nemertes RESEARCH
INDEPENDENCE INTEGRITY INSIGHT
issue paper

Securing the Physical, Virtual, Cloud Continuum

By Ted Ritter, CISSP
Senior Research Analyst

Executive Summary

The data center is undergoing a radical shift, from virtualization towards internal cloud environments where workloads dynamically move, start and stop driven by real-time performance needs. At the same time, IT practitioners are interested in exploring external cloud computing options---but security and compliance concerns are squelching adoption. A key concern is trust. Moving to a cloud provider shifts the burden of trust onto the provider--something that few providers are able to handle today. To overcome this concern, responsibility for security and compliance needs to stay with the customer. This requires an overhaul of security practices – the same practices we've been using for 15 years. We need new security and compliance controls that span the physical, virtual, cloud continuum (not everything will be virtual so security must continue to protect physical assets). We also need security controls that are location-aware and dynamically enforce policy regardless of workload location. This requires an adaptive perimeter defense and restoration of depth for defense in depth.

The Issue

Information security best practices remain largely the same as 15 years ago, based on a strong perimeter defense and defense in depth still the primary security controls. However, virtualization and cloud computing are radically changing data center operations, and thereby imposing new challenges to security and compliance (where is the perimeter around a cluster of virtual servers?). Securing this new environment requires revisiting best practices to adapt to the dynamics of this new infrastructure. Security and compliance controls need to extend across the physical, virtual, cloud continuum. This requires the adaptive perimeter defense.

The Rise of the Cloud

Currently, 93% of participants in Nemertes' virtualization research are in some stage of deployment: Evaluation, pilot, partial or full. Virtualization's draw is so strong that many data center operators must justify why they are not virtualizing an application. "Virtualization is the rule in this environment, not the exception," says the network administrator for a higher education institution. Moreover, virtualization is driving the movement to cloud computing.

There are three primary categories of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). (Please see Figure 1 - Internal to Cloud Continuum, Page 2.) Simply, SaaS – the most mature service – delivers an application to end users without any upfront cost or on-premise software; PaaS provides a complete application development environment as an on-demand service delivery; and, IaaS provides compute workloads that dynamically move between virtual hosts in the data center to virtual hosts at the cloud provider. The focus of this paper is IaaS because it is the vehicle for cloud computing, both internal and external to the data center.

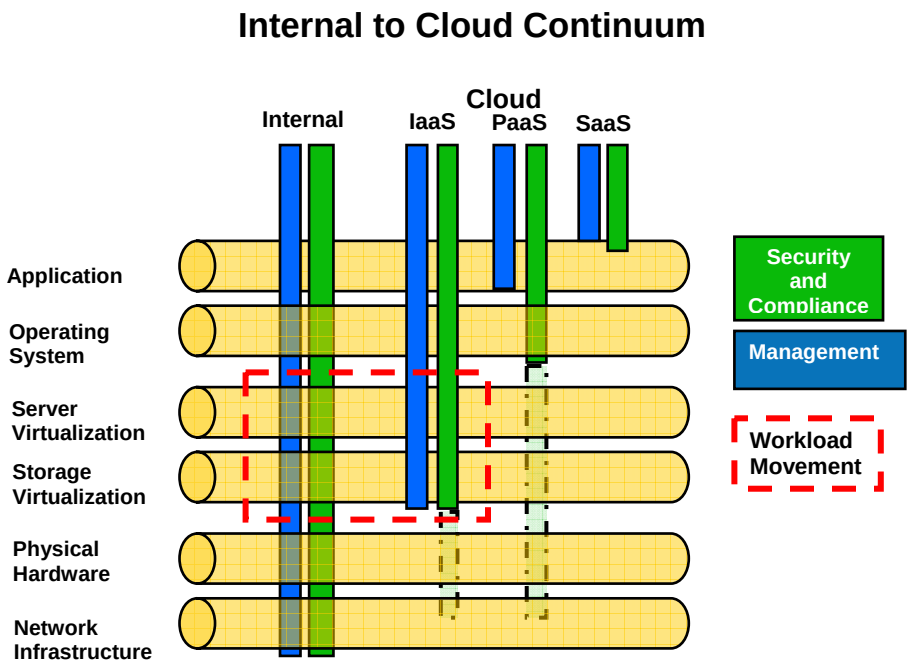

Figure 1 - Internal to Cloud Continuum

Interest in IaaS services is very high, with 33% of organizations planning evaluations in the next 24 months. Yet, security and compliance are the top two

concerns holding adoption of to less than 1% of organizations, currently. These concerns result from the fact that cloud services are unlike anything we have seen – and have had to protect – before. IaaS results in virtual machines (VM) and applications moving within the data center and to virtual hosts outside of the data center.

Same Old Security Architecture

Despite the drive to virtualization and high interest in cloud, security architectures look much the same today as they did 15 years ago, still built on two key best practices: A strong perimeter defense and defense in depth. The strong perimeter defense is an approach focused on placing firewalls and intrusion detection/prevention systems (IDS/IPS) at all access points to the network to create a strong shell of security. Defense in depth places additional layers of security inside the perimeter to better position against insider threat and the potential breach of the strong perimeter defense.

Securing the virtualized and cloud infrastructure with physical security products fails to achieve either defense in depth or a strong perimeter defense: Traffic among VMs never hits the physical network, physical security devices do not deal well with virtual machine movement and virtualization flattens the infrastructure.[1]

Virtualization security via virtual appliances and virtualization-aware host-based security is the only means to implement depth and a security perimeter in the virtual infrastructure. Still, less than 10% of organizations are doing this. Instead, some IT shops pipe virtual network traffic onto the physical network via VLANs to physical network security devices. This is cumbersome, susceptible to misconfiguration and ultimately unsecure.

So, should we abandon strong perimeter defense and defense in depth? The answer is a firm "no", for three reasons. First, the practice is not fundamentally flawed; it is implementation that fails. Second, virtual servers run on physical hardware, so there will always be some level of physical network protection required. And, third, only 42% of workloads on average run on a hypervisor despite people talking about 100% virtualization—which means that for the foreseeable future, security architectures must protect both virtualized and non-virtualized infrastructure. Yes, most of the remaining 58% workloads will move to virtualization, but migration to virtualization will be slow for a significant percentage of workloads will not for the following reasons:

1. Performance – Virtualization optimizes CPU utilization by multitasking multiple workloads. This also requires multitasking of network bandwidth and storage operations. Some applications

[1] For a more detailed discussion of defense in depth in virtualization, please see Nemertes' 'Virtualization Security Key Trends, 2009.

require dedicating hardware and OS running on bare metal to meet network bandwidth, processing and storage input output per second (IOPS) demands. For example, some trading floor applications will not use virtualization for this reason.

2. Legacy Systems – There are legacy applications that cannot support operating within a virtual machine. Either the software is hard coded to the hardware or proprietary protocols are incompatible with virtualization's use of standard protocols.
3. Compliance Reasons – Some systems are not yet certified to operate on a virtualization platform. For example, the FDA has yet to certify virtualization for most patient-facing systems. Also, some value-added resellers (VARs) have yet to certify their version of software or hardware. Even though the software may technically run in a virtual machine, doing so voids the maintenance contract.

For a long time to come, therefore, physical security devices will be the first layer of defense for both physical and virtual servers. In other words, neither strong perimeter defense nor defense in depth goes away, but the execution and implementation must change. The first step is to shift to an identity-based approach (who is the system you are trying to talk to, who the system is trying to talk to you, etc) and away from location-based approach, (physical addresses defining you and your needs). The second step is to become cloud aware.

Cloud Security – It's All About Trust

The unique dynamics of cloud computing (dynamic and elastic workloads, on-demand services, metered service, and multi-tenant environments) raises unique security issues. (Please see Table 1 - Cloud Security Issues, Page 5.)

Cloud Dynamic	Description	Security Issues
Dynamic and elastic workloads	Workloads (virtual machines) move from physical to virtual to cloud depending on resource requirements and availability	Policy moving with the workload. Protection of VM in transit and at rest. Logging of all administrator actions for both VM and Guest OS
On-demand services	Clients use a self-service portal to provision workloads, storage and security	Requires significant trust
Metered Service	A basic trait of cloud services is pay (or be charged back by the drink)	Security must match service turn up and turn down without hurting performance

Multi-tenant	Resource pooling and multitenant architectures are core to cloud architecture	1. Logging, monitoring and verification of all access 2. Restricted access to Guest OS, applications or data 3. Customers cannot access each other's systems

Table 1 - Cloud Security Issues

Cloud dynamics shift the burden of trust onto the cloud provider that it is implementing, managing, monitoring and auditing the controls necessary to meet corporate security and compliance requirements. For example, how does a cloud provider guarantee encryption of all communications between two specific VMs? In a cloud environment, the customer is flying by wire. This requires trust that the provider is implementing the right controls to protect servers, data and applications. For example, compliance requirements, such as the Payment Card Industry Data Security Standard (PCI-DSS) and the Health Insurance Portability and Accountability Act (HIPAA) require routine audits and logging of all security controls. This is a significant challenge for a cloud provider that has led one IaaS provider to tell users not to store sensitive credit card data on their servers.

Even if the auditing is possible, what happens in the event of an adverse audit finding, or worse; a breach? In this event the customer requires direct support of the cloud provider to assist in remediating the finding or investigating the breach. Again, this is a challenge for cloud providers.

Trust extends to include the physical location of data. For example, the EU Personal Data Directive mandates the management of any personally identifiable information in any EU member state. A US company that has a cloud provider hosting US customer data in an EU country is subject to far more onerous privacy rules than if they host the data in the USA.

The good news is, over time as cloud providers deploy more sophisticated security controls and follow recommendations from groups, such as the Cloud Security Alliance[2] and the Jericho Forum[3], cloud providers will increasingly address these trust issues. In addition, auditors need to become cloud aware and acknowledge that cloud security controls are not the same as traditional data center security controls.

Finally, enterprise users interested in deploying cloud services should modify auditing procedures to address cloud environments. One large law firm, for example, audits its cloud-based data quarterly (as compared with annual audits for its internal data). Over time, this company expects to decrease the frequency of audits for the cloud services, as both the auditing team and the external cloud

[2] http://www.cloudsecurityalliance.org/
[3] http://www.opengroup.org/jericho/

provider become more familiar with the issues and challenges posed by cloud computing.

In the meantime, the onus goes back onto the enterprise security team to implement a security architecture that mitigates any security and trust issues. The best defense is to minimize this burden of trust by tightly coupling security controls to the dynamic workloads as they move within the data center and out into the cloud. This requires rethinking the way we approach defense in depth and the strong perimeter defense.

Multi-dimensional Security Model

We need to redefine the concept of the perimeter. As noted, in the physical virtual cloud infrastructure, the strong perimeter must remain to monitor and control all egress and ingress to the data center (whether it be an enterprise data center or a cloud provider data center) as well as protection of physical server workloads. However, we also need an adaptive perimeter that protects all workloads, regardless of location: Physical, virtual, internal cloud, external cloud. (Please see Figure 2 - Cloud Security and Compliance Control Points, Page 7,) The adaptive perimeter must be a malleable security layer that envelops core components (hypervisor, virtual machine, guest OS, virtual switch and storage) using virtualized security controls. These controls must cover the entire ISO stack (virtualized versions of firewall, IDS/IPS, web application firewall, logging and access control and anti malware).

The adaptive perimeter defense must be virtual machine aware. In the virtual environment (virtual server, internal cloud, external cloud) workloads move around - as virtual machines - including moving through the strong perimeter. Virtual machine awareness distills down to three primary attributes:

1. Virtual machine protection while in motion and rest – The adaptive perimeter defense must virtual machine movement (VMware VMDK, Microsoft VHD, Xen HVM) as more than just multi gigabyte file transfers. It also must incorporate anti-malware and patching to protect VMs and guest OS from attack while in motion and at rest.
2. Stateful and sticky policies – Policy must be movement aware as VMs move from virtual server to internal cloud to external cloud. For example, a VM that contains corporate intellectual property must have at least the same level and type of security controls outside the data center as inside the data center. In fact, the policy may be to ratchet up security controls (additional levels of access control) when the VM is outside the strong perimeter.
3. Distributed policy management and enforcement - Policy enforcement must follow the VM regardless of state and location. When a VM is frozen in an external cloud, controls must be in place to validate and remediate patch and anti-malware status of the VM upon restart, despite the fact that all of this is happening outside the data center.

Cloud Security and Compliance Control Points

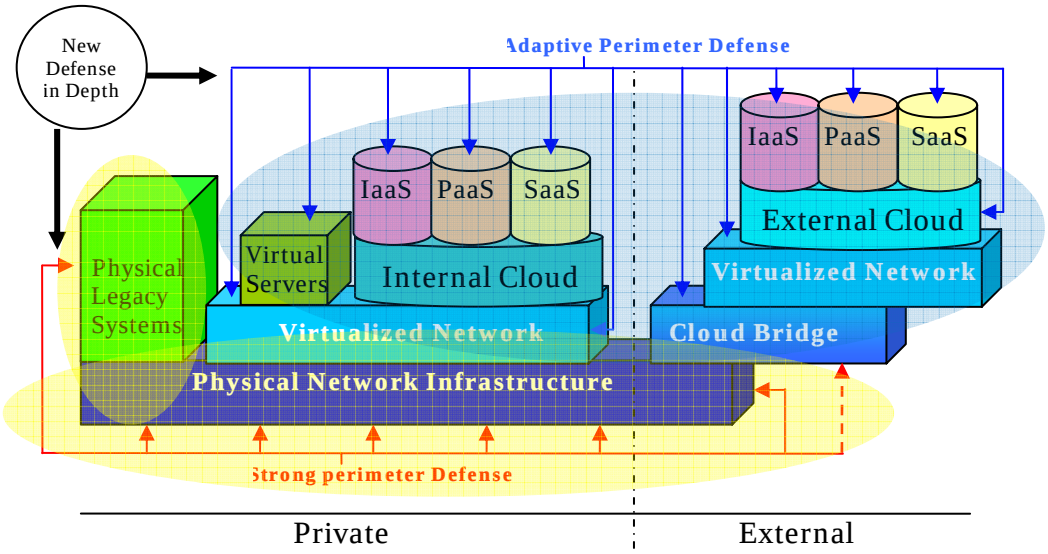

Figure 2 - Cloud Security and Compliance Control Points

VM awareness requires both host based and appliance-based virtual security. Virtual security appliances operate at the virtual network layer on a single or distributed virtual switch. The advantage of this approach is better performance management by dedicating computing resources to security functionality; anti-malware for example. At the same time, host-based security guarantees that the security function moves with the VM whether it be on a virtual host in the data center or running on an IaaS platform in the cloud. Together, host based and virtual appliance security restores a lost layer of depth enabling the adaptive perimeter defense and defense in depth.

The adaptive perimeter defense also must include compliance. Security controls for compliance requires awareness of guest OS actions and tracking all access to the VM. Logging must cover access to physical servers, virtual machines, the guest OS, and the applications. Logging must also be state and location aware. For example, logging an unauthorized database access in the external cloud has different ramifications and remediation processes than logging an unauthorized database access on a virtual server in the data center. The first case may be an external hacker attempting access to sensitive data and the latter case may be an insider threat. Having the controls in place to discern one from the other assists in developing effective countermeasures and provides the audit logs necessary for IT compliance.

The Cloud Bridge

The consolidation point of the strong and adaptive perimeter defense is the cloud bridge. This is a new concept that bridges the physical and virtual infrastructure in the data center with the physical and virtual infrastructure of the external cloud provider. Today, the cloud bridge may be as simple as a VPN that links a router in the data center with a router at the cloud provider's point of presence. On the other hand, VMware vSphere customers using VMware-based cloud services can use either the vNetwork virtual switch or the Cisco Nexus 1000V to bridge private and public.

Ideally, the cloud bridge will be an open platform that supports multiple hypervisors and virtual security controls from multiple vendors. Today, Open vSwitch supports Xen/XenServer, KVM and Virtualbox.[4]

Conclusion and Recommendations

The data center computing environment is undergoing radical change. The emergence of virtualization as the primary computing platform and the inevitable migration to cloud is creating a new reality for security and compliance teams:

1. For performance, legacy system and compliance reasons workloads will continue to be physical and virtual for many years to come. This requires continuation of the strong perimeter defense and defense in depth.
2. Virtualization of workloads will continue to grow, steadily eroding the ability of physical devices to provide robust defense.
3. External cloud adoption will grow, requiring security controls, policies, and auditing practices in the data center that automatically move into (and adapt to) the cloud, along with workload and data movement.

A hybrid environment is the name of the game: physical, virtual, internal cloud, external cloud. This forces security and compliance staffs to broaden and deepen security practices: Broaden by adding an adaptive perimeter to the strong perimeter defense and deepen by adding virtualized security tools; both appliance and host based. This new security continuum also requires strong coordination of policy across the strong and adaptive perimeters. Policy must be rule based, role based and state aware so different policies apply when a VM is on a virtual server in an IaaS cloud versus on a virtual server in the data center.

Finally, the dynamics of cloud computing and virtualization make the best defense a strong offense where security and compliance controls follow VMs and corporate data, independent of physical location. This reduces the burden of trust

[4] http://openvswitch.org/

on the cloud services provider but requires implementation of virtual security appliances and applications for continual access control, protection and monitoring along with detailed logging of access to physical servers, virtual machines, the guest OS, and the applications.