

Securing Privilege Delegation in Public and Private Cloud Computing Infrastructure

Abstract

This white paper discusses the drivers for data centers moving to the cloud, the role of virtualization in both public and private cloud infrastructures and outlines the security and compliance implications of cloud computing - providing insight into the protection of sensitive data in the cloud via administrative access and privileged delegation.

Table of Contents

Introduction	3
Data Centers Moving to the Cloud	3
Virtualization as an Enabler	4
Public vs. Private Clouds	4
Insider Threat in the Cloud	6
Top Threats to Cloud Computing	7
Compliance Concerns	8
Securing the Cloud: Administrative Access & Privileged Delegation	9
PowerBroker for Virtualization	9
Case Study: How One of the World's Largest Global Financial Services Firm Uses BeyondTrust to Secure its Private Cloud Infrastructure	10

Introduction

In today's economic environment, organizations are focused on reducing costs and doing more with less while still trying to remain competitive. This means that IT departments are facing greater scrutiny to ensure that they match key business needs and deliver intended results in the most efficient and cost-effective manner. To meet these challenges, IT organizations are increasingly moving away from device-centric views of IT, to one that is focused on applications, information, and people and more towards the new paradigm of cloud computing.

As an emerging trend that provides rapid access to dynamically scalable and virtualized IT resources, cloud computing promises new and exciting opportunities for organizations to create lean, robust and cost-effective IT infrastructures that better align with business goals. However, certain tradeoffs concerning control, compliance and security must be addressed before fully realizing those benefits.

This white paper discusses the drivers for data centers moving to the cloud, the role of virtualization in both public and private cloud infrastructures and outlines the security and compliance implications of cloud computing - providing insight into the protection of sensitive data in the cloud via administrative access and privileged delegation.

Data Centers Moving to the Cloud

Why would organizations want to move their data center to the cloud? For one, IT managers are realizing they may be able to expand their infrastructure by shifting from the capital spending line (build your own data center) to the operating expense line (a service subscription). Another great advantage of cloud computing is the notion of Green IT.

When businesses use current assets instead of purchasing additional hardware, they reduce the size of their carbon footprint because it is one less server that is consuming electricity. In fact, green technologies can reduce energy costs by 50 percent.¹ Add to that reduced software maintenance, increased reliability/redundancy, increased scalability and efficiency, and greater accessibility for mobile/remote users, and the cloud becomes a very compelling value proposition.



In fact, the market for cloud/datacenter-delivered services has become a lucrative opportunity for service providers and will continue to be so for the foreseeable future. IDC predicts that the market opportunity for services delivered from cloud-based

¹ <http://www.cloudave.com/link/global-green-computing-fund>

infrastructures will grow from nearly \$40 billion in 2009 to \$73 billion by 2015 (10.6% CAGR).²

Virtualization as an Enabler

While the cloud is not in and of itself virtualization, virtualization is a critical component and major enabler of cloud computing. Cloud providers are rapidly adopting virtualization, as the cost savings attract them. However, organizations moving their data onto the cloud must consider the risks they face if the virtual environment is not administered properly.

Virtual machines make it possible to separate hardware acquisition and deployment from software deployment, and can improve delivery within an enterprise to 10, 20, or even 30 times faster.

*Thomas J. Bittman
VP Distinguished Analyst, Gartner*

Many cloud providers utilize a virtual environment, which exposes client data to new security vectors not found on physical servers. Security risks are compounded when the virtual hypervisor is compromised that could affect and possibly bring down all the virtual (guest) machines sitting on top of it.

Additionally, virtualization is enabling the IT department itself to be, in effect, a service provider for the business. Server virtualization “helps IT behave more like a cloud provider, and prepares the business to be a better consumer of cloud computing.”³ Virtualization is becoming the standard for how a company should design its IT resources for the future in that it allows for greater operational efficiency at much less cost.

Not only does this architecture result in tremendous cost savings due to shared resources and reduced hardware acquisition costs, but it also provides for better availability and ongoing maintenance since one server being taken down doesn’t impact the others. Furthermore, as IT begins to be regarded as a service provider within the organization, the IT department can charge back to business units based on dynamic usage.

Public vs. Private Clouds

There are essentially four deployment models for cloud services, the main two being public and private clouds:

- **Public Cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services (e.g., [Amazon’s EC2](#), [GoogleApps](#), [Salesforce.com](#)). Although many organizations use public clouds for private business benefit, they do not control how those cloud services are operated, accessed or secured.

² IDC, “Datacenter-Delivered Services: The Service Provider Opportunity”, by Curtis Price and Melanie Posie, Doc#220878, Nov 2009

³ Gartner, “Server Virtualization: One Path That Leads to Cloud Computing”, RAS Core Research Note G00171730, Thomas J. Bittman, 29 October 2009

- **Private Cloud.** The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party and may exist on- or off-premises.

While the organization does not need to physically own or operate all the assets, the key is that a shared pool of computing resources can be rapidly provisioned, dynamically allocated and operated for the benefit of a single organization.

- **Community Cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations).

It may be managed by the organizations or a third party and may exist on-premises or off-premises.

- **Hybrid Cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).⁴

So which is more popular among enterprises – public or private cloud? Research actually shows that private cloud is the most popular with enterprises, deployed either on-premise, or using a mix of on-premise and off-premise (hosted) services.

Specifically, 75 percent of organizations with existing or planned cloud adoption are choosing private cloud, while only 16 percent are using or planning to use solely off-premise cloud outsourced to a third-party service provider.⁵

To further bolster this fact, according to research from International Data Corporation (IDC), server revenue for public cloud computing will grow from \$582 million in 2009 to \$718 million in 2014, but server revenue for the much larger private cloud market will grow from \$7.3 billion to \$11.8 billion in the same time period.⁶

Now is a great time for many IT organizations to begin seriously considering this technology and employing public and private clouds in order to simplify sprawling IT environments.

*Katherine Broderick
IDC Research Analyst,
Enterprise Platforms and
Datacenter Trends*

⁴ Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", December 2009
www.cloudsecurityalliance.org/csaguide.pdf

⁵ Enterprise Management Associates, "The Building Blocks for Private Cloud: Automation, Virtualization, and Cloud Service Management", December 2009

⁶ IDC, "Worldwide Enterprise Server Cloud Computing 2010–2014 Forecast" by : Katherine Broderick, Michelle Bailey, Matthew Eastwood, Doc #223118, May 2010

Insider Threat in the Cloud

According to an IDC Enterprise Panel survey, the number one concern of companies moving into cloud computing environments is security (see Figure 1). Silos of dedicated IT infrastructure built around specific applications, customers, business units, operations, and regulatory compliance are often the result of the dramatic growth in scale and complexity of enterprise IT environments.

While cloud computing removes the traditional application silos within the data center and introduces a new level of flexibility and scalability to the IT organization, the support for multi-tenancy compute environments also introduces additional security risks, the most insidious of which is data theft.

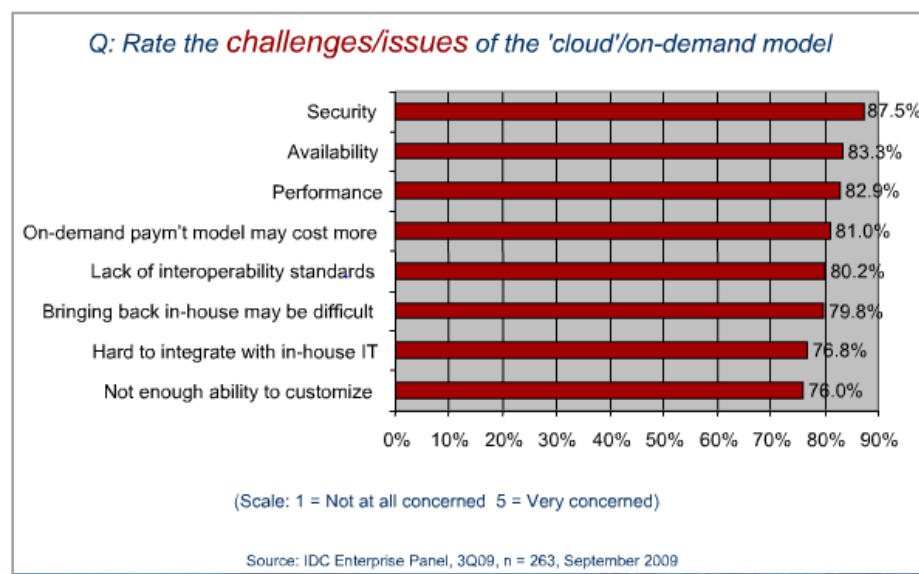


Figure 1

A general lack of transparency into provider processes and procedures, such as how its employees are granted access to physical and virtual assets, makes preventing data theft more difficult. The concentration of valuable data from a multitude of customers represents an appealing target for attack from unethical system administrators as well as malicious Internet-based attackers, and should raise concerns regarding privileged user access.

Plus, there is lack of visibility into the hiring standards and practices for cloud employees. Depending on the level of access granted, a malicious insider may be able to harvest an organization's confidential data or even gain control of the entire infrastructure with little or no risk of detection.

As an alternative to public clouds, organizations are adopting private cloud infrastructures as a means of gaining more control over their data; however, they still need to take steps to detect and defend against the malicious insider threat.

Although the cloud helps free organizations from operating their own servers, storage, networks and software, it also eliminates many of the traditional, physical boundaries that help define and protect an organization’s data assets, and introduces new risks as virtual servers and mobile virtual machines replace physical servers and firewalls. For instance, malicious users with admin credentials to the virtual infrastructure could clone virtual machines to gain access to all data contained in the guest machines.

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

*Cloud Security Alliance
“Top Threats to Cloud
Computing v1.0,” March 2010*

Since the cloud introduces ever-changing chains of custody for sensitive data and applications, protecting those assets becomes all the more difficult. Sensitive information should not be stored or processed in the cloud without visibility into the supplier's technology and processes to ensure the appropriate level of information protection.

The administrative tools used to access the Hypervisor/VMM layer a cloud vendor manages must be tightly controlled to maintain a strong security posture. Organizations need to carefully analyze business and security requirements, and must evaluate the depth and reliability of security features and cloud service levels.

The majority of organizations today are highly motivated to transition further into a cloud model, but hesitant to put their most mission-critical data in untested waters. There is an entire ecosystem of technologies to facilitate the cloud that is still growing, but licensing models and technology have been slow to get to where regulated companies can feel comfortable.

Top Threats to Cloud Computing

<ul style="list-style-type: none"> • Abuse and nefarious use of cloud computing 	<ul style="list-style-type: none"> • Malicious insiders
<ul style="list-style-type: none"> • Insecure interfaces and APIs 	<ul style="list-style-type: none"> • Account or service hijacking

Source: Cloud Security Alliance, “Top Threats to Cloud Computing v1.0,” March 2010

Compliance Concerns

One of the greatest challenges for organizations leveraging cloud environments is demonstrating policy compliance. For many business functions commonly run in the cloud, such as hosting websites and wikis, it is often sufficient to have a cloud provider vouch for the security of the underlying infrastructure. However, for business-critical processes and sensitive data, it is absolutely essential for organizations to be able to verify for themselves that the underlying cloud infrastructure is secure.

The use of virtual machines adds further complexity into the mix, since creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion can be challenging for even the most mature virtualized environments. Proving that the physical and virtual infrastructure of the cloud can be trusted becomes even more difficult when those infrastructure components are wholly owned and managed by external service providers.

Cloud providers must be able to demonstrate that they have tested and can ensure that privileged user access is controlled and monitored. For instance, ISO/IEC 27001 requires an organization to create an Information Security Management System (ISMS). This enables an organization to use a risk-based approach to identifying and satisfying all compliance requirements, justify the selection and implementation of controls, and provide measurable evidence that the controls are operating effectively.

Organizations that claim to have adopted the ISO 27001 standard can therefore be formally audited and certified compliant with the standard. It is already fairly well known and accepted outside of the United States and is slowly gaining awareness and acceptance within the U.S. ISO 27001 requires that management:

1. Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
2. Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
3. Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Another key regulation is The Payment Card Industry (PCI) Data Security Standard (DSS), which is a set of comprehensive requirements for enhancing payment account data security in an effort to thwart the theft of sensitive cardholder information. The core group of requirements are as follows:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program

4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

When appropriate, organizations should also ask for a commitment from providers to meet regulatory standards such as PCI DSS, Health Insurance Portability and Accountability Act (HIPAA) in the U.S., and the EU Data Protection Directive.

Securing the Cloud: Administrative Access & Privileged Delegation

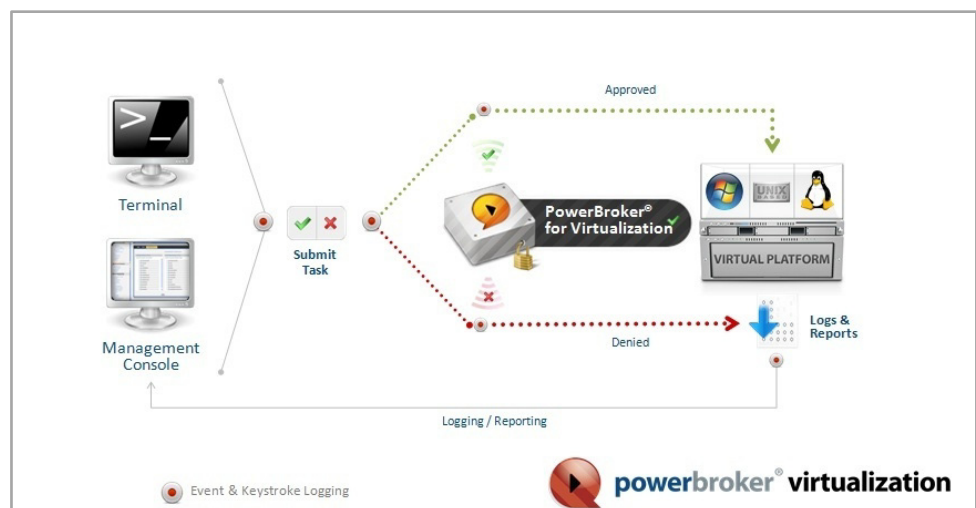
Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several cloud-computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary precursor towards strategic use of on-demand computing services.

BeyondTrust is the market-share leader for privileged identity management (PIM) solutions and enables security best practices for a company's most sensitive information, even in the cloud. Its PowerBroker suite is the only comprehensive enterprise-wide solution for servers, desktops, applications and devices in heterogeneous IT environments, including virtual servers, Windows and Linux/Unix.

PowerBroker for Virtualization

PowerBroker for Virtualization provides a unified solution to centrally address risks from undermanaged privileges in virtualized datacenter environments and privileged access tools to mitigate security risks and meet compliance requirements so organizations can adopt virtualization with confidence. It provides a cost-effective solution for consistent granular privilege identity management across guest operating systems as well as hypervisor hosts, through a single centralized management console.

How PowerBroker for Virtualization Works



Privileged access security risks are mitigated, compliance requirements met, and organizations can adopt virtualization with confidence. Key benefits of PowerBroker for Virtualization include:

- Granular delegation of administrative privileges to ensure support for compliance mandates and security standards
- Detailed and flexible reporting including keystroke logging of admin activities
- Two-click entitlement reports
- Programmable role-constrain mechanisms for segregation of duties
- Secures virtual guest and host hypervisors
- VMware ESX, Solaris Zones, AIX WPAR, and IBM z/VM
- Support for more than 30 guest operating systems

Case Study: How One of the World's Largest Global Financial Services Firm Uses BeyondTrust to Secure its Private Cloud Infrastructure

One of the world's largest financial services firms, with a centralized IT organization, provides IT "services" to its business units, with internal cross-charges. The firm decided that the most efficient way for the IT organization to meet business units' requirements in a cost-effective manner was to develop a private cloud infrastructure. IT determined virtualization was a necessity to ensure cost efficiencies in this private cloud delivery model.

Before moving forward with the private cloud infrastructure, the business units had a key concern that needed to be addressed: they wanted to make sure that their confidential data would remain secure and that any requirements around compliance would be upheld in the private cloud infrastructure. Since virtualization would be employed and compliance was a concern, it would be difficult for IT to segregate the infrastructure by business unit while still ensuring authorization levels were in line with compliance mandates.

In order to meet the security and compliance requirements of the business units, the firm deployed BeyondTrust® PowerBroker Virtualization and PowerBroker Unix & Linux Servers to provide unified protection from host to guest operating systems. As a result of using PowerBroker for the private cloud infrastructure (built on VMware), privilege delegation is now centrally governed for both guest VMs as well as the ESX hypervisor. The solution allows the IT organization to centrally monitor and control administrative access and privilege delegation throughout the companywide infrastructure. The IT organization and discrete business units are also able to produce compliance reports that include the logging and auditing down to the keystroke as well as event data for ad-hoc drill down validation of their key SOX, PCI and FFIEC compliance needs.