

Cyber Security Starts with Password Management

Solving the Password Problem

The experts agree, passwords are here to stay. Despite emerging security technologies like biometrics, passwords persist as the most used tool for access to enterprise and cloud resources. That doesn't mean passwords aren't challenging to manage or an inconvenience for users. That's why single-sign-on (SSO) technology continues to gain acceptance as a crucial part of enterprise security.

sswords are Here to Stay 🙃



- There are more than 300 billion passwords that need to be protected (up from 80 billion in 2017)
- Enabling mobile password management increases employee use of password management systems
- Small businesses (1-25) employees) average 85 passwords per employee

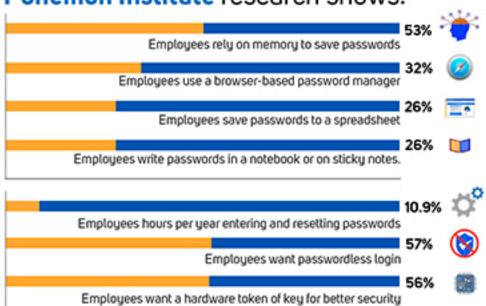
by 30%.

- Fewer than 50% of companies have an SSO solution
- As of January 2021, there are 4.66 billion Internet users-59.5% of the world population
- 45 percent of employees are using their mobile device for work
- 8 Large corporations (1001-10,000 employees) average 25 passwords per employee
- There are 5.22 mobile users and 8.02 billion mobile connections
- 6 Despite this, 25 percent of IT security respondents say their organizations have no plans to adopt 2FA for customers. Of these 25 percent:
 - 60 percent say usernames and passwords provide sufficient security
 - 47 percent say 2FA will affect convenience by adding an extra step during login.

Employees reuse passwords an average of 13 times

The Ongoing Need for SSO The average user has more than 100 passwords

Ponemon Institute research shows:



By the end of 2021, the SSO market should reach \$1,599.8 million (\$1.6 billion) at a CAGR of 13.6%

Analyst Research Shows Value of SSO 🔣 for Password Management



Forrester says 25% to 40% of help desk calls are for password issues



\$1 million (700,000 UK pounds) per year spent on password support



of Help Desk calls are password related at cost of \$70/call or more



Password issues take 2 to 30 minutes to fix



a trouble ticket is 7 hours 4 minutes

Average response time to

Large organizations spend



Widmeyer says US businesses lose \$200,000 per year on employee password issues

Gartner says 20-50%



4,000 passwords per uear at a cost of 24 work hours

One third of workers enter



37 percent of workers create 50 new accounts annually

SSO Improves Security 🗸 SSO is more secure due to encryption – passwords are never exposed. Consider



the protection from data breaches: Global cost of data breaches in 2021 is \$6 trillion (up from \$3 trillion in 2015)

- Cost of average data breach up 12% in last 5 years to \$3.86 million in 2020. 3 20% increase in corporate data breaches with work from home
- 4 24% of data breaches led to unexpected expenses
- 18% of companies say security is not a priority for employees 6 28% say employees use personal devices which create new attack opportunities
- Remote work has increased the cost of a data breach by \$137,000

About Avatier SSO

and Password Management

Avatier's SSO offers a portable, scalable, and secure single sign-on solution that can run anywhere: on any cloud, on-premise, private instance hosted by Avatier. Avatier SSO teverages existing groups and users in your native directory to delegate web application access. To learn more about Avatier SSO,

visit https://www.avatier.com/products/sso/



Avatier's Identity Anywhere Password Management gives self-service control over password resets, synchronization, and administration via web browser, mobile devices, or a wide array of multifactor authentication providers. Avatier Password Management increases security and employee productivity while reducing Help Desk and IT costs. To learn more about Avatier Password Management, visit https://www.avatier.com/products/pm/