

Why Centralized Cloud ID Management Is Crucial For The Enterprise

Executive Overview

It is well established that we are experiencing a radical model shift in enterprise computing to hybrid-cloud models. Corporate applications and services are being delivered via the Web versus being built or maintained at each company and legacy applications in-house will be retired over time. Call these services Software as a Service (SaaS), or the vogue term, "Cloud Applications", the effect of having employees leave the relatively safe virtually confines of the firewall to the wild Web with corporate identities demands we look to shift our security and identity models to accommodate these new computing model realities. This paper should demonstrate the issues with identity management when incorporating cloud applications into the enterprise and why we need to centralize employees' IDs across applications.

Table of Contents

The Shift to the Cloud in the Enterprise	3
The Proliferation of Passwords in the Enterprise	3
The Password Quandary	3
The Social Networking Phenomena and Passwords in the Enterprise	4
The “Easy Fix”	4
Password Strength	4
Enter Reality for the Enterprise: People Are Not Machines.	6
An Inexpensive and Intelligent Solution For The Cloud Computing Password Quandary.	6
How To Centralize ID Management When Incorporating the Cloud.	7
About the author:	7

The Shift to the Cloud in the Enterprise

A time not long ago, many companies were able to maintain strict security and policy standards, as they were largely “Microsoft shops” or “Novell Netware houses.” We had one password, it was strong and we were forced to change it often. Once authenticated at our workstations, we were let into an Intranet filled with applications at work from email to time reporting. It was standard practice for IT to have centralized control of all authentication and provisioning activities in the company. With centralized control, a company could enforce a logical set of security policies - for example the requirement of a strong password, changed monthly, perhaps with capital letters and random characters mixed in.

However, the era of Web services has arrived and new business applications are more apt to be delivered as a service (SaaS) over the Web. Popular press is increasingly referring to this shift as a “move to the Cloud.” Today, our CRM systems, supply chain management, human resource management or even expense reporting tools are all likely to be Cloud Apps, well outside of the direct control of our IT administrators who used to be able to centrally direct and control authentication and provisioning.

The Proliferation of Passwords in the Enterprise

Naturally, as the workday now consists of commanding applications both inside and outside the company firewall, this has driven a proliferation of userIDs and passwords, eliminating the ability for centralized IT management of a single, consistent security policy. In fact, a 2009 password survey conducted by The Osterman Research Group shows just how quaint the idea of having centralized Identity Management in companies really has become. The survey average showed 12.3 passwords¹ per employee including HR, email, CRM, procurement, expense reporting and other applications.

The Password Quandary

Chances are your banking PIN number matches your home alarm code or your Yahoo login password. Statistically, some of these passwords, if not all of them, will be related to your birthday or some other memorable code of numbers or letters like a pet’s name. Psychologically, when faced with three or more things to remember, we tend to create patterns from them in order to remember. This is how our brains work. We operate no differently in the workplace and with the increasing loss of centralized control of authentication, due to the growth in Cloud Applications in the workplace, there is no ability for the IT group to force unique and changing passwords.

The numbers bear out in a 2008 password survey in which only 18% of workers polled indicated that they use a unique password for each application.²

1 <http://www.ostermanresearch.com/whitepapers/download92.htm>

2 Results of Two End-User Surveys on Email, Attachment and Password Management Issues; An Osterman Research Survey Report Published June 2008

The Social Networking Phenomena and Passwords in the Enterprise

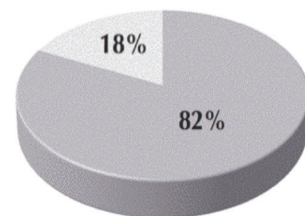
Many enterprises now face the triple threat of security management:

1. Loss of centralized password and security control due to Cloud Apps
2. The number of login and passwords balloons for employees
3. Employees use memorable passwords and reuse them

Would-be hackers use to rely solely on a combination of what is termed a “brute force hack” technique using dictionary hacking applications and social engineering whereby calling individuals close to the target would help reveal personal information used to derive passwords.

This process just got a lot easier with the proliferation of our personal information on social networks like Facebook and LinkedIn. Your employees’ information such as birthdays and other password hints sit ready to pluck without having to talk to anyone. There was no better documentation of the simplicity of this hack than the 2009 hack of Twitter, Inc’s corporate information.³

8. Do you ever use the same username/password combination for more than one application/system, or does each application/system have a unique username/password?



³ I sometimes use the same username/password combination for more than one application/system
⁴ Every username/password combination is unique

The “Easy Fix”

Some doomsayer’s position the security challenges above as a harbinger of disaster for Cloud Computing overall. But there is no question that the power of the Web and its ability to drive efficiency, mobility and savings for all of us is here to stay and grow in our personal and business lives. The value we provide as IT professionals is how we can help our companies embrace these new technologies without the compromises they may ordinarily bring. In this case, the password in the Cloud quandary is relatively easy to fix with a three-part approach:

1. Strengthen passwords for all business applications, Cloud or internal
2. Enforce centralized policy not only for strength, but frequency of change
3. Consider multi-factor authentication methods for added peace of mind

Password Strength

If the password is not an actual word from a standard dictionary or related to the individual’s personal information like a birthday, the complexity of the hack becomes exponentially greater if not impossible. One ethical hacker recently displayed the math in a blog post aptly named, “How I Would Hack Your Weak Passwords.”⁴ As is stated in the blog post, the most common password combinations look like this:

³ Twitter hack raises questions about ‘cloud computing’
<http://edition.cnn.com/2009/TECH/07/16/twitter.hack/>

⁴ <http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/>

1. Your partner, child, or pet’s name, possibly followed by a 0 or 1 (because they’re always making you use a number, aren’t they?)
2. The last 4 digits of your social security number
3. 123 or 1234 or 123456
4. “password”
5. Your city, or college, football team name
6. Date of birth – yours, your partner’s or your child’s
7. “god”
8. “letmein”
9. “money”
10. “love”

Using the brute force method where every possible character combination is randomly tried by a computer, you can see the advantages of a strong password mathematically:

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Netting it out, a minimum of eight characters with one being a capital letter and one being a non-letter character provides a brute-force shield tough to penetrate.

Enter Reality for the Enterprise: People Are Not Machines

So it's solved. All a company needs to do is to force its employees to change all 12.3 of their passwords to be unique eight-character sets with a capital letter and a symbol; all on a monthly basis. This is the crux of the matter. Humans find it impossible to operate this way and companies have lost the ability to centrally help them. Name one of your applications that do not simply build a "Forgot Your Password?" link right into the application. If a company is faced with using six Cloud-based applications, they are likely facing 3-6 different password standards, none of which match the internal policies of the subscribing company.

An Inexpensive and Intelligent Solution For The Cloud Computing Password Quandary

Thanks to the early embrace of the emerging security industry standards such as Security Assertion Markup Language (SAML), there are applications which can unify the management and authentication to applications both in the Cloud and internal to the company. This provides two immediate, tangible benefits to employees and the company alike:



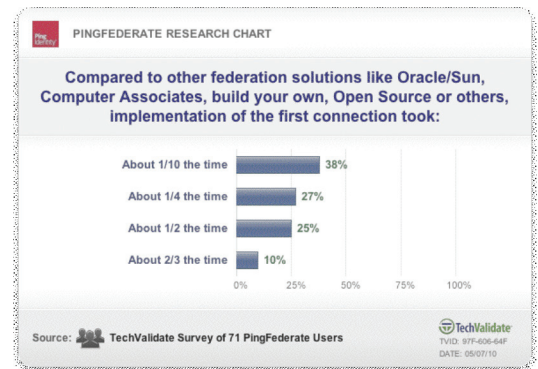
1. Employees can have ONE strong password for all business applications
 - a. Though it is strong and unique, it is one password instead of "12.3" passwords
2. IT can once again have centralized policy management and administration to most applications both in the Cloud and internally
 - a. IT can add value by masking the complexity of strong password management for users
 - b. Prevent the use of unsafe passwords

Indeed Federated Identity Management pays for itself almost immediately without even considering that it is making the enterprise safer. The Human Resources department can now efficiently prepare for a new employee's starting day or have much better assurance on an employee's last day by having one place to visit to immediately disable the employee from most if not all company applications internally and in the Cloud. Many companies report the ability to redeploy valuable IT management time to higher value activities once the password reset calls stop for the "12.3" passwords per employee. Finally, and perhaps most importantly, the employee base can spend more time working rather than logging in again and again interrupted only by a lost password and a call into the help desk for yet another password reset.

How To Centralize ID Management When Incorporating the Cloud

There are a few very large application companies that bundle federated identity management solutions in support of their broad suites. Examples of these companies include Oracle (and its recent acquisition of Sun Microsystems), CA, IBM, and Microsoft. Though these are options to be considered for some companies with largely homogenous application environments and light federation requirements, they tend to be very complicated and costly in their implementations. This is due to the fact that the vendors' first priority is protecting their software suites and then secondarily cross collaboration with other vendors through loose adherence with open standards. This is commonplace across many of the enterprise oligopoly technology spaces and no different here. Consistent reports indicate that vendors "give away the Federated SSO software for FREE" and yet the implementation takes six months and \$500K in services.

The fastest growing independent provider of Cloud Identity solutions to enterprises, government and service providers Worldwide is Ping Identity, headquartered in Denver Colorado in the United States. Ping Identity is implemented in 40 of the Fortune® 100 so far. This explosive growth is due, in part to the company's "no software or services agenda". It leads to implementation times of days or weeks resulting in total costs that are a fraction of the big application companies, even ironically, when they include the Federated SSO software for "Free". You can check out Ping Identity at www.pingidentity.com and take steps to make your company's embrace of the Cloud a safe and convenient one.



About the author:

Jonathan W. Buckley, founder of The Artesian Network, LLC, is an independent writer, marketing consultant and sometimes white-hat hacker. In 2000, Jonathan was a founding team member in an infrastructure monitoring and control company that elevated to the highest levels of the US government the real threats to critical infrastructure through simple hacks using phone lines into telephone and power companies' SCADA systems using poor password conventions. Some of these papers are still referenced today. Over 35 companies were interviewed for this paper.

About Ping Identity Corporation

Ping Identity is the market leader in Internet Identity Security, delivering on-premise software and on-demand services to hundreds of customers worldwide. For more information, dial U.S. toll-free **877.898.2905** or **+1.303.468.2882**, email sales@pingidentity.com or visit www.pingidentity.com.



© 2010 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, PingFederate Express, PingConnect, PingEnable, the Ping Identity logo, SignOn.com, Auto-Connect and Single Sign-On Summit are registered trademarks, trademarks or servicemarks of Ping Identity Corporation. All other product and service names mentioned are the trademarks of their respective companies.