CENTRIFY WHITE PAPER

A Practical Path to Unified Identity Across Data Center, Cloud and Mobile

Abstract

The major trends challenging IT organizations today are the increasing heterogeneity and hybridization of platforms inside and outside the organization, the rush to deploy SaaS applications and the explosion in smart phone and tablet devices users are bringing to work for personal productivity. As a result organizations are struggling to manage identity silos for enterprise applications, web applications, SaaS applications (one ID store per app), UNIX/Linux and also have dedicated silos for Macs and mobile devices. This fractured identity environment results in significant management challenges for IT and frustration and lower productivity for users forced to remember multiple usernames and passwords.

There is a growing dissatisfaction with single-purpose identity vendors that only provide basic capabilities and only address a subset of identity silos organizations must consolidate. While these products provide single sign-on for just SaaS or mobile device management or "Active Directory Bridging" to UNIX/Linux systems they don't solve the fundamental problem organizations face when trying to lower the costs and risks associated with their fractured identity environment.

Centrify delivers unified identity services that centrally manage identities across data center, cloud and mobile to optimize cost, agility and security. These identity services include integrated authentication, access control, privilege management, policy enforcement and auditing. This means IT does not have to sacrifice control of corporate identities and can leverage their existing Active Directory skillsets and processes to take advantage new capabilities, cost and deployment models available inside and outside the enterprise while also enabling productivity and secure access for a dynamic and increasingly mobile workforce.

Contents

Contents 3
Introduction 4
Identity Management Challenges 5
Centrify Unified Identity Services Vision 7
Centrify Unified Identity Services Defined 9
Unified Identity Services Benefits 10
Conclusion 11
Additional Resources 12
About Centrify 12
References 12

Introduction

Establishing and maintaining a security and compliance posture, in what is a disparate and dynamically changing IT environment, is regularly cited as the top concern of IT leaders who are responsible for mitigating risk and protecting the information assets of their organizations. The major trends at the heart of this changing IT environment is the increasing heterogeneity and hybridization of platforms inside and outside the organization, the rush to deploy SaaS applications and the explosion in smart phone and tablet devices users are bringing to work to for personal productivity.

Platform heterogeneity and hybridization

Across organizations increasing platform diversity is demonstrated in the battle for server OS market share with mainframe share declining, Window growing at 13% and Linux growing at 20% (according to 2011 IDC projection). IT organizations are more likely than ever to have a mix of Windows, UNIX and Linux systems in their data center environment. And the trend towards increased hybridization of these systems on physical and virtual machines has made the deployment of multiple systems; each tuned to a specific operational need or application requirement, possible including using many of the dozens varieties of Linux distributions. In fact, the penetration of virtualized systems in the data center environment is between 50 – 60% (IDC). Multiple platforms and virtualization of systems will continue to add flexibility and management complexity to the data center environments.

In a similar fashion platforms for desktop computing are also increasing in diversity. With the dominance of internet based networking protocols and browser based applications Mac OS systems are finding their way into organizations in increasing numbers. In fact, IT decision makers reported a 52% increase in Macs deployed in 2012 (Forrester). IT organizations are more accepting of a wide variety personal systems (Mac OS and Linux workstations) but, still must grapple with security and management of these systems in a environment where Windows systems benefit from an existing, well understood set of management tools and processes. Central to the complexity of this environment is the multiple, incompatible approaches to identity management between Windows, UNIX/Linux and Mac OS systems.

Rush to 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. 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.[1.] Also, this year Forrester estimated that organizations that have embraced cloud-based application deployment models are already using 10 or more SaaS applications. IT organizations should be concerned about the relative ease with which non-IT departments and individuals can purchase and activate SaaS applications without considering the security implications of adding an additional identity store and giving users another credential to remember.

But, executives and IT managers are also 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 upsurge of iOS and Android devices) 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. The key issues associated with bring-your-own application are how identities should be managed and control established so IT organizations can ensure security and compliance.

Explosion in bring-your-own mobile devices

Users are increasingly bringing their own devices into the workplace, first Mac OS systems then smart phones and now tablet devices. Most companies still have not dealt with these waves of new devices in a comprehensive fashion and many firms are not even aware of the real number of personal devices that are being used to access corporate network services such as email, WiFi and VPN connections. There can't be a more telling statistic than one quoted in a recent IDC study that reported 40% of IT decision makers say they let workers access corporate information from employee-owned devices, but 70% of employees indicated they access corporate networks this way. And the use of personally owned devices is only growing — according to one study there will be close to 15 billion network connected devices (e.g. smart phones, notebooks and tablets) by 2015. This translates into 7 connected devices per U.S. citizen by this date. Given this explosion in mobile devices and mobile applications access IT organizations are appropriately concerned about how they can cost effectively secure and manage the multiple devices their employees and contractors want to use for mobility and productivity.

In the face of all these major trends impacting organizations, IT leaders still must deal with compliance including new regulations and industry mandates, more stringent enforcement of existing regulations and corporate governance. And IT executives are now in the spotlight as concerns about data breach risks and brand protection take center stage with corporate boards that only have to glance at daily news reports to understand that visibility into the effectiveness of IT security and compliance is as critical as every other part of the business.

All levels of management now realize that identity is at the center of their ability to improve visibility and ensure control over servers, applications and endpoints, whether these resources reside inside or outside the enterprise firewall. Understanding the path to improved identity management starts with a review of identity challenges organizations face.

Identity Management Challenges

As organizations seek to increase productivity and accelerate business initiatives they deploy servers, on-premise and SaaS applications each with their own separate infrastructure for identity management and control of policies and privilege. Today, organizations most likely manage individual identity stores for enterprise applications, web applications, SaaS applications (one ID store per app), UNIX/Linux (e.g. NIS and LDAP) and may also have dedicated silos for Macs and mobile devices. This fractured identity environment results in significant management challenges for IT and frustration and lower productivity for users forced to remember multiple usernames and passwords.

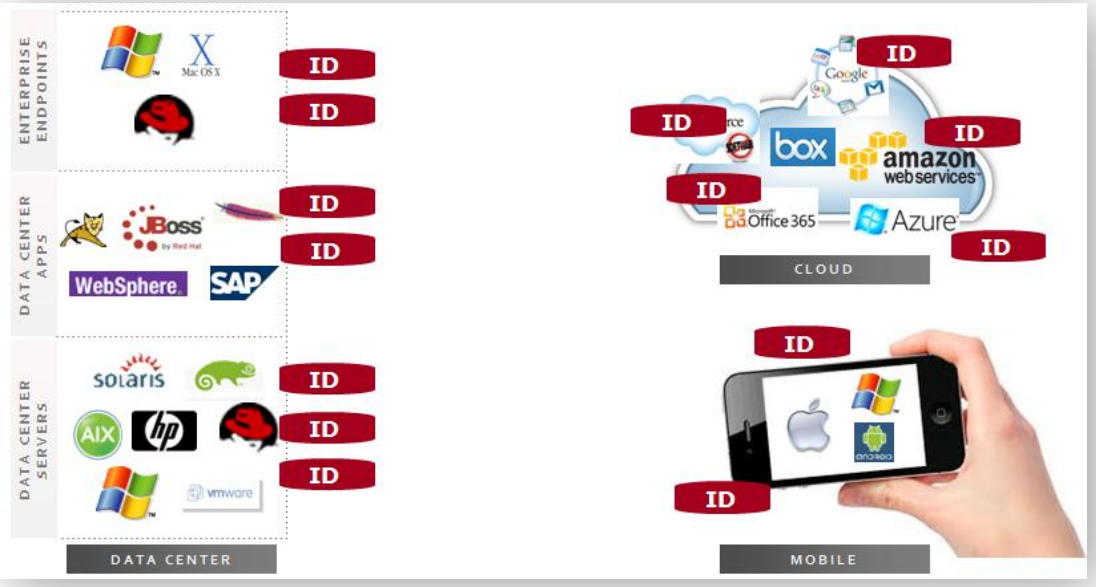
Multiple identity infrastructure challenges

As these identity silos have proliferated across organizations the ability to understand who has access to what resources, with what rights and what each user can do with their access rights has almost disappeared. Multiple identity infrastructures means IT administrators have multiple "panes of glass" to on-board, off-board and to update user account details and manage roles. IT operations and security staff must also generate compliance reports from multiple consoles and can't correlate user accounts across silos without cumbersome manual processes to tie separate accounts to a specific individual – this is especially painful during regular "recertification" reviews when IT must match a user's access rights to their current job function.

Multiple user login challenges

IT organizations should be concerned about the relative ease with which departments and users can bring-there-own devices and applications without considering the security implications of adding an additional identity store and giving users another credential to remember. The explosion in usernames and 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. Also, users react to the increasing number of

passwords with other coping techniques like creating weak passwords that are easy for hackers to determine and sharing account credentials which destroys any accountability for individual user actions. The greatest user frustration comes when attempting to authenticate on a mobile device. The interface on mobile devices makes typing logins impractical and erodes the real productivity gains mobile devices bring to users. Whether users are accessing applications via a mobile browser or using native mobile applications they need secure mobile login without typing usernames and passwords.



The state of enterprise identity is a fractured identity environment with multiple identity infrastructures to manage and multiple logins for users to remember.

Costs and risks of a fractured identity environment

IT leaders see the cost and risk associated with multiple identity infrastructures every day. The cost of a single help desk call to reset a password can be as high as $60 and the staff time required to handle user accounts across different identity stores can be measured in hours while the opportunity costs to have skilled IT staff performing manual tasks rather than focused on improving the competiveness and agility of the business may be hard to fully calculate. And compliance costs continue to rise largely because demonstrating compliance in most organizations involves sidetracking experienced resources that understand how to extract and organize data from systems and applications required by auditors. This makes IT operations less efficient and limits what IT management can achieve with constrained staffing and tight budgets.

And there are barriers to leveraging cloud models and mobile access for cost advantage if IT can't ensure the control and visibility. Central to securing SaaS applications is managing user access to these applications and eliminating error prone manual processes for de-provisioning users across multiple identity stores. Making a mistake can create orphan accounts and the opportunity for malicious users to gain unauthorized access leading to a costly data breach. IT organizations need a way to shutoff all access (from mobile devices outside and systems inside the enterprise) from one console.

Key capabilities to consider

There is a growing dissatisfaction with single-purpose identity vendors that only provide basic capabilities and only address a subset of identity silos organizations must consolidate. While these products provide single sign-on for just SaaS or mobile device management or "Active Directory Bridging" to UNIX/Linux systems they don't solve the fundamental problem organizations face when trying to lower the costs and risks associated with their fractured identity environment. In fact, organizations may see increased costs as they struggle to deploy multiple point products that are difficult to integrate, require intrusive changes to their IT environment and still require the installation of new infrastructure with additional consoles administrators must learn and use. And customers are finding that the minimal single sign-on capability from these products 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. In addition, many SaaS single sign-on vendors put identity data at risk by duplicating this data to the cloud.

Before organizations go to the time and expense of deploying single-purpose identity management 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 SaaS applications and Zero Sign-On for mobile 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?
- Is there integrated support for granular authorization — role-based access and polices — enabling the enforcement of least access security and privilege?
- Can user activity be audited through integrated and detailed session capture and centralized reporting?
- Does the product support a non-intrusive deployment model that does not require 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 Unified Identity Services Vision

Centrify provides unified identity services across data center, cloud and mobile — resulting in one single login for users and one unified identity infrastructure for IT. Centrify's software and cloud services let organizations securely leverage their existing identity infrastructure to centrally manage authentication, access control, privilege management, policy enforcement and auditing across on-premise and cloud resources.

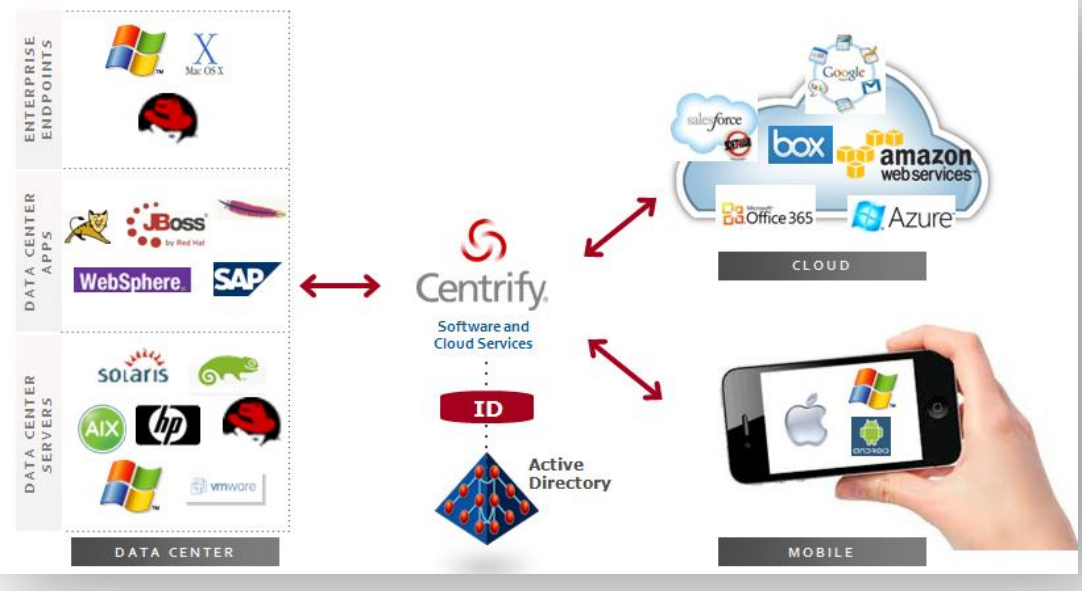
One login for users

Centrify's unified identity services approach decreases the cost of providing mobile and SaaS application access 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 their 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 to 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 system and 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). This is critical since single-purpose approaches require use of multiple consoles and redundant infrastructures to achieve the same result.



Centrify securely leverages your existing identity infrastructure across data center, cloud and mobile – resulting in one login for users and one unified architecture for IT.

Why leverage Active Directory?

The vast majority of organizations have given their users Active Directory accounts to enable corporate email and control access to network resources such and file shares. Today, Active Directory is the strategic identity platform in almost all business environments.

Active Directory has critical advantages for establishing a centralized and authoritative directory for identity, policy and access management, advantages not found in any other directory:

- Fault tolerant, distributed and high availability deployment model with automated DNS lookup service and one-way trust.
- Built-in support for Kerberos authentication and single sign-on.
- A fully featured and integrated Certificate Authority (Microsoft CA) that makes it easy to support PKI-based authentication for email, WiFi and VPN and encryption of data-in-transit.
- Group Policy for centralized security enforcement of computer objects based on type, organizational unit or functional grouping.
- Existing skills, processes and staff already familiar with Active Directory management.
- A rich ecosystem of administrative tools already familiar to an organizations helpdesk and IT staff that makes supporting the identity and device access management lifecycle easy.

The simplest and most practical approach is to fully leverage Active Directory for centralized management of on-premise and SaaS applications, mobile devices and non-Windows systems (UNIX/Linux, Mac OS) for true unified identity lifecycle management.

Centrify Unified Identity Services Defined

Centrify delivers unified identity services that centrally manage identities across data center, cloud and mobile to optimize cost, agility and security. Our identity services include integrated authentication, access control, privilege management, policy enforcement and auditing. This results in one login for users and one seamless identity infrastructure for IT.

Centrify unified identity services across data center, cloud and mobile

Centrify's Unified Identity Services is an integrated architecture comprised of software and cloud services that enable organizations to securely leverage their existing infrastructure to centrally manage authentication, access control, privilege management, policy enforcement and auditing across on-premise and cloud resources. This means IT does not have to sacrifice control of corporate identities and can leverage their existing Active Directory skillsets and processes to take advantage new capabilities, cost and deployment models available inside and outside the enterprise while also enabling productivity and secure access for a dynamic and increasingly mobile workforce.

Centrify delivers a unified identity architecture with software and cloud services that span on-premise systems and applications, SaaS applications, mobile apps and devices all centrally managed through your existing Active Directory infrastructure

Centrify for Servers

Centrify for Servers is built on a single architecture that leverages your existing Active Directory investment. Centrify goes well beyond the authentication and Group Policy support of single-purpose "Active Directory Bridging" products with integrated features such as privileged user management, detailed user activity auditing and server isolation. In addition, our patented Zones technology accelerates deployment and provides unique, granular access controls and delegated administration. Centrify's solution is non-intrusive requiring no schema extensions in Active Directory, no kernel modifications on UNIX/Linux systems and no software to install on domain controllers.

Centrify for SaaS and Apps

Centrify's support for Apps and SaaS enables IT to provide users with a single Active Directory login to access all of their business applications including SAP and on-premise web applications such as Apache and WebSphere as well as cloud-based SaaS apps such as Salesforce.com and WebEx. A cloud-based self-service portal makes users even more efficient, giving them one-click access to apps and the ability to reset passwords, edit account information, and even locate, lock or wipe their mobile devices. This means IT spends less time provisioning accounts and responding to help desk calls.

Centrify for Mac and Mobile

With Centrify, you can control user access from Macs and mobile devices with Active Directory-based single sign-on to resources inside and outside the enterprise. And instead of configuring Macs and mobile devices one by one, you can centrally enforce Group Policy-based security settings across Macs, iOS and Android devices. And like all Centrify solutions it is non-intrusive requiring no additional infrastructure, problematic firewall configurations or appliances in the DMZ.

Unified Identity Services Benefits

Centrify Unified Identity Services centrally authenticates users with their Active Directory identity which gives IT valuable insight into which systems and applications are actually used and when — restoring visibility and control.

In addition, Centrify Unified Identity Services further benefits users and IT through:

Enhanced user productivity: Users are happier when they only have one login to remember and get don't have repeatedly enter their credential when accessing SaaS and mobile applications. Users further benefit by having super easy self-service portal that gives them quick access to their applications, devices and AD account management.

Reduced compliance costs: Frees up expensive IT resources with easy and thorough reporting on who in the organization has access to which resources and what they did with their access. Quickly demonstrate compliance with regulations and industry best practices.

Reduced helpdesk costs: Centrify returns value in improved help desk staff productivity and as much as a 95% reduction account and password reset calls.

Lower identity lifecycle costs: By tightly integrating data center and desktop systems, cloud and mobile applications with Active Directory the delivery of 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 everything 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.

Conclusion

Unified identity services return on investment

Centrify helps customers maximize return on their identity management investment by centralizing identity and privilege management in one place greatly reducing and automating many labor intensive tasks. Centrify customers tell us they experience significant reductions in IT staff hours spent performing common tasks for identity lifecycle management, help desk requests and compliance reporting. Below is a sample of average savings experienced by collection of small, medium and large customer using Centrify today.

Hours	Add/ de-provision users	Manage and maintain security policies	Manage and maintain user privileges	Helpdesk calls (password resets)	Produce a compliance report
Without Centrify	250 hrs/mo	25hrs/mo	15 hours/mo	20 hours/mo	80 hrs/mo
With Centrify	75 hrs/mo	5 hours/mo	7.5 hrs/mo	12.8 hrs/mo	53.6 hrs/mo
% improvement	70% reduction	80% reduction	50% reduction	36% reduction	33% reduction

Overall our customers report reducing the hours spent managing a user throughout the identity lifecycle by 50 – 60%.

Why Centrify?

Centrify's unique, easy-to-deploy, software and cloud-based services ensures your on-premise Active Directory infrastructure can be securely leveraged to quickly bring servers (UNIX ,Linux, Windows), applications (on-premise, SaaS and mobile) and endpoints (Mac and Mobile devices) into line with security best practice and compliance. In addition, Centrify offers important business and technical advantages when compared to other approaches and vendors including:

- An unified architecture for security and single sign-on – not just another point solution — with support for 400+ systems and 100+ SaaS, mobile and on-premise apps
- Rich mobile capabilities (resident mobile apps and browser based access to SaaS) and Mobile SDK for ISV and in-house developers to add AD authentication to custom apps
- Unparalleled integration with Active Directory means no replication of identities — creating yet another silo — while maximizing ROI by leveraging existing Active Directory infrastructure and skillsets
- Proven technology deployed by 4500+ customers including 40% of Fortune 50 and over 60 Federal government agencies
- The largest team in the industry dedicated to creating the most complete, robust and easy-to-deploy and use software and services
- Best-in-class 24X7, follow the sun dedicate technical support
- Centrify Express, a collection of free software and service offerings, to speed deployments and further lower acquisition costs

Additional Resources

Centrify for Servers

Centrify for Servers Web Site

http://www.centrify.com/products/centrify-for-servers.asp

Centrify Suite Brochure

http://www.centrify.com/downloads/public/centrify_ds019_centrify_suite.pdf

Centrify Suite Videos Demonstrations

http://www.centrify.com/products/product_demos.asp

Centrify for SaaS and Apps

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 for Mac and Mobile

Centrify for Mac and Mobile Web Site

http://www.centrify.com/products/centrify-for-mac-mobile.asp

Centrify DirectControl for Mobile Data Sheet

http://www.centrify.com/downloads/public/centrify_ds024_directcontrol_for_mobile.pdf

Centrify DirectControl for Mobile Videos Demos

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

Centrify Express — Free Security and Authentication Offerings

http://www.centrify.com/express/free.asp

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.

References

1. "Forecast: Software as a Service, All Regions, 2010-2015, 1H12 Update," Gartner Market Analysis Report #1949616, March 13, 2012