WORK FROM HOME: AN APPLICATION AND IDENTITY MANAGEMENT GUIDE

BACKGROUND

SaaS is exploding. Unless you live on Mars this is a pretty obvious statement! But what isn't perhaps as obvious is the gaping hole this explosion is causing in your IT security posture. In many organizations Active Directory (AD), which used to control all access to company resources, now only governs 20% of applications while 80% of a user's application load comes from a 3rd party like Salesforce.com or Concur.

That also means IT is no longer the linchpin to get applications up and running. If a user or group of users want to share files, they can have an app up and running in 5 minutes with a credit card. Similarly, when internal applications are not easy to use, the workforce is finding they now have the power to go out and sign up for tools on their own.

IT is struggling to provide users with the flexibility to get tools the way they want them, while also trying to get their arms around provisioning, usage and de-provisioning.

IDENTITY AND ACCESS MANAGEMENT DEFINED ... (LOOSELY)

It's important to define these terms before we dive into these 2 distinct functions within an IT security framework.

Identity Management – This refers to the process of assigning and then managing the attributes of a user. Who are they, what groups they are a part of etc. For example, "This person is remote, part of the Marketing functional area", and so on.

Access Management – This refers to the process of taking the above identities, or groups of identities, and deciding what IT resources they have access to.

These terms are very closely related and often are used interchangeably. This is likely due to the fact that traditional IT environments where corporate assets have been housed internally have utilized Active Directory (AD) to address both of these dynamics. Basically, who you are and what you can access?

However, with the explosion of SaaS, AD isn't able to perform these functions by itself any longer.

IDENTITY MANAGEMENT

Solutions for identity management can be segmented into 2 buckets:

Here are a few of the options:

Traditional AD – Companies not yet "cloud enabled" are using this tried and true structure, whether hosted on-premises or in some sort of private cloud environment. It works great, it's robust and very familiar and easy to manage. But, it's lacking when companies start venturing out to SaaS applications and identities must be created and maintained at these providers individually; it's extremely time consuming for IT to create, manage and audit.

Directory as a Service – Seriously … another DaaS?? In all seriousness, these are purpose-built solutions hosted by 3rd parties specifically for managing user identities. They are often built to integrate with other cloud solutions like SaaS applications. A great example of this would be Azure AD which is very popular. Mostly due to the fact it's given away for free in some instances. These are great for companies that are completely "cloud enabled" but they aren't built upon full blown AD. So, companies that have any legacy infrastructure that requires full AD must maintain both. And while these two can integrate with each other, it can only be managed using the full AD instance as opposed to the cloud directory instance since that's the scaled down version.

ACCESS MANAGEMENT IDENTITY

One of the key tenants of Access Management is (Single Sign-On) SSO. According to LastPass, users at large organizations of 1,000+ firms have on average 25 sets of credentials – and the number skyrockets inside of smaller firms - due to all the different legacy and SaaS applications they are using to do their job. SSO is a way to try and reduce the number of credentials a user must remember in order to do their job. It also serves as a central "choke point" to combat the age-old yin and yang battle in the security space of productivity and efficiency versus enforcing corporate controls.

WHAT IS SSO?

This is best described by example:

When using SSO, a user logs into a central portal at the beginning of their day. From there, based on their identity, tiles will appear to their corporate SaaS applications. They click on each application like Office 365, Salesforce, Concur, etc. and are granted access into those applications without having to login again.

For these integrated applications the portal is passing a token to the SaaS application and verifying that the user is allowed access. Think "Sign in with Facebook" as a consumer example. Facebook says 'you're good' so whatever application you're trying to get into trusts Facebook's opinion of you.

HOW DOES SSO WORK?

Almost all the major players are using a technology called SAML to make this work. We're not going into a dissertation on what this is – that's what Google is for if you're curious to dive deeper. Essentially there are two main components:

1. For SaaS applications that are integrated using SAML, users have no idea what their actual password is because they don't have a password anymore. Similar to the Facebook example above, the SSO provider has verified your identity, often times with multiple factors, known as multi-factor authentication (MFA) and then decided that you should be granted access based upon your identity.

2. Almost all SSO providers are on par since they're all "speaking the same language". So, if a SaaS Application is using SAML, everyone can integrate with the service. If the application isn't using SAML, no provider will be able to natively integrate with it. But all hope is not lost for applications that aren't yet up to speed on SAML, there are some options to make things easier for IT and the users.

WHY USE SSO?

From the user's perspective - you're providing them with one place to login and then allowing them to access other applications by authenticating to the initial site and being passed along as a trusted user. There's a tremendous benefit to the end user and the efficiency they gain while reducing their exposure to forgetting passwords and having to perform multiple logins throughout the day. But it goes much deeper than just password management.

From the business' perspective – There are 3 main areas to focus on:

1. Security – Based on the LastPass data earlier, SaaS just expanded the threat vector, on average, 25-fold when it comes to credentials. Which means 25 more ways for a user (the most vulnerable part of your defense mechanisms) to be compromised. SSO brings that back down to one set of credentials. Additionally, Shadow IT, the use of unauthorized SaaS solutions, represents a major Trojan horse threat to the organization as these applications are used without IT's knowledge and the enforcement of best practices. By providing an extremely efficient and better user experience, IT is making it easy for users to abide by the solutions that have been blessed by IT and deterring them from going outside corporate standards to (in their eyes) just get their job done.

2. Reduce Help Desk Tickets – Time and again when surveying our customers, password resets are the #1 or #2 source of help desk tickets. It's also been reported that every helpdesk ticket costs an organization $70 to complete! Every time a SaaS application is added to the mix, it's one more reason to generate a password reset ticket. Some SSO providers provide the ability for the user to self-administer password resets which virtually eliminates this source of tickets.

3. De-provisioning – There are two factors that come into play when looking at the offboarding or de-provisioning process. First, from a security perspective, IT has to figure out what applications a user had access to when they were onboarded and disable them. Next, they have to figure out what applications the user gained access to throughout their tenure and disable those. This points back to identity management and what's known as identity scope creep. As a user is moving from one functional area to another are their rights from the prior area revoked or are access rights just added to their identity? Hopefully they find them all. In an amicable parting of ways, this isn't as big of an issue. But in a negative or sensitive situation, it could represent a major security risk. Secondary to the security considerations, the process of actually going to each SaaS application and de-provisioning the user individually is a resource intensive process.

WHAT IF MY SAAS APPLICATION DOESN'T SUPPORT SAML?

Luckily the SaaS industry is tuned into the SSO movement and most new and updated apps are using SAML today or working feverishly to get there. Frankly, the ability to use SAML to integrate should be one of the key decision criteria businesses use to evaluate SaaS solutions.

For applications that aren't SAML enabled, some providers are offering a way to cache credentials in their portal. What this means is that the user will enter their credentials manually into the portal and then, when they click on that app, the portal will manually input their cached credentials.

This is not nearly as seamless, but it does provide the user with the SSO experience they are looking for to make their lives easier and continues adherence to corporate standards and solutions. It's also important to note that some solutions don't offer password management tools at all, letting the user continue to store them in Excel, on sticky notes or "somewhere else."

WHAT IS IAM ORCHESTRATION?

Some providers are touting "orchestration". You can think of this as trying to recreate the AD experience of creating a user, assigning them an identity and then enabling their access to 3rd party resources all in one "automatic" swoop.

SSO vendors are attempting to provide this by having their software actually go out and create accounts at the different SaaS solutions and then create the user and their privileges. This sounds REALLY cool and for the applications that can do this, it's slick. HR enters the user into their HR application such as ADP, they are assigned an identity, and based on this identity … poof they are given IT credentials and privileges (access) and all their SaaS apps come to life.

However, what these vendors aren't telling you is that this works for about 1% of the SaaS applications out there. So, if you're only using those apps, this should be an option to consider. But for the majority of applications, the industry just isn't there yet. Keep in mind this is a VERY expensive solution so make sure your turnover rates, and therefore time savings, will justify this increased expense.

Orchestrated solutions are custom, costly and typically avoided by midmarket companies who are just getting started. Crawl before you can walk!

INTEGRATED REMOTE WORKSPACES - A BETTER SOLUTION

As BYOD, remote work and work-from-home have shifted businesses away from internally hosted server solutions in favor SaaS applications, Evolve IP has pioneered an offering that meets the demands of how users want to work, with the best way to secure the enterprise; all while enabling access to both legacy and SaaS applications.

SSO, MFA and AD Together as One - Evolve IP's Clearlogin SSO portal greatly enhances an organization's security posture by providing users with just one set of credentials. Evolve IP then layers multi-factor authentication into the offering to enhance security even further. We then take it a step further and host customer AD environments within our HITRUST, PCI and SOC compliant data centers.

Clearlogin delivers full-fledged identity and access management frameworks and with additional security features such as "full lock out" which detects compromised accounts at a single credential challenge point and proactively locks those accounts down. If we hear someone at your back door, we're going to proactively lock all your doors and windows thwarting would be attacks.

Legacy Applications - Remember the legacy applications mentioned above? Evolve IP can provide these applications to users as a tile making it perform and feel like a SaaS application. And, if users require a desktop OS delivered to them, users can access that desktop as a tile inside the browser making the solution completely portable to any device. While SaaS is now the dominant way to access applications our surveys of mid-market and enterprise businesses show that about 50% of apps are still hanging out in the data center; and that's a real risk, or a real pain in the neck, for IT in work from home scenarios.

User Adoption – Because Evolve IP's SSO solution includes both SaaS and legacy applications users are more likely to fully adopt company standards and not engage in shadow IT behaviors as the corporate way is just easier – and they still get what they need. Users are also given full self-service password maintenance capabilities which means they no longer have to wait on tickets to be opened with IT.

IT Efficiency – Some estimates have a single password reset costing upwards of $70 per incident. IT will eliminate the #1 or #2 source of help desk tickets while users will be deprovisioned from all legacy and SSO integrated SaaS applications with one click freeing up IT resources for more value-creation activities within the enterprise.

CONCLUSION

During the novel coronavirus outbreak an estimated one third of the world's population was told to stay home and stay safe. For typical employees, working from home was challenging but manageable; they had their SaaS apps and a collaboration tool and were able to make do. But for IT, this heightened an already difficult situation. Home networks and devices were unsecured, helpdesk tickets went through the roof, and many users were unable to access vital on-premises applications living in a very lonely corporate data center.

An integrated identity and access management program that delivers all of a business' SaaS and on-premises applications in a single Web portal is the answer. Check out a demo of that solution here: www.evolveip.net/workspaces

Why Business Choose Evolve IP

Evolve IP enables people to **Work Anywhere**™, more productively, more securely and with less dependence on IT resources. We design Purpose-Built® solutions, tailored just for your business, that unify workspaces, collaboration and communications, and contact centers. Integrating blue-chip technology partners like Microsoft, Cisco, Citrix and VMware, with our intellectual property, Evolve IP's analyst-acclaimed solutions have been deployed globally to 500,000+ users and into the world's most well-known brands. All Evolve IP associates are focused on driving successful client outcomes and that has resulted in our scoring at the top of verified analyst and client satisfaction rankings.