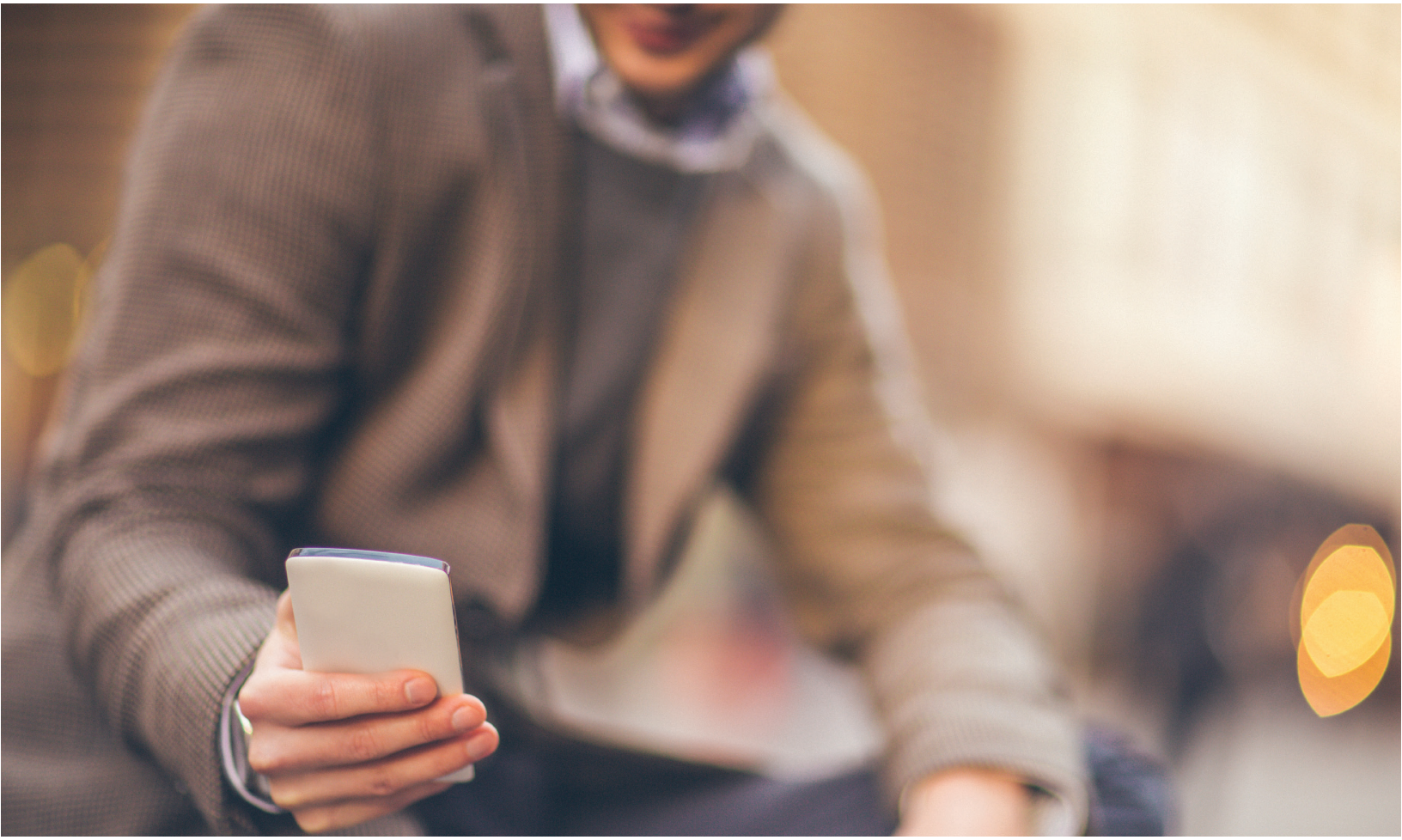
FIVE REASONS IT'S TIME FOR FEDERATED SINGLE SIGN-ON



WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

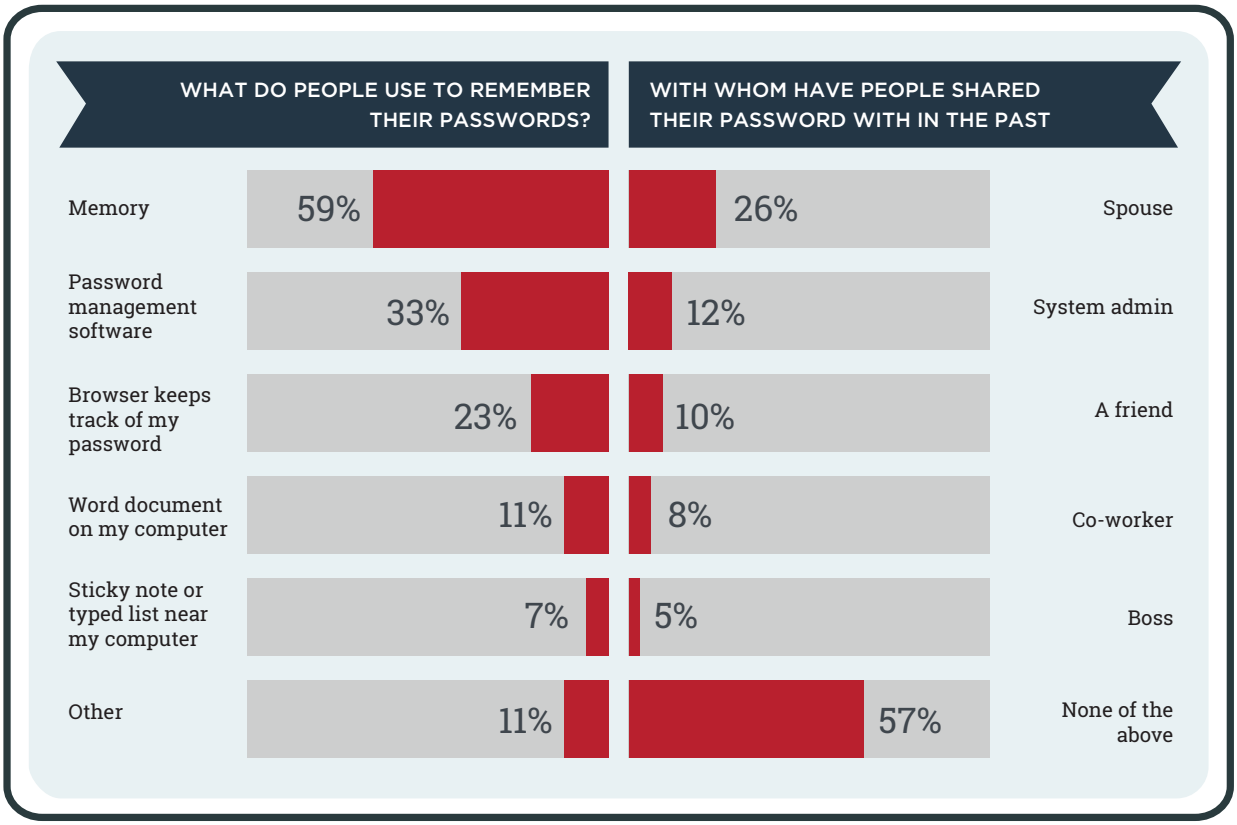
From improved security to increased customer engagement, secure single sign-on is a smart choice.

While Cloud-based applications provide many business benefits including lowering capital expenditures, but they can also drive up operational expenses by requiring more administration and lowering employee productivity due to more application loginins, password resets and helpdesk calls. Single sign-on (SSO) eliminates much of this overhead, increasing the overall ROI of cloud-based applications. Because SSO removes barriers to using cloud applications, it also can dramatically increase user adoption rate.

INTRODUCTION

How many usernames and passwords do you have? How many do you remember? And how often do you have to change them all? At the end of the day, there are only so many noteworthy dates, old pets' names and memorable combinations of numbers and letters we can all keep track of. And constantly having your staff reset passwords—either by policy or because they frequently forget—costs your business time and money.

You want identity and access management (IAM) to work as well for employees as is it does for the needs of the organization.



INTRODUCTION

A simple and elegant solution to this dilemma is enabling secure SSO through federation.

Federation has one major advantage over most cloud-based SSO products: the user's identity and password are stored in a single place controlled by the user's organization. Federation is based on the notion that users can authenticate once with their organization and that authentication is good for all other applications that the users are authorized to access. Rather than storing and forwarding many usernames and passwords like most cloud-based SSO products, federation uses standard encrypted tokens to share the users' authentication status and identity attributes to facilitate access to applications.

Federated SSO enables a trust relationship between the organization and the application vendor. When the user accesses the application, the user's identity is transparently and securely passed to the application vendor.

Here are five reasons that your organization should seriously consider moving to secure, federated SSO and why you should also urge your application vendors to move to a secure, standards-based approach.

- Enhance customer engagement
- Answer BYOD and mobile access demands
- Lower costs
- Improve security
- Increase productivity

01 IMPROVING CUSTOMER ENGAGEMENT IS ON YOUR CMO'S RADAR

Despite the proliferation of corporate Facebook pages and Twitter accounts during the last few years, most businesses still effectively remain on the sidelines. The gap between the early adopters and those waiting to take the plunge has actually widened.

The average billion-dollar company spends $750,000 a year on social media, according to Bain & Company analysis, but some early adopters such as Dell™, Wal-Mart®, Starbucks™, JetBlue® and American Express® invest significantly more. In some instances, the investment is tens of millions of dollars.

However, the benefits of social media can outweigh many sources of hesitancy. Chief among these benefits is the ability to embrace and engage with empowered consumers. Customers who engage with companies over social media are more loyal and they spend up to 40 percent more with those companies than other customers.

Federated SSO can improve customer engagement and loyalty by offering a tailored experience based on user identity. Leveraging credentials for account registration from a variety of social media sites like Twitter and Facebook allows the user to access your services quickly. For IT, leveraging cloud identity providers drives the cost and burden of external user management out of the enterprise.

02 BYOD AND MOBILE - IT'S BIG AND GETTING BIGGER

As smartphones and tablets become the de facto devices used to access the Internet, users will expect secure and seamless mobile access to business-critical applications and resources anytime, anywhere.

If your existing IAM solution can't accommodate mobile devices, or if your customers and employees can't access apps from where they are and on their smart device, you're missing a key revenue and productivity opportunity.

- Federated SSO keeps corporate data secure. Removing authentication and access from mobile applications allows IT to centralize access control as well as streamline audit and reporting to ease governance and compliance requirements.
- All users get access with one identity, regardless of device. If your IAM system takes a standards-based approach, users can leverage one identity to access your apps and services. Your employees, customers or partners can use their personal devices and tablets to gain access to business apps.

03 YOU'LL SAVE MONEY

When employees call the helpdesk for assistance with password resets, the organization incurs helpdesk costs in addition to lost employee productivity. In fact, helpdesk password resets cost on average $51 to $147 per employee per reset. Also, consider that some SaaS and BPO vendors charge their customers for password-reset calls.

So when it comes to convincing your manager, how does federated SSO translate to savings? It will:

- Reduce the annual volume of inbound password reset requests from employees and decrease staffing and resource requirements for your helpdesk.
- Decrease administrative costs due to automated Internet user account management.

[This is my p@55w0rd]

With so many passwords, users may opt to write them down and leave it out in the open.

EVEN WORSE...
Some users may keep a spreadsheet of passwords on their computer. This one file can compromise identity security.

BETWEEN 10% AND 30%

of all helpdesk calls are for password resets. Password reset costs range from:

$51 TO $147 FOR THE LABOR ALONE

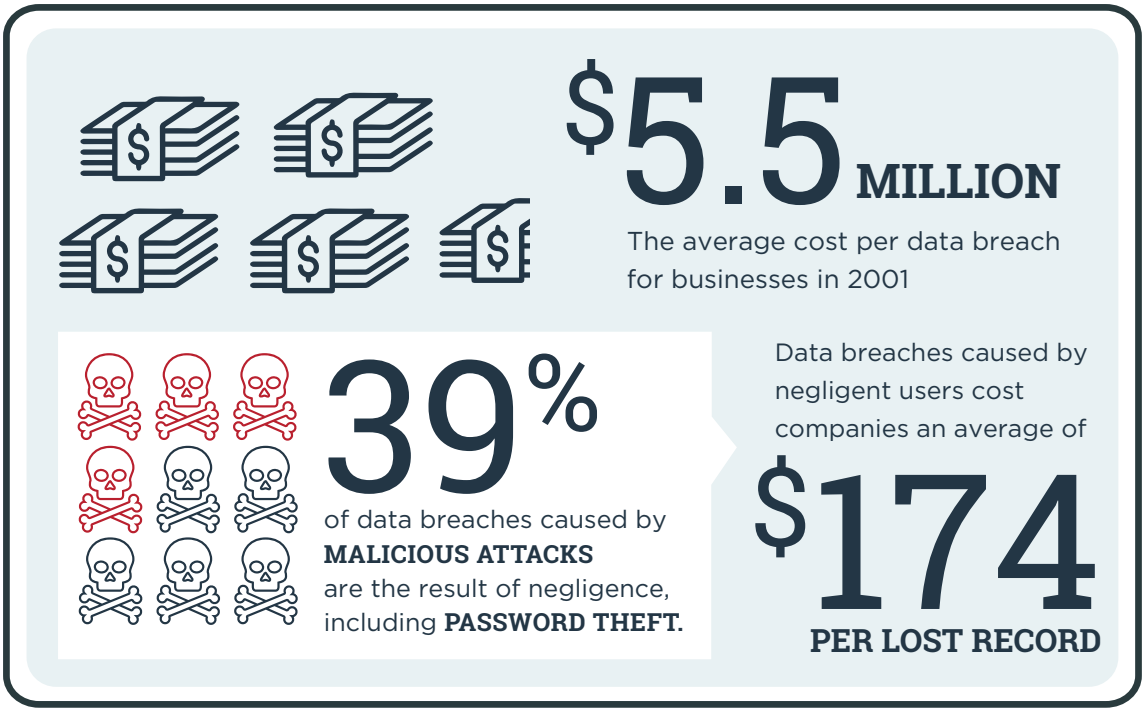
04 YOU'LL IMPROVE SECURITY

Dependence on passwords for enterprise-critical application access leaves your security perimeter vulnerable to breach.

When the number of applications running outside of an organization's firewall increases, so does the risk of password theft. The more unique usernames and passwords a user must memorize, the higher the chance they'll choose easy-to-guess passwords ("password fatigue"). Also, the chance is greater that they'll store those passwords in places they can easily be stolen.
Even some of the most common password policies leave themselves open to human error.

- 27% of organizations require that their employees remember six or more passwords.
- The average corporate user maintains 15 passwords within both the private and corporate spheres.
- 60% of people say they can't memorize all of their passwords.
- 61% of consumers reuse passwords among multiple websites.

Username and password management is an employee burden that also impacts IT. If your IT department manages user access manually, there's a chance that there are "zombie accounts" in your enterprise. Zombie accounts are active user accounts that belong to users who have been otherwise deactivated. At best, this presents a problem for IT security and compliance, as many cloud-based applications' pricing models are per user per month.



05 YOU'LL BOOST PRODUCTIVITY ALL-AROUND

Federated SSO solves this challenge by centralizing user access management. When a user is deactivated in the enterprise, access to all apps is deactivated. Cloud-based applications provide substantial CapEx savings, but those savings can be reduced due to lost employee productivity. Assume that a cloud application user logs in to an application three times per day and assume that each login takes approximately five seconds to complete (assuming a successful login). This may not seem like a lot of time, but consider this:

- Three logins per day equals 15 seconds per day, per user, per application.
- Logins cost an organization with 1,000 users 250 minutes per day, per application.
  (That's 62,500 minutes or 130 work days per year, assuming 250 work days per year.)

With federated SSO, users can reduce the amount of time spent on redundant login attempts across applications, increasing available capacity for conducting more critical business activities.

- For your workforce, SSO means that they have only one set of credentials to manage. With mobile and Internet SSO, employees can do more work when away from their desks.
- For IT departments, centralizing access control means one place to manage and monitor app access. In addition, less calls to the help desk for password issues also boosts productivity for IT and general staff.
- For your partners, SSO means that they can securely and conveniently do business with your organization.

CONCLUSION

In an age where more B2B and B2C interaction takes place in the cloud, secure SSO makes sense from an efficiency and security standpoint. Fewer passwords means less to remember, less time resetting and more time getting work done. When working remotely or accessing critical applications and data via mobile, a streamlined login process makes even more sense.

A well-planned, carefully implemented SSO strategy will help any organization improve security, increase productivity, decrease costs, meet increasing demands for mobile and remote access and enhance customer engagement.

THE CORRELATION BETWEEN PASSWORDS AND WORKPLACE PRODUCTIVITY:

1. Employees who can't remember passwords have to call helpdesks, burning time and money.
2. Forgetting passwords forces employees to go through self-service resets.
3. Also, having to frequently change your password disrupts productivity.

WHY CHOOSE PING?

So when it comes to convincing your manager, how does federated SSO translate to savings? Ping can:

- Reduce the annual volume of inbound password reset requests from the workforce and decrease staffing and resource requirements for your helpdesk.
- Decrease administrative costs due to automated Internet user account management.
- Easily integrate with your existing infrastructure. Working with your existing systems saves you time, frustration and money.

The Ping Identity Platform platform gives enterprise customers and employees one-click access to any application from any device. Over 1,200 companies, including half of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people.
For more information, visit www.pingidentity.com.

#3115 | 08.22 | v00b