netmagic®
An NTT Communications Company

WHITEPAPER

Is my Public Cloud too Public?

Addressing security concerns of the Public Cloud

Enthusiasm for cloud computing has as much to do with economics as technology. Growth in the number of applications and the volume of data that must be managed have made datacenters a major item of corporate expense. Public cloud computing looks like a way to get a handle on some of these costs.

The concept of cloud computing is straightforward: you replace capital-intensive IT assets that must be internally managed with rented "pay-as-you-go" IT capacity and services at commoditized prices. These services are built with new technologies such as virtualization and service-oriented architectures and leverage the Internet to reduce the cost of IT hardware and software resources for computing, networking and storage. At the same time, enterprises are using the same concepts and technologies to build out private clouds to capitalize on centralized, commoditized IT services that meet their security needs.

Today, both public and private cloud deployments must embody an appropriate set of core security principles and thereby assure users and customers of a trustworthy cloud-computing environment.

The main issues with Cloud Security

For many CIO's today, the perceived barriers to Cloud computing remain security, regulation and compliance amongst others.

Organizations seek reassurance on several points: accessing the Cloud will not compromise their security; their sensitive data and intellectual property will be protected; they can retrieve their data if they want to change their current Cloud provider, or their provider winds up operations; and they can maintain their customer service standards and competitive performance.

CIO's 2011 Global Cloud Computing Adoption survey reveals that 56% of the IT and business leaders say managing access to data in the cloud is a top challenge. With the quantum of data being generated, the number of identities and devices accessing the cloud, and the ever-changing infrastructure, these leaders recognize that today, they may not have the needed controls and lack real-time visibility. They can't manage what they can't see and they can't secure what they can't manage. Many organizations have siloed environments that are complex and difficult to manage. In such organizations, the dynamic nature of cloud environments, where data and applications move about at a moment's notice only add to the complexities. However, for organizations with siloed environments, starting with a foundation of virtualization before moving on to the cloud will provide greater visibility than legacy approaches.

Scalability and Multi-tenancy in Public Clouds

Public cloud computing describes a computing architecture that extends the service oriented approach (exemplified insuch concepts as "utility computing," "service-orientedarchitectures" and "software as a service") into amarketplace model. Providers offer services that "run in thecloud" as they are accessible using Internet Protocol andare location independent, meaning that users have no needto know where the underlying IT resources exist.

Cloud services have two hallmarks: They are scalable (therequired resources of storage and computing power can beincreased or decreased based on customers' needs), andthey are multi-tenant (they provide simultaneous, securehosting of services for various customers utilizing the samecloud infrastructure resources).

Perceived risks in Public Cloud

Please indicate your view on the seriousness of each public cloud risk of your organization on a scale of 1 to 5
1= Minimal Risk
3 = Moderate Risk
5 = Extremely Serious Risk

Data Security	**62%**
Data and Systems Integration	**42%**
Data and System Portability	**41%**
Viability of Third-Part Providers	**40%**
IT Governance	**39%**
Service Level Agreements	**35%**
	n=481

Source: PWC IT Outsourcing and Cloud Computing Survey

The good news is…

While the biggest obstacle facing public cloud computing is security, the cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of information technology administrators and security personnel, and lack the economies of scale available to larger organizations with sizeable datacenters.

Potential areas of improvement where organizations may derive security benefits from transitioning to a public cloud-computing environment include the following:

Staff Specialization

Cloud providers, just as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Increases in the scale of computing induce specialization, which in turn allows security staff to shed other duties and concentrate exclusively on security issues. Through increased specialization, there is an opportunity for staff members gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties.

Platform Strength

The structure of cloud computing platforms is typically more uniform than that of most traditional computing centers. Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also benefit from a uniform, homogeneous cloud infrastructure; as do system management activities, such as fault management, load balancing, and system maintenance. Many cloud providers meet standards for operational compliance and certification as well which adds to their credibility.

Resource Availability

The scalability of cloud computing facilities allows for greater availability. Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents. When an incident occurs, an opportunity also exists to capture information more readily, with greater detail and less impact on production. In some cases, however, such resiliency can have a downside. For example, an unsuccessful distributed denial of service attack can quickly consume large amounts of resources to defend against and cause charges to soar, inflicting serious financial damage to an organization.

Backup and Recovery

The backup and recovery policies and procedures of a cloud service may be superior to those of the organization and, if copies are maintained in diverse geographic locations, may be more robust. Data maintained within a cloud can be more available, faster to restore, and more reliable in many circumstances than that maintained in a traditional datacenter. Under such conditions, cloud services could also serve as a means for offsite backup storage for an organization's datacenter, in lieu of more traditional tape-based offsite storage.

Data Concentration

Data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur. Many organizations have already made the transition to support access to organizational data from mobile devices to improve workflow management and gain other operational efficiencies.

Besides providing a computing platform or substitute for in-house applications, public cloud services can also be focused on provisioning security to other computing environments:

Datacenter Oriented

Cloud services can be used to improve the security of datacenters. For example, electronic mail can be redirected to a cloud provider via mail exchange (MX) records, examined and analyzed collectively with similar transactions from other datacenters to discover widespread spam, phishing, and malware campaigns, and to carry out remedial action (e.g., quarantining suspect messages and content) more comprehensively than a single organization would be able to do.

Cloud Oriented

Cloud services are available to improve the security of other cloud environments. Cloud-based identity management services can be used to augment or replace an organization's directory service for identification and authentication of users to a cloud.

The not so good news is…

Besides its many potential benefits for security and privacy, public cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional datacenters. Some of the more fundamental concerns include the following:

System Complexity

A public cloud-computing environment is extremely complex compared with that of a traditional datacenter. Many components comprise a public cloud, resulting in a large attack surface. Besides components for general computing, such as deployed applications, virtual machine monitors, guest virtual machines, data storage, and supporting middleware, there are also components that comprise the management backplane, such as those for self-service, resource metering, quota management, data replication and recovery, workload management, and cloud bursting. Cloud services themselves may also be realized through nesting and layering with services from other cloud providers. Components change over time as upgrades and feature improvements occur, confounding matters further.

Shared Multi-tenant Environment

Subscribing organizations typically share components and resources with other subscribers that are unknown to them. With threats to network and computing infrastructures increasing and becoming more sophisticated year on year, sharing an infrastructure with unknown outside parties can be a major drawback for some applications.This will require a high level of assurance for the strength of the security mechanisms used for logical separation. While not unique to cloud computing, logical separation is a non-trivial problem that is exacerbated by the scale of cloud computing. Access to organizational data and resources could inadvertently be exposed to other subscribers through a configuration or software error. An attacker could also pose as a subscriber to exploit vulnerabilities from within the cloud environment to gain unauthorized access.

Internet-facing Services

Public cloud services are delivered over the Internet; exposing both the administrative interfaces used to self-service an account and the interfaces for users and applications to access other available services. Applications and data that were previously accessed from the confines an organization's intranet, but moved to the cloud, face increased risk from network threats that were previously alleviated at the perimeter of the organization's intranet. Further, these applications and data after moving to the cloud are subject to new threats that target the exposed interfaces.

Loss of Control

While security and privacy concerns in cloud computing services are similar to those of traditional non-cloud services, they are augmented by external control over organizational assets and the potential for mismanagement of those assets. Migrating to a public cloud requires a transfer of control to the cloud provider over information as well as system components that were previously under the organization's direct control. Loss of control over both the physical and logical aspects of the system and data diminishes the organization's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization.

Compliance

Many business units are being drawn into using cloud services by the attractive economics, bypassing IT departments to host their applications and data in the cloud directly. This creates several problems for the IT organizations with reduced internal and external control. The business units' activities multiply the IT department's compliance challenges even while legal and compliance departments are expecting the IT departments to be able to report on and demonstrate control over sensitive information. Additionally, a cloud provider's SAS-70 compliance must be carefully assessed by each enterprise customer to see if the certification meets the compliance policy established by their own enterprise.

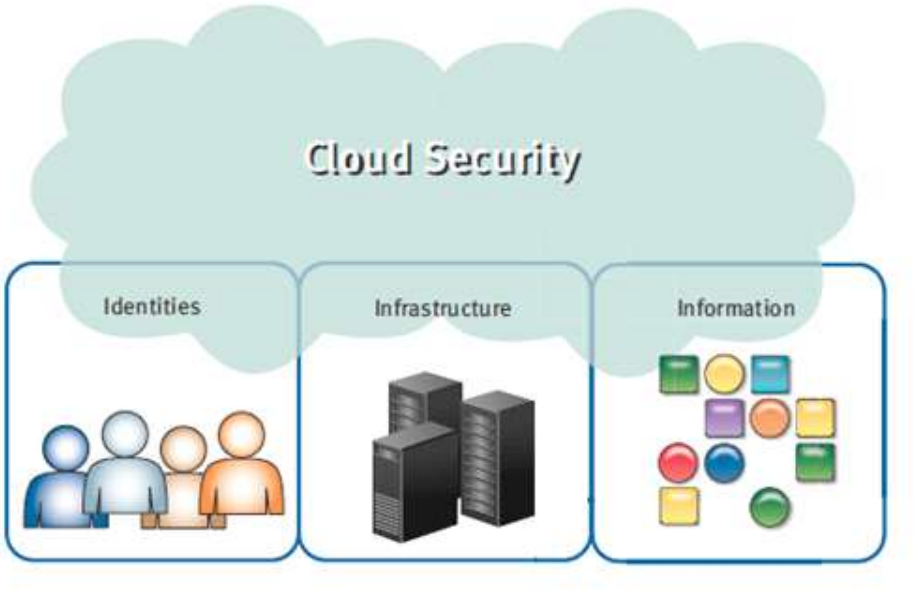
Portability between public clouds

While cloud computing conveys a promise of open architecture and easy integration, the early cloud offeringshave tended to create security "silos" - users need an Amazon account to use Amazon's EC2 service and a Google account to access App Engine applications. Enterprises will require information and identity portability between varying clouds so that they can mix and match their services in an open, standards-based environment that permits interoperability.

Taking the bull by its horns - Secure Identity, Information, Infrastructure

Public cloud computing requires a security model that reconciles scalability and multi-tenancy with the need for trust. As enterprises move their computing environments with their identities, information and infrastructure to the cloud, they must be willing to give up some level of control. To do that, they must be able to trust cloud systems and providers, and verify cloud processes and events. Important building blocks of trust and verification relationships include access control, data security, compliance and event management – all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud.

Securing the Public Cloud



End-to-end identity management, third-party authentication services, and federated identity will become a key element f cloud security. Identity security preserves the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components will be a major requirement for cloud computing, and identity will have to be managed in ways that build trust. It will require:

Strong authentication:
Cloud computing must move beyond weak username-and-password authentication if it is going to support the enterprise. This will mean adopting techniques and technologies that are already standard in enterprise IT such as strong authentication (multi-factor authentication with one-time password technology), federation within and across enterprises, and risk-based authentication that measures behavior history, current context and other factors to assess the risk level of a user request. Additional tiering of authentication will be essential to meet security SLAs, and utilizing a risk-based authentication model that is largely transparent to the users will actually reduce the need for broader federation of access controls.

More granular authorization:
Authorization can be coarse-grained within an enterprise or even a private cloud, but in order to handle sensitive data and compliance requirements, public clouds will need granular authorization capabilities (such as role-based controls and Information Rights Management (IRM)) that can be persistent throughout the cloud infrastructure and the data's lifecycle.control, data security, compliance and event management – all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud.

Information security

In the traditional datacenter, controls on physical access, access to hardware and software and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. To compensate, security will have to become information centric. The data needs its own security that travels with it and protects it. It will require:

Data isolation:
In multi-tenancy situations, data must be held securely in order to protect it when multiple customers use shared resources. Virtualization, encryption and access control will be workhorses for enabling varying degrees of separation between corporations, communities of interest and users. In the near future, data isolation will be more important and executable for IAAS, than perhaps for PAAS and SAAS.

More granular data security:
As the sensitivity of information increases, the granularity of data classification enforcement must increase. In current datacenter environments, granularity of role-based access control at the level of user groups or business units is acceptable in most cases because the information remains within the control of the enterprise itself. For information in the cloud, sensitive data will require security at the file, field, or even block level to meet the demands of assurance and compliance.

Consistent data security:
There will be an obvious need for policy-based content protection to meet the enterprise's own needs as well as regulatory policy mandates. For some categories of data, information centric security will necessitate encryption in transit and at rest, as well as management across the cloud and throughout the data life cycle.

Effective data classification:
Cloud computing imposes are source trade-off between high performance and the requirements of increasingly robust security. Data classification is an essential tool for balancing that equation. Enterprises will need to know what data is important and where it is located as prerequisites to making performance cost/benefit decisions, as well as ensuring focus on the most critical areas for data loss prevention procedures.

Information rights management (IRM):
IRM is often treated as a component of identity, a way of setting broad-brushcontrols on which users have access to which data. But more granular data-centric security requires that policies and control mechanisms on the storage and use of information be associated directly with the information itself.

Governance and compliance:
A key requirement of corporate information governance and compliance is the creation of management and validation information –monitoring and auditing the security state of the information with logging capabilities. Here, not only is it important to document access and denials to data, but to ensure that IT systems are configured to meet security specifications and have not been altered. Expanding retention policies for data policy compliance will also become an essential cloud capability. In essence, cloud computing infrastructures must be able to verify that data is being managed per the applicable local and international regulations (such as PCI and HIPAA) with appropriate controls, log collection and reporting.

Sensitive data in the cloud will require granular security,maintained consistently throughout the data lifecycle.

Infrastructure security

The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS. It will require:

Inherent component-level security:
The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components, and, finally,supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust. For these flexibly deployed components, device fingerprinting to ensure secure configuration and state will also be an important security element, just as it is for the data and identities themselves.

More granular interface security:
The points in the system where hand-offs occur – user-to-network, server-toapplication– require granular security policies and controls that ensure consistency and accountability. Here, either the end-to-end system needs to be proprietary, a de facto standard, or a federation of vendors offering consistently deployed security policies.

Resource lifecycle management:
The economics of cloud computing are based on multi-tenancy and the sharing of resources. As a customer's needs and requirements change, a service provider must provision and decommission those resources – bandwidth, servers, storage, and security – accordingly. This lifecycle process must be managed for accountability in order to build trust.

The ideal cloud equation

Control + Visibility = Trust

A cloud deployment that overcomes these myths is built on trust. Trust cannot be achieved without control and visibility across the cloud infrastructure, identities, and information.

Control

Availability:
Ensure access to resources and recovery following disruption or failure

Integrity:
Guarantee only authorized personnel can access specific information and applications.

Confidentiality/privacy:
Protect how information and personal data is obtained and used.

Visibility

Compliance:
Meet specific legal requirements and industry standards and rules.

Governance:
Establish usage rights and enforce policies, procedures, and controls.

Risk management:
Manage threats to business disruptions or derived exposures.

Changing realities

Cloud computing promises to change the economics of the data center, but before sensitive and regulated data move into the public cloud, issues of security standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections, and regulatory reporting. All are elements of a secure identity, information and infrastructure model, and are applicable to private and public clouds as well as to IAAS, PAAS and SAAS services.

While security emerges as a major concern among the barriers to adoption of cloud computing, the key to understanding security in cloud computing is to realize that the technology is not new, or untested. It represents the logical progression to outsourcing of commodity services to many of the same trusted IT providers we have already been using for years.

Having said that, cloud security is part of the inevitable progression of IT. It must be embraced by organizations to stay competitive. Companies who approach cloud computing in a mature manner need not be afraid about entering the cloud because of security concerns. Dealing with security in the cloud is no more difficult than addressing it internally. And there are steps you can take that can make cloud security just as effective-or even more so-as your internal IT.