okta

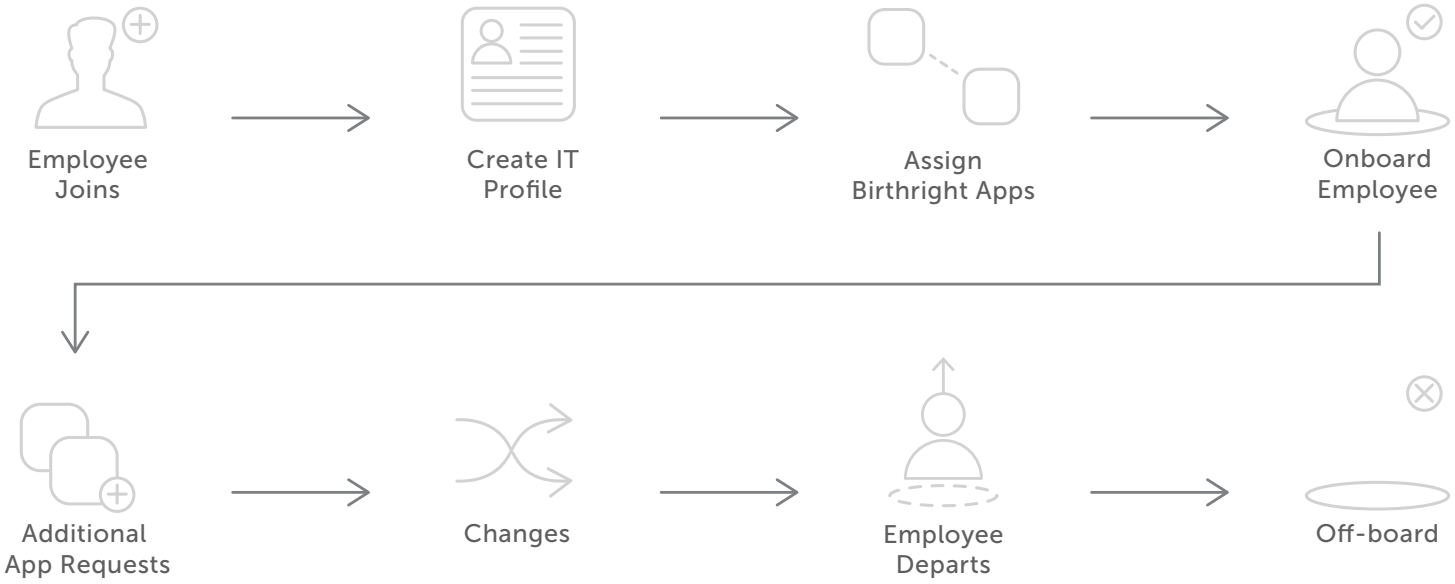
Top 5 Reasons to Automate Identity Lifecycle

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Introduction

You're an IT leader trying to bring the best technology to your organization. IT can help companies be more efficient and productive, making a sizable impact on business results. You believe in selecting the best technology from the best vendors, and know that this is the future of IT, but being on the cutting edge can feel difficult sometimes. You've allowed users to carry any number of whatever devices they want and you encourage and cooperate with teams so they can use the best applications. You're probably doing 10x more than you could have done with on-prem technology and completely locked down IT, but you're starting to hit a wall. Your team is at capacity, and it just feels like there is so much more you can do, but don't have the time.



Let's face it, you have an identity problem. Actually, it's an identity lifecycle problem to be specific. What you need is to automate how users are created in all your IT systems, how identity and access is managed as users change roles and how you handle the clean-up after users leave. There are 5 big reasons to make an investment in a serious tool to automate identity lifecycle and provisioning.

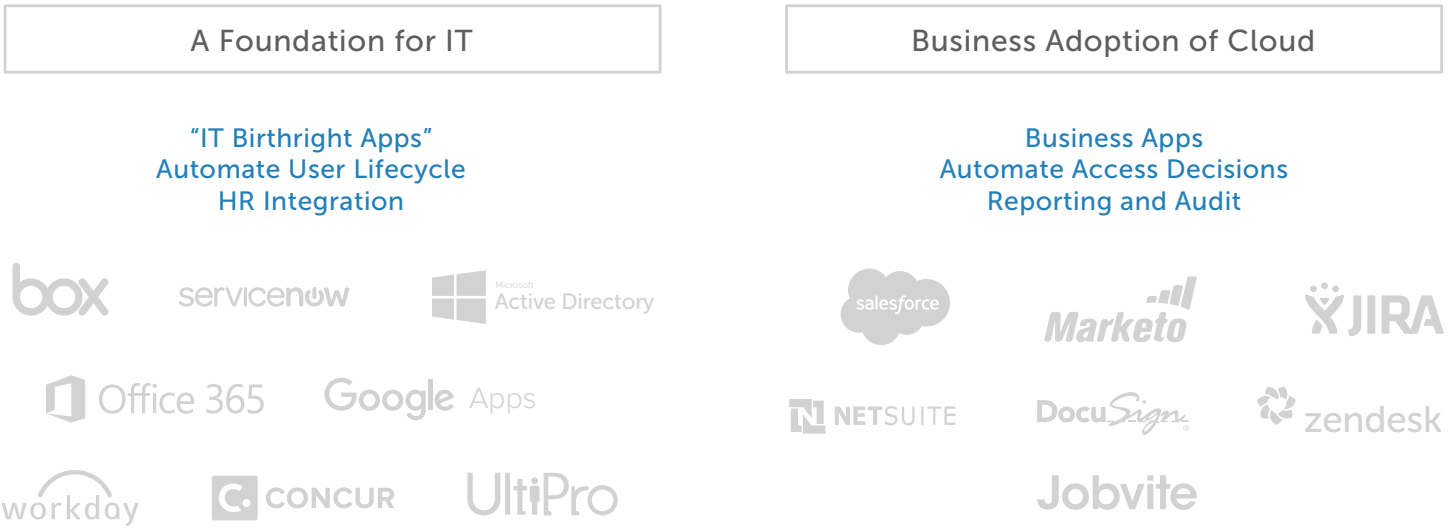
Reason #1: Creating and changing users in applications is time consuming

Okta customers typically tell us that they spend roughly 30 minutes of IT admin time per provisioning request. The more change you have in users within your organization, or more applications you bring on, greatly impacts the total time you spend here.

You might have started with a few "IT Birthright" apps in the cloud, like Google Apps or Box. Everyone in the company got access to these, and you only had to set up access once–when employees joined. It felt like application provisioning was a contained problem.

However, you started to need to give access to contractors and partners to Box as well. Those users often have more of a 30-90 day access cycle. Add on the provisioning requests!

As you add applications, the problem also gets worse. Now you have applications that users might get at any point in time, and their access level might change as well as they move between teams. An average Okta customer has about 20 applications connected to Okta. When you reach that level, you need to automate!



Reason #2: Your process for coordinating with HR feels like it's from 1998

How does HR tell IT that a new employee has joined? Some customers tell us it's literally a phone call. Many companies do this over email. Either way, it's redundant, manual work for IT.

If you get a CSV file with changes from HR, and you've written scripts to process it and add users to Active Directory, then you're somewhat ahead of the game. But you probably have to go back and update those scripts every 6 months when vendor APIs change. And, it's software, running on a server, that has to be kept secure and up-to-date. Something you are probably trying to avoid as you leverage the cloud.

This is a tough one to automate, because it's core to how you manage access for users. It's not enough to just have a tool that automatically imports from HR and provisions Active Directory, Office 365 or Google Apps. What you really need is to build logic into the process. You need to stage new employee accounts before granting access. Or, you need to program in what security groups should be assigned to which users based on user attributes.

Reason #3: Different teams have different business processes, and it's hard to keep up

Over time, your business groups started bringing on business-specific applications like Salesforce and Marketo, and some teams wanted to use their own collaboration tools, like Slack. In addition to wanting to manage access centrally to these applications, you now have an increasingly complex matrix of who has access to what that is getting hard to manage using Excel spredsheets.

You need to empower business teams to do more here–they know these business apps the best, and they know who should get access to them and the level of access. They, and you, will be happier.

Reason #4: It's not easy for end users to set up their device or get access to niche apps

BYOD is fantastic, but it's pretty useless if you bring a device to work but can't actually do any work on it. A lot of applications are end-user friendly, but it can be a maze for new employees to get all the stuff working on their personal device. This often leads to lots of helpdesk calls to help get users configured. And, the more devices they want to use—tablet, home computer, smart watch—the more work this becomes.

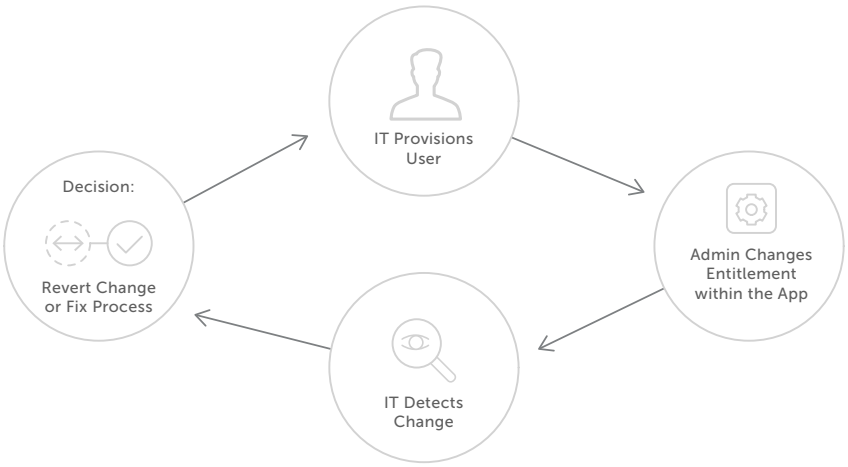
Users also don't want to wait forever to get access. If you know you need an app to get work done, every minute you don't have that app is painful. Automating this process with some lightweight application approval workflow can work wonders.

Reason #5: You don't have full control over business apps, yet you're responsible for security

Last but not least–security. This starts with having some basic reporting around what users are accessing and verification that users have been deprovisioned from applications when they leave an organization.

Beyond that, what about all the applications and systems you don't have full control over? It's likely still expected that IT is keeping the company secure, even though you know there are admin users for business apps like Salesforce that can make changes to user accounts without any IT oversight.

Rather than a manual audit process, automate the discovery of user accounts in all your applications, and remediate access by enforcing the right accounts and entitlements if you find there has been any "drift" in accounts.



Conclusion

Cloud-first and mobile-first IT has unleashed a massive amount of change in IT organizations. IT can now be "the department of yes!" instead of just saying no to everything. The challenge is how to continue to drive efficiency so users can take advantage of all the technology available to them and keep your company secure at the same time.

Okta is the identity management foundation for a cloud-centric IT architecture that enables you to take the lead in adopting new applications and enabling mobile for your organization to drive growth. Instead of depending on manual processes, Okta enables your IT organization to say yes to more of what the business wants, get out of maintenance mode, strengthen security and delight your end users.