scorpion software | A Kaseya Company

10 Questions You Should Ask Your Single Sign-On Vendor

TEN QUESTIONS YOU SHOULD ASK YOUR SINGLE SIGN-ON VENDOR

Cloud computing has quickly disrupted the world of IT. The number of web-based applications, both on-premise and in the Cloud, is expanding at a remarkable rate. If your company is moving up to a single sign-on (SSO) solution to simplify the login experience to these services, here are ten questions to ask any vendor you are considering as a potential solution.

1 DOES YOUR SOLUTION REQUIRE ANY SPECIAL SOFTWARE FOR THE END USER?

If their solution requires additional software that must be provided to every user on your system, it could require significantly more administration time to deploy and configure above and beyond the initial installation.

Be sure you ask about all the software that you use. Whether you need to control access to SaaS products or to internal applications, you'll want to make sure that the solution you're considering for your single sign-on is flexible enough to handle whatever you need to log into.

2 WHAT APPLICATIONS CAN YOUR SOLUTION PROTECT BY DEFAULT?

Some applications are more widespread among business users than others and it's important that your single sign-on solution accommodates those applications by default. Your CRM, RMM, and PSA solutions for example, should be protected without workarounds or custom implementations.

Cloud applications should definitely be included among the applications that are given default protection by your single sign-on solution. Whether your business is using Office 365, Google Apps, or something entirely different, the advantages of having those applications protected by default are important.

3 HOW QUICKLY CAN NEW APPLICATIONS BE IMPLEMENTED?

Ideally, your single sign-on solution should provide out-of-the-box authentication for as many applications as possible. However it is inevitable businesses will need to expand past the default catalog and also include the specific applications that they are using. It's imperative that you ask the vendor how quickly those applications can be implemented.

A good single sign-on should make implementing new applications a relatively simple process, and one that does not always require the involvement of the vendor themselves. If it does, it's vital you are working with a vendor that is able to provide adequate and intelligent support to your IT professionals so that your business can get any custom applications implemented as quickly as possible.

4 HOW ARE USERS PROVISIONED? CAN YOU SYNC WITH ACTIVE DIRECTORY?

Just about every company will have people who come and go. In addition to normal employee turnover, companies frequently have consultants, contractors and vendors who may temporarily need access to applications and other resources.

This makes it absolutely vital to ask any vendor you are considering how new users are provisioned and managed. How difficult is the process? How long does it take? What resources are provided by the solution to make it easier?

Active Directory integration is another important feature for any single sign-on solution. If the solution can synchronize with your existing Active Directory, it should streamline the process of quickly provisioning users and avoid creating a manual process where administrators need to add new users individually.

5 CAN I ASSIGN ACCESS TO SPECIFIC USERS BASED ON ROLE OR DEPARTMENT?

A single sign-on solution should provide you with a way to assign access based on overarching criteria, such as the department in which an employee works, their role in the IT infrastructure or the company itself.

With this capability, it's possible to add users more quickly and without holding up your business processes. It also ensures that it is easier to change user permission levels if they move to a different department or take on a different role.

6 DO YOU HAVE SUPPORT FOR MULTI-FACTOR AUTHENTICATION BUILT IN?

This is another question that speaks to the need for businesses to have software solutions that are flexible, expandable, and secure. A single sign-on solution should have support for multi-factor authentication built into the system from the start. Single sign-on systems essentially vouch for the user's identity for different services and thus, should require a much higher level of identity assurance at the login than a static password alone.

7 CAN A USER'S ACCESS BE QUICKLY AND EFFECTIVELY REVOKED IF NECESSARY?

One of the main purposes of having a single sign-on solution is improving overall security and convenience. Without the ability to revoke user access quickly, the point is defeated.

Any single sign-on solution you review should make it very easy to revoke user access whenever that needs to be done. This could be because a contractor or a vendor no longer needs to have the temporary access that they were granted, or because an employee leaves the company and continued access to internal systems and applications would constitute a security risk.

8 WHICH IDENTITY STANDARDS DO YOU SUPPORT?

SAML is one of the most popular identity standards and one that any solution you are considering should support. It offers you extremely high security, ease-of-use, prevention against common types of attacks such as phishing, and makes it easier for your IT department to manage authentication.

9 DOES YOUR SYSTEM OFFER OPTIONS FOR REDUNDANCY AND FAILOVER?

The single sign-on system should make it simple and reliable to hook up a failover server, or another backup resource, in the event you have a failure on the primary server.

This should be a seamless process that ensures access to your business applications are still available in the event of some sort of a network or system outage. Ideally, the solution should allow you to configure backup and failover servers with very little effort.

10 HOW DOES YOUR SOLUTION INCREASE WORKER PRODUCTIVITY OR PREVENT ROADBLOCKS?

There's really no point in purchasing any software solution unless it increases worker productivity. In fact, a good solution can increase worker productivity substantially by eliminating some of the roadblocks that tend to manifest when a company implements what amount to sensible security standards.

CONCLUSION

With a properly deployed single sign-on solution, the advantage and benefits should be fairly obvious. Workers only need to utilize one sign-on for all of the various services that they use in a given day. They are empowered and more productive by not having to remember multiple passwords, or repeatedly logging into the same resources. It's easier for them, and safer for your business.

Before you consider any single sign-on solution, ask how the implementation of that solution will impact your operations by making your business more efficient, and thus, more profitable. If you're interested in seeing a solution designed from the ground up with security and usability in mind, download the AuthAnvil Password Solutions Quick Peek.