Centrify
THE BREACH STOPS HERE™

WHITE PAPER

WHO MOVED MY SECURE PERIMETER?

Six risks and opportunities to strengthen security using Identity-as-a-Service

Contents

Introduction

Before cloud computing, Software-as-a-Service, smart phones, tablets, and wearable devices, there was the data center. It defined an organization's perimeter. People came into the office and worked on computers and laptops within the realm of the defined network. When they worked remotely, they connected to their networks using VPNs. IT established a secure perimeter around you and your organization's sensitive information, protecting you from the rest of the Internet using firewalls, security appliances, VPNs and more.

Now, your organization's sensitive information is everywhere. If you looked, you would find it on mobile devices, in the cloud and, of course, behind your firewall. So where is your secure perimeter?

Some applications are hosted on-premises, yet are accessible from outside the network using VPNs. Software-as-a-Service (SaaS) business apps are in the cloud, and your organization's sensitive information now resides in multiple cloud data centers, accessible by employees both on and off the corporate network. Many organizations are migrating some or all of their servers, databases and storage into Infrastructure-as-a-Service (IaaS), while newer ventures that are "born in the cloud" host no in-house infrastructure.

In today's mixed on-premises and cloud IT environment, securing one network perimeter is not enough. This paper examines six common risks of this "perimeterless" world, and proposes six opportunities to strengthen security using Identity-as-a-Service.

RISK #1:

Compromised credentials are the easiest and most common vectors of attack

According to the latest Verizon Data Breach Investigation Report (DBIR), 81% of breaches were due to compromised credentials.[1] Anyone who has followed the Verizon DBIR through its many iterations, the findings for 2017 should come as no surprise as they reiterate that credentials theft still remains as one of the leading top attack vectors. In addition, Centrify recently surveyed several hundred IT decision makers in the United States and United Kingdom, and found that fully one half of the organizations have suffered a security breach in the past. Nearly 60 percent of respondents in the US reported sharing access credentials with other employees at some time. 82 percent of the respondents who report granting access to contractors, say it would be somewhat easy for those contractors to gain access to the company's digital assets.[2]

Nearly **60%** of respondents in the U.S. reported sharing access credentials with other employees at some time

THE OPPORTUNITY:

Strengthen security with strong authentication

Verizon cites compromised user credentials as the "keys to the digital kingdom"

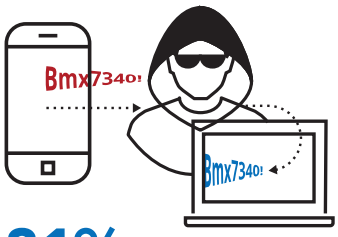
> "While we have tried to refrain from best practices advice this year, there's no getting around the fact that credentials are literally the keys to the digital kingdom. If possible, improve them with a second factor such as a hardware token or mobile app and monitor login activity with an eye out for unusual patterns."

Requiring multi-factor authentication (MFA) for specific applications or servers can add an additional layer of security. Many companies may have been able to prevent data breaches by applying two-factor authentication policy consistently across all of their servers.

Requiring multiple factors of authentication to prove who we are lets us create a more secure system. Combining a knowledge factor, such as a personal identification number, with a possession factor, such as an ATM card, we can withdraw cash from our bank accounts at the ATM machine. Often, we are forced to use clumsy knowledge factors like those annoying and sometimes easy to forget security questions ("Who was the lead singer in your favorite band when you were in high school?"), and additional possession factors, such as a hardware token that generates expiring one-time passcodes, to perform more complex transactions from a web browser or mobile device.

The trick is finding the right balance between good security, and irritating inconvenience. For most enterprise-grade cloud and on-premises applications, we can and should find ways to require multi-factor authentication that is minimally disruptive. An Identity-as-a-Service (IDaaS) solution with a well-integrated mobile application can let us use our registered mobile device to authenticate, without the worry of remembering to carry smart cards or tokens, or typing in one-time passcodes. Most people who own mobile devices tend to carry them everywhere, and like to use them. So why shouldn't they be able confirm or deny an authentication request by simply tapping on their mobile phone or smart watch? Even providing biometric evidence using a smartphone's built-in fingerprint scanner is a quick and easy task that adds more security.

But why are credentials so easy to compromise? Is this problem caused by its intended solution? Risk #2 explains more.



81% of web application attack incidents involve harvesting credentials stolen from customer devices, then logging into web applications with them

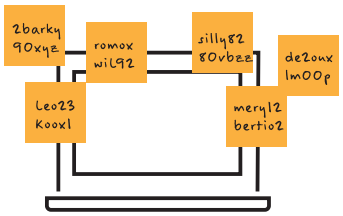
[1] http://www.verizonenterprise.com/DBIR/2017/

[2] http://www.centrify.com/about-us/news/press-releases/2015/centrify-survey-managing-identity-at-heart-of-protecting-data/

RISK #2:

Strong passwords make us weak. They are inefficient, hard to remember, and costly

Traditional IT best practices demand we enforce strong passwords: eight or more characters, upper and lower case letters, numerals and special characters. And we are somehow expected to create wholly unique passwords every time, remember these unique passwords, and never write them down.



40% of consumers surveyed in the US and UK create more than 50 account profiles a year

Many of us write our passwords down on paper, sticky notes, or store them in spreadsheets on our hard drives. We forget to encrypt the files. Then someone gains access to the credentials of a privileged account, hacks into our systems, and finds those spreadsheets full of passwords. That's what reportedly happened in the infamous 2014 Sony Pictures data breach. Hackers known as Guardians of Peace released spreadsheets of passwords onto the Internet for the 245 PC's, 811 windows servers, and 1,700 Unix/Linux machines they claimed to have hacked.[3]

Meanwhile, account profiles are spreading rapidly. 40 percent of the people Centrify surveyed[4] are creating more than 50 account profiles a year for various cloud services. One in four people are entering about 4,000 passwords a year. And one in three have been completely locked out of an account forever because of multiple attempts to login using a forgotten password. Small businesses with 500 employees lose $200,000 annually to employees struggling with remembering or taking time to reset passwords.

THE OPPORTUNITY:

End the vicious password cycle once and for all

1 in 3 people have been forever locked out of an account because of a forgotten password

We all need to use strong passwords, and change them regularly. At the same time, we shouldn't be expected to create and remember a different password for every application and service we use.

Tools like consumer password vaults offer more security by issuing temporary tokens or URLs to authenticate individual users' accounts to various websites and cloud services. However, when managing larger groups of users across multiple corporate applications, these individualized services fall short.

Enterprises can adopt IDaaS to provide end users with single sign-on to cloud and on-premises applications. Instead of requiring that we enter separate usernames and passwords for each account, an IDaaS service uses industry standards such as SAML, WS-Fed and OpenID Connect to establish trust to different websites or services by linking our electronic identity and attributes from a central identity store like Active Directory. IDaaS can also simplify how IT provisions accounts for new employees, and de-provisions them when they leave the organization. Which brings us to the next risk.

[3] http://fusion.net/story/31338/hackers-claim-to-have-compromised-thousands-of-sony-pictures-computers/

[4] http://www.centrify.com/downloads/public/Centrify-Password-Survey-Summary.pdf

How Are Compromised Credentials Used?

When we reuse the same or similar username and/or password for our work and personal accounts, our identities become easy to hack. Password cracking tools can leverage botnets to automate their work. Hackers correctly assume that people tend to use the same usernames and passwords across other services. They dump harvested credentials (hashed or clear text) onto public sharing sites. They can sell thousands of these reused or overused credentials to those people who want to launch brute force attacks on other systems. Often, detecting a breach happens long after the damage has been done.

One such example is healthcare — a $3 trillion market where computer systems are often out of date and lack sufficient security.[9] Stolen health credentials can be sold for 10 to 20 times the price of a stolen credit card number. While a stolen credit card number can be detected and canceled quickly, healthcare records can be compromised months or years before their impact becomes known. The rise in electronic health records and patient portals that are protected by only username and password, have made healthcare an easy target for identity theft and Medicare fraud. Compromised credentials of just one system administrator can result in millions of patient records being accessed.[10] Patient names, social security numbers, birth dates, policy numbers, diagnostic codes, and billing information can be used to fraudulently bill for medical services, equipment, or drugs that can be resold.

RISK #3:

Departing employees retain IT access for a week or more

In a recent Centrify survey, we learned that half of the IT decision makers surveyed in the US and UK admit that it would be somewhat easy for a former employee to access systems or data using their old passwords. 82 percent in the US said it might take a week or more to completely remove a former employee's access to sensitive systems, representing a tremendous security and compliance risk to the organization.

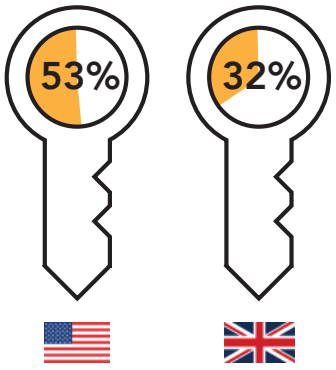
Many of the sensitive systems we use — CRM, finance, file sharing to name a few — are now externalized into Software-as a-Service (SaaS) accounts in the cloud. User account information is stored in each of these services. Absent any unifying identity management system, IT would have to disable a former employee's accounts in each of these SaaS systems, one at a time.

"I always feel that I have two duties to perform with a parting guest: one, to see that he doesn't forget anything that is his; the other, to see that he doesn't take anything that is mine." — Alfred North Whitehead

THE OPPORTUNITY:

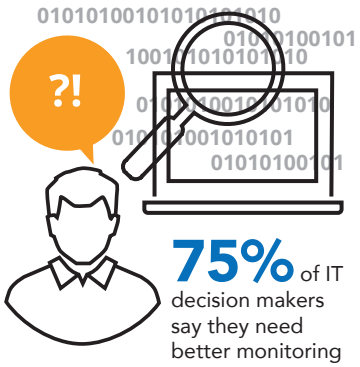
When they leave, make it a clean break

Using an IDaaS solution, we can disable a departed employee's access to all the services at once. It's just as simple as removing that person from the organization's directory service. An IDaaS solution that enables IT to provision new user accounts — by creating a new user and managing them with group policy in Active Directory, LDAP or cloud directories — also makes it easy for IT to de-provision — or revoke — user accounts, automatically deactivating their access to cloud or on-premises applications. This means less work for IT, and more security for the organization.



53% of IT decision makers in the US say it would be at least somewhat easy for a former employee to log-in to access systems or data with old passwords, as do **32%** in the UK.

[9] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
[10] https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack



75% of IT decision makers say they need better monitoring of who is accessing data, where it is going

70% to **80%** of users are storing files on cloud file sharing sites like Box, DropBox, and Google Drive

RISK #4:

Employees resort to SaaS apps and cloud file sharing to meet business needs

Also in our survey, we learned that three-quarters of respondents in the US and more than half in the UK admit that they need to better monitor who is accessing their data. One main concern is the rise of SaaS applications that are being adopted by lines of business, outside of the control of IT. Cloud-based file sharing applications like Box, Dropbox, and Google Drive top the list of most commonly used, and most easily abused Shadow IT applications. Files containing sensitive information are stored in the cloud, and are potentially accessible by anyone.

THE OPPORTUNITY:

Provide secure access to all the SaaS apps they need

If we wish to maintain visibility and control over our sensitive data, we must make it easy for employees to collaborate and store files, and provide a comprehensive solution to manage identity and access to authorized file sharing services and other SaaS applications.

With IDaaS, we can deploy enterprise accounts for SaaS file sharing apps, through a simple user interface. Users simply click on an app tile to get access without entering in a username and password. The file-sharing app redirects the login request back through the IDaaS solution, to verify with that the user is a trusted member of their organization.

We can combine IDaaS application access policy with Cloud Access Security Broker (CASB) solutions to examine the types of files being stored on these sites, and track who is using unauthorized file sharing sites, and what types of sensitive data is being leaked. By driving the authentication process through an IDaaS solution, CASBs utilize the necessary information about users, their devices and their location to effectively manage access to and monitor user activity within cloud apps.

And remember from Opportunity #3: using IDaaS, when an employee leaves, we can automatically deactivate and remove their ability to access these accounts to reduce the possibility of additional exposure.

RISK #5:

Remote access to on-premises resources exposes other parts of the network

Enterprises have traditionally relied on virtual private networks (VPNs) to provide employees with remote access to internal resources — servers, applications, and devices — that sit behind the corporate firewall.

Using VPNs, we can interconnect users together through encrypted "tunnels" over the Internet, enabling employees to connect to their organization's network no matter where in the world they may be. VPN connections working at the network layer are good for connecting branch offices to the main office, but risk exposing more of the network than is necessary.

VPNs also limit the types of users that can access the network. Suppliers, vendors, partners, and even certain remote workers may not be permitted to access certain internal applications they need — because it's too risky to allow full network access to these external users. VPNs require investment in dedicated concentrators that have a limited number of physical ports, and require ongoing maintenance and support contracts. VPNs can also create hassle for end users, especially when they time out or stop working altogether.

VPNs are traditionally used for remote access to internal apps

VPNs risk exposing more of the network than is necessary

THE OPPORTUNITY:

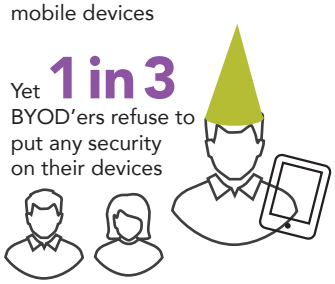
Invite remote access, but only for specific applications

Look for an IDaaS service that enables remote access to internal web applications without the hassle or risk of a VPN. Ideally, IT should be able set up end users with single sign-on access to specific on-premises applications, without requiring changes to firewall policies or an end user to initiate a VPN session. End users should be able to click on an on-premises app tile from the same user portal, using single sign-on trust.

Half of all workers use personal laptops and mobile devices for business purposes

Your corporate data can be accessed from unsecured mobile devices

Yet **1 in 3** BYOD'ers refuse to put any security on their devices



RISK #6:

Mobile and BYOD are new attack vectors

Nearly every organization has seen an increase in the use of personal laptops and mobile devices connecting to corporate networks in the past two years.

Half of all desk workers Centrify surveyed use their personal devices (bring-your-own-device or "BYOD") for business purposes.[11] Yet one in three refuse to put any security mechanism, such as a passcode or fingerprint, on those devices.

IT needs to be able to see and manage all personal devices on the network that are accessing internal resources or data. And IT should have policies in place to detect and remove any rooted or jail-broken mobile devices from the internal network, and manage updates for any apps that are used for business purposes. Device owners also need to be able to locate, lock and wipe their devices if they become lost or stolen.

When an employee using their own laptop or mobile device leaves the organization, IT should be able to remove access only to those applications under management, while leaving personal applications and data alone.

THE OPPORTUNITY:

Protect data by tying mobile and BYOD to identity, and multi-factor authentication

An ideal IDaaS solution can protect sensitive corporate data by defining the parameters by which any cloud or on-premises application or network resource can be accessed.

While mobile device management (MDM) solutions can help bring mobile devices under centralized management, they don't actually protect the device, or the network from malware or other malicious attacks. But we can minimize the attack surface by tying all endpoints to user identity.

An IDaaS solution that integrates mobile devices and MFA can add security to sensitive applications, like CRM or accounting. Using an IDaaS service, IT can create policies that restrict access to certain applications based on time of day, IP address range, or device location, leveraging an employee's managed mobile device for stronger authentication.

For example: a sales manager is working at headquarters between 8am and 5pm can access Salesforce data from her laptop, tablet or smart phone. If she is away from the office, in a different country, using a different (unregistered) device, or simply working late into the evening, she will be sent an MFA request to her registered smartphone or smart watch. Once she has tapped the "approve" button, the IDaaS service automatically gives her access to the applications she needs.

[11] http://www.centrify.com/downloads/public/Centrify-Password-Survey-Summary.pdf

Summary: Securing the perimeter with Identity-as-a-Service

The traditional data center no longer defines the secure perimeter. Whether we like it or not, most organizations have sensitive information stored both behind their firewalls and in the cloud. This trend will continue. We are accessing information from any location, any network, and from any device. Because our secure perimeter has moved beyond the data center, we must create the secure perimeter around our users, and their devices.

An IDaaS solution can help us implement least privilege access to applications, infrastructure, and services based on user identity. Centrify Application and Endpoint Services provides that solution.

Centrify Application and Endpoint Services provides is an IDaaS solution that secures access to cloud, mobile, and on-premises applications using single sign-on, user provisioning and de-provisioning. Centrify Identity Service is recognized as the leader in securing modern enterprises against cyberthreats that exploit employee identities, strengthening the security of your applications.

Start a free, full-featured 30-day trial of Centrify today.

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 100, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit www.centrify.com. The Breach Stops Here.

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com

WHP001882en-08262017