


A background image showing a person's hand pointing at a laptop screen. Overlaid on the image are several semi-transparent circular gauges or dials with numerical markings, suggesting data analysis or security metrics.

Addressing Data Security Challenges in the Cloud

Coordinate Security. 

A red circular icon containing a white arrow pointing to the right.

The Need for Cloud Computing Security

A Trend Micro White Paper | July 2010

I. INTRODUCTION

Enterprises increasingly recognize cloud computing's compelling economic and operational benefits. Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerates deployment of new applications. However, those valuable business benefits cannot be unlocked without addressing new data security challenges posed by cloud computing.

Deploying confidential information and critical IT resources in the cloud raises concerns about vulnerability to attack, especially because of the anonymous, multi-tenant nature of cloud computing. Applications and storage volumes often reside next to potentially hostile virtual environments, leaving information at risk to theft, unauthorized exposure or malicious manipulation. Moreover, it's possible for remnant data to persist when consumers vacate cloud volumes but vendors do not recycle storage devices securely. Governmental regulation of data privacy and location presents the additional concern of significant legal and financial consequences if data confidentiality is breached, or if cloud providers inadvertently move regulated data across national borders.

As a global leader in content security, Trend Micro has pioneered SecureCloud – a next-generation advancement that enables enterprises and other organizations to operate safely and securely in the cloud. SecureCloud represents a patented security infrastructure specifically engineered to control the security and privacy of data deployed to any cloud computing environment.

II. CLOUD COMPUTING DEFINED

Cloud computing is the latest extension of an evolution in distributed computing that takes advantage of technology advances. The cloud's roots date back to early mainframe processing, when users connected to a shared computing resource through terminals to solve their computing needs. The advent of faster and cheaper microprocessors, RAM and storage brought computing into the client-server model, which grouped sets of users into networks sharing computing power on decentralized commodity servers. As bandwidth became more ubiquitous, speedier, and less costly, these networks interconnected to form the Internet. IT departments typically provisioned their datacenters in house, protected inside a firewall.

Eventually, enterprises took advantage of higher throughputs to reexamine the need for monolithic onsite datacenters. Accessing servers virtually through a browser window presented substantial advantages in software and hardware maintenance. Software vendors began capitalizing on the concept that a scaled datacenter could also deliver remote content to customers almost immediately at a reduced cost, giving rise to on-demand Software-as-a-Service. Today's mature virtualization platforms now enable contemporary cloud computing: a new model of rapid, on-demand, low-cost, al-a-carte computing.

Like its predecessors, present-day cloud computing features a multitude of users connected to remote computing resources over the Internet. Cloud computing delivers software and services over networked connections, relying on a steady flow of throughput to and from the virtualized datacenter in order to maintain high service levels. Thanks to scalable virtualization technology, cloud computing gives users access to a set of pooled computing resources that share the following attributes:

- Multi-tenancy
- Highly scalable and elastic
- Self-provisioned
- Pay-per-use price model

In contrast to the significant capital expenditures it takes to purchase and provision the launch of a traditional in-house operational site, as well as the months of lead time that effort involves, cloud computing lets administrators spin up virtual servers at will. They can provision necessary storage and launch an operational site within minutes or hours and for a fraction of historical costs.

III. TYPES OF CLOUDS

Several different configurations of cloud computing and its deployment models exist to serve the enterprise's needs. Each approach offers its own strengths, risks, and level of control it provides the cloud consumer. See figure 1 for a representation of the types and deployments models.

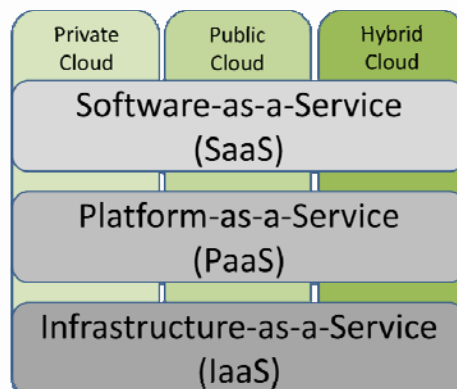


Figure 1: Types of Clouds

SOFTWARE AS A SERVICE

In an October 2009 publication, Peter Mell and Tim Grance of the U.S. National Institutes of Standards & Technology (NIST) defined Software as a Service (SaaS) as the capability for a consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure – including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. An example of SaaS would be online tax filing.

PLATFORM AS A SERVICE

Platform as a Service (PaaS) provides the cloud consumer with the capability to deploy applications onto the cloud platform using programming languages and tools that are supported by the cloud provider. The cloud consumer does not manage or control the underlying cloud infrastructure – including network, servers, operating systems, or storage, which is all fully managed by the cloud provider. However, the cloud consumer can control the deployed applications and possibly the application hosting environment configurations. Microsoft™ Azure and Google App engine are examples of PaaS.

INFRASTRUCTURE AS A SERVICE

Infrastructure as a Service (IaaS) gives the cloud user the most control of the three types of clouds. The cloud consumer has the ability to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software such as operating systems and applications. Although the cloud consumer has control over the operating system, storage and deployed applications, the cloud provider is still responsible for the control of the underlying cloud infrastructure. However businesses using the IaaS cloud service model are typically responsible for securing their own virtual machines and the applications and data that reside on them. Amazon EC2 or vCloud are examples of IaaS.

CLOUD FORMATIONS

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

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, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.*

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.*

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).*

Source: The NIST Definition of Cloud Computing, October 2009

IV. CLOUD COMPUTING SECURITY CHALLENGES

In traditional datacenters, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves. In the private and public cloud, however, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers.

MULTI-TENANCY

Cloud computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions. The virtual machine running next to the consumer's environment could be malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system.

Because the cloud consumer's data sits on common storage hardware, it could become compromised through lax access management or malicious attack. In a joint paper published in November 2009 by MIT and UCSD entitled "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," the authors exhibited the possibility of a side-channel attack in a cloud environment in which an attacker would be able to implant some arbitrary code into a neighbor's VM environment with little to no chance of detection.

In another scenario, a security bulletin from Amazon Web Services reported that the Zeus Botnet was able to install and successfully run a command and control infrastructure in the cloud environment.

DATA MOBILITY AND CONTROL

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries. Further, legislation such as the US Patriot Act allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners' consent.

DATA REMANENCE

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

DATA PRIVACY

The public nature of cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

V. SOLVING THE CLOUD SECURITY CHALLENGE: TREND MICRO SECURECLOUD

SecureCloud alleviates data security and privacy risks associated with deploying information into any cloud-computing environment. SecureCloud's patented key-management technology combined with industry-standard encryption allows businesses to control access to sensitive data stores and operate safely in public, private and hybrid clouds.

EASY DEPLOYMENT

With a simple agent installed on the virtual machine image, SecureCloud is able to ensure that data in the cloud environment is tamper proof, protected through encryption at the kernel level. Communication between the agent and SecureCloud management server is secure, thus avoiding the risk of any man-in-the-middle attacks to gain access to the encryption keys.

SECURE KEY MANAGEMENT

With SecureCloud, cloud consumers have exclusive control of the encryption keys, and therefore control of their own data. The encryption key management is not hosted by the cloud service provider, but rather by Trend Micro or by the cloud consumers themselves. This provides the cloud consumers the ability to take advantage of the cloud services, but still maintain full control of the encryption keys within their environments.

SecureCloud uses VM-level encryption, which provides the ability to encrypt data in the working storage, while using different keys for each cloud consumer's information. This feature mitigates the risk of compromise between cloud consumers if one were to obtain recycled disk blocks from another cloud consumer or fall victim to a configuration error that would otherwise compromise data privacy.

INDUSTRY STANDARD ENCRYPTION

SecureCloud uses industry standard AES encryption to make data unreadable and unusable to those without the encryption key. Rendering the data useless greatly reduces the risks associated with data theft, exposure to unauthorized parties or data seizure through judicial subpoena. SecureCloud's ability to encrypt data adds additional benefits to the cloud consumer when changing vendors or terminating storage agreements. Any encrypted data remaining on vendor storage devices is unrecognizable and secure.

GRANULAR CONTROL

SecureCloud's unique policy-based approach to key management and data access allows users to determine exactly which server gets access to secure data. Virtual servers spinning up in the cloud consumer's environment must first authenticate to the SecureCloud key server with credentials that have been encrypted in the virtual machine's kernel. Based on the defined policies, information provided back to the key management server is then vetted, ensuring the cloud environment is safe to release the keys into. Along with detailed key management policies, SecureCloud offers role-based access to the administrators, with specific permission levels ranging from full access, key approval, to audit logging only.

CUSTODY OF ENCRYPTION KEYS

SecureCloud helps users control data access with the option of isolating the physical storage of keys away from the cloud infrastructure provider. This stops infrastructure administrators from accessing data or keys and gives customers the freedom to move data from one provider to another without the fear of vendor lock-in. SecureCloud's on-premise solution gives customers even more control by keeping keys within their trusted environment and controlling custody at all times. Further, if a regulatory agency presents vendors with subpoenas and seizes data without informing or getting consent from data owners, the encrypted volumes remain useless without the encryption keys.

REPORTING

SecureCloud accommodates the frequent need to view system configuration settings by providing a full audit trail of key approvals occurring on the management server. SecureCloud also offers detailed logging and reporting for any actions performed within the system and any key approvals. All events and changes, whether they come from an administrator or the system itself, are logged and can be called upon for a full detailed audit trail.

VI. CONCLUSION

As enterprises make plans to deploy applications in private and public cloud environments, new security challenges need to be addressed. Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines; centralized key management that allows the user (and not the cloud provider) to control cloud data; and ensuring that cloud data is accessible according to established enterprise policies.

Trend Micro SecureCloud empowers businesses to operate securely in the cloud through the use of encryption and patented key management that protects and manages data in virtualized environments. By giving enterprises control over how and where data is accessed, it allows them the flexibility to move between cloud vendors without being tied to any one provider's encryption system. SecureCloud defends information against manipulation or theft, helps ensure compliance with encryption requirements and automatically facilitates the delegation of encryption keys. Delivered as an on-premise console or a Software-as-a-Service, SecureCloud represents a complete solution for safeguarding information in private clouds and public Infrastructure-as-a-Service environments.

© 2010 Trend Micro, Incorporated. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. (WP01_VirtSec_080911US)