EzeCastle INTEGRATION

Thought Leadership Paper

Cloud Computing in the Hedge Fund Industry

About Eze Castle Integration

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 600 alternative investment firms worldwide, including more than 80 firms with $1 billion or more in assets under management. The company's products and services include Private Cloud Services, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Geneva, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

Table of Contents

With the changing economy and new regulations in effect, alternative investment firms are constantly looking for new ways to increase efficiencies and gain a competitive advantage. One area where firms have started to differentiate themselves from their competition is through technology.

Cloud computing, specifically, has allowed investment firms to leverage a robust and scalable technology platform that can reduce capital expenditures and increase performance efficiencies while satisfying regulatory requirements and investor demands for transparency.

Today's investment firms are grappling with a host of new challenges, and technology decisions are coming to the forefront of the conversation. Cloud computing continues to play a key role for both new startup firms as well as established funds. In fact, more than eight out of 10 investment management firms contacted during a 2012 market study indicated they were either currently using or planning to use some form of cloud services in the near future.

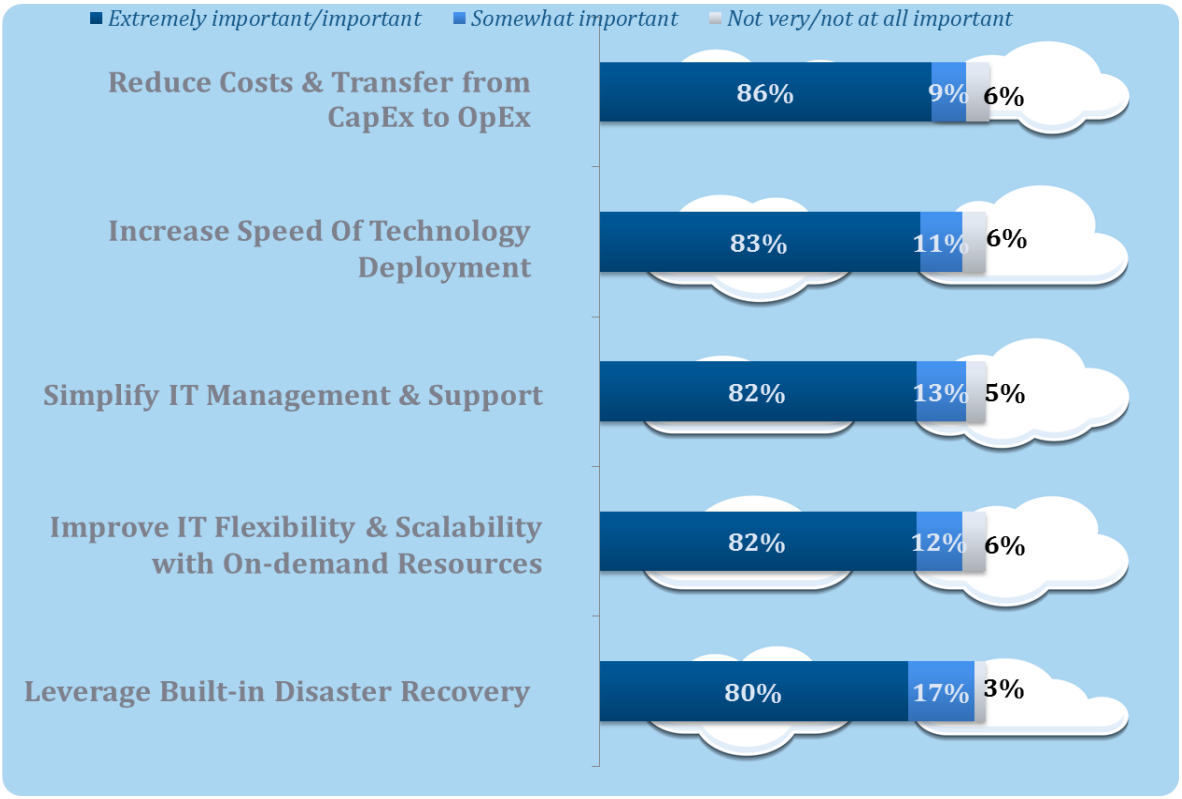
WHAT IS CLOUD COMPUTING?

Although cloud computing has become popular in recent years, many businesses and financial firms still do not understand what it is and how it works. Cloud computing is when a service or software application is hosted in a web-based repository – known as the "cloud." The service is hosted by a third-party provider who then provides access to that service to users on an on-demand basis. In essence, a firm's data and applications are hosted, alleviating that firm from having to purchase and maintain costly infrastructure in-house.

WHY ARE FIRMS GOING TO THE CLOUD?

Cloud computing can support front-, middle- and back-office functions – everything from business applications and client relationship management systems to data management solutions and accounting systems.

Five key drivers for adopting cloud services highlighted below:



Cost Containment: CapEx to OpEx

Through cloud services firms gain the opportunity to convert from CapEx to OpEx. While building out a comm room or data center requires capital expenditures, using an external cloud service that offers a pay-as-you-go service falls into ongoing operating expenditures. The transition to a cloud service provides many cost-savings beyond just eliminating the need to purchase and refresh equipment.

When weighing the costs associated with maintaining a server and other data center equipment in-house it is important to consider:

- **Direct costs** including power, real estate/floor space, storage, and IT staff to manage the resources
- **Indirect costs** including network and storage infrastructure and IT staff to manage the environment
- **Overhead costs** including procurement, accounting and IT

When added to the cost of an internal server, these factors significantly raise the monthly overall cost to host a server and make cloud services more attractive.

Improve Flexibility and Scalability of IT

One of the most beneficial aspects of cloud computing is that firms are only required to pay for the resources and capabilities they need. With traditional infrastructure models, firms must invest in advanced servers and storage devices that generally come at fixed costs. Cloud computing is uniquely flexible and scalable, operating on a utility basis - allowing firms to pay as they go and only for the resources they will use.

Because the cloud computing solution is virtualized, there are other distinct advantages not offered by traditional infrastructure models. Space, storage, and RAM are quick and easy to add. There is no need to wait for quotes to be drafted and equipment to be ordered and shipped. Instead of taking days, your firm's needs are fulfilled in a matter of hours. Cloud computing also supports a sharing of resources among multiple users – also known as multi-tenancy – which allows for increased utilization and efficiency.

Simplified IT Management = Less Maintenance

Unlike traditional infrastructure models where the firm is solely responsible for its own IT needs, the cloud computing model puts all of the responsibility on the third-party provider. Firms are no longer tasked with managing constant server updates, hardware installs and other computing issues. This allows the firms' internal IT staffs to focus on more business-critical matters and spend less time on mundane and time-consuming maintenance issues. Or in the case of many smaller firms without internal IT staffs, it saves them from having to hire and train additional employees.

Green Benefits

The resources and energy needed to maintain and manage a dedicated comm. room can be astronomical. Power, cooling, and basic energy supply equipment must be at peak performance at all times in order to facilitate maximum uptime for investment firms. In the case of cloud computing, however, firms don't need to host internal equipment, thereby saving on all-around energy costs.

The reduction of overall energy consumption is also multiplied with third-party providers utilizing custom data centers specifically designed for better energy efficiency.

HOW ARE FIRMS USING THE CLOUD?

A significant range of traditional on-premise technologies can be delivered via the cloud. The most popular include:

- Complete IT Outsourcing/Hosting
- Application Hosting/Infrastructure as a Service
- Hosted Cloud Voice
- Managed Security
- Managed Disaster Recovery

Complete outsourcing of a firm's IT infrastructure is a way to have all IT services, including file services, email, mobility services, backup and disaster recovery, delivered by a cloud service provider. One advantage of this approach is that the service provider is responsible for virtually everything. Furthermore, costs are predictable because you typically pay by user or usage. Todays, start-up hedge funds are predominantly selecting to use a cloud solution for their IT environment. Established funds typically evaluate moving to the cloud when their existing infrastructure is due for a refresh.

Established firms are more commonly first dipping their toes in the cloud via **application hosting services**. Firms are increasingly moving their applications, including OMS, Risk, and CRM, to a hosted model. The benefits to adopting the hosted model include gaining a highly available infrastructure on which to run your applications that is monitored and managed around the clock.

Hosted voice cloud solutions are another way that firms are using the cloud. Hosted voice solutions eliminate the need for an on-site PBX. By using a cloud voice service, such as a hosted PBX infrastructure, firms gain a cutting edge, professionally managed voice solution while eradicating large upfront capital outlays and management challenges.

Managed security is an area gaining attention as hedge funds become more aware of malicious threats. Using basic security tools is no longer an acceptable solution for growing hedge funds – particularly those seeking institutional money. By using a cloud service, firms can take advantage of a wide array of cloud security measures that are employed to protect their sensitive client data and resources. These cloud-based security practices range from physical security, isolation and virtualization security to policy enforcement and access control, encryption and resiliency.

Finally, firms are taking advantage of the **disaster recovery services** that a cloud solution provides. The ability to purchase cloud based DR services has dramatically lowered the cost of entry for firms of all sizes. In the past, firms had to buy two of everything and then manage the duplicate environments. Cloud computing removes the responsibility of purchasing and managing a secondary site from the firm , and delegates it to the cloud provider. This allows firms to focus solely on running their business effectively. Additionally, the complete data protection and business resiliency portfolios provided by the cloud enable hedge funds and alternative investment firms to utilize cloud computing to effortlessly protect themselves.

With all of these services, accessing a cloud service is seamless to an end user. A user simply logs onto a computer and is able to access their key systems and information. We except both startups as well as established hedge funds to continue embracing cloud services, making it a key trend to be aware of in 2013.

PUBLIC AND PRIVATE CLOUDS

When it comes to cloud deployment models, investment firms continue to rely on a variety of models. The most common choice, however, is a private cloud. While not all private clouds are alike, they are often better suited for hedge funds and investment firms who require a great deal of sophistication, application integration and support. Here is a quick review of the cloud types:

Private Cloud: Infrastructure provisioned solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

Public Cloud: The cloud infrastructure is provisioned by the cloud provider for open use by the general public. It may be owned, managed and operated by a business, academic, or government organization or some combination of them. (e.g. Amazon Web Services, Google Docs, etc.)

Hybrid Cloud: A composition of two or more clouds that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

WHY GO PRIVATE?

Public cloud tools, such as those offered by Google and DropBox, are wholly owned and managed by third-party providers. Because infrastructure costs are spread across all users who are employing the service, each individual client is able to operate at a low cost. Public cloud tools are typically larger in scale than private enterprise clouds, which provide users with seamless, on-demand scalability.

These factors may seem to support the belief that Google Apps or DropBox would suffice for a business's basic infrastructure and file sharing needs. However, upon closer examination, it is clear that there are a number of areas in which these tools fall drastically short of meeting the crucial business needs of investment management firms.

FEATURES & CAPABILITIES: WHAT DO YOU REALLY NEED?

While services such as DropBox enable file sharing among small groups of people, they are not easily scalable to support small businesses, and can quickly become clumsy and inefficient as the firm grows. Once your firm expands to the point of requiring additional applications such as a CRM, OMS and accounting tools, DropBox's capabilities will no longer be enough to support your needs. While this tool may be suitable in helping your firm get off the ground with minimal upfront costs, it is not a viable long-term solution.

While Google Apps is a slightly more robust tool, it is not nearly as feature-rich as a dedicated private cloud system, and is much more challenging to integrate with other systems or applications. For instance, although Gmail may be able to handle basic email needs, it will not provide the full business email experience as is attainable via Microsoft Exchange, and is lacking many of the features and capabilities that Exchange provides.

Additionally, Google Apps does not support integration with CRM, OMS or other third party systems, which firms will require as they grow. It also lacks integrated voicemail capabilities, which means users cannot manage voice messages easily from their PC.

IT Support: Avoiding Being Just a Number

For investment management firms, uptime is crucial to operational efficiency and profitability. Free public cloud services such as Google Apps and DropBox are not accompanied by dedicated, vertical-specific IT support that are incorporated with quality private cloud infrastructures. In fact, Google has experienced several outages in recent years, some of which have lasted for hours or days at a time. Just as importantly, if a Gmail outage does occur, there is no way to effectively communicate with an IT support expert to address and resolve the issue in a timely manner. With private cloud providers such as Eze Castle Integration, your solution is accompanied by 24x7x365 help desk support equipped with the knowledge and resources to resolve technical issues quickly.

Data Security

Google's primary source of revenue, advertising, is based on the premise that the company is able to "see" keywords in your emails, searches and other online activities, provided you have an active Google account. In a business setting, this could mean that sensitive company or client data is exposed externally.

Also, because security measures are typically much more lax than with an enterprise-grade private cloud service, emails and other communications may be susceptible to interception by hackers. This type of exposure puts your firm at risk for a reputation-damaging information breach.

Disaster Recovery: Who will you Call?

Having a comprehensive disaster recovery solution in place helps protect your fund's data as well as its reputation. It also instills confidence with investors and other stakeholders while providing a competitive advantage. Public cloud tools may not include a built in disaster recovery solution, so this is a significant additional cost that your firm will have to consider.

With a top quality private cloud infrastructure, disaster recovery is built directly into the offering and is seamlessly integrated to ensure your data is protected at all times.

Investor Confidence

Institutional investors will likely not be comfortable having their information shared via DropBox or another public file sharing service. These tools have earned a negative perception due to their lack of effective security precautions.

Compliance Issues

The financial services industry continues to face compliance pressures and increased regulation. One area of particular focus is email and instant message archiving. The SEC currently advises that funds retain all internal and external email and IM business communications, a perspective that is shared by the majority of investors as well.

Tools such as Gmail do not contain effective archiving and recovery capabilities, and could put your firm at risk of compliance violations should an issue arise. Comprehensive enterprise private cloud services can easily integrate with archiving tools to help ensure that all emails, IMs and attachments are indexed and easily retrievable.

ACHIEVING SECURE COMPUTING IN THE CLOUD

Despite its clear advantages and rapidly increasing adoption rate, the notion of cloud computing still meets some resistance. Investment firms tend to be concerned with data security and performance. Many firms are reluctant to migrate to virtualized platforms because they don't fully understand the system and its benefits.

Privacy and security concerns are common among financial firms given the sensitivity of their data. The idea of hosting this sensitive information on the Internet is not always a comfortable one. Third-parties that provide cloud computing services, however, are quick to point out that the system is just as secure as maintaining one's own equipment, with comparable data protection measures, firewalls, security checkpoints and passwords as traditional infrastructure models. Performance concerns, as well, seem to be easily thwarted by third-parties, who insist cloud computing is just as efficient and effective as non-web hosted systems.

Ensuring infrastructure and data security is critical to any investment firm, regardless of whether its technology infrastructure lives on-premise or in a cloud environment. But there have been lingering concerns throughout the industry about security in the cloud for quite some time, particularly for hedge funds and other financial services firms who rely so heavily on the safety and security of their data.

The reality is that there are security concerns with any type of technology infrastructure. By doing a comprehensive due diligence around cloud architecture, management, security policies and selecting the right service provider, you can minimize the risk of a security threat in the cloud. service provider, you can minimize the risk of a security threat in the cloud.

THREE ELEMENTS OF A SECURE CLOUD

Proper security in a cloud environment requires specialized practices and processes at both the physical and virtualization levels. Following are some key features to look for when evaluating a cloud services provider:

Physical Security at Data Centers

- 24x7x365 manned lobby with visual verification of identity
- Two-phase authentication of visitors (card and biometric)
- Secured access doors and elevator banks
- Monitored security cameras
- Additional door, motion and camera sensors
- Visitor logs for cages
- Key-locked cages and cabinets

Infrastructure Security

In what is sometimes known as a multi-tenant environment, cloud subscribers share the same underlying infrastructure, databases or applications. In public cloud environments, multi-tenancy can pose a security risk if proper isolation measures are not put into place to securely separate data and resources. If you're looking for more security through a private cloud, be sure to look for these requirements:

- *Availability:* Redundancy should be built into every layer of the technology infrastructure to minimize the risk of unplanned downtime.

- *Secure Separation*: Ensure that your cloud provider will use secure separation to isolate your silo and resources from other cloud customers.

- *Service Assurance*: Computing, networking and storage resources should be readily available to you as needed to deliver top performance and accommodate fluctuations in user demands.

- *Management and Monitoring*: Work closely with your cloud services provider to ensure they will have comprehensive control and extensive visibility over your cloud infrastructure at all times. You need to ensure it is highly secure, your environment is separated and you receive the highest level of service.

Policies, Policies, Policies
Additionally, plan to vet your service provider around the policies and procedures they have in place for access control to your cloud environment. Following are some must-haves:

- *Access Control Policy*: How is access to and control of the storage, virtualization and network infrastructures managed? What protocols are in place for monitoring, granting access and logging changes to client information systems?

- *Information Security Management Policy*: What safeguards does the provider have in place to protect against physical and virtual threats? How are security violations and incidents reported and managed? What information does the provider collect about clients and how is it handled? Has the provider ever had a security breach, and if so, what was the outcome?

- *Employee, Visitor and Contractor Physical Security Policy*: What practices are in place for monitoring employees, visitors and contractors while on premise (office or data center)? What background verification, screening agreements and employment agreements are established?

CHECKLIST FOR QUESTIONING SERVICE PROVIDERS

Following is a list of questions to consider as your evaluate potential cloud service providers.

QUESTIONS ON PRACTICES

- Is the provider's cloud infrastructure built with an N+1 configuration to withstand equipment failure?
- What are the cloud provider's backup and retention procedures? How long is data retained?
- What is the provider's disaster recovery strategy, and how frequently is it tested?
- How does the cloud provider handle a mass disaster recovery activation?
- What type of security and monitoring practices are in place? Is proactive intrusion prevent used to prevent breaches?
- Who can access the provider's data and at what level?
- Can the provider share an audit trail which logs who has accessed what?
- Is data encrypted at rest as well as in transit?
- What Service Level Agreements (SLAs) are in place for the infrastructure and applications? What is the agreed upon uptime?
- How are support requests handled, and what is the expected response time?
- Has the provider ever experienced a security breach? If so, how was it resolved, and what safeguards were implemented to prevent a repeat experience?
- Is the data center SAS70 Type-II or SSAE 16 Type II (new standard 2012) certified?

Questions on Internal Practices

- How financially stable is the cloud provider? Can they provide audited financials? Can they sustain business in the long run?
- When an employee leaves, what is the process for blocking access to applications to prevent data downloads?
- How do we prevent employees from sharing login credentials with unauthorized employees?
- How do we define and enforce user roles to control access levels?
- Who has the authority to add new users?
- How often will employees be required to reset passwords? Are there requirements around complexity standards for passwords?

Questions on Application Hosting

- Which application vendors have systems operating in the cloud?
- Does the application vendor confirm their product works in a hosted environment?
- Are there any issues associated with virtualizing the applications?
- How is the application deployed? Does the software run native over the Internet, or does it require a delivery mechanism such as Citrix?
- Are there any limitations with this type of deployment? Are there certain pieces of functionality that will not work if remotely deployed? Are there display limitations?
- How many clients for the specific application have a hosted implementation?
- What certification levels does the cloud provider have with these application vendors?
- Will the application vendor help with a "proof of concept"?
- Will there be any changes to the level of service if the application is deployed in a hosted environment?

ABOUT EZE CASTLE INTEGRATION

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 600 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management. Our Eze Private Cloud is the most widely used hedge fund cloud spanning three continents and supporting over 2,000 users and a petabyte of data. In addition to our cloud services, our solutions portfolio includes Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Geneva, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

The Eze Private Cloud is an enterprise-grade, private cloud infrastructure that provides hedge funds and investment firms a highly redundant, secure and available IT environment. The Eze Private Cloud is the backbone for Eze Managed Suite and Eze Managed Infrastructure.

Eze Managed Suite is a fully managed IT solution for hedge fund and investment firms that provides flexibility and simplified IT operations. The solution combines a robust, highly secure private infrastructure via the Eze Private Cloud with key business applications and professional IT management.

Eze Managed Infrastructure provides clients easy access to an enterprise-grade private environment with the latest hardware and software without capital expenditures, expensive upgrades or ongoing maintenance and monitoring.

To learn more about Eze Castle Integration, visit www.eci.com or contact us at 1-800-752-1382 or sales@eci.com.