Cloud Computing Security

Server Security

Making Virtual Machines Cloud-Ready

A Trend Micro White Paper | May 2010

CLOUD COMPUTING
MAKING VIRTUAL MACHINES CLOUD-READY

I. INTRODUCTION

Cloud computing has been compared to the early proliferation of electricity. Homes, businesses and towns did not want to produce or rely on their own source of power. They began connecting into a greater power grid, supported and controlled by power utilities. Along with this utility connection came time and cost savings, in addition to greater access to, and more reliable availability of power.

Similarly, cloud computing represents a significant opportunity for service providers and enterprises. Relying on cloud computing, enterprises can achieve cost savings, flexibility, and choice for computing resources. They are looking to cloud computing to expand their on-premise infrastructure, by adding capacity on demand.

This paper covers the delivery model of cloud computing that is also called utility computing, or Infrastructure as a Service (IaaS). It looks at the security implications and challenges that IaaS presents and offers best practices to service providers and enterprises hoping to leverage IaaS to improve their bottom line in this severe economic climate.

II. THE CLOUD COMPUTING OPPORTUNITY

Looking outside the organization to gain increased competitiveness is not new—it is simply outsourcing. So why has there been so much hype and excitement around cloud computing?

Industry Momentum: Industry analysts and companies like Amazon, Citrix, Dell, Google, HP, IBM, Microsoft, Sun, VMware and many others appear unanimous in support of cloud computing. Throughout 2009, the VMware vCloud initiative continued to win recognition and awards for its key technology role in bringing service providers, applications and technologies together to deliver the next generation of flexible, reliable IT services to enterprises through private clouds, public clouds, and hybrid cloud environments.

NIST Cloud Computing Service Models

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but does control the deployed applications and possibly application hosting environment configurations.

Cloud Software as a Service (SaaS). The capability provided to the consumer is 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.

The US National Institutes of Standards & Technology (NIST) Definition of Cloud Computing
Peter Mell and Tim Grance, October 2009

Flexibility: The flexibility for enterprises is unprecedented. Enterprises can choose to outsource hardware while maintaining control of their IT infrastructure; they can fully-outsource all aspects of their infrastructure; or, often driven by departmental initiatives, enterprises are deploying both fully and partially outsourced segments of their infrastructures.

Cost Savings: Infrastructure on demand leads to more efficient IT spending. Restrictions on headcount and capital expenditures often hold back innovation. Seasonal demands spike capacity requirements and require a robust infrastructure that is frequently underutilized. Cloud computing is a cost-effective alternative.

Mobility and Choice: Technology is leading the evolution. Virtualization technologies like VMware enable applications and services to be moved from internal environments to public clouds, or from one cloud service provider to another.

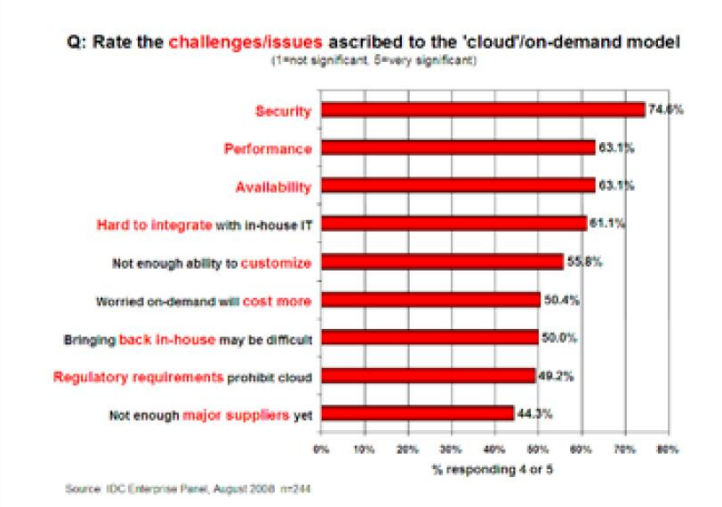
How are you flying in the cloud?

Enterprises are flying in the cloud in two ways. First, CIOs, recognizing that increased competitive advantage, cost savings, expanded capacity and failover flexibility are just too enticing to pass up, are looking at cloud computing and asking how they can maintain security policy and compliance integrity in this new and dynamic environment. Second, departments or workgroups, eager for immediate computing resources and results, are jumping at cloud computing, possibly oblivious to the security implications of putting critical applications and data in cloud

SCALABILITY:

Infrastructure as a Service (IaaS) is synonymous with scalability. Is there an immediate need for servers, but no time to complete capital acquisitions? All you need is a credit card to get infrastructure on demand. Departments and SMBs (including smaller service providers/MSPs) that need capacity on demand are poised to take advantage of cloud computing. Disaster recovery and redundancy are also high-impact opportunities to leverage cloud computing.

Cloud computing extends an enterprise's ability to meet the computing demands of its everyday operations. Put simply, leveraging cloud computing offers significant benefits, including flexibility and choice, mobility and scalability, all coupled with potential cost savings. However, the area that is causing organizations to hesitate most when it comes to moving business workloads into public clouds is security.



For example, IDC conducted a survey of 263 IT executives/CIOs and their line-of-business (LOB) colleagues to gauge their opinions and understand their companies' use of IT Cloud Services. Security ranked first as the greatest challenge or issue attributed to cloud computing.

"By far, the #1 concern about cloud services is security. With their businesses' information and critical IT resources outside the firewall, customers worry about their vulnerability to attack."

—Frank Gens, Senior Vice President and Chief Analyst, IDC

III. SECURITY AND COMPLIANCE IN CLOUD COMPUTING

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. CIOs, recognizing that increased competitive advantage, cost savings, expanded capacity and failover flexibility are just too enticing to pass up, are looking at cloud computing and asking:

- Will I still have the same security policy control over my applications and services?
- Can I prove to my organization and my customers that I am still secure and meeting my SLAs?
- How can I minimize the scope of a compliance audit?
- Am I still compliant, and can I prove it to my auditors?

To begin to answer these questions, let's quickly look at the security of the traditional datacenter and the impact of virtualization technology, which is enabling the cloud computing revolution.

TRADITIONAL DATACENTER SECURITY

The word 'datacenter' has long evoked images of massive server farms behind locked doors, where electricity and cooling were as important as network security to maintain reliability and availability of data. Perimeter security controls are the most common approach taken for traditional datacenter security. This approach typically includes perimeter firewall, demilitarized zones (DMZ), network segmentation, network intrusion detection and prevention systems (IDS/IPS) and network monitoring tools.

VIRTUALIZATION – THE CATALYST OF THE CLOUD

Advancements in virtualization technologies enable enterprises to get more computing power from the underutilized capacity of physical servers. The traditional datacenter footprint is shrinking to enable cost savings and "greener" IT through server consolidation. Enterprises and service providers are using virtualization to enable multi-tenant uses of what used to be single-tenant or single-purpose physical servers.

Extending virtual machines to public clouds causes the enterprise network perimeter to evaporate and the lowest-common denominator to impact the security of all. The inability of physical segregation and hardware-based security to deal with attacks between virtual machines on the same server highlights the need for mechanisms to be deployed directly on the server, or virtual machines.

Deploying this line of defense at the virtual machine itself enables critical applications and data to be moved to cloud environments.

IV. CLOUD SECURITY CHALLENGES

At first glance, the security requirements for cloud computing providers would appear to be the same as traditional datacenters — apply a strong network security perimeter and keep the bad guys out. However, as previously stated, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. For cloud computing providers to gain from the efficiencies of virtualization, virtual machines from multiple organizations will need to be co-located on the same physical resources. The following outlines some of the primary concerns that enterprises should be aware of when planning their cloud computing deployments.

ADMINISTRATIVE ACCESS TO SERVERS AND APPLICATIONS

One of the most important characteristics of cloud computing is that it offers "self-service" access to computing power, most likely via the Internet. In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in system control.

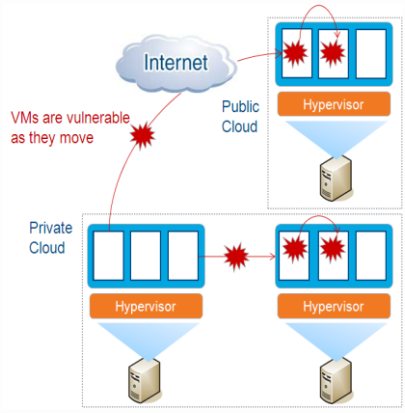
DYNAMIC VIRTUAL MACHINES: VM STATE AND SPRAWL

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

VULNERABILITY EXPLOITS AND VM-TO-VM ATTACKS

Cloud computing servers use the same operating systems, enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition, co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems need to be able to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualized cloud environment.

> *"As more and more workloads are virtualized, as workloads of different trust levels are combined and as virtualized workloads become more mobile, the security issues associated with virtualization become more critical to address.*
> *Survey data from Gartner conferences in late 2009 indicated that about 40% of virtualization deployment projects were undertaken without involving the information security team in the initial architecture and planning stages."*
>
> **Gartner**, *"Addressing the Most Common Security Risks in Data Center Virtualization Projects," January 2010*



SECURING DORMANT VIRTUAL MACHINES

Unlike a physical machine, when a virtual machine is offline, it is still available to any application that can access the virtual machine storage over the network, and is therefore susceptible to malware infection. However, dormant or offline VMs do not have the ability to run an antimalware scan agent. Dormant virtual machines may exist not just on the hypervisor but can also be backed up or archived to other servers or storage media. In cloud computing environments, the responsibility for the protection and scanning of dormant machines rests with the cloud provider. Enterprises using cloud computing should look for cloud service providers that can secure these dormant virtual machines and maintain cohesive security in the cloud.

PERFORMANCE IMPACT OF TRADITIONAL SECURITY

Existing content security solutions were created prior to the concept of x86 virtualization and cloud computing and were not designed to operate in cloud environments. In a cloud environment, where virtual machines from different tenants share hardware resources, concurrent full system scans can cause debilitating performance degradation on the underlying host machine. Cloud service providers providing a baseline of security for their hosting clients can address this problem by performing resource-intensive scans at the hypervisor level thereby eliminating this contention at the host level.

DATA INTEGRITY: CO-LOCATION, COMPROMISE AND THEFT

According to the 2009 Data Breach Investigations Report conducted by Verizon Business Risk Team, 64% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are neither being tampered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored.

ENCRYPTION AND DATA PROTECTION

Many regulations and standards such as the PCI DSS and HIPAA include requirements for the use of encryption to protect critical information—such as cardholder data and personally identifiable information (PII)—to achieve compliance or safe harbor in the event of a breach. The multi-tenant nature of the cloud amplifies these requirements and creates unique challenges with the accessibility and protection of encryption credentials used to ensure data protection.

"This year's findings continue to support the idea that a patch deployment strategy focusing on coverage and consistency is far more effective at preventing data breaches than "fire drills" attempting to patch particular systems as quickly as possible."
2009 Data Breach Investigations Report, Verizon Business Risk Team

PATCH MANAGEMENT

The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

POLICY AND COMPLIANCE

Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources.

> *"…we are no longer needed by our customers to acquire and use these technologies. But the real CIO power comes from her ability to help her organization and her customers use these technologies for 'good'."*
> **Linda Cureton, CIO, NASA, Goddard Space Flight Center**

PERIMETER PROTECTION AND ZONING

In cloud computing, the enterprise perimeter evaporates and the lowest-common denominator impacts the security of all. The enterprise firewall, the foundation for establishing security policy and zoning for networks, can either no longer reach cloud computing servers, or its policies are no longer in the control of the resource owner, but the responsibility of the cloud computing provider. To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself.

ROGUE CORPORATE RESOURCES

Eager for immediate computing resources and results, non-IT savvy individuals and groups are jumping at cloud computing. Important corporate data and applications are being deployed in the cloud, possibly oblivious to the security implications.

V. MAKING VIRTUAL MACHINES CLOUD–READY

Virtualization is the enabling technology for cloud computing. Organizations not leveraging cloud computing today are likely looking to cloud computing for tomorrow. Datacenters that have consolidated physical servers to multiple virtual machine instances on virtualized servers can take immediate steps to increase security in their virtualized environment, as well as prepare these virtual machines for the migration to cloud environments when appropriate.

The following outlines distinct security technologies—firewall, intrusion detection and prevention, integrity monitoring, log inspection, malware protection, and cloud encryption and data control—that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environments.

FIREWALL

Decreasing the attack surface of virtualized servers in cloud computing environments.

A bi-directional stateful firewall, deployed on individual virtual machines, can provide centralized management of server firewall policy. It should include pre-defined templates for common enterprise server types and enable the following:

- Virtual machine isolation
- Fine-grained filtering (Source and Destination Addresses, Ports)
- Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
- Coverage of all frame types (IP, ARP, …)
- Prevention of Denial of Service (DoS) attacks
- Ability to design policies per network interface
- Detection of reconnaissance scans on cloud computing servers
- Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources

INTRUSION DETECTION AND PREVENTION (IDS/IPS)

Shield vulnerabilities in operating systems and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks.

As previously noted, virtual machines and cloud computing servers use the same operating systems, enterprise and web applications as physical servers. Deploying intrusion detection and prevention as software on virtual machines shields newly discovered vulnerabilities in these applications and OSs to provide protection against exploits attempting to compromise virtual machines. In particular, vulnerability rules shield a known vulnerability—for example, those disclosed monthly by Microsoft—from an unlimited number of exploits.

INTEGRITY MONITORING

Monitoring files, systems and registry for changes

Integrity monitoring of critical operating system and application files (files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

An integrity monitoring solution should enable:

- On-demand or scheduled detection
- Extensive file property checking, including attributes (enables compliance with PCI 10.5.5)
- Directory-level monitoring
- Flexible, practical monitoring through includes/excludes
- Auditable reports

LOG INSPECTION

Visibility into important security events floating in log files in cloud resources

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

- Suspicious behavior detection
- Collection of security-related administrative actions
- Optimized collection of security events across your datacenter

VIRTUALIZATION-AWARE MALWARE PROTECTION

Closes security gaps unique to virtualized and cloud environments

Virtualization-aware malware protection leverages hypervisor introspection APIs such as the VMware VMsafe APIs to secure both active and dormant virtual machines. Layered protection uses dedicated scanning virtual machines coordinated with real-time agents within each virtual machine. This ensures that virtual machines are secure when dormant and ready to go with the latest pattern updates whenever activated. Virtualization-aware malware protection can also preserve performance profile of virtual servers by running resource-intensive operations such as full system scans from a separate scanning virtual machine. These measures ensure:

- Prevention of malware impact on active and dormant virtual machines
- Protection from attacks that uninstall, inhibit, or fraudulently patch antivirus security
- Tight integration with virtualization management consoles such as VMware vCenter
- Automatic security configuration of new virtual machines

CLOUD-READY ENCRYPTION AND RETAINING CONTROL OF DATA IN THE CLOUD

Ensures control of data in cloud environments

Placing sensitive data outside of the datacenter in the public cloud poses a new IT challenge, and enterprises need to plan to retain control of such data. Control comes in the form of controlling the data used in their cloud-based virtual machines and validating that cloud data is made accessible to the right parties and in the right location. The cloud poses new challenges for auditing, and encryption with enterprise-controlled key management enables IT to comply with security best practices, internal governance and external regulation. As a result, enterprises realize a significant reduction in the scope of compliance audits. Such enterprise-controlled encryption and key management enable portability between cloud vendors, as data security is not tied to any single cloud vendor. Best cloud security practices should include:

- Encryption of sensitive data used by cloud-based virtual machines
- Centralized encryption key management for cloud data controlled by the enterprise to facilitate portability and retain business power, separate from an individual cloud vendor
- Ensuring that cloud data is accessible according to enterprise policies

SECURITY DEPLOYMENT CONSIDERATIONS

Cloud computing deployments are going to increase over time. Virtual environments that deploy the above mentioned security mechanisms on virtual machines, effectively make these VMs cloud-ready. Three additional considerations will help to maximize the effectiveness of any security deployment:

- Software agents on virtual machines enable greater security for these virtual machines. Consolidating protection mechanisms will enable economies of scale, deployment and ultimately cost savings for enterprises and service providers.
- Enterprises will not likely move all computing to cloud resources. Any security mechanisms should be consistent across physical, virtual and cloud computing instances of servers and applications. Such security mechanisms also need to span multiple cloud providers to facilitate portability between vendors should business circumstances require such movement. These deployments should also be able to be centrally managed and integrated with existing security infrastructure investments such as virtual integration tools (for example, VMware vCenter), security information and event management solutions (like ArcSight, NetIQ, and RSA Envision), enterprise directories (Active Directory) and software distribution mechanisms (such as Microsoft SMS, Novel Zenworks and Altiris).
- Many tools that are currently deployed, such as software firewall and host-based intrusion prevention systems (HIPS), may migrate seamlessly to cloud environments. In addition, free tools and software, such as VM Protection, are available for deployment in virtual and cloud environments.

VI. GETTING STARTED TODAY

Cloud computing, like all variations of computing preceding it, involves security risks and challenges. This does not mean that it should be avoided, or delayed. The resulting benefits are potentially too great to forego.

As an enterprise investigating cloud computing, review the cloud computing security challenges described in this paper and consider the following:

- Is cloud computing currently in use in your organization? Are those deployed applications or data, critical to business continuity? Are they meeting or breaching existing corporate security policy? Are they causing undue exposure to existing enterprise resources?
- What security mechanisms currently in place on the enterprise network will not migrate to the cloud, and what exposure does this represent?
- What virtualization platform does the chosen cloud computing service provider offer? Does it enable the enterprise to move resources securely and freely, to and from the cloud?
- Which security software can be used to provide sufficient protection to begin moving virtual machines to cloud environments? While providing some baseline security for their environment, cloud service providers typically place the responsibility for data and application security with their customers. Software tools such as VM Protection allow enterprises to quickly provide a line of defense for cloud computing resources.

For cloud computing service providers, consider:

- Is the virtualization platform readily able to accept existing virtual machines from enterprise customers migrating existing resources to our cloud environments?
- How do we help customers meet zoning and segregation requirements on resources in our cloud environments, while maintaining lowest total cost of ownership by maximizing the benefits of fully-shared virtual resources?
- What security mechanisms can we deploy or recommend to enable our customers' virtual machines to become cloud-ready?

VII. SUMMARY

Cloud computing service providers are leveraging virtualization technologies, combined with self-service capabilities, to offer cost-effective access to computing resources via the Internet. For cloud computing service providers to gain the most from the efficiencies of virtualization, virtual machines from multiple organizations need to be co-located on the same physical resources. Enterprises looking to cloud computing to expand their on-premise infrastructure must be aware of the security challenges that may compromise the compliance integrity and security of their applications and data.

Extending virtual machines to public clouds causes the enterprise network perimeter to evaporate and the lowest common denominator of protection to impact the security of all. The inability of physical segregation and hardware-based security to deal with attacks between virtual machines on the same server highlights the need for mechanisms to be deployed directly on the server, or virtual machines.

Deploying a line of defense including firewall, intrusion detection and prevention, integrity monitoring, log inspection, and malware protection as software on virtual machines is the most effective method to maintain integrity of compliance and preserve security policy protection as virtual resources move from on-premise to public cloud environments. Forward thinking enterprises and service providers are applying this protection today on their virtual machines, to achieve cloud-ready security so they can take advantage of cloud computing, ahead of their competition.

For more information please call or visit us at.
www.trendmicro.com/go/enterprise
+1-877-21-TREND

TREND MICRO™