CENTRIFY WHITE PAPER

Stop Password Sprawl with SaaS Single Sign-On via Active Directory

Abstract

Organizations are rushing to SaaS in an effort to move business initiatives along faster than the traditional cycle of implementation, integration and on-going maintenance associated with on-premise applications. But, executives and IT managers are realizing that SaaS adoption is part of a larger set of trends where mobile devices and resident mobile applications are playing a key role (driven in large part by the bring-your-own device upsurge of iOS and Android devices in corporations) and IT managers understand that their deployment environment remains a mix of business critical on-premise and SaaS applications. And lost in the rush to adopt SaaS applications is the cost and complexity of managing an additional identity silo for each new application including integration costs, increased help desk load and lower productivity as users struggle with multiple passwords, password policies and frustrating login interfaces for browsers and client applications on mobile devices.

Centrify integrates essential identity services including authentication, access control, privilege management, policy enforcement and audit with software and cloud services that unify user login and identity management across data center, cloud and mobile applications. This unified identity architecture results in one login for users and one unified identity infrastructure for IT. Using Centrify DirectControl for SaaS organizations can address password sprawl with single sign-on — and zero sign-on for mobile apps — while also centralizing control over an ever-increasing numbers of SaaS applications. Users get single sign-on and self-service features that let them locate, lock or wipe their mobile devices and also reset their Active Directory passwords. IT gets an easy-to-deploy, cloud-based service for access control and visibility to SaaS application usage which seamlessly integrates into Microsoft Active Directory.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2004-2013 Centrify Corporation. All rights reserved. WP-027-2012-12-01

Centrify, DirectControl and DirectAudit are registered trademarks and Centrify Suite, DirectAuthorize, DirectSecure and DirectManage are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction 4
Challenges to Adopting SaaS Applications 4
Hidden Costs of SaaS 5
Key Capabilities to Consider 5
Centrify's Unified Identity Services 6
Centrify DirectControl for SaaS 7
How DirectControl for SaaS Works 7
Centrify DirectControl for SaaS Benefits 12
Conclusion 13
Additional resources 13
About Centrify 14

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Introduction

Today, enterprises of all sizes are adopting Software-as-a-Service (SaaS) applications at an accelerated pace, and not just for customer relationship management but in every application category traditionally deployed as software including personal productivity, project planning and communication, supply chain and business intelligence. In fact, Gartner estimates combined spending on SaaS applications will grow 15.8% per year and will experience healthy growth through 2015 when worldwide revenue is projected to reach $22.1 billion. And this year Forrester estimated that organizations that have embraced cloud-based application deployment models are already using 10 or more SaaS applications.

Organizations are rushing to SaaS in an effort to move business initiatives along faster than the traditional cycle of implementation, integration and on-going maintenance associated with on-premise applications. And IT organizations and business lines alike hope to leverage SaaS in a cost constrained environment to shift from a capital to operational expense model.

But, executives and IT managers are realizing that SaaS adoption is part of a larger set of trends where mobile devices and resident mobile applications are playing a key role (driven in large part by the bring-your-own device upsurge of iOS and Android devices in corporations) and IT managers understand that their deployment environment remains a mix of business critical on-premise and SaaS applications. These larger trends mean that cost savings from SaaS may be less certain than organizations expect and the rush to adopt SaaS applications comes with risks that are often only considered after these applications are in use. Central to the costs and challenges associated with SaaS are how identities should be managed and control established so IT organizations can ensure security and compliance.

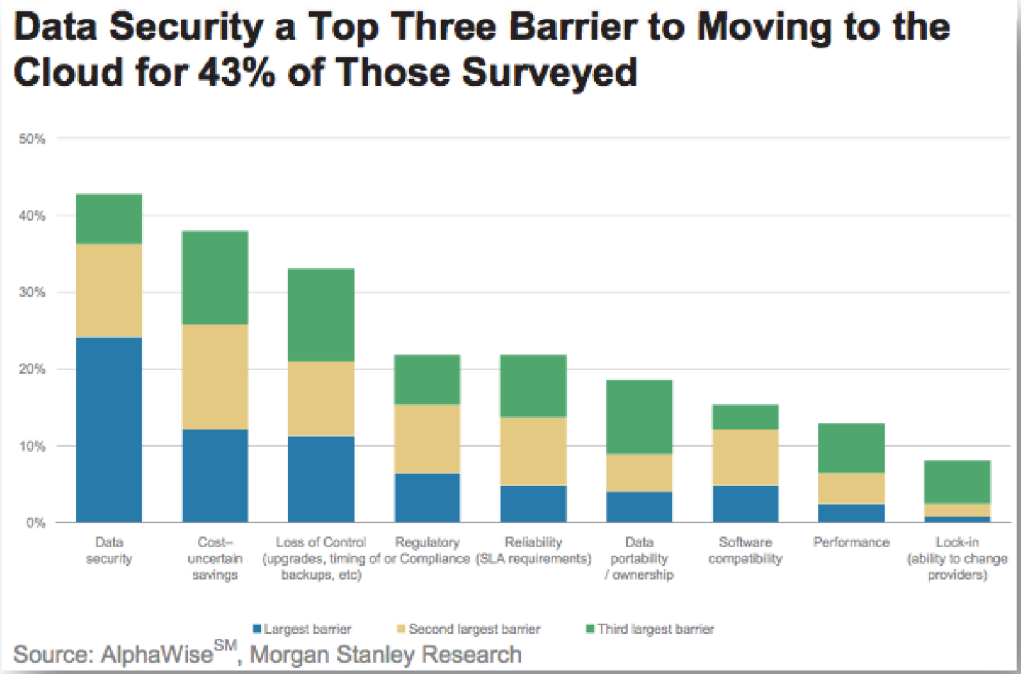
Challenges to Adopting SaaS Applications

Clearly, IT organizations should be concerned about the relative ease with which non-IT departments can purchase and activate SaaS applications without considering the security implications of adding an additional identity store and giving users another credential to remember. The explosion in passwords for business and IT staff has lead to users writing down credentials on sticky notes or keeping catalogs of usernames and passwords in unencrypted files. And when SaaS application rollouts are rushed critical controls for approving employee access are often overlooked resulting higher costs and dissatisfaction among users.

Besides SaaS security issues the implications for visibility and accountability demanded by corporate governance and regulation are just as challenging. IT organizations need to report on who has access to specific applications and track what users are doing with their access rights in order to demonstrate compliance to auditors. Without visibility and control over who is accessing the myriad of SaaS applications enterprises can’t enforce least access security and eliminate orphan accounts, two common requirements in compliance standards. This is especially important when IT needs to shutoff access of departing staff quickly and with the certainty that no access remains. Manual processes for de-provisioning users across applications are error prone and leave organizations at risk of a data breach resulting in costly remediation efforts and fines from regulators.

All these issues can erode the cost savings and return on investment that organizations expect to achieve when moving to SaaS. In fact, one global survey found that uncertainty about costs and return on investment (ROI) rank second only to data security as a barrier for organizations considering the move to the cloud. Central to all these “hidden” costs of SaaS is identity management.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.



Data security, cost-uncertain savings and loss of control rank highest among the barriers organizations cite when looking to move their applications to the cloud.

Hidden Costs of SaaS

Lost in the rush to adopt SaaS applications is the cost and complexity of managing an additional identity silo for each new application including integration costs, increased help desk load and lower productivity as users struggle with multiple passwords, password policies and frustrating login interfaces for browsers and client applications on mobile devices. Organizations will also experience increased costs to acquire new skillsets and train staff on multiple administration consoles and tools. And as the number of SaaS applications increase manual procedures for on-boarding and off-boarding users becomes labor intensive and error prone. All these costs can't be addressed without consistent control of identities across SaaS applications and user productivity will suffer without single sign-on. Plainly, to realize the cost savings and return on investment promised by SaaS requires a unified architecture for identity management and single sign-on for SaaS, on-premise and mobile applications access.

Key Capabilities to Consider

Most SaaS single sign-on vendors provide a basic capability to present a list of SaaS applications that users can login to without having to use individual usernames and passwords. But these SaaS vendors force IT organizations to install additional infrastructure, learn new processes and make intrusive changes to their IT environment just to deploy this rudimentary level of single sign-on. And customers are finding that this minimal SaaS single sign-on capability comes at a cost premium but only solves a fraction of the organizations single sign-on needs while completely ignoring the related issues of identity lifecycle management, mobile device security and mobile app authentication.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Before organizations go to the time and expense of deploying single-purpose SaaS single sign-on there are key capabilities that should be considered:

- Does the vendor require that identity data get duplicated or synchronized to the cloud — removing it from the control of the enterprise?
- Can the vendor provide control and single sign-on for both browser-based and resident mobile applications on smart phones and tablets?
- Can the vendor support SSO for web-based and other packaged apps such as SAP deployed on premise?
- Does the product support a non-intrusive deployment model that does not require any additional infrastructure, problematic firewall configurations and appliances in the DMZ?
- Does the vendor seamlessly integrate with Active Directory so the organization can fully leverage their existing infrastructure, skillsets and processes for complete identity lifecycle management?

Centrify's Unified Identity Services

IT organizations require visibility and control consistent with security best practices and users demand ease-of-use and self-service to their applications regardless where they reside and transparent to the devices they prefer. Centrify integrates essential identity services including authentication, access control, privilege management, policy enforcement and audit with software and cloud services that unify user login and identity management across data center, cloud and mobile applications.

One login for users

Centrify's unified identity services approach decreases the cost of rolling out and managing SaaS applications while at the same time improving user adoption, satisfaction and productivity. Users have one credential and a unified view of all their applications via a browser, smart phone or tablet app. Centrify makes it easy for users to have one-click access to these applications and perform password resets and locate, lock or wipe a missing mobile device. And whether using native or browser based applications on their mobile device users further benefit from secure Zero Sign-On (ZSO), greatly enhancing productivity on devices where typing a username and password is cumbersome.

One unified infrastructure for IT

Centrify understands the pressure on IT organizations to optimize costs while enforcing controls and demonstrating compliance. With Centrify's unified identity services approach IT operations and security staff don't have sacrifice control and visibility as users bring their own mobile devices into the workplace and business managers move ahead with SaaS application procurement. Centrify's Active Directory-centric architecture keeps identity data secure within the enterprise while giving administrators an efficient and flexible role-based control of application access using familiar tools for user, group and device management. Users get the access they need based on their roles and group membership and IT has one place to off-board departing staff (on-premise, SaaS and mobile). For SaaS applications this is critical since single-purpose approaches require use of multiple consoles and redundant infrastructures to achieve the same result.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Unified identity services business advantages

Centrify's cloud-based approach for unifying identity management of SaaS applications also has significant costs advantages for the business. The Centrify Cloud Service lets enterprises leverage their existing Active Directory investment to secure SaaS applications permitting organizations to transition to an operational expense model without making new capital investments for security and control. This Active Directory-centric architecture means user profile management, self-service and reporting is all centralized; lowering identity lifecycle management, help desk and compliance costs.

Centrify DirectControl for SaaS

Centrify DirectControl for SaaS addresses password sprawl with single sign-on — and zero sign-on for mobile apps — while also giving enterprises centralized control over access to ever-increasing numbers of SaaS applications. Users appreciate the single sign-on and self-service features that let them locate, lock or wipe their mobile devices and also reset their Active Directory passwords. IT gets an easy-to-deploy, cloud-based service for access control and visibility to SaaS application usage which easily integrates to Microsoft Active Directory.

How DirectControl for SaaS Works

Centrify takes a unique approach to SaaS security and single sign-on by enabling you to use Active Directory to centrally manage authentication and access policies to control SaaS applications.

SaaS applications are displayed to users in the MyCentrify portal based on users' identity and roles within Active Directory. So, for example, the sales organization only sees sales apps, and the finance organization only sees finance apps. Centralized role-based access control for SaaS applications benefits your enterprise by ensuring that there is quick, convenient access to the applications needed to perform work while you retain control over which applications users get access to and visibility over how applications are used.

In addition, the MyCentrify portal provides users with self-service capabilities to manage their devices and their Active Directory profile, lowering your helpdesk burden to end-users through a more cost-effective "self-support" approach.

Focus: Support for authentication methods and SSO standards in use today
Organizations need to enable SaaS SSO whether or not standards are supported. Centrify DirectControl for SaaS supports authentication methods and options to facilitate SSO including:

Username and password: Centrify automates sign-on with basic username and password to any web-based application. Users can add apps that an administrator has approved onto their MyApps menu and the credentials are securely vaulted in the Centrify Cloud Service.

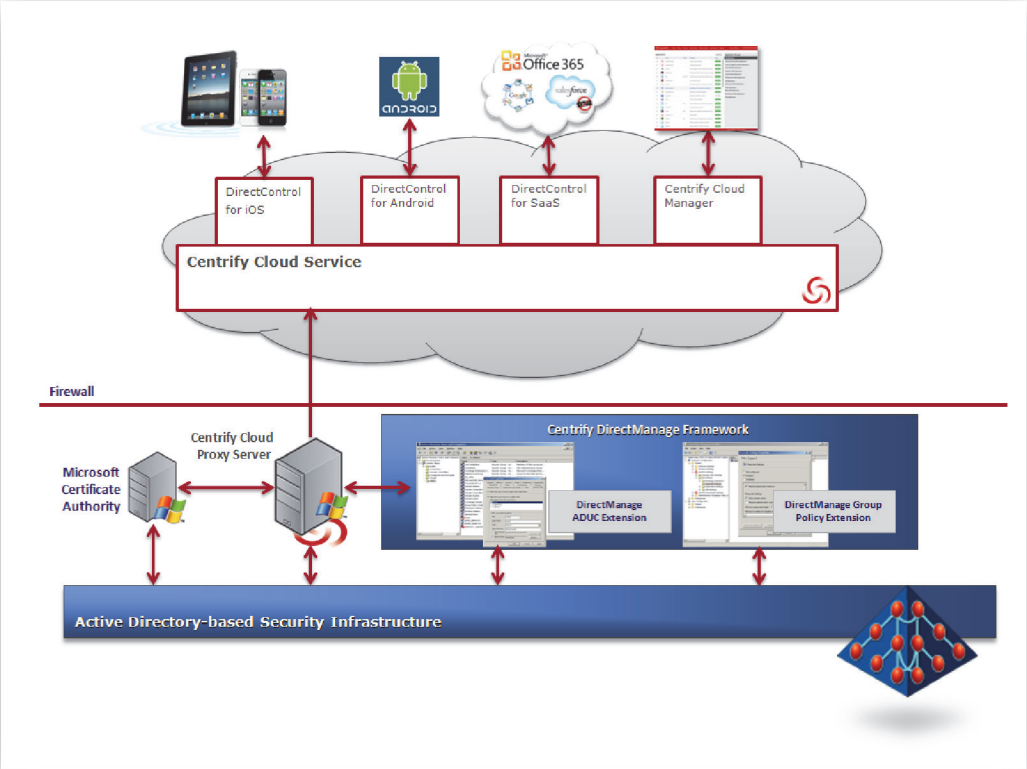
SAML: Centrify supports all the identity provider and service provider initiated SAML SSO options allowing administrators to easily setup SSO for any option a specific SaaS provider has implemented.

Silent Authentication: Centrify allows administrators to configure Windows integrated authentication for Internet Explorer, Firefox and Google Chrome browsers allowing silent authentication into the Centrify portal after signing on to the Windows desktop.

Bookmarks: For authentication while on the corporate network Centrify supports a bookmark app that allows users to click on a bookmark for an application and access that application directly without typing a username and password.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Architecture and components



Centrify's cloud-based services makes DirectControl for SaaS easy to deploy, with no need for additional management silos or intrusive firewall reconfigurations.

Centrify DirectControl for SaaS is a complete SaaS security and single sign-on solution delivered via the Centrify Cloud Service and supporting hundreds of SaaS applications and providing zero sign-on for mobile applications.

Centrify DirectControl for SaaS includes the following components:

The ***MyCentrify*** portal is an Active Directory-integrated and cloud-delivered user portal with the following user-facing services:

- ***MyApps*** delivers one-click access to hundreds of SaaS apps, decreasing the cost of rolling out and managing SaaS applications while at the same time improving user adoption, satisfaction and productivity. Centrify supports of 100s of popular SaaS apps including Google Apps, Salesforce.com, WebEx, Marketo, Zendesk and NetSuite.

- ***MyDevices*** delivers user self-service for all of their mobile devices, including info on location and status and actions such as passcode reset, device lock and remote wipe. Users feel safer and helpdesks can spread the burden to end-users through "self-support".

- ***MyProfile*** allows users to view all and edit select Active Directory account attributes, see where they fit in the organization and even reset their password or unlock their Active

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Directory account all while improving the accuracy and value of your directory infrastructure.

- ***MyActivity*** provides activity reports detailing personal activity for the purpose of self-spotting suspicious activities.

The MyCentrify portal lets users log in once and then point, click and launch the SaaS applications they are authorized to use without having to remember their username and password for each app.

Centrify Mobile Manager App provides mobile app management for any custom or third-party resident app while giving users Zero Sign-On to SaaS applications. Zero Sign-On for resident mobile apps is supported via Centrify's Mobile Authentication Service SDK. In addition, the Mobile Manager App provides self-service enrollment to the Centrify Cloud Service.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The Centrify Mobile Manager App gives users one-tap, Zero Sign-On access to SaaS applications eliminating the need to struggle with typing usernames and passwords on smart phones and tablets.

The ***Centrify Cloud Service*** is a multi-tenanted cloud service that provides secure communication from your on-premise Active Directory to your SaaS applications accessed from the MyCentrify user portal. The Centrify Cloud Service facilitates secure single sign-on and controls access to your SaaS applications by acting as a security token service, which can authenticate users to the user portal with Kerberos, SAML or an Active Directory username/password; then logs the user into their SaaS application through a one-click selection from a list of permitted SaaS applications. The Centrify Cloud Service also enables mobile zero sign-on for browser and resident mobile apps through a secure certificate delivered to the mobile device during device enrollment. Additionally, the Centrify Cloud Service enables user self-service for mobile device and Active Directory profiles while auditing all management and user activities.

Centrify Cloud Manager is a single pane of glass to administer SaaS application access and SSO, mobile devices, user profile management and to centrally report and monitor all SaaS and mobile activity. Not only does this improve security and compliance in your organization through improved visibility, but also reduces administrative complexity by reducing the number of point solutions with different monitoring and reporting interfaces or integrations.

The rich management and reporting services of the Centrify Cloud Manager include:

- **Dashboard**
  - At-a-glance overview for health and status
  - Live stream of current activity for spotting suspicious activity

- **User Management**
  - Role based access control to centrally managed applications

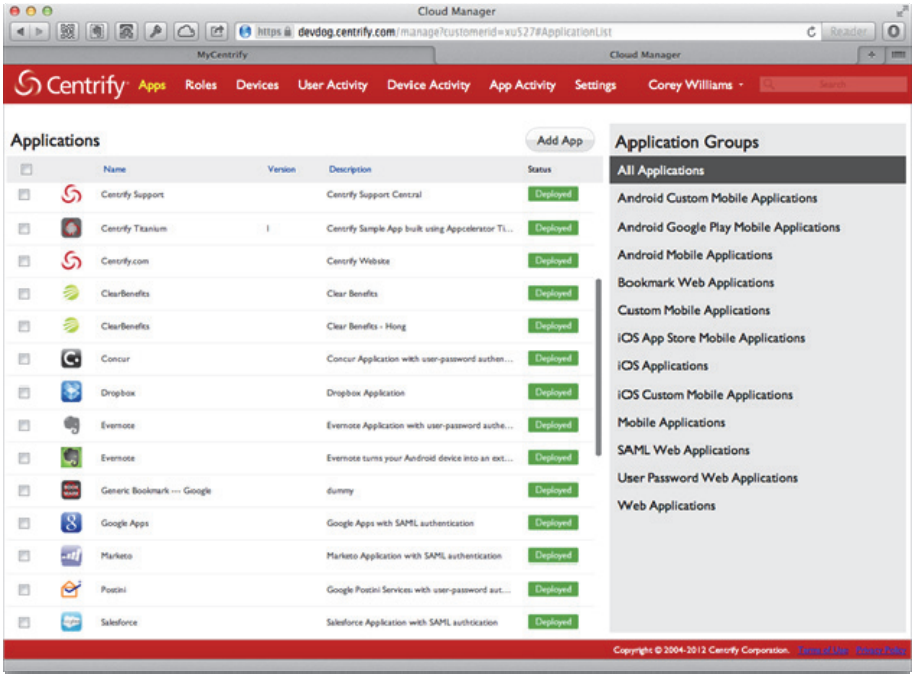
© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

- Basic Active Directory account management (e.g. lock, disable, update)

- **App Management**
  - Centrally manage app integration and access
  - Define and manage user access roles and rights

- **Cloud Management Settings**
  - Centrally configure security and access policies
  - Configure and manage cloud proxy services

- **Reports**
  - Access reporting including scheduled reports
  - Analysis reporting (e.g. top users, orphaned/unused access)



DirectControl for SaaS allows IT organization to regain control and visibility over the ever-increasing numbers of SaaS applications adopted across the enterprise through centralized role-based access controls and application access logging and reporting.

Centrify Cloud Proxy seamlessly leverages and extends your Active Directory investment to SaaS and mobile devices via the Centrify Cloud Services. A simple Windows service that runs behind your firewall provides real-time authentication, policy and access to user profiles without synchronizing data to the cloud. You keep control of your valuable Active Directory data while extending a common-sense identity services to your users for cloud and mobile.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Centrify DirectControl for SaaS Benefits

Centrify DirectControl for SaaS makes users happy

Centrify puts smiles on users' faces by providing a single destination to get one-click access to all of their SaaS applications. This greatly reduces the frustration of having to deal with password sprawl, thereby significantly enhancing user adoption, satisfaction and productivity. And Centrify gives users secure mobile zero sign-on for easy access to their applications from smart phones and tablets.

Centrify DirectControl for SaaS makes IT even happier

DirectControl for SaaS centrally authenticates users with their Active Directory identity which gives IT valuable insight into which applications are actually used and when — restoring visibility and control. In addition, DirectControl for SaaS further benefits IT through:

> ***Reduced compliance costs***: Frees up expensive IT resources with easy and thorough reporting on who in the organization has access to which SaaS applications and what they did with their access. Quickly demonstrate compliance with regulations and industry best practices.
>
> ***Reduced helpdesk costs***: Centrify DirectControl for SaaS returns value in improved productivity and as much as a 95% reduction in SaaS account and password reset calls.
>
> ***Lower identity lifecycle costs***: By tightly integrating SaaS applications with Active Directory the delivery of SaaS single sign-on and security is more cost efficient because IT uses technology, skillsets and processes already in place.
>
> ***Improved security***: IT can remove users' access to all SaaS applications by simply disabling their Active Directory account, which is already a common practice at the time an employee leaves the company. And unlike other solutions, it does not duplicate your existing identity data into the cloud and out of your control — it remains secure inside Active Directory.

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Conclusion

Why Centrify for SaaS?

Centrify's unique, easy-to-deploy, cloud-based architecture ensures your on-premise Active Directory infrastructure can be securely leveraged to quickly bring SaaS applications into line with security best practice and compliance. In addition, Centrify offers important advantages for organizations when compared to other approaches including:

- Broad support for hundreds of SaaS applications, on-premise applications and mobile apps
- Rich capabilities for mobile environments including an app catalog with support for resident mobile apps, browser based access to SaaS applications and Moblile SDK for ISV and in-house developers to add AD authentication to custom apps
- Super easy-to-use MyCentrify portal for single-click access to apps and self-service for mobile device and AD account management
- An unified architecture for security and single sign-on – not just another point solution — with support for 400+ systems and mobile devices and on-premise apps
- Unparalleled integration with Active Directory means no replication of identities in the cloud — the creating yet another silo — while maximizing ROI by leveraging existing AD infrastructure and skillsets

Organization can further lower their acquisition costs with Centrify Express for SaaS, a free cloud service, that supports SaaS single sign-on for up to three applications. And Centrify's unified identity services and coverage across data center, cloud and mobile eliminates the need for a multitude of single-purpose products.

Additional resources

Centrify DirectControl for SaaS Web Site

http://www.centrify.com/saas/overview.asp

Centrify DirectControl for SaaS Data Sheet

http://dev.centrify.com/downloads/public/centrify-directcontrol-for-saas-datasheet.pdf

Centrify DirectControl for SaaS 5-minute Video

http://www.centrify.com/saas/directcontrol-for-saas-demos.asp

Centrify Express for SaaS Free Offering

https://www.centrify.com/saas/free-saas-single-sign-on.asp

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

About Centrify

Centrify Corporation provides unified identity services across the data center, cloud and mobile — resulting in one single login for users and one unified identity infrastructure for IT. Our solutions optimize costs and increase agility and security by leveraging your existing identify infrastructure to enable integrated authentication, access control, privilege management, policy enforcement and compliance. Centrify customers typically reduce their costs associated with identity lifecycle management and compliance by over 50%. With over 4,000 customers, including 40% of the Fortune 50, Centrify is deployed on over a million resources across our customers' data centers, cloud and mobile environments.

WP-027-2012-12-01

© 2013 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.