gamechanger Game changing technology for SaaS management

Game Changing Solutions for SaaS Management

By Brien M. Posey

Despite the challenges, adopting SaaS enhances security and frees up IT with the right solutions

It has been said that every organization is a technology company, because technology plays such a critical role. It holds the potential to improve operational efficiency, to make an organization more agile, and to vastly improve the customer's experience.

At the same time, technology can be something of a double-edged sword. We have all seen organizations that have become so bogged down by technology that the solutions put in place to solve business problems, actually impede productivity, and get in the way of employees doing their jobs.

Ideally, technology should mesh with existing business processes so seamlessly that it becomes invisible. Unfortunately, this ideal situation stands in stark contrast to what many organizations are experiencing when it comes to operating in the cloud.

Software as a Service (SaaS) holds enormous potential to improve productivity for both knowledge workers and IT pros. For knowledge workers, SaaS means they will always have the latest version of their applications. It also means that applications can be accessed from anywhere and on any web-enabled device, thereby giving employees far more flexibility.

Blackboard / iStockphoto.com

For IT professionals, SaaS applications come with a guarantee of uptime and availability. SaaS also frees IT pros from application-related tasks such as installation, patch management, version upgrades, and end user support. Furthermore, because SaaS is based on a subscription model, organizations are spared the upfront expense of purchasing software licenses.

In spite of its many benefits however, SaaS does present some challenges, especially around authentication and identity management. Consider for a moment, organizations that rely solely on applications installed locally. Users typically log into a PC using Active Directory domain credentials then are given access to their desktop and all applications installed on that PC. The credentials also might provide access to backend storage where application data is saved.

Just as the adoption of SaaS applications can be challenging for users who have to remember additional passwords, SaaS adoption adds complexity for the IT staff that manage those applications.

In this example, the authentication process is almost entirely seamless. The end user is only prompted for their credentials once, giving them access to their applications without re-entering their password each time they move from one application to another.

Although this type of single sign on works well for a locally installed set of PC-based applications, the user's credentials are typically not valid for SaaS applications. SaaS actually increases password dependency. Unlike the traditional, on-premises environment described earlier, each SaaS provider maintains its own set of user credentials. This means an employee using 20 different SaaS applications would be issued 20 different sets of credentials they have to remember.

Needless to say, it is difficult for an employee to manage so many different sets of credentials, especially since IT commonly requires periodic password changes. Not only does having multiple passwords make life difficult for users, it also increases an organization's costs. The more passwords a user is required to remember, the more password resets are likely to be required. According to numerous studies, there are direct costs that are incurred every time an organization's helpdesk has to reset a user's password.

SaaS related credential sprawl is annoying for end users forced to enter "yet another password" each time they switch between applications. What is more troubling however, is the increased risk of a security breach that credential sprawl creates. Users who have to remember multiple sets of credentials are often tempted to use the same password for every application or, worse yet, resort to writing passwords down. In either case, security is weakened.

Just as the adoption of SaaS applications can be challenging for users who have to remember additional passwords, SaaS adoption adds complexity for the IT staff that manage those applications.

If an employee leaves an organization that only uses on-premises applications, the administrator can easily disable that user's account to prevent the user from accessing the company's applications or data. SaaS cloud applications complicate user management, because when a person leaves, the IT staff must figure out the cloud applications he or she had access to, then revoke access to each application individually. This is a time consuming and error prone task.

Like any new technology, SaaS solves certain problems, but introduces some new challenges. However, organizations should not let these challenges deter them from adopting SaaS. On the contrary.

Organizations today should be actively moving toward a cloud-first IT model. SaaS has the ability to dramatically reduce an organization's costs, while also improving employee productivity, security, application availability, and overall agility. And let's not forget that SaaS providers handle security updates and mundane maintenance tasks such as patch management, which frees IT to focus on more important things.

Rather than dealing with credential sprawl and user account management challenges, organizations should consider how their existing identity and access management model might evolve to better accommodate SaaS applications. Moving to cloud-first IT is not as difficult or scary as it might seem. The key to a successful transition is to make sure you have a way to manage user identities that will allow for the cohesive management of permissions for both cloud and on premises resources.

GAME CHANGING IDENTITY MANAGEMENT FROM OKTA

SaaS is changing the way companies license and use software, but its decentralized nature presents challenges such as credential sprawl and difficulty with onboarding and offboarding users.

Okta is a cloud-based, identity and access management solution that directly addresses the challenges of moving to a cloud-first world. Its job is to act as a bridge between an organization's existing environment and the SaaS applications that organizations are beginning to adopt. Okta provides several services to help organizations move more securely and easily to the cloud.

SINGLE SIGN ON

Okta Single Sign On consolidates access so all users have only one credential for seamless, easy access to all their SaaS apps. This frees users from having to memorize and maintain separate credentials for each application. User profiles can be synced in real time with existing AD or LDAP directories.

Okta also makes it easier to access cloud apps through a centralized user portal containing chiclets for each app. Rather than having to navigate to a separate website for each SaaS app, users simply click a chiclet to get directly to the application without typing a URL or password.

MULTI-FACTOR AUTHENTICATION

Okta recognizes that the data within cloud applications is sensitive, and that organizations may wish to protect certain cloud applications using multi-factor authentication. Okta allows multi-factor authentication to be enforced on a per application basis, even if the underlying cloud application does not natively support multi-factor authentication.

LIFECYCLE MANAGEMENT

When a new employee joins the organization, that person needs access to a number of different SaaS applications. In the past, IT would manually on-board the user by creating accounts to each individual application.

Okta automates this time consuming and error prone task using rules-based provisioning that is tied to Okta's expansive Okta Integration Network of over 5,500 applications.

Okta also provides automated deprovisioning when a user moves to a new role or leaves the organization. This ensures employees no longer have access to applications they shouldn't have. Automatic deprovisioning also reduces licensing costs, because only current employees will be licensed for SaaS applications.

CONCLUSION

Adopting a cloud-first approach to IT means taking a different approach to user and application management. Just as administrators of on-premises resources rely on tools to orchestrate common tasks, orchestration tools can also be used in the cloud to simplify the management of SaaS applications.

Find out more: www.okta.com

okta

whiteMocca / Shutterstock.com