What is **Single Sign- On?**

www.sennovate.com

SENNOVATE

CONTENTS

Industry leaders also see the growing importance of SSO, Senthil Palaniappan, Founder & CEO at Sennovate, a US based company focused on delivering services and solutions in the security space observes, “the traction for cloud environment is gaining high importance, this will bolster SSO adoption, whereas on the enterprise front, the on premises model will sustain itself.”

Overview

Evolution of Single Sign-On (SSO) has come into being since the late 1990’s, during the days when organizations began to move into IT custom built authentication systems, as part of their overall security strategy. Later this gathered momentum, and began to gain recognition as enterprise SSO, this evolved to web-based plugins methods better known as web access management (WAM). The big seismic change took place with the coming of the cloud-based systems, with software as a service(SaaS), becoming dominant.

This shift was imperative as enterprise legacy systems were not just confined to their security walls, now it had applications on the cloud as well. At the mid-tier level, small business enter-prise (SME) is going the cloud way. Mobile device handhelds, Bring Your Own Devices (BYOD) and emerging technologies such as IoT, AI is creating greater value proposition for SSO based technologise.

What is SSO?

Single Sign-On (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials, across domains. Essentially, there is a central domain through which authentication is performed, and then the session is shared with other domains.

A real-world example of SSO authentication is Google's suite of online applications. Log into a single Google application and then you are able to access other Google applications as well, thereby saving the task of reentering password every time you toggle between your Gmail Inbox and Google Drive.

SSO Authentication Process

SSO authentication process is highlighted below.

- A user logs into a website or app
- The website or app directs the user to a central SSO login tool, and the user enters credentials like username, password.
- The SSO domain authenticates the user credentials, validates the user, and generates a token
- The user is directed back to the website and the embedded token acts as proof that it has been authenticated. This grants the user to access associated apps and sites that share the same central SSO domain.

SSO features & benefits

- Eliminates the need to manually log into each separate application thereby offers big benefits to users and administrators
- Best end user experience, and encourages end users to stay engaged with the website or apps
- Eliminates credentials re-authentication, and reducing help desk requests, thus saving costs
- Streamlines local & remote application and desktop workflow
- Improves compliance through a centralized database.
- Provides detailed user access reporting

SSO by Type

Enterprise SSO:

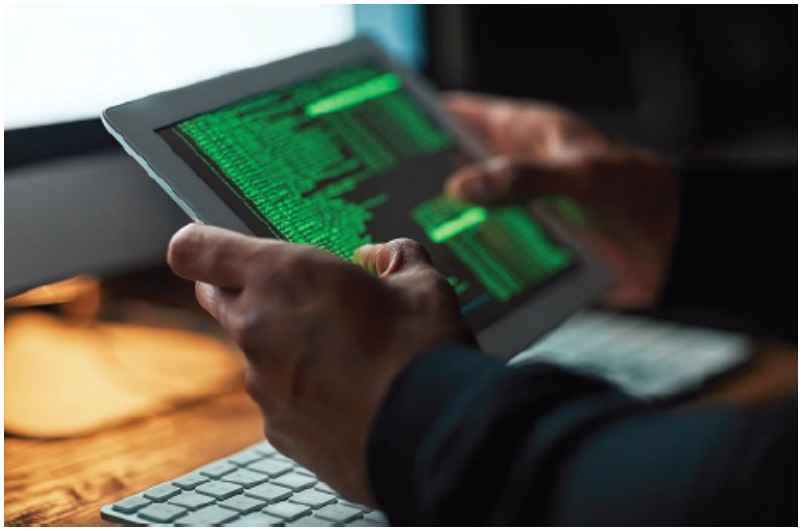
On premise applications, enterprise SSO is best used. The administrator implements Enterprise SSO as a desktop client that manages user credentials. It is non-intrusive by capturing a user's credentials, and then detecting the same credentials the next time the same user attempts to authenticate and automatically logging them into the application.

Web SSO

Web SSO is different from enterprise SSO as it focuses on web-based applications. As more and more applications are becoming cloud-based authenticatating these services becomes increasingly important. The web SSO works with help of enforcement agent intercepting traffic.

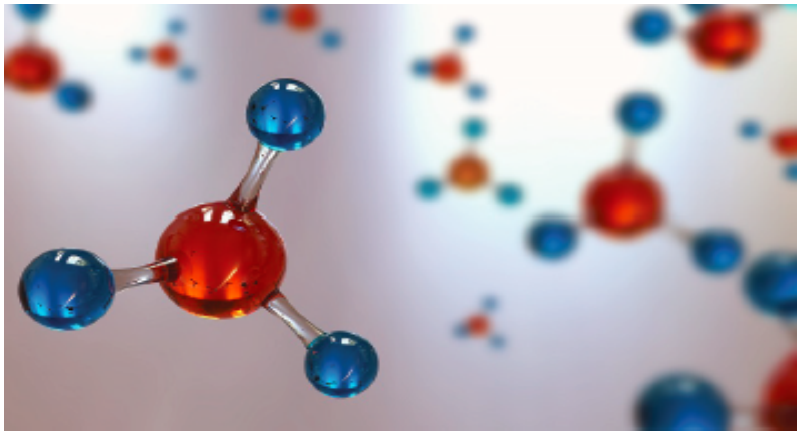
Security concerns with SSO

Seemingly SSO is becoming more secure when properly deployed, and used along with other complimenting cyber security technologies. Arguably there is a factor of risk in centralizing multiple processes into a single system. Take for instance a hacker were to get into a central system to steal a user's password, they would get access to all the apps and tools connected to that SSO system. To mitigate this concern SSO is able to add extra security tools to its login system in form of two factor logins (2FL) resulting in a double layer check before granting access.



Identity Protocols for SSO

Identity management protocols provide standards for security, To provide access management, and help in compliance, and to create a uniform system for handling interactions between end user requests to access data residing over applications and systems, identity proto-cols are used.



LDAP

Perhaps the oldest protocol standard which has been in use since mid 90's, LDAP has been mostly been used with Linux and techni-cal apps and on-premise apps. LDAP is seen with its LDAP as a service a cloud variant of it.

LDAP is widely used in Linux devices, technical apps, on-premise apps and examples are active directory, open ldap, Open DJ, IBM Tivoli, oracle directory.

Kerberos

Developed at MIT, Kerberos is primarily used by Microsoft for its Windows and its related systems. Examples include Windows Systems Microsoft Applications / server infrastructure.

RADIUS

Remote Dial in User service (RADIUS) primarily used in network services like wireless networks, network infrastructure, VPN's equipment. RADIUS act as interface with the application and a central directory serve to check user credentials. RADIUS now has RADIUS as a service is availabe with pre-built pre-configured scalable and full managed RADIUS servers.

SAML

Security Assertion Markup Language (SAML) is mostly associated with SSO for web based applications. This is an open standard protocol, and it needs to be defined by an identity and service provider. Shibboleth, Ping Identi-ty, are popular SAML identity providers. OASIS (organi-zation for the advancement of structured information standards) has published specifications for this protocol. Its core specification includes - Core, Bindings, Profiles, Metadata and Conformance, these specs are mandatory for an identity provider to support SAML.

WS-Trust/WS-Federation

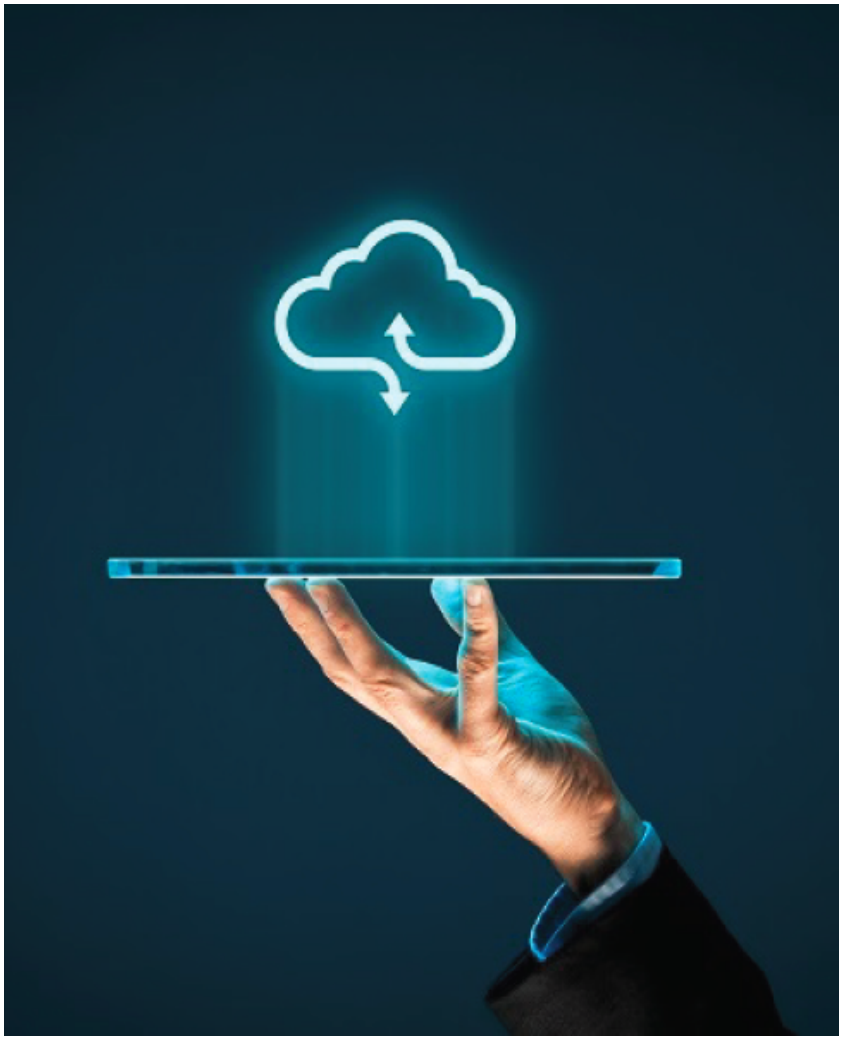
WS-Trust(Web Services Trust Language), provides extensions to WS-Security (Web Services Security), a protocol used for securing SOAP (Simple Object Access Protocol) communication.

WS-Trust and WS-Federation are OASIS open standards with primary corporate backing from Microsoft and IBM.

SSO Market trends

Today's IT is in a state of boundary less not limited to an organization's perimeter, but has expanded into the cloud. Accordingly security solutions are rapidly pacing up to meet market needs. Industry reports suggests that small business environment (SME) business is adopting cloud solutions and this typically SME's use more than 10 cloud based apps for their business. At the enterprise level, SSO is mostly con-fined to on-premise model, and now enterprises see value to have a mix with extending some apps on the cloud, making a good enough case for SSO based solutions.

Keeping in pace with ever changing tech landscape AI, IoT, Bring Your Own Devices (BYOD), Bring Your Own App (BYOA) is making a splash, resulting in scope for SSO solutions . North American market is the largest contributor in terms of market demand for SSO deployments in various verticals.



Key SSO providers

How to select the best SSO provider

To select a good SSO solution provider, the following metrics can prove handy, before you close in on a particular one.

- Usability – must have ease of use
- Easy implementation
- Supports security policies
- SAML authentication support
- Password vaulting
- Customization
- Customer Support

Role of an Integrator & Managed services provider

Organizations often select a SSO solution provider but may not have the skill to deploy in a complex environment such as mix and match on premises SSO infrastructure and SaaS offerings . This calls for an integrator, can step-in to integrate it. The role of an integrator may begun from being a referral partner and later get becoming an integrator.

Sennovate SSO Service offerings

To select a good SSO solution provider, the following metrics can prove handy, before you close in on a particular one.

- Assess your needs and select the best SSO products to fit those needs.
- Design and implement the SSO solution.
- Seamlessly integrate all your applications, including legacy and custom apps as well as those hosted on-premises and in the cloud.
- Provide ongoing managed services for your SSO solution.

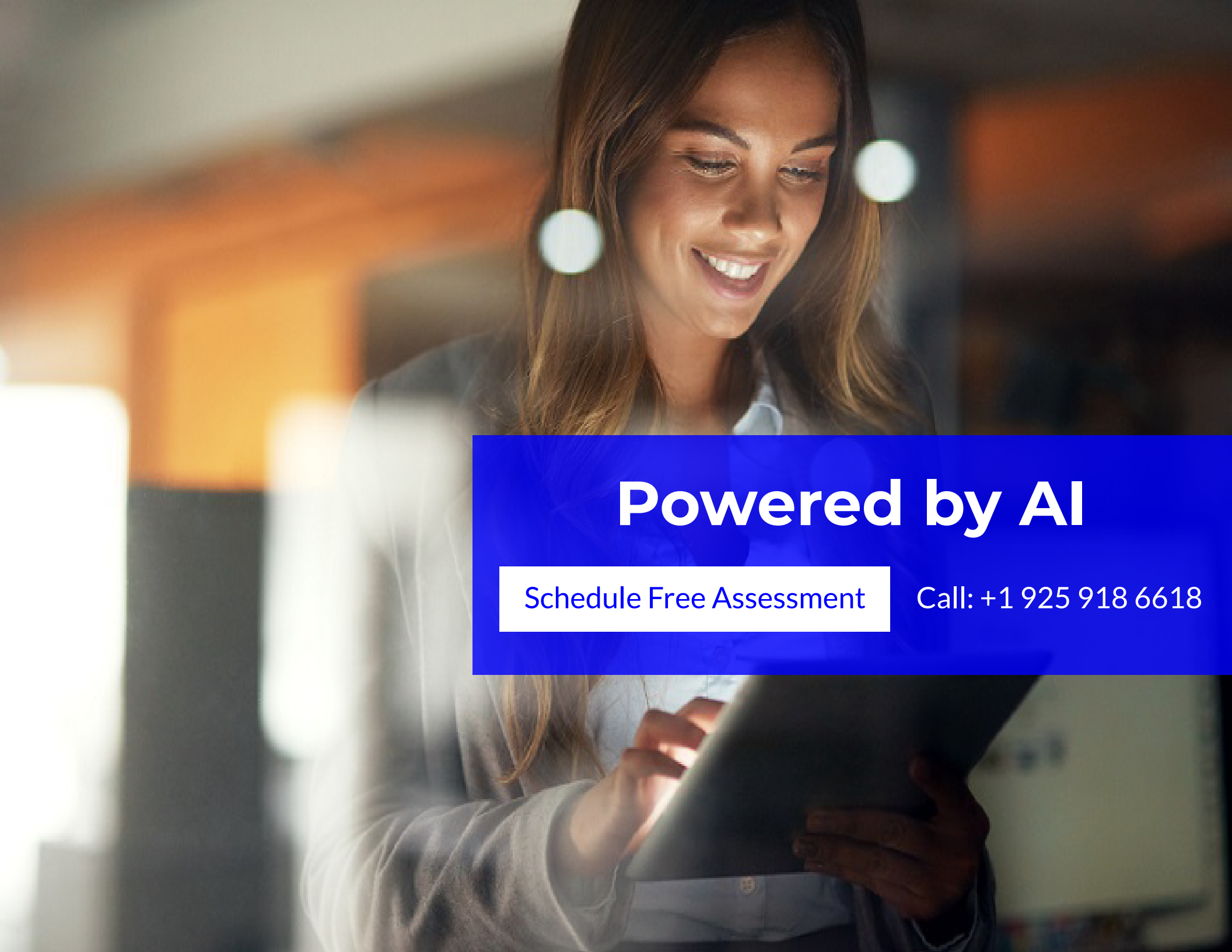
Unifying Data Security Across Enterprises

Why Sennovate?

Mesh
VP Development TriMark

"Sennovate Team was a tremendous partner for TriMark, with their knowledge and skill of Oracle Access Manager and Active Directory we were able to design, build and deliver a seamless User Experience which made 4 separate Oracle Products seem like one solution via Single Sign On.

They were able to be deal with the challenges and work through the intrici's dealing with systems that were purely cloud as well as hosted to deliver a final product".


Powered by AI
Schedule Free Assessment
Call: +1 925 918 6618

SENNOVATE

Sennovate is a global Managed Security Services Provider (MSSP) that specializes in Identity and Access Management (IAM). Our solutions helps companies meet complex compliance requirements, and leverage their IT more effectively for better business results.


Sennovate


Sennovate


Sennovate

+1 925 918 6618 | sales@sennovate.com | www.sennovate.com