

An Abacus Group White Paper



767 Third Avenue
New York, NY 10017
Phone: (646)-808-0200
www.abacusgroupllc.com

Is My Cloud Secure? Secure Multi-Tenancy Overview

April 6, 2011



Advancements in virtualization and the shift to cloud-based services are changing how technology is acquired and implemented at investment management firms. Historically, infrastructure was bought piecemeal -- servers, network switches, cables, storage arrays, etc.—and then assembled; with the entire process being repeated with each replacement / upgrade cycle. Virtualization and Cloud-based services have given rise to purchasing capacity, which already contains the required server, network, bandwidth and storage resources, on demand. This new model shortens the length of time required to get up and running and facilitates on-the-fly upgrades. Virtualization and the “Cloud” bring the promise “to overcome historical limitations and reduce future IT spending by as much as 47%.”¹

However, as is often the case, technology advancements bring new concerns. Among these concerns -- *separate and independent firms will now be sharing the same physical resources*. Security has always been a concern for fund managers and their clients. US investment managers operate businesses where data security is a preeminent concern. Funds must adhere to regulatory and compliance standards whereby all investor information needs to be private and protected. Further, the applications, models, and processes used by fund managers to make decisions are what provides them an edge, and any compromise to the availability of these items could hurt their performance.

This white paper will provide an insight into how virtualization and cloud-based technology provides fund managers with significantly better security and protection versus running individual servers out of their office. Common misperceptions are that data which resides on a free standing server is more secure than data that resides on a shared environment; as well as, that infrastructure equipment in your office is more secure than equipment which resides in a third-party data center. This paper will provide the details around how fund managers can reassure themselves their data and applications are secure and protected in the cloud.

Physical Server vs. Shared Environment

Adoption of cloud-based services has prompted questions around the security and protection of data in a shared environment. A traditional assumption is that a company’s data and applications sitting on an independent server are more secure than if they were in a shared environment. It should be noted the principal difference is that an independent, physical server has a tin/metal covering, which does very little except keep dust off of the components. The traditional method of segregating various applications and data on separate physical hardware does not necessarily translate into better security. Data residing on servers in a firm’s office could be more vulnerable than data that resides on a shared hosted platform. Prime Brokers, fund administrators, even your personal bank all make use of pooled and partitioned hardware resources to deliver their services.

1 NetApp Solution Brief: NetApp, Cisco, and VMware Deliver End-to-End Secure Multi-Tenancy 2010



In a service provider's data center, multiple companies will share services on the same infrastructure. Secure multi-tenancy guarantees the logical separation of virtual resources in a shared physical infrastructure. The key is to properly implement and manage the pool/partitions of hardware resources as well as the many security layers. The hosted service provider will make use of many tools to ensure secure multi-tenancy, including:

- ◆ Enterprise Class Technology
- ◆ Network Segmentation
- ◆ Server and Storage Virtualization and Segmentation
- ◆ Unique and Independent Active Directory Environments,
- ◆ Permissions Based Data Access Within a Firm's Authentication Realm
- ◆ Internal Security Auditing
- ◆ Managed Antivirus and Antispyware
- ◆ Web Filtering
- ◆ Intrusion Detection / Intrusion Prevention Solutions
- ◆ Independent Third Party Audits (*i.e. SAS70, Security, etc*).

In short, when resources are shared; security and separation must be guaranteed at every layer -- from the server to the network to the storage. This is also true for funds who continue to manage their infrastructure on independent servers. It will be important for fund managers to ensure their service providers are adhering to best practices in managing to the proper security protocols for Physical, Server, Network and Storage.

Physical Security

Physical security is often overlooked when evaluating data security. The majority of data breaches do not take place in exotic cyber-attacks but occur when hard disks or backup tapes are misplaced or stolen. A common backup procedure for an on-site server is to rotate tapes off-site. This procedure is inherently a weak link in any security policy as backup media, containing the entire data set, is often unencrypted as it is transported off-site on a daily basis. This media is prone to loss or theft, resulting in a compromise of all of the firm's data. Further, on-site server rooms are often poorly secured. This can lead to theft of equipment or tampering.

A secure cloud provider will house their infrastructure in a SAS 70 certified data centers. These data centers have documented / audited access policies and controls for access and equipment removal.



Server Level Security

Server virtualization is integral to the delivery of hosted services. The hosted service provider should monitor and manage security and access across the virtual infrastructure, including role-based access/privileges, audit trails of configuration changes and reports, as well as real-time performance monitoring and analysis.

Another positive aspect of virtualization is the ability to move sessions between physical machines to minimize downtime, be it from hardware failure, scheduled maintenance, etc. The hosted service provider that the firm chooses should utilize the proper resources to monitor and maintain security even during movement between physical machines.

Network Level Security

The next layer of secure multi-tenancy lies with the network. While the hardware that is utilized is shared physical equipment, the client servers are virtualized and must be segregated. The hosted service provider should implement the virtual servers on separate networks and, thus, ensure servers from different firms are unable to communicate with each other. In addition, the hosted service provider should configure switches and firewalls to “lock down” each client’s network to ensure that no data intermingles.

Storage Level Security

The hosted service provider is responsible for supplying the firm with a storage solution that provides for secure data segmentation, as well as enables rapid resource allocation. Furthermore, the hosted storage solution should provide high availability and disaster recovery; protecting the firm against the full gambit of “events” ranging from physical hardware failure to accidental deletion to corruption of data; as well as providing data replication for off-site backup and archiving.

Summary

As cloud-based technologies move into the main stream, the myth of adverse security implications will subside. In the mean-time, it will be important for fund managers who see the benefit of cloud-based services to evaluate their service providers with respect to how their infrastructure is being managed in a shared environment. Service providers deploying secure multi-tenant environments make use of layered security to logically separate the virtual resources in a shared physical infrastructure as well as isolate and secure a firm’s data. In most cases, by consolidating multiple clients on one properly configured centralized platform, the service provider has greater capacity and more options to properly implement multiple security layers and secure the data versus traditional on-site implementations.



When evaluating service providers, fund managers should ensure the following needs will be met:

- ✓ Deployment speed and the ability to fulfill requests quickly.
- ✓ On demand capacity must be immediately deliverable where multiple workloads owned by different companies share the same infrastructure.
- ✓ Fund managers must be able to count on the service levels, the security and the audibility of the service.
- ✓ Resource allocation must be transparent; one customer's needs cannot interfere with another customer's ability to grow.

Cloud based services offer their clients the ability to scale their business quickly and effectively at a reasonable cost. Fund Managers must be careful to select a service provider who understands their unique business needs and the importance of security to them and their clients.

About The Abacus Group

The Abacus Group is an IT Solutions firm focused on helping hedge funds and private equity funds deploy and manage hosted IT solutions. Our objective is to provide investment managers and technology executives with solutions to improve their IT service experience. Abacus has developed a scalable, redundant and highly available IT platform to allow investment managers to run all of their technology as a service. The days of purchasing new hardware every few years are over. Abacus manages mirrored data centers throughout the US and provides cost effective and efficient solutions to firms whom require redundancy, high availability and disaster recovery. Firms connect to their IT applications and data through high speed circuits with minimal onsite equipment.