GOOD ENOUGH ISN'T ENOUGH:

5 Rules for Choosing an Identity Solution that Lasts

okta

Introduction

Today more than ever, people and technology are the lifeblood of the modern enterprise and, thanks to the cloud, these two worlds are changing more rapidly than ever before.

On the technology side, we're living in a best of breed world, and there is more innovation coming our way than most organizations know what to do with. Powerful new applications and tools that – when implemented quickly and used effectively – can have a huge impact on your organization's growth. The challenge is how to keep pace with it all - not just because doing so might save some money or improve productivity by "x"%, but because your organization's success actually depends on it. Technology sits behind every challenge and every opportunity that an organization faces. It's core to every business initiative you're driving - so much so, that most companies are thinking about how to reinvent themselves as technology companies. So, in today's world, your organization's ability to adopt, use, and even build the best technology will become one of the biggest drivers for your future success.

Just as the cloud unleashed this wave of innovation, it also opened the floodgates to the number and types of people organizations need to manage. It's not just about your employees anymore. It's about contractors, partners, customers, and consumers - literally anyone who has a relationship to your business. Add them all up, and IT can now be responsible for managing and securing millions of users, each of whom sits on a different network, uses a different combination of devices, and is constantly on the move.

Today's world is a whole new paradigm for IT. Success depends on an organization's ability to securely connect its people and technology, no matter how fast these worlds are changing. And when your people and technology are everyone and everything, identity is the only constant. If you definitively know who someone is – where they are, what device they're using, what network they're on, what their relationship to your business is, and how these things are changing over time – then you should always be able to provide that person with the most productive, most personalized, and most secure experience possible.

Identity is the lynchpin for the modern cloud ecosystem. It's the new security standard in a world where there is no perimeter anymore. And it's the foundation on which any company can become a technology company.

Like technology leaders, identity has a much more important role to play in this world. It needs to be thought of and evaluated on different terms, based on its elevated role and this new paradigm for IT. So, we came up with a short list of things to look for from your identity provider to help you thrive in the modern cloud era.

We've had conversations with thousands of technology and security leaders, from the largest enterprises to small and medium-sized businesses across every industry, non-profits, government agencies and universities. Based on these conversations, we've developed a cheat sheet. Because there are certain elements of an identity solution that every organization should have.

RULES

1. **DON'T GET BOXED IN. BEST OF BREED IT REQUIRES INDEPENDENCE AND NEUTRALITY.**
2. **YOUR APP STACK IS DYNAMIC. YOUR SOLUTION MUST BE FUTURE PROOF.**
3. **AVOID FRAGMENTATION. USE ONE PLATFORM TO MANAGE EVERY TYPE OF USER.**
4. **PEOPLE ARE YOUR PERIMETER. PROTECT THEM.**
5. **NOT ALL CLOUDS ARE CREATED EQUAL. FIND A SOLUTION THAT'S BORN AND BUILT IN THE CLOUD.**

RULE #1

DON'T GET BOXED IN. BEST OF BREED IT REQUIRES INDEPENDENCE AND NEUTRALITY.

Choosing an identity solution is about preserving choice. Your provider shouldn't be tethered to the success of any proprietary applications.

Quite the contrary. Your identity provider should be committed to connecting everything you want to use with a consistent level of quality and depth.

Can you trust an identity provider that's trying to sell you other apps or favors certain apps over others you deeply want to use? Does a provider who bundles their identity solutions in with their own applications prioritize identity in the same way as one who doesn't?

You know your organization best. And you should always choose the technology that's best for you, not your identity provider.

If you want to be truly best of breed, this is a necessity.

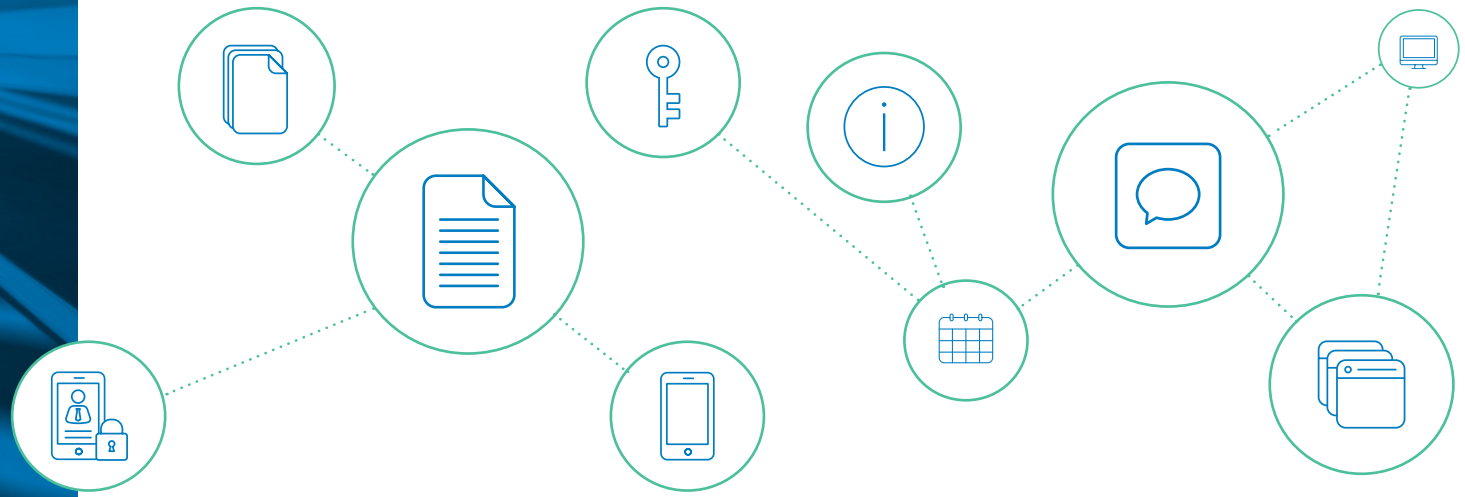
RULE #2

YOUR APP STACK IS DYNAMIC. YOUR SOLUTION MUST BE FUTURE PROOF.

A best of breed world is defined by the fact that what works best for your business today can, and will, be replaced by something better tomorrow.

There is always going to be new technology - new apps, new devices, and new tools that your teams will want to use. You need the ability to use these new tools and to roll them out as quickly and efficiently as possible to keep your teams productive.

Make sure the identity solution you choose connects to everything you want to use today, and will connect to everything you want to use in the future as well. This will enable countless growth opportunities for your company.



RULE #3

AVOID FRAGMENTATION. USE ONE PLATFORM TO MANAGE EVERY TYPE OF USER.

Identity today isn't just about your employees. It's about everyone, including contractors, partners, suppliers, and customers.

The volume of users that IT teams need to manage is exponentially larger in today's world. For every employee you have, you might also have a dozens of contractors, hundreds of partners or suppliers, or thousands of customers. Not only that, but every one of these users is constantly on the move - accessing critical apps from an infinite number of networks and devices. And their relationship to your business isn't static. Employees get promoted, contractors operate on short term contracts, partners and suppliers come and go. All of these changes come with a set of actions that need to be managed and permissions that need to updated.

For any extended enterprise, this poses a challenge. In order to effectively manage these different user types at scale, you need a single, centralized identity solution. This solution should be able to support millions of users and automate how all users access (and use) the tools that make them most productive, regardless of who they are or where they work.

RULE #4

PEOPLE ARE YOUR PERIMETER. PROTECT THEM.

10 years ago, IT could draw a perimeter around the people and technology IT needed to keep secure. In today's world, that's impossible.

When the world you need to manage and secure must account for everyone and everything everywhere, there is no perimeter – at least not in the traditional sense.

Security isn't a network problem anymore, nor is it a VPN or firewall issue. These approaches to security made sense when you could restrict people based on where they were located. But that's no longer the case.

In a perimeter-free world, infrastructure isn't the target threat. The target is end users, and specifically, their credentials. Safeguarding end users has become increasingly difficult for IT teams because end users have so much flexibility today. They can choose which device to work on, where to work from, and the apps they'd like to use.

Just as hackers have shifted their target to the end user, security leaders must shift their focus to be user-centric as well.

THE NUMBERS DON'T LIE

42,000
security incidents in 2016

1,935
confirmed security breaches

$3.6M
Cost of average breach

81%
of breaches used stolen and/or weak credentials

*Verizon 2017 Data Breach Investigations Report, Ponemon Institute's 2017 Cost of Data Breach Study

Your identity provider should have a security stack that picks up where the traditional security stack stopped working.

It needs to be flexible, work for every device, and in every location. And it needs to do so without adversely affecting the end user experience.

Finally, confirm that your identity provider has the proper certifications.

If you're a healthcare company, your provider should be HIPAA compliant. If you're a government agency, they need to be FedRAMP certified. All organizations should verify that their identity provider is SOC 2 and ISO compliant. These are formal measures to protect your data and personally identifiable information.

They are critical!

FedRAMP

Information Security Management System ISO 27001 Certified

Information Security Management System ISO 27018 Certified

RULE #5

NOT ALL CLOUDS ARE CREATED EQUAL. FIND A SOLUTION THAT'S BORN AND BUILT IN THE CLOUD.

A company's ability to win, differentiate, and achieve its mission as quickly and effectively as possible hinges on its ability to use the best technology it possibly can.

This simply isn't possible in an on-premises environment. And it's also not possible by taking premises-based technologies (like Siebel, PeopleSoft, or Microsoft AD) and putting them in the cloud.

A lot of vendors will say they have a complete, integrated identity stack. But if your identity solution wasn't built in the cloud from day 1, then that's not the case. 7 different products, with 7 different interfaces, is not fully integrated.

A true cloud identity solution will enable:

- A better user experience
- A more powerful platform
- Central management, with changes that permeate throughout your ecosystem
- A faster and more elegant solution

Your identity solution should be 100% multi-tenant.

That way, your identity provider can focus on making one (and only one) environment extremely robust in terms of scale, redundancy, monitoring and processes. And the service should be replicated across various availability zones and geographic regions.

As you evaluate a solution to solve your identity challenges, make sure the vendor you choose delivers near-perfect availability of its service and is transparent about any outages that take place. Ask your vendor about cell architecture and global distribution.

CONCLUSION

Organizations rely on their identity provider to securely connect all their users to the technologies and devices that enable them to do their most important work. We know selecting the right identity provider can be daunting. But it doesn't have to be.

Evaluate every potential identity provider on these 5 rules. Don't settle for an identity solution that meets 3 out of 5 criteria. Or even 4 out of 5. Make sure they meet them all.

Identity enables your business to succeed. But not just any identity vendor. The right identity vendor.

About Okta

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners.

The Okta Identity Cloud is made up of six products that function as a single integrated platform: Okta Single Sign-on, Okta Universal Directory, Okta Mobility Management, Adaptive Multi-Factor Authentication, Okta Lifecycle Management and Okta API Access Management. Today, more than 5,000 cloud, mobile, and web applications are pre-integrated to the Okta Identity Cloud. We manage and constantly improve the quality of those integrations so that they can work seamlessly with all of our products. Customers and partners can also easily add their own applications to the Okta Identity Cloud. To date, our customers have added more than 50,000 custom or private applications.

Thousands of organizations trust Okta to help them fulfill their missions. Our customers range from some of the world's largest enterprises, to small and medium-sized businesses, universities, nonprofits and government agencies.

experian
dish
20th Century Fox
flex
Adobe
News Corp
pitney bowes
Nasdaq

okta