SECURITY IN THE HYBRID CLOUD:
Putting Rumors to Rest

FROM VIRTUALIZATION TO GROWTH OF THE PUBLIC CLOUD

IDC predicts that public cloud computing services will grow to a $72.9 billion market in 2015, up from $21.5 billion in 2010. This equates to an annual growth rate of 27.6 percent. Cloud is also increasingly leveraged by IT. IDC estimates that public cloud adoption will account for 46 percent of new growth for overall IT spending.[1] This rate and pace of adoption is very similar to the early acceptance and expanded use of virtualization technology over the last five years.

EXECUTIVE SUMMARY

Today's IT organizations are faced with an increase in the challenge and complexity of optimizing their IT budgets for the best possible delivery of services to internal and external clients. Whether it's reducing infrastructure costs, streamlining IT management, elevating service delivery, or something else, strategic IT decision making must not only support and enable day-to-day operations—IT must also facilitate competitive advantage in some way. And IT must keep data safe while they're at it.

Enter the cloud. In only a few years, cloud computing adoption by progressive organizations in every industry around the globe has skyrocketed. Whether moving development and testing workloads or production environments into the cloud or between the private and public cloud, many organizations are discovering that cloud services can deliver returns on IT investments that simply cannot be achieved in traditional IT infrastructure models.

While these business benefits are compelling, security in the cloud is still a major concern for many IT organizations. In fact, a 2011 IDG Research study conducted globally among IT decision makers at enterprise companies found that security concerns and loss of control over data were the top barriers to cloud deployment.[2]

Knowing what to look for in a service provider, gaining visibility into their security practices, and taking into account the compliance requirements of the particular industry are among the practices discussed in this White Paper to help organizations get over the security hurdles that often stand in the way of gaining executive management buy-in on cloud adoption. Overcoming those security hurdles is far from insurmountable.

As John Pescatore, vice president and research fellow at Gartner Research, noted in *Key Issues for Securing Public and Private Cloud Computing, 2011*, "The use of public and private cloud technologies raises security and management challenges, but none that are impossible to meet. In order to effectively and efficiently secure the use of cloud computing, enterprises need to match threats and business demands

with the right management security approach. Public, private, and hybrid cloud technologies will also present opportunities to develop new architectures and processes that will advance security and management capabilities in ways that were not possible with physical computing restrictions." [3] Therefore, while the hybrid cloud concept introduces new architecture considerations such as data migration, multi-cloud management, and distributed security models, it also presents new possibilities where security is concerned.

Another key benefit of the hybrid cloud approach is the flexibility it offers. Companies wanting to capitalize on the benefits of both the private and public cloud approach are turning to a flexible hybrid cloud model. The hybrid approach allows businesses to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers, in combination with private cloud computing and a strategic decision to keep some server operations on premise.

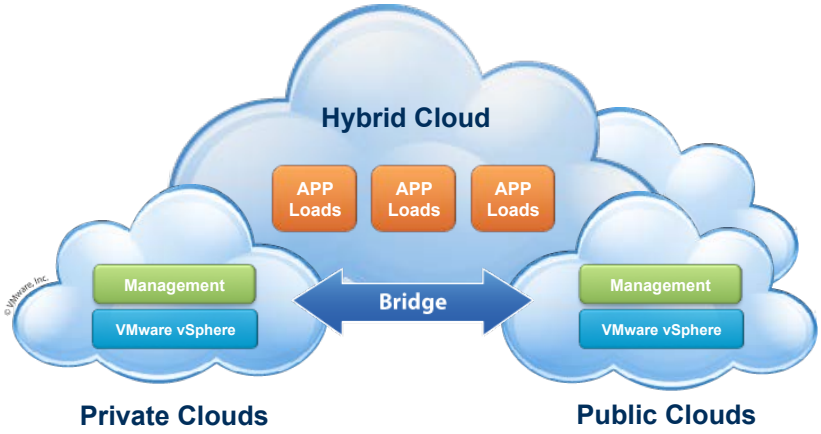

Figure 1: Hybrid Cloud Model

With appropriate due diligence, concrete knowledge that can dispel common myths about security in the cloud, and an understanding of the security capabilities offered by a hybrid cloud service provider, organizations can reap the financial and operational rewards that the hybrid cloud has to offer.

TYPICAL CONCERNS WITH HYBRID CLOUD SECURITY

Cloud computing can be implemented under a variety of service and deployment models, with a notable difference among them in how application and data security is addressed. Decisions about whether to use the cloud and which services to adopt often come down to whether IT management is convinced that the cloud will offer sufficient security practices and controls. With the obligation to protect confidential data, ensure ongoing application availability, and meet

"Enterprises need an appropriate level of control and visibility to ensure that sensitive data is being properly managed, that the right access is being granted to the right people, and that organizational and industry security standards are being upheld—just like they have in their internal environments, but with the dynamic control and change management necessary for a cloud environment."

David Hunter,
CTO of platform security,
VMware

corporate governance and industry compliance regulations while adding value and supporting innovation in the business, today's IT leaders must forge ahead with their cloud initiatives while being mindful of cloud security.

The security concerns themselves vary based on industry, services delivered, compliance and auditing requirements, and other factors, just as they do with a traditional non-cloud approach. However, some security concerns are fairly typical for any organization considering cloud adoption: the security of data when migrating to the cloud; the protection of data that resides in the cloud; the potential impact to application availability if data protection and disaster recovery practices fail; the ability to meet the security requirements of application regulatory compliance standards; and whether the IT organization will be able to maintain enough visibility into and power over their security stance.

MIGRATING TO THE CLOUD - For most organizations, transferring data into the cloud can be accomplished efficiently and securely with the right combination of in-house due diligence and cloud service provider migration expertise, as well as proven security technologies and best practices like secure tunnels and VPNs. One of the largest challenges here is the classification of existing and new application workloads.

Typically, the internal or private IT infrastructure and the external cloud infrastructure have noteworthy differences. While striving toward parity is a good goal, in some cases it cannot be achieved. Data might be sensitive enough, such as confidential or proprietary health record datasets, that the available public cloud options may not be effective. By classifying workloads based on their security requirements, they can be sorted into groups that serve as a guide to whether or not any specific workload will still be compliant with the security policy if it is run outside the corporate firewall.

By determining the security requirements of your data, you'll gain greater insight into which cloud model is most appropriate for your organization and whether your needs would best be served by an experienced cloud service provider. Table 1 shows an example of how an organization might weigh their cloud options for their particular context.

SECURITY REQUIREMENTS BY CLOUD MODEL

Security Requirement	Private Cloud	Commodity Cloud	Bluelock Virtual Datacenters
Data in motion - encrypted	N/A	Yes	Yes
Data at rest - encrypted	Yes	No	Optional
Audits and certifications	Internal	PCI	AT101, can support PCI and HIPAA
ICSA-compliant firewall	Yes	Yes	Yes
Secure remote access	Yes	Yes	Yes
Backup frequency	24 hours	N/A	24 hours
Multi-site failover	No	No	Optional
Mandatory background checks	No	No	Yes

Table 1: Identifying your organization's security requirements helps to determine which cloud model would best suit your needs.

A detailed list of additional security and privacy guidelines is available from the National Institute of Standards and Technology at http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

PROTECTING DATA IN THE CLOUD - Security concerns among IT organizations choosing to move workloads to the hybrid cloud include controlling access to critical applications and the fear of data breaches or loss. Maintaining the integrity and confidentiality of corporate data in the hands of a cloud service provider raises serious concerns for IT managers who often envision increased risk associated with data that resides in the cloud environment.

However, regular security breaches at commercial and government organizations illustrate that efforts to secure onsite data throughout its lifecycle can expose businesses to the risk of data breaches and reputational damage. So is storing data in a public cloud environment and delivering applications as services putting companies at greater risk to data loss or breaches?

The answer depends on the public cloud that is employed. Sound security practices must be followed by the hybrid cloud service provider, such as

segregating customers first at the network level and then using multi-tenant technologies to ensure there is complete segregation at the storage level and no part of the infrastructure overlaps between customers. In addition, network security capabilities that help prevent malicious attacks on critical systems and ensure only authorized users can access systems hosted in the cloud are imperative. When the cloud hosting service incorporates appropriate physical, operational, and network security into the cloud infrastructure and delivery of its service, companies are assured that data protection will be as good as or even better than in their on-premise data center.

ENSURING BUSINESS CONTINUITY - Another significant concern for organizations opting for hybrid cloud services is the ability of the service provider to deliver continuous service 24/7 of their business-critical applications. Whether concerned with data protection or disaster recovery practices, many IT executives are apprehensive about turning their applications and data over to a service provider, given the impact that downtime can have on employee productivity, client satisfaction, and profitability.

IT executives need assurance that the hybrid cloud service is architected for high availability. Cloud service providers can even improve on a company's existing disaster recovery program, with the ability to duplicate data across geographically distributed servers, which reduces chances of data loss. Their protocols may include replicating data nightly to offsite disk storage while providing on-demand online restoration. Ultimately, a hybrid cloud strategy can potentially offer a better degree of business continuity than when housing data in onsite servers and storage devices.

MEETING COMPLIANCE REQUIREMENTS - Faced with intensifying regulatory requirements, IT organizations are typically concerned with which kinds of security controls are in place in a hybrid cloud environment, and whether they can satisfy auditors. Some companies are especially reluctant to use the public cloud for customer and other sensitive data because of their security and regulatory compliance concerns.

After investigating cloud service providers, they often discover a lack of visibility into security controls or even where primary and secondary data centers are located. They also question whether auditors will have the access needed to perform required audits. While "security through obscurity" might work in some cases, it does nothing to convince today's proactive IT managers that their regulatory compliance obligations can be met after adopting a particular hybrid cloud strategy.

SECURING THE CLOUD: What to Look For in a Hybrid Cloud Service Provider

When investigating hybrid cloud options, and after selecting a service provider and reviewing the master services agreement, make sure you have a clear understanding of the following:

- *Who owns the data you upload into the cloud*
- *Whether you can easily move your workloads back from the cloud service provider to your local environment*
- *Rules around roaming between clouds*
- *Licensing portability*
- *Details on the security controls implemented in their cloud infrastructure*
- *Whether the vendor has achieved compliance against security standards like ISO 27001*
- *Access to documentary proof necessary to demonstrate compliance to an auditor*
- *Who pays for the time the provider spends when you request an audit*

Reading the fine print is vital to guaranteeing that the right security provisions are included in hybrid cloud service-level agreements (SLAs) and contracts, and that the provider is working diligently to help maintain compliance. For instance, be sure that the cloud services company addresses regulatory compliance and security at the environment and user levels. Ensure that the provider is certified for various standards, including Sarbanes-Oxley and AT 101 compliance. In addition, for industries with specific requirements such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations or the Payment Card Industry Data Security Standard (PCI) for companies handling credit card transactions, organizations should work with the cloud provider to develop a solution that aligns with their particular guidelines.

MAINTAINING CONTROL OF THE DATA - When corporate and customer data is no longer stored in an onsite data center, IT managers need to know that they will still have control of the data. Although security and privacy concerns around hybrid cloud services are similar to those of traditional IT services, they tend to escalate with the fear of external control over organizational assets and the potential for mismanagement of those assets.

Migrating to hybrid cloud services means that the cloud provider is responsible for securing the infrastructure that an organization's data and applications operate from. However, IT organizations can and should maintain control of corporate data and applications. While reducing the costs of purchasing and managing the physical hardware and operating system environment, organizations can still have full control over the logical aspects of their systems and the intellectual property that fuels their day-to-day operations. In addition, companies remain in control of moving their data, applications, and workloads back from the cloud service provider to their onsite data center if they decide to modify their cloud strategy.

WHAT MAKES A HYBRID CLOUD SERVICE SECURE?

Following an intensive due diligence process, IT executives must decide on the best mix of public and private cloud services, as well as the right cloud service provider, to meet their unique IT and business objectives. Adequate research into hybrid cloud solutions will succeed in dispelling the typical myths associated with the hybrid cloud. Considering that government organizations with stringent security requirements, such as the U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, and Federal Emergency Management Agency, have adopted public cloud strategies, it is clear that cloud security rumors are being put to rest.[4]

However, as with any IT services, not all clouds are created equal, and security in particular must be evaluated intensely and holistically. One thing that companies should keep in mind while considering the adoption of cloud services is that they already depend on cloud computing in some way. IT departments are delivering software as a service through virtual desktop initiatives. Companies with sophisticated collaboration platforms offer share drives to employees for storing and sharing valuable documents among team members and across geographies. Organizations depend on virtual private networks (VPNs) to provide access to systems for remote employees. Even Wall Street banks store customer data in the cloud through the Salesforce.com customer database. Many companies use ADP payroll services and upload confidential data regularly to the service provider's cloud environment.

Therefore, it is clear that some private and public cloud solutions can be as secure as an on-premise approach to delivering IT services, and companies can be confident that the secure cloud does exist. IT organizations can start by leveraging the practices and technologies already in use in house to protect applications and data, such as intrusion prevention systems, security information management practices, and log management functions. Using these same capabilities to protect systems in the hybrid cloud is no different than protecting data and applications in remote offices.

In the case of hybrid cloud offerings where service providers are responsible for the infrastructure, companies can find themselves ahead of the security curve by leveraging the physical infrastructure, security controls, and security expertise offered by the cloud service provider. Leading cloud providers as a rule possess more security expertise and make use of more current technology to adequately protect the data and applications that reside on their infrastructures.

Cloud providers can bring value by making it easier for organizations to understand how their applications are being attacked by current threats and can even offer firewalls as part of their service. The cloud provider can integrate employee and contractor directories with access control policies, for a centralized and comprehensive approach to managing access to systems in the cloud. Also important, data thefts sometimes involve employees stealing hard drives, so housing data offsite at a hybrid cloud provider's facilities eliminates this potential risk.

Organizations can also gain the net benefit of security requirements demanded by the other tenants in a public cloud environment. Companies may not be able to justify multi-factor security in the data center, AT 101 compliance, or having a Certified Information Systems Security Professional (CISSP) on staff. However, if any of these apply to other tenants in the cloud, all tenants reap the benefits. In

FIND A VMWARE vCLOUD SERVICE PROVIDER

Visit http://vcloud.vmware.com/vcloud-ecosystem/ to access the world's largest enterprise service provider ecosystem and choose a vCloud Service Provider and service type to match your hybrid cloud needs.

addition, instead of organizations trying to solve issues like PCI compliance on their own, which requires the investment in the technologies and practices to accomplish this, companies can spread the cost among all of the tenants.

BLUELOCK'S SECURE HYBRID CLOUD SERVICES

Although security is one of the biggest concerns for companies considering cloud adoption, Bluelock's innovative architecture and heightened emphasis on security provides organizations the assurance they need no matter what type of workloads and data they choose to migrate to the cloud hosting environment. With extensive cloud security expertise, Bluelock can help organizations begin to take strategic steps toward a logical public or hybrid cloud business model that meets their unique business and IT requirements.

Bluelock is a certified provider of the VMware vCloud Datacenter service and offers an enterprise-class cloud service that enables hybrid cloud computing consistent with the technology and management tools that VMware virtualization clients currently use to manage their own private clouds internally.

The VMware vCloud Datacenter service is the highest level of certification a cloud provider can achieve from VMware. The vCloud Datacenter service leverages a platform built on VMware's cloud infrastructure technology including vCloud Director, vCloud API, VMware vSphere, and vShield security. Using these VMware technologies, Bluelock provides a common management and security model that enables workloads to move between internal data centers and the Bluelock hybrid cloud. VMware vCloud Datacenter delivers consistent and auditable security and performance through AT 101 compliance certifications as well as technical capabilities such as network isolation, role-based access control, and directory services integration.

IT managers benefit from visibility into security logs generated by the VMware infrastructure and direction from Bluelock on how to capture and use them. Through a feature of VMware vCloud Datacenter, companies can synchronize their corporate directories with user access with their corporate directory for advanced, end-to-end access control. A virtual firewalling capability built into the VMware vCloud infrastructure software tracks applications as they move through the cloud, ensuring that the correct firewall configuration is in place at any point in the network. In other words, by adopting the VMware vCloud Datacenter provided by Bluelock, companies are adopting the cutting-edge cloud practices of the global leader in virtualization.

CONCLUSION

More and more companies searching for intelligent ways to optimize their IT spend for the greatest flexibility in delivery of services are turning to a hybrid

ABOUT BLUELOCK

Bluelock is an award-winning provider of cloud hosting solutions for the enterprise. Hosted in the public cloud, Bluelock Virtual Datacenters help companies get started quickly and deal with the unknown, while delivering the freedom to change their minds as IT needs evolve. With AT 101-compliant datacenters, Bluelock's VMware vCloud Datacenter service provides world-class SLAs, guaranteeing enterprise-level uptime. The organization prides itself in its engagement model driven by greater control, price visibility, and personal service relationships. Bluelock is a long-term VMware service provider with a shared vision for cloud computing and was one of the first certified VMware vCloud Datacenter service providers.

ABOUT VMWARE

VMware delivers virtualization and cloud infrastructure solutions that enable IT organizations to energize businesses of all sizes. With the industry-leading virtualization platform—VMware vSphere—customers rely on VMware to reduce capital and operating expenses, improve agility, ensure business continuity, strengthen security, and go green. With 2010 revenues of $2.9 billion, more than 250,000 customers and 25,000 partners, VMware is the leader in virtualization, which consistently ranks as a top priority among CIOs. VMware is headquartered in Silicon Valley with offices throughout the world.

cloud approach. IT executives tasked with exploring their options are finding that the hybrid cloud offers the same or better security for their company's business-critical applications and data, dispelling the myths that have caused them to question the sensibility of moving workloads to the cloud.

Leading hybrid cloud providers have the data center infrastructure and expertise to ensure that adequate security is in place to safeguard information in the cloud. The physical, operational, and network processes and controls used in their clouds are commensurate with those used for an organization's internal systems—or better yet, often surpass them. By leveraging the secure hybrid cloud, companies can free up valuable internal IT staff resources, reallocate IT budgets for business innovation, and rest assured that their applications and data will be available 24/7 and will continue to provide competitive advantage.

FOR MORE INFORMATION

- Bluelock Virtual Datacenters:
  http://www.bluelock.com/bluelock-cloud-hosting/virtual-datacenters/
- Bluelock Security:
  http://www.bluelock.com/information-center/security/
- VMware vCloud Datacenter Services:
  http://www.vmware.com/solutions/cloud-computing/public-cloud/vcloud-datacenter-services-providers.html
- VMware Security:
  http://www.vmware.com/solutions/cloud-computing/benefit-cloud-computing/security.html
- Cloud Security Alliance:
  https://cloudsecurityalliance.org/

REFERENCES

1. Worldwide and Regional Public IT Cloud Services 2011–2015 Forecast, IDC, June 2011.
2. IDG Research, "CIO Global Cloud Computing Adoption Survey," January 2011.
3. "Key Issues for Securing Public and Private Cloud Computing, 2011," John Pescatore, Gartner Research.
4. "Cloud Security Fears Exaggerated, Says Federal CIO," Patrick Thibodeau, Computerworld, July 28, 2011. (http://news.idg.no/cw/art.cfm?id=62DE7B46-1A64-67EA-E4E3D0EB9C453EC5)

VMware, Inc. 3401 Hillview Ave., Palo Alto, CA 94304, USA
Tel 877-486-9273, Fax 650-427-5001, www.vmware.com

Bluelock 6325 Morenci Trail, Indianapolis, IN 46268, USA
Tel 888-402-2583 (BLUE), Fax 317-222-3055, www.bluelock.com