McAfee
An Intel Company

Top 10 Tips to Make SaaS Access Secure at Your Enterprise

So you want seamless login from your enterprise applications to Software-as-a-Service (SaaS) applications in the cloud? What flavor of single sign-on (SSO) is best for your organization: enterprise, Internet, federated, cloud SSO, or one-time password (OTP)? It's hard to know where to start. User convenience, helpdesk/password reset ROI, or corporate mandates to leverage all things in the cloud may have started you down this path. The bottom line is: you have an important task before you to select a solution that will provide security for everyone in your organization.

There are many options available, ranging from open source to stand-alone SSO gateway products. The good news is that the technologies are mature and standards deliver rapid interoperability with most providers. The days of custom coding of proprietary or open source access to partners or hosted application providers are gone.

Today, the new challenge is to apply the same level of enterprise-class security controls available internally to the cloud. The number of security breaches is on the rise, driving a new mandate to deliver more secure SSO.

Here are the top 10 tips from McAfee on how to make your federated SSO implementation a success and enterprise-class secure.

1. Leverage Microsoft Active Directory for Simple, Fast SSO and Provisioning to SaaS

Almost every enterprise has Active Directory (AD) or some enterprise lightweight directory access protocol (LDAP) identity repository deployed. A quick win is to leverage your existing directory for both provisioning and authentication. This will allow you to deploy SaaS accounts (Google Apps, Salesforce.com, and others) for users without reinventing your existing infrastructure and will provide a standardized foundation for adding other applications quickly and easily. As a result, you'll be able to demonstrate rapid progress to your management.

2. Add Strong Authentication for Critical SaaS or Custom Applications

When you move critical applications or data to the cloud, you may need to establish an alternative strong authentication method, such as one-time password (OTP), that can provide stronger authentication than passwords alone. Since most SaaS providers don't directly support authentication technology (other than SAML or a userid/password prompt), this may require you to deploy hardware or software OTP capability to users. What you need to consider are the costs and integration requirements for deploying OTP to your users. For example, if you select a soft token-based approach, rather than a hard token, the distribution and management costs are going to be significantly lower. Plus, a soft token architecture is more flexible and will allow you to support multi-factor authentication for multiple SaaS applications with one token.

3. Find a Scalable Solution that Meets the Security Needs of Different Users

Select a solution that is flexible and can apply a range of security capabilities, depending on differing scenarios. Different user groups—employees, contractors, road warriors, and students—have different access needs. This is also true for different application categories. Some applications containing sensitive or regulated data require stronger security than applications with lower confidentiality requirements. Make sure that the solutions you are evaluating are adaptive and flexible enough to accommodate the access needs for each user group or application category.

4. Bundle Strong Authentication for a More Secure Federated SSO

While ease of use is a high priority, strong authentication systems deliver great value based on the applications that they can protect. You should look for ways to apply strong authentication to platforms, while maintaining the high assurance and usability levels for your users.

Flexible federation systems can be used to extend strong authentication to multiple applications. For example, a federation system can accept OTP authentication, then give the user a security assertion markup language (SAML) credential, which provides SSO into a protected, hosted application. When functioning in a service provider mode, the federation system can convert a SAML credential into a locally consumable credential like a Kerberos ticket.

5. Make Strong Authentication Easy for Users

If you select a soft token-based multi-factor authentication system, you can provide your users with a self-service portal, where they can register their mobile device, change phone numbers, select the most appropriate OTP delivery channel, and more. If the user loses their mobile device or switches cell providers, they can easily update the site with their new phone number, effectively blocking the old device. This approach makes multi-factor authentication easier and cheaper to deploy, particularly if the target population is on smartphones—and a lot easier to update in case of an attack.

6. Rapid Automated De-Provisioning

The number one security priority in today's organization is to make sure an employee/contractor's access gets disabled or deleted immediately when the employee/contractor is terminated. Removing user access for all the applications that a user has access to is one of the key requirements of an audit. This issue becomes more critical when it comes to SaaS application access because the user can access the application from anywhere. This is another reason why you want to maintain a single system of record (such as AD) that contains up-to-date information on all user profiles and can automatically trigger a de-provisioning event when the record is updated or deleted.

7. Keep and Monitor Audit Records On Premises

Many SaaS applications are subject to internal security or regulatory compliance mandates. Logging of all identity events related to cloud applications is an important capability to put in place as soon as is practical. For example, you should monitor all SaaS application user activity, including account creation/deletion, login/logout event and, in particular, events that generate an error. Alerts can be generated to bring attention to events in real time, while logs should be archived for compliance, incident response, and detailed forensic analysis. While some cloud applications provide practical audit data, your logging and audit data should be kept separate from the application to ensure higher integrity and assurance levels.

8. Plan for Change

Every company's IT and federated environment is different. A one-size-fits-all approach won't work for most organizations. During your product evaluation, find out what application performance interfaces (APIs) and software development kits (SDKs) are available to extend the product to fit your unique requirements today—and in the future.

9. Choose the Most Secure SSO Approach

There are multiple ways that various SaaS applications can authenticate a user, ranging from standards-based federated SSO to a simple HTML form-based userid/password challenge. Choose the most secure, flexible model available from the target application. For example, if you choose SAML over any other method, you may find that it's the most reliable and robust standards-based form of SSO. On the other hand, if the target application doesn't support SAML, you might want to investigate whether you can implement SSO using an API or agent, either of which would be preferable to password vaulting and replay to an HTML form.

10. Clearly Understand the Services Required to Deploy and Maintain Your SSO Solution

Depending on the complexity of your SaaS environment, it may be necessary to use a services partner to implement a security solution. Asking your internal IT organization to try to implement such solutions may present challenges, such as incorrectly configured systems, non-standard/complex implementations that increase maintenance overhead in the long run, inability to manage change, and other issues. If you don't have the internal expertise, you should consider partnering with industry experts who can help reduce deployment time, incorporate best practices, and help your team cultivate the skills they need moving forward. This enhances seamless knowledge transfer and the internal team's ability to deliver security solutions in the future.

For more information on cloud single sign-on and one-time password, visit *www.mcafee.com/identity*.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60196brf_10-tips-saas_0413_fnl_ETMG