Centrify
THE BREACH STOPS HERE

SOLUTION BRIEF

The Top 5 Application Security Risks

Are your cloud, mobile, and on-premises apps giving attackers a foothold in your business?

Applications — and the sensitive data within them — are everywhere today. Cloud apps have quickly made their way into the enterprise, but traditional on-premises apps are still critical to many businesses as well. In both cases, access is the primary concern for users, and often for IT. But often making apps available to onsite, remote, and mobile employees can introduce security risks.

1 All Cloud Apps Have the Same Flaw

Cloud applications have made their way into the enterprise thanks primarily to ease of use, and speed to value. Additionally, the security aspects of cloud apps can also be compelling. Typically, app vendors provide hardened cloud infrastructure to protect against breach, a commitment to multi-tenancy to ensure data privacy, and fully encrypted communications to thwart snooping or passing data in clear text over the Internet.

Each of these are critical to ensure that app data is protected against loss or theft — but none of them address the single biggest security risk inherent to all cloud applications: User Authentication.

Nearly every cloud application, by default, relies on a simple username and password for authentication and access. That means that even the strongest backend, and the most sophisticated encryption keys, are all moot if an attacker simply steals the username and password for an account.

The 2017 Verizon Data Breach Investigation Report states that 81% of hacking-related leveraged stolen usernames and passwords. Attackers have learned that simply brute forcing a password, or using one of the billions of exploited passwords available for purchase, is much easier than attempting to actually break through cloud app defenses. With so many passwords having been compromised, and no way to differentiate between legitimate users, and attackers who are simply using legitimate accounts, Enterprise IT needs to implement another layer of security for cloud application authentication.

2 The Fallacy of VPN

The rise of cloud applications and modern mobile devices mean that employees expect access to their business applications from anywhere, at any time. Cloud app vendors make this paradigm easy for employees with both browser-based access, as well as simple mobile apps available in all the popular app stores. Providing the same level of access for on-premises apps isn't so simple.

Providing mobile or remote access to on-premises apps has traditionally meant one of two things: Hosting some kind of web application front-end in your DMZ, and/or extending VPN access to remote employees and mobile devices.

VPN seems like a safe choice. The traffic is fully encrypted against snooping, and IT retains some level of control over both the devices that get access, and the concentrator configuration. However, equating VPN with "Secure access" is a fallacy.

Often VPNs provide more access than is really necessary — certainly in the case of IP-sec VPN, remote machines can easily receive full L3 network access, when really the end users only needs access to one or two applications — not the entire network infrastructure. This makes VPNs juicy targets for attackers, as they can provide a path straight through firewalls and into the heart of business networks.

3 Mobile Apps Mean Data is on the Move

The smartphone, has revolutionized the way consumers and employees interface with applications. Dedicated apps, available free from app stores, mean that users can be productive on the go — and often help to drive business agility and responsiveness.

While employees have the best intentions for mobile productivity, downloading and using apps on personal devices opens a large security hole, namely, cached credentials within apps mean that anyone who picks up a user's phone can get immediate access to all the apps and data on that device. In a recent survey, Centrify found that nearly two thirds of people don't protect access to their phones with even a simple PIN, yet

© 2017 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

the vast majority of people are willing to use those devices for business. This disconnect between productivity and security means lost or stolen devices are a direct path to private business data — and by default IT has no visibility or control of this attack vector.

With app data so easily spread across smartphones, Macs, and other personal devices, businesses have got to find ways to keep mobile data from moving outside of IT control.

4 Line of Business and Shadow IT

Another example of good intentions gone bad, is Line of Business (LOB) application adoption. In the past, if marketing, sales, development or any other business unit needed an application to facilitate their jobs, or to drive business, they had to work closely with IT to build or buy the correct application, and then deploy and maintain it.

Today, LOB leaders who want to drive productivity can simply look to the cloud for solutions. Apps like Salesforce, Marketo, Concur, Box, DropBox, Zoom, and many more are bought and deployed without IT's consideration or approval — meaning that they often are not evaluated for security risks.

While these apps, and many others, have been architected to be safe against attack, they still require user setup, which is often not tied to any master directory and is outside of IT control. User database maintenance is no small challenge, even for a small team, and often is overlooked by LOB — which leads to users to have too much access within a given app, and often means that user access is never terminated. Stories of contractors retaining Salesforce access years after their contracts expire, or former employees still being able to access time and expense approval apps are rampant today.

While the apps themselves may be safe, stale or over-privileged accounts provide attackers easy targets that can lead directly to some of the most sensitive data within a business — all outside IT's secure perimeter, and outside of IT control.

5 Passwords are Poor Security

Passwords are poor security — that's covered above. But compounding the risk is the fact that a single password is often re-used across multiple apps.

Users have countless passwords to remember, some used daily, others that might be only used once or twice a year. Trying to remember a unique password for each of a dozen or more applications is simply unreasonable for most folks, so they don't. Instead they reuse the same password across various sites apps and services.

Combine this reality with the fact that in most cases, the password is something like "123456" or "password" and it's easy to see just how backwards password-based "security" really is.

Many applications can be configured to trust an Identity Provider for authentication, which removes the passwords from those apps completely — easing user access, and eliminating any passwords that could be stolen by attackers. This is single sign-on, and it's good for both users and IT, but only if combined with a second factor of verification that isn't just another password.

Secure and Productive: An App Impossibility?

Businesses can't wait for all app vendors to standardize on SAML or other standards that eliminate passwords. VPN access can't be eliminated overnight, and the sprawl of mobile devices is going to continue.

That's why businesses need to look for solutions that integrate mobile security, secure remote access, single sign on, and multi-factor authentication. With each of these covered, IT can provide anywhere, anytime access from secured devices, mitigate password risk, and bolster security with MFA — for on-premises apps, cloud apps, and VPN.

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 50, 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.

Centrify is a registered trademark and The Breach Stops Here and Next Dimension Security is a trademark of Centrify Corporation in the United States and other countries. Other trademarks mentioned herein are the property of their respective owners.

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

BRF003739EN-09112017