor Authentication (MFA) to enhance security by adding an extra layer of protection.

## BLOCK SUSPICIOUS LOGIN

ZTrust has a built-in feature to prevent brute force attacks by detecting and blocking unauthorized login attempts from unknown devices or locations. It notifies system administrators or security teams of multiple failed attempts from a single IP address, including details of the compromised account and the attacker's IP address.

# Problems faced and solutions provided by Ztrust

| | | |
|---|---|---|
| 01 | **Password Fatigue -** As part of daily routine, users have to remember multiple passwords to login to multiple applications. To login into one application, it may take 15-30 seconds. This repetitive process can significantly take up a lot of users' time. | ZTrust provides a seamless and consistent login experience. Users no longer need to log in separately to multiple applications. With just one set of credentials, users can effortlessly navigate between different applications. |
| 02 | **Compliance Challenges -** Failure to comply with specific requirements for protecting user data can lead to legal consequences. | ZTrust offers features such as Multi-Factor Authentication (MFA), OTP/Authenticator based login, CAPTCHA for login and registration, email notification on deactivation of idle users. All these features make ZTrust GDPR compliant. |

| | | |
|---|---|---|
| 03 | **Security Issues -** If an attacker manages to find valid credentials through trial and error, they can gain unauthorized access to the account, thereby enabling them to access all associated resources. | ZTrust incorporates a Brute Force Detection feature, which detects and prevents unauthorized access attempts by identifying and blocking suspicious activity. It also alerts the IT Security Team if multiple failed login attempts are detected from a single IP Address within a specified time period. |
| 04 | **Lags in data retrieval -** System might encounter latency issues, which impacts the speed and accuracy of data retrieval. Users need a solution that ensures rapid access to their data. | ZTrust incorporates a feature that utilizes Infinispan to re-engineer the cache. This ensures efficient data storage and retrieval, allowing users to quickly access their data. Any updates made centrally are immediately reflected in the cache, without any delay. |
| 05 | **Improper session handling -** Inadequate session management practices may result in session hijacking, where an attacker may get access to the session ID and take control of the session. | ZTrust offers a Session Invalidator feature, which ensures that when a user logs in from a new device or location, or initiates a new session, they are automatically logged out from all previous sessions. This ensures that only the current session remains active. |

| | | |
|---|---|---|
| 06 | **Inconsistent themes -** Delivering a consistent brand experience is crucial for clients to maintain customer trust and foster strong relationships. | ZTrust offers customization features, through which the SSO login page can be modified o align with the client's branding and theme. Dynamic HTML/CSS templates are utilized to ensure that email themes are consistent with the client's theme design. |
| 07 | **Scalability & Integration issues -** When the customer base expands, there is a need to update, add or update the systems. Seamless integration with existing infrastructure and applications is essential to ensure proper functioning. | ZTrust offers effortless integration with existing IT infrastructure and applications, along with scalable capabilities that adapt according to the client's evolving requirements. |
| 08 | **Complex Access Management -** Clients with multiple applications typically require users to log in separately to each application using different sets of credentials. It makes the process complicated and time-consuming. | With ZTrust, users can log in once and seamlessly navigate between different applications without the need to log in separately to each one. It also provides the option for users to log in using their social network accounts, such as Google, Github, Facebook, or LinkedIn. |

| | | |
|---|---|---|
| 09 | **Connecting Modern apps -** Sometimes, linking modern applications may require manual integration with the chosen authentication provider. This can lead to a less user- friendly experience for certain users. | ZTrust offers the Extended Authentication API feature, allowing authentication functionalities to be accessed via API calls. The API can be granted direct authorization, enabling it to authenticate on behalf of the user. |
| 10 | **Huge Token size -** Users frequently logs into numerous applications resulting in the creation of large ID Tokens as the number of realm increases. These oversized tokens affect application performance and also raise security concerns. | ZTrust provides a feature called Identity Token Size Optimization, which enables the creation of more compact tokens. These smaller tokens improve data transmission efficiency and decrease the potential attack surface. |

# Contacts

## Reach Us Out

Send us a message or reach us by phone during our regular business hours.

403, 4TH FLOOR, SAKET CALLIPOLIS,
RAINBOW DRIVE, DODDAKANNELLI,
BENGALURU, KARNATAKA 560035

contact@prodevans.com

+91 97044 56015