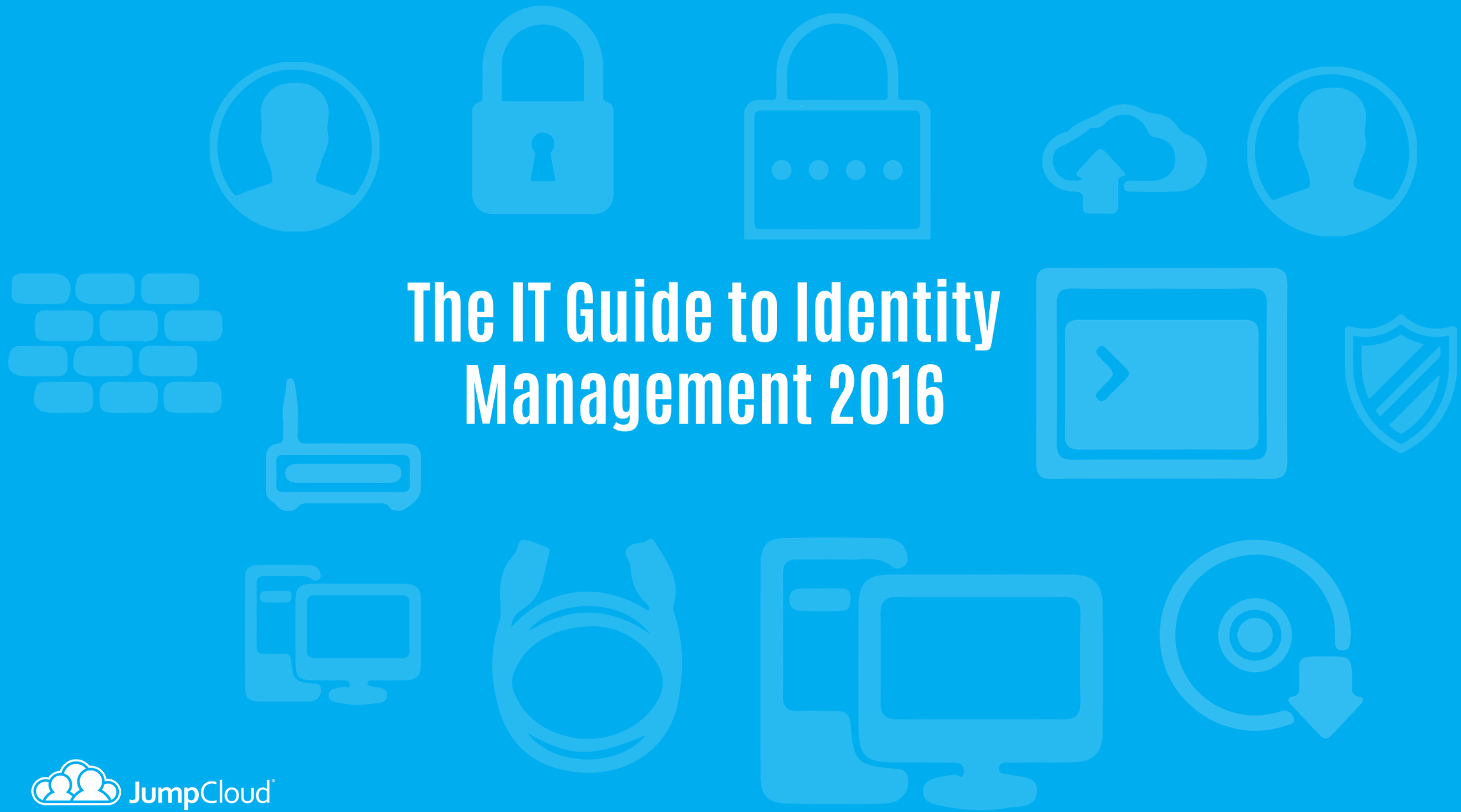
The IT Guide to Identity Management 2016



JumpCloud®

The IT Guide to Indentity Management 2016

Identities have quietly become the most critical digital assets in the modern era. And whether management knows it or not (hint: they don't) many of the most critical conversations they have with IT are really conversations about identities.

Want better security? If hackers steal your company's identities, they steal the very core of your business. This fear would keep any IT team up at night.

How about more efficiency? Wouldn't it be nice if with just one click, you could grant and revoke access to the myriad of resources your employee needs? This would allow your team to focus on building and strengthening your business.

A fast-moving, efficient, secure business orbits around successfully managing an employee's identities – and it always has. But today, there is more to connect to than ever before. This is contributing to a fundamental shift in the Identity and Access Market (IAM). If you're not keeping up, then you're putting your company at risk of breaches, loss of productivity, and falling behind your competition.

Don't want that to happen? You've come to right place.

This guide doesn't just show how the Identity and Access Management landscape is shifting. It shows you how to shift along with it. There's a brave new world of IAM – and you can use it to your advantage to move your business forward even faster and more efficiently.

JumpCloud®

Table of Contents

PART 1: Overview

PART 1:
Overview

The New Identity

Let's start by taking a look at everything IT is supposed to provision access to in 2016:

Internal Apps

Developed in-house and stored on-premises

Third Party Apps (SaaS)

e.g. SalesForce, Google Apps

Infrastructure-as-a-Service (IaaS)

Virtual Machines (VMs) from AWS, etc.

WiFi

The all-important Internet

Documents

Text, spreadsheets, pdfs, and reports

Devices

Windows, Mac, and Linux Devices

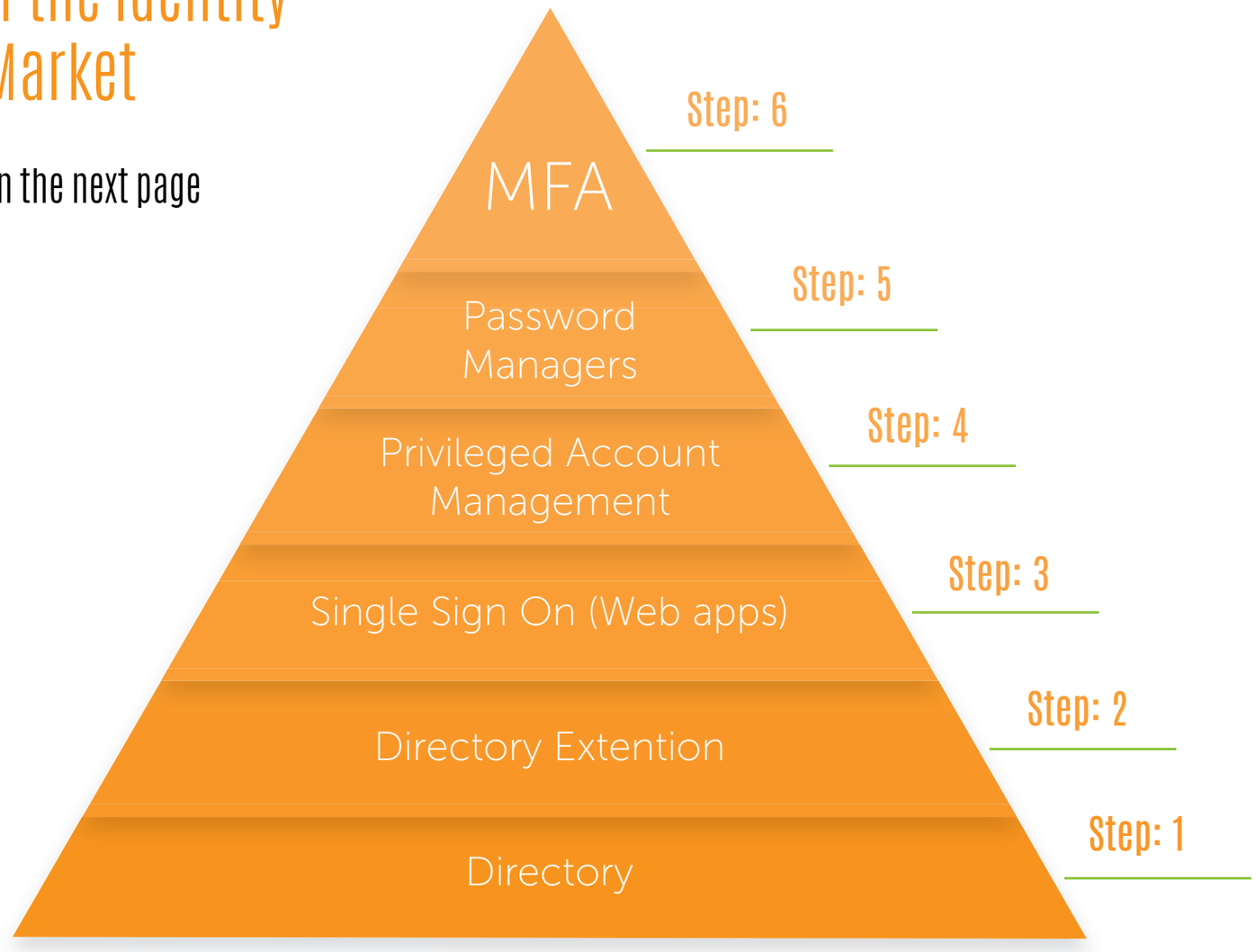
For years, IT has tried to use existing systems to manage this jumble of new resources, even though that means a proliferation of unmanaged identities. The "identity crisis" has been simmering for a decade now and it's about to reach a boil. IT admins around the world are getting overwhelmed and fed up.

Here's the good news. When a problem gets big enough, people have to stop ignoring it. In the last few years, there have been some concerted efforts to create better identity management solutions for enterprise.

We are on the brink of an identity revolution – and if you take advantage of it now, you won't just make life easier for everyone in the IT department, you'll get a leg up on the competition.

Categories of the Identity and Access Market

Steps 1-6 explained on the next page



Categories of the Identity and Access

1. **Directory** – directories connect users to the IT resources they need. As the core user store, a directory is the foundation of any identity and access management program. There are two primary classifications of directories on-premise directories such as Microsoft Active Directory and cloud-based Directory-as-a-Service® (DaaS) alternatives.

2. **Directory Extension** – since conventional on-premises directories are ill-equipped to manage many of today's resources (e.g. SaaS, IaaS) a whole category of solutions has been created to extend credentials to other platforms and other locations. This step can be eliminated with a Directory-as-a-Service®.

3. **SSO** – single sign-on solutions strive to consolidate the plethora of accounts and resources in use into one login.

4. **Privileged Account Management** – some directories don't provide sufficient security or management over critical systems like databases and network infrastructure. Privileged account management has sprung up to fill the void. These systems provide more stringent access controls, including the ability to log command and ensure that access is disconnected when complete. A complete directory will have this built-in.

5. **Password Managers/Vaults** – end users need to remember so many passwords that a category of solutions has emerged to help. These solutions utilize a password vault that stores the passwords to your sites and systems.

6. **Multi-Factor Authentication** – Passwords are an imperfect form of identity protection. To prevent the breach of high-value resources, a second method of authentication is essential. A solid identity management solution should have MFA options available.

JumpCloud®

The Checklist

What you should look for as part of your IAM strategy in 2016.

- [ ] Centralized Management
- [ ] Multi-Factor Authentication
- [ ] Single Sign-On
- [ ] Automatic Password Rotation
- [ ] Manage by Groups
- [ ] Customizable Password Requirements
- [ ] Compatible with Windows, Mac, & Linux (Vendor Neutral solution)
- [ ] Uses core protocols, such as LDAP, SAML, RADIUS, SSH, REST
- [ ] Extensible to SaaS Apps (e.g. Google Apps, AWS)
- [ ] Automated Provisioning & De-Provisioning

(Add up your check marks) How does your current IAM strategy measure up on this checklist?

=

_____

Scoring:
0-4: Poor
4-7: Fair
7-8: Good
9-10: Excellent

JumpCloud®

The Checklist

Poor (0-4): If you're in this range, then your IAM strategy is actively hurting your company's efficiency and security. You probably either don't have a directory or you need to scrap your existing one. Giving your IAM strategy a makeover should be your top priority.

Fair (4-7): You're keeping your head above water, but you're not getting anywhere. Your IAM is either causing lapses in security or incompatibility with critical resources. Survey your needs and consider making a major change.

Good (7-8): If you scored in this range, that means your IAM is serving you well. Still, all it takes is one missing plate in your armor for a hacker to deal a costly strike. Keep reading to find ways to address your IAM's shortcomings.

Excellent (9-10): Give yourself a pat on the back. You've already got a high-functioning IAM. Focus your efforts on staying ahead of the curve and being prepared for the changes coming in the identity market.

In 2016, there's no excuse for a company's IAM strategy not to be scoring in the 'Excellent' range. That said, there are a host of good reasons why it probably isn't. We'll get into that in the next section.

PART II: Challenges

Vunerable Identities

61% of defrauded data breach victims attribute their fraud to the breach of credentials.
The Consumer Data Insecurity Report,Javelin Strategy & Research

Everyone likes to say,

"It will never happen to me."

But the threat of hacked identities has never been more clear. In 2014 alone, more than one billion personal records were illegally accessed (Gemalto)**.**

In 2016, the need for greater security and stronger authentication is paramount for every organization, large or small. These are some steps you can take to fortify your identities:

- **enforce strong identity controls, including strict password requirements**
- **multi-factor access on devices and applications**
- **consistent training to teach employees to use separate passwords per service**
- **implement a password manager**

We'll go further in-depth in the third section, 'Solutions'.

Identity Sprawl

Think about all of the accounts and passwords the average person has today: email, social media, banking, and on and on. The average internet user has a whopping 25 online accounts – and growing. (Halock)

This is called 'identity sprawl' and it is even worse at workplaces where you have to factor in a variety of internal and SaaS-based apps. Users have a different account for SalesForce, Box, Google Apps, etc. Aside from being a headache from a compliance perspective, identity sprawl hurts companies in two big ways:

Security

Identity sprawl creates a chaotic environment that is difficult to secure. When an employee leaves, instead of being able to de-provision access to all resources with one click, IT must be very meticulous and de-provision access individually. One mistake, one little oversight, and someone has access who shouldn't.

To hackers, identity sprawl looks a lot like opportunity.

> "People average 25 accounts, but only 6.5 passwords"

So when a third-party hack happens (e.g. LinkedIn, Sony, Target), the passwords for internal accounts are often compromised as well. But IT has no way of knowing because it exists entirely out of their purview.

Identity Sprawl

Efficiency

At the user level, identity sprawl leads to more time logging in and looking up passwords (and ringing the help desk when they inevitably can't remember what key goes to what account).

On the admin side, it's even worse. IT loses centralized control. They make a change in the central directory and it ends up propagating to only some IT resources. This requires that the admin keep track of which resources require separate control.

The solution is to consolidate identities, but out next challenge, legacy systems, is a major roadblock toward that goal...

Legacy Systems

Microsoft Active Directory has served valiantly as the core identity provider since its release with Windows 2000. It earned an early stranglehold on the market and is still in place at a commanding

95% of Fortune 1000 companies (Enterprise Systems Journal).
But a lot has changed since 1999.

The preeminence of Microsoft AD is in fact the single biggest reason for identity sprawl.AD doesn't effectively manage devices that don't run Windows – and the number of Mac and Linux devices has been on the uptick year after year.

Legacy Systems

AD is also poorly equipped to authenticate SaaS-based identities and other cloud resources. The result is a multiplicity of unmanaged identities. So identity sprawl is stemming directly from companies where the IT department's hands are tied because they still have to use AD.

The other major legacy directory in place in companies is OpenLDAP. LDAP is better with Linux and Unix systems than AD, but it has the same difficulties managing cloud infrastructure. Furthermore, OpenLDAP is partial to LDAP (go figure) and other ascendent protocols like SAML, Kerberos, and RADIUS are out of reach.

Ultimately, as long as these these legacy systems continue to lock companies into their systems, IT will be unable to keep up with the changing identity landscape.

Shadow IT

Shadow IT refers to systems and solutions implemented inside organizations without the IT department's knowledge or approval.

Widespread
83% of CIOs report "some level of unauthorized provisioning of cloud services" (Brocade, 2015)

Risky
89% of CIOs feel Shadow IT presents a long-term security risk (Vanson Bourne, 2015)

Expensive
CIOs reported an average of $13 million in annual spending on Shadow IT (Canopy, 2014)

Shadow IT

Shadow IT leads to gaps in security, chaotic workflows, and a proliferation of unmanaged identities. But that's not the worst part.

> "The worst part of Shadow IT is that it is not connected to the core directory structure. Many IT admins have no idea how to connect all of these newly implemented devices, applications, and networks back to their core directory."

James Brown
Chief Architect, JumpCloud

In other words, Shadow IT is a major factor contributing to the "identity crisis" that IT faces today. Whether its for collaboration, communication, or the transfer of files, Shadow IT means more unmanaged identities.

Shadow IT can also be cast as 'innovative' and 'proactive'. That's why TechCrunch has said it's "time to embrace Shadow IT" and why Forbes has opined that "CIOs should be happy about Shadow IT".

Ultimately, you can't (and shouldn't) eliminate Shadow IT altogether. The approach must be twofold:

1st Train employees about Shadow IT, discouraging risky behavior

2nd Eliminate the need for Shadow IT by improving your IT infrastructure to better accommodate and manage the types of apps that are likely to implemented by rogue innovators.

Vendor Lock-In

The market for your identities has never been so competitive.

As a result, one of the more subtle factors working against identity management is vendor lock-in. This refers to all of the companies that are trying to woo enterprises into using their identities (often for free) so that you become dependent on their services. Eventually, this means they can lock you into to paying for their services.

Where I come from, this is known as

"the long con."

Microsoft, Google, Amazon... they all know that if they lock up your corporate identities now that you'll be beholden to them later. These are savvy businesses. Why do you think that they offer so many valuable services for free?

For them, storing your identities (on their infrastructure) means additional revenue elsewhere. For Microsoft, it's O365 or Active Directory. For Google, it's their Apps for Work platform. For Amazon, it's AWS. Often, it is a good a deal for businesses. Who doesn't like to receive valuable services for free? But being naive about it is a recipe for disaster.

Why? Because they want you to do things their way. Microsoft wants you to use Windows systems. Google wants you to bypass quality apps from their competitors in favor of Google Apps. Amazon doesn't want you to implement any VMs apart from AWS.

So naturally they design their infrastructures to be funnels – funnels that eventually guide you to paying for their services and excluding alternatives.

Don't be a pawn in another player's game. Understand that your corporate identities are perceived as long-term

PART III: Solutions

Better Security

Enterprise security once meant installing anti-virus software and a firewall. It used to be that easy. Today, there are five layers of depth of security, shown here:

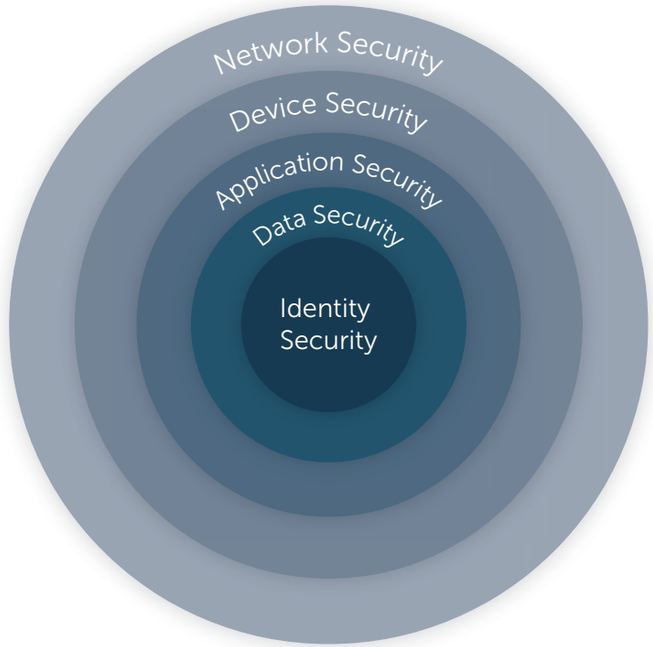
Network Security: firewalls, intrusion detection/ prevention solutions, VPNs, and others.

Device Security: servers, desktops, and laptops.

Application Security: internal and web applications.

Data Security: all data must be encrypted.

Identity Security: the core of enterprise security.



Each layer is integral, but identity security is fundamental. That's because if a hacker can get credentials, then the rest of the security measures can be bypassed. At that point, the hacker is already "inside" and can do as they please.

Better Security

Multi-Factor Authentication

Conventional passwords no longer cut it. They are prone to employees using the same password across multiple sites, employees using weak passwords, and the possibility of them being stored in insecure ways.

MFA is an easy way to give some extra peace of mind over your business. With MFA, the standard password is supplemented with another form of authentication, be it a code sent to your phone, a fingerprint, or a retinal print.

This doesn't make it twice as difficult for hackers. It makes it exponentially more difficult.

Password Requirements

A high-end computer can now crack an eight-character password in 5.5 hours. (Halock)

Luckily, IT has the ability to implement password requirements. Most experts recommend enforcing a 12 character password requirement. At JumpCloud, we recommend at least 18 characters.

Factors to consider for password complexity:

- Set length of password
- Uppercase and lowercase requirements
- Number requirements
- Special characters
- Password reuse

Better Security

Complexity also plays a vital role in password security. You can train your employees to make passwords of this length, but people are just people and they are inevitably beset by “password fatigue”. I encourage you to use the only fail-safe method: use a password manager to ensure that passwords meet stringent complexity requirements.

One-Way Hashing and Salting

However you store your identities, they should be one-way hashed and salted. This makes it very difficult for credentials to be decrypted.

Training

Identities are intrinsically linked to user behavior. Password managers can largely circumvent this, but when everyone on the team understands the dangers associated with identity sprawl, then everyone is invested in eliminating it and keeping the company secure.

Leveraging SaaS Identities (e.g. Google Apps)

More and more startups are bypassing traditional on-premises directories altogether. Instead, they’re leveraging SaaS-based apps as their core identities. This can be a huge boon for companies. SaaS directories are exceptionally effective on the cloud while requiring little investment and maintenance from IT departments.

The only problem with this is that Google Apps was never built to be a true directory. Google Apps doesn’t offer the degree of control required from a directory. Say goodbye to grouping identities, automation, and security compliance.

Better Security

SSO is all about identity management and access, which is managed by your organization's core directory. So SSO can only be as capable as your directory. Unfortunately, conventional directories like Microsoft Active Directory don't provide management for most of the multitude of devices and apps in use today.

Cloud-based directory services have been built from the ground up to manage identities and resources across the cloud. Google Apps? Check. WiFi networks? Check. AWS, SalesForce, and more? Check, check, and check.

A Directory-as-a-Service (DaaS) integrates seamlessly across on-premises and cloud-based resources. One identity can now traverse the plethora of different apps and infrastructure that modern business requires.

Cloud-based directory services offer true Single Sign-On for the first time in the modern era.

Discovering Your True Identity

When people look back on the trajectory of the Identity and Access Market decades from now, they'll see 2016 as an inflection point – the moment when identities stopped proliferating out endlessly and began to consolidate back in. The future of identities is simpler, more efficient, and more secure.

The future of identities is on the cloud. As more and more resources move to the cloud, there's no way around the fact that it is the most efficient way to manage identities.

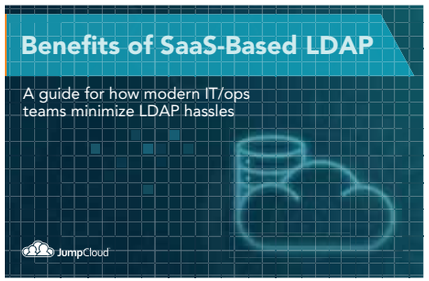
But what about security? It may seem that the cloud is an easy target, but with correct security practices applied to the cloud, the opposite is in fact true. In December 2015, InfoWorld announced, "The Public Cloud is Now More Secure than Your Data Center."

So move forward into the new world of Identity Management with confidence. High costs and insufficient management are in the rear-view. Better security and true SSO lie ahead.

If you would like to learn more about how Directory-as-a-Service solves today's identity management challenges, drop us a note at sales@jumpcloud.com.

Looking for more information?

Click these guides to learn more about DaaS:



JumpCloud®

About JumpCloud:

JumpCloud®, the first Directory-as-a-Service® (DaaS), is Active Directory® and LDAP reimagined. JumpCloud securely manages and connects employee identities to IT resources including devices, applications, and networks. Try JumpCloud's cloud-based directory free at JumpCloud.com or **contact us at 720.240.5001.**

Contact us

For additional reading, blog updates, and the latest news please visit our **blog**

Or follow us: