# ENTERPRISE WORKFORCE SSO SOLUTION BUYER'S GUIDE

Your Comprehensive Decision

Evaluation Checklist

BUYER'S GUIDE

# INTRODUCTION

When security leaders think of single sign-on (SSO), they usually think of user convenience and experience. But SSO also plays a critical role in delivering security for data and applications.

Relying on passwords for user authentication is risky business. Stolen credentials are the number one cause of data breaches, according to the 2018 Verizon Data Breach Investigations Report. Yet the average enterprise employee struggles to manage dozens of passwords. Not surprisingly, users often rely on easy-to-guess passwords and store them in unprotected ways, like on sticky notes.

## 91% OF PEOPLE SAY THEY KNOW REUSING PASSWORDS IS RISKY.[1]

**YET**

## 62% OF PEOPLE USE THE SAME PASSWORDS FOR WORK AND PERSONAL ACCOUNTS.[2]

SSO replaces multiple usernames and passwords with one set of corporate credentials to access resources securely. By minimizing password sprawl, SSO decreases the risk of a security breach.

But not all SSO solutions are created equal. Some manage authentication for users accessing resources from desktops in a single security domain. Others deliver universal SSO across complex hybrid environments that encompass legacy on-premises, cloud-based, and software-as-a-service (SaaS) applications. Yet others are capable of acting as an authentication authority across multiple identity types and broad use cases from cloud to on-premises.

With all of the options available, you may feel challenged to identify an SSO solution that both satisfies your workforce's expectations and achieves your IT and business objectives. And sacrificing worker productivity and efficiency for a highly secure, but hard to use and administer solution is not an option.

Read on to gain a deeper understanding of what matters most in a workforce SSO solution and ensure you're asking the right questions to arrive at the best solution for your enterprise.

1 "The Psychology of Passwords: Neglect is Helping the Hackers Win," LastPass by LogMeIn, May 1, 2018.
2 Ibid.

# USER EXPECTATIONS

## Provide Anywhere, Any Device Access

Employees don't like the friction associated with password rules, nor the shear number of sign-ons and passwords they have to manage—they just want to get their jobs done from anywhere, on any device. In its Best Practices for Securing and Empowering a Mobile Workforce report, Forrester found that 70% of information workers use a smartphone at least weekly for work.

At the same time, the modern enterprise has a globally distributed workforce, requiring access to numerous applications. According to the 2018 IT Security Survey conducted by B2B market research firm Clutch, 67% of employees are using their personal mobile devices to access corporate resources. But only 40% of those employees are subject to regulations regarding the use of personal devices. The rising trend of employees using their own personal devices to access business applications and data increases companies' security risks.

**67% OF EMPLOYEES USE PERSONAL DEVICES TO ACCESS COMPANY RESOURCES. FOR WORK AND PERSONAL ACCOUNTS.[3]**

An SSO solution that securely supports mobile devices and a global workforce gives your enterprise users the seamless access they expect, while helping drive business efficiencies.

## Deliver a Frictionless Experience

The one-click purchase capabilities and self-service options that are prevalent in today's consumer marketplace have conditioned your employees, as well as your business partners, suppliers and contractors, to expect the same seamless experience in the workforce environment. They want convenient access to the applications they need to do their work. Implementing an SSO solution with self-service options will improve your workforce experience, boost productivity and make it easier for partners to do business with you.

**3** Grayson Kemper, "How Employees Engage With Company Cybersecurity Policies," Clutch, May 15, 2018.

# IT AND BUSINESS OBJECTIVES

## Protect Users' Data and Mitigate Security Risks

The average cost of a data breach is $3.9 million, according to the 2018 Cost of a Data Breach Study by Ponemon Institute and IBM. Needless to say, enterprise and IT leaders have a lot at stake. You need reliable technology partners who:

- Protect your users' data regardless of the user's application, device or location.
- Provide a scalable and flexible platform based on open standards that meets current and future security needs.
- Drive forward-thinking innovation in identity and access management (IAM), while offering a proven track record in making enterprises successful.

**$3.9 MILLION IS THE AVERAGE COST OF A DATA BREACH.[4]**

## Decrease IT and Administrative Costs

IT leaders need solutions that leverage existing investments, are simple to integrate and efficient to administer. Gartner estimates that between 20% to 50% of all helpdesk calls are for password resets, which can cost up to $147/reset for the labor alone.

## Centralize Authentication

Enterprises need a central authentication authority so that they can quickly plug in new and additional authorization capabilities to improve their overall security posture and business agility. Implementing a central authentication authority solution with federated SSO capabilities also enables enterprises to reduce operating costs by eliminating many separate silos of IAM providers.

## Boost Productivity

By reducing the number of helpdesk calls, your IT organization can focus on more strategic tasks, and your workforce and partners can get back to doing their jobs. Implementing an SSO solution with self-service capabilities reduces password sprawl and enables users to efficiently manage their access to enterprise data and applications.

**4** 2018 Cost of a Data Breach Study, Ponemon Institute.

# SELECTING THE RIGHT VENDOR & SOLUTION

To identify vendors for consideration, you can consult industry organizations, trade publications and peers. You'll also gain third-party expert insights from leading analysts like Gartner, Forrester and KuppingerCole. Each regularly reports on SSO trends, technologies and solution providers.

Once you've identified a shortlist of vendors, invite each of them to respond to your requirements. You'll want to request presentations, demonstrations and other support materials, like white papers, eBooks, datasheets and so on. This can be as formal (or informal) as fits your organization, but clearly communicating your objectives and requirements is imperative.

Striking a balance between user expectations, IT objectives and business objectives raises the bar for enterprise SSO vendors. The requirements below do not represent an exhaustive list of key capabilities, but are a helpful starting point to decide which vendors get a seat at the table.

## EMPLOYEE REQUIREMENTS

| EVALUATION CRITERIA | WHY IS THIS IMPORTANT? |
|---|---|
| What is the overall user experience? Is the login experience consistent? | Usability equates to better productivity and higher adoption rates. Having a consistent login experience with common credentials across digital properties improves enterprise security and makes it easier to do business. |
| Can users access the portal via an application on their phone or tablet? | The workforce is more mobile than ever. Supporting both desktop and mobile devices improves productivity. |
| Does the solution offer a strong/multi-factor authentication (MFA) solution that is easy to use? | MFA greatly strengthens security compared to passwords alone. Ease of use ensures faster adoption. |
| Does the solution support registration of multiple devices per user? | Supporting more than one authentication device allows users to authenticate even when they don't have their primary device. |
| Does the vendor offer self-service registration and account management mechanisms? | Self-service registration mechanisms accelerate user adoption and minimize frustration. Once registered, users need self-service capabilities to manage, add, update and/or delete their own data. |

# IT REQUIREMENTS

| EVALUATION CRITERIA | WHY IS THIS IMPORTANT? |
|---|---|
| Can the SSO solution support hybrid deployments (on-premises and cloud-based)? | In addition to supporting multiple applications that are deployed in various locations, long-standing enterprises may also have multiple SSO or federation servers across multiple domains. |
| Cloud services (IDaaS offering)? | IDaaS is quick to set up, easy to use and provides access to cloud apps. |
| On-premises offering? | Support for on-premises applications is often necessary for more diverse enterprise needs. |
| Does the solution support integration with any directory store, whether on-premises or in the cloud? | To avoid siloed SSO solutions, it is critical to connect to all identity stores, whether they are multiple AD domains, or on-premises or cloud-based directories. |
| Does the vendor support multiple second-factor and MFA solutions? | Most enterprises have a range of second-factor and MFA deployments that they need to support. |
| Does the solution support a simple setup for Microsoft® Active Directory (AD) connection? | The ability to connect to AD to authenticate without having to synchronize to the cloud is preferred. |
| Does the solution support out-of-the-box integrations to all common on-premises applications, like SAP? | Most enterprises have on-premises applications for ERP or HR that are critical to include on the SSO portal. Tested and proven out-of-the-box integrations deliver faster time-to-value for your organization. |
| Does the solution work out-of-the-box with your existing WAM solutions, like Oracle® Access Manager or CA SiteMinder®? | Many enterprises have existing WAM systems that they would like to integrate with a modern SSO solution. |
| Does the solution support all of the relevant standards including SAML, OAuth and OpenID® Connect? | Solutions that support industry standards are better suited to meet your needs today and in the future. |
| Does the solution support contextual authentication? | Solutions that support contextual authentication and integrate with major mobile device managers (MDMs) enable enterprises to enhance security and support BYOD initiatives. |
| Does the SSO solution support federated identity management? | Federation identity management takes advantage of standards to securely exchange user information and offers greater security than simple store-and-forward solutions, because it replaces passwords with signed assertions (or tokens), which minimizes attack vectors. |

# IT REQUIREMENTS (CONT.)

| EVALUATION CRITERIA | WHY IS THIS IMPORTANT? |
|---|---|
| Does the solution support all of the following SSO scenarios?<br>• IdP-initiated SSO?<br>• SP-initiated SSO?<br>• SSO for non standards-based applications?<br>• SSO for APIs, mobile applications and web services? | Today's modern enterprises serve multiple identity types, from workforce to customers to partners. This complex ecosystem is most effectively managed by identity federation, which provides a bridge to connect all of those different user identities in one place, while reducing your administrative overhead. |
| Does the solution support multiple identity types and use cases with a single authentication authority for customers, partners and workforce? | An SSO solution that is part of an authentication authority enables enterprises to efficiently address all of their current and future use cases, support multiple authorization methods, and quickly improve their overall security posture. An authentication authority addresses a diverse range of identity types and use cases with ease, which is essential for today's large enterprises. |
| Can the solution easily integrate with a wide range of identity providers, password credential validators (PCVs), cloud applications and APIs? | An SSO solution with numerous out-of-the-box adapters, integration kits, connectors and PCVs makes it easy for enterprises to centralize authentication for all of their users, applications, APIs and existing infrastructure. |

# BUSINESS REQUIREMENTS

| EVALUATION CRITERIA | WHY IS THIS IMPORTANT? |
|---|---|
| How do the vendor and solution rank with analysts such as Gartner, Forrester and KuppingerCole? | Analysts provide valuable insights into how solutions stack up. |
| Is the vendor considered a thought leader that is driving the identity market toward open standards? | Thought leaders generally have solutions better suited to meet today's and tomorrow's challenges. |
| Does the vendor focus on IAM, or is it a minor part of their business? | Organizations that focus on the IAM space tend to provide more up-to-date features, better knowledge and support. |
| Does the vendor's technology platform and pricing support a simple upgrade path from workforce SSO to support additional enterprise IAM use cases for employees, partners and customers? | Flexibility in both technology and pricing allows enterprises to scale solutions as needed. |
| What is the vendor's customer satisfaction rating (independently verified)? | Customer satisfaction is a strong indicator of a great product or solutions. |
| What is the vendor's customer renewal percentage? | Renewal rates are a strong indicator of successful customers. |

# VENDOR EVALUATION & SELECTION

After you've defined all of your requirements, you'll want to organize them in a way that makes it easy to evaluate how each vendor stacks up. A Sheets or Excel spreadsheet works well. Create rows for each of your final criteria, organized by key stakeholder requirements as we've done above. Next, add columns for each vendor you want to evaluate. Rate each vendor on how well they meet your criteria using a point-based rating system like this:

**0** = Does not meet requirement
**1** = Very limited support for requirement
**2** = Partially meets requirement
**3** = Meets or exceeds requirement

Using this system, rate each vendor from 0-3 on each of the criteria. Then tally each vendor's total. The vendor with the highest total score is the vendor that best meets your requirements.

**Want more tips on choosing the right SSO solution for your enterprise?**
**Get the white paper: Five Reasons It's Time for Federated Single Sign-On**

Contact us for additional information on how Ping Identity SSO solutions can improve workforce productivity, strengthen security posture and lower IT costs.



#3043 | 08.18 | v03