Solution Brief

5 Reasons Your SaaS is not Connected to SSO

Introduction

Single Sign On (SSO) has become a core security requirement for companies who want to implement SaaS security and a popular way to comply with the access control requirements defined in standards such as SOC2 or ISO 27001. There are many benefits such as better password policy enforcement, multi-factor authentication, and less time wasted for password recovery, among others. SSO works great for sanctioned applications that have been integrated. However, the world of SaaS has changed dramatically, and organizations are now finding that 80% of the SaaS applications used by employees are not in their SSO portals. The reasons for this are both technical and operational, and the problem is only getting worse every day.

Grip Security has discussed this problem with over 100 CISOs to understand how SSO has helped companies improve their SaaS security and why more SaaS applications are not monitored through their SSO implementations. The discussions confirmed that SSO is a key component to their overall architecture, but there are five key reasons for why SSO is not able to fully solve the SaaS security problem completely.

1. SSO License cost

SaaS companies fully realize that SSO is a core security requirement for most enterprises, and they charge a hefty premium to allow companies to manage their users through a third party identity provider. The site sso.tax displays what they call "The SSO Wall of Shame" that shows the price difference between the base pricing and SSO pricing. In many cases, they charge 200% or more for users managed through SSO. Another common tactic is to bundle SSO integration with other features in an "enterprise tier" with large user minimums and contract minimums. The increase in licensing costs could force CISOs to choose between security and the exorbitant licensing costs and forgo SSO integration.

2. SSO Not Supported

SSO vendors have an extensive list of pre-integrated applications that are supported, and they are constantly adding more. The problem is that there are new SaaS applications being created and coming online, and the pace of new applications is far higher than the number of new integrations. The reality is that today many workers also use consumer applications for work, and these are unlikely to support SSO integrations. In this case, companies may want to add the application to their SSO product, but they are unable to do so.

3. Third Party Owned SaaS

Even if the application is supported by the SSO application, there are instances when the company cannot integrate it to their SSO product. One scenario when this occurs is when two companies are collaborating but they use different storage applications. Company A might use Box.com while Company B uses Dropbox. When Company A's employee sends a Box.com file or folder to Company B's employee for collaboration, Company B's employee must create a Box.com account. The security team at Company B would not even be aware of the Box.com account, and even if they were, they would not be able to add it to their SSO product since they do not own the subscription.

4.SSO Implementation Backlog

Assuming the security or IT team knows the SaaS applications that are being used and SSO is supported, the applications may still not be set up in the SSO product. Most companies have a backlog of applications to be added to their SSO portal. Adding them requires IT or security to evaluate the risk and prioritize it. Once an application has been identified for SSO, the SSO upgrade license needs to be purchased, which usually means a significant budget increase and a new contract. If it is a new vendor, they would need to go through the whole vendor onboarding process, which is not an easy process at large enterprises. Facing one of the worst staffing shortages and unprecedented workload, working through the SSO backlog is a cumbersome process that often gets deprioritized.

5. Shadow SaaS

Employees today expect to be able to use any SaaS application to get their job done, and increasingly, they are just going out and acquiring it themselves. New applications are created daily, and employees will adopt them if they find them useful. As a result, most companies have a serious SaaS sprawl problem, and it has gotten to the point where IT and security teams can no longer manage them effectively. The problem with shadow SaaS is that they are completely unknown, meaning they cannot be monitored or closed down even when an employee is no longer with the company. This poses a risk far greater than those applications that are known but are not supported in SSO.

What's the Solution for Applications not Protected by SSO?

Employees are going to use SaaS to get their job done, and that means a company's SaaS security strategy needs to take this into account. The solution starts with discovery but does not end there since SSO is not able to cannot take over automatically once a new SaaS application has been discovered. In addition to discovery, access control and data governance are required.

Grip Security provides the industry's most comprehensive SaaS discovery platform. By taking a completely different approach from every SaaS security product on the market today, the solution is able to discover SaaS applications and control user access to them. The discovery is truly unique, and it can even go back historically to find active SaaS access of former employees or accounts set up that are no longer used. Then with a click of a button, the access can be turned off. All of this happens without the need of network devices, traffic mirroring, or an agent.