Cloud & Virtualization Security: The Evolution of Traditional Security

By Andrea Bilobrk
Cloud & Virtualization Strategist, CCSK

Contents

Introduction

The emergence and proliferation of virtualized environments has significantly changed the way traditional IT departments operate. Not since the adoption of mainframes became mainstream has a technology made such an impact on IT infrastructure design and operations.

But why has the concept of cloud & virtualization suddenly become so important in business transformation? The simplified answer is that it fundamentally changes the way in which IT infrastructure and usage functions. All of a sudden we have moved from large datacenters with server farms to streamlined stacks with virtual machines interconnected via the Internet. Cloud and its foundation in virtualization have transformed the way organizations do business. However, this change isn't self-contained in infrastructure; it affects every interconnected system and has a significant impact on the way these systems function. Most noticeable is the affect it has made in IT security, and the evolution required for security solutions to address the unique risks that these environments bring.

Traditional IT Security & Cloud

IT Security has continued to evolve over the last decade to address the rapid increase in sophistication of attacks. The continued adoption of next-generation firewalls and web application security solutions rests in line with the increased amount of attacks that originate through Internet-based protocols. No longer are attacks designed solely at penetrating the IT network through traditional channels which are protected with firewalls and intrusion

detection/prevention. New threats are entering the network through Wi-Fi, SQL injections on websites and through mobile devices. The dynamics of securing corporate assets has changed significantly and traditional IT solutions cannot address some of these changes.

Traditional IT has always focused on security the perimeter of the IT environment. Security professionals install endpoint security to lock down desktops and laptops, and firewalls to protect the network from unauthorized access. The shift to web based attacks saw market adoption of next generation firewalls and web application firewalls to prevent against DDoS and SQL injection attacks. These solutions provide advanced protection for networks against next generation attacks, but do not address the unique security concerns that affect virtualized or cloud environments.

The key difference between a traditional and virtualized or cloud infrastructure lies in how systems are designed and operate. In a traditional environment, processes, applications and databases were separated across multiple physical servers and ran dedicated operating systems and resources. The shift to virtualization and cloud environments meant consolidating these servers through virtualization, and running several of these virtual machines (VMs) in tandem on a single server stack. This meant decommissioning inefficient servers and better utilizing shared resources for these applications.

The issue is that when these new processes and infrastructure designs were implemented, security was often not a primary concern. The main reason for this is the separation of duties between the infrastructure teams who design and implement the virtualized environment and the security personnel who are normally tasked with the overall security of the environment. It is rare to see organizations utilize both teams during the design and implementation stages, not to mention the learning curve associated with understanding how security and virtualization function together. Security departments have been tasked with securing physical environments, which means when the infrastructure becomes more and more virtualized and spread out across multiple locations (as in cloud implementations), the complexity of securing these environments becomes increasingly difficult. We cannot expect to see full adoption of security practices across private cloud environments until there is increased awareness of the differences and key areas of vulnerability as it relates to next generation security practices.

Over the last few years we have seen an increased number of security solutions tailored to virtual environments. VMware, one of the leading virtualization solution manufacturers, released a set of APIs that allowed third-party vendors to create security solutions that would work natively in these environments. This has been one of the key reasons for the availability of solutions that focus on securing virtualized and cloud environments. Using traditional security solutions which are focused on detecting network traffic that connects to and from servers cannot be expected to provide

visibility and security within a virtual environment. These tools have no visibility beyond the physical NIC of the server, which means internal movement and changes will be unnoticed by monitoring devices and will not produce log reports. It is this key difference that has prompted security manufacturers to start designing solutions to enable security within the new virtualized and cloud infrastructure.

The first waves of security solutions see the availability of endpoint, firewalls, intrusion detection/prevention, security event management, identity management and single sign-on. Security professionals might assume that these technologies operate in a similar manner between physical and virtualized environments; however, due to the unique features of virtual environments, simply porting an existing security practice to a virtual environment can have significant impact on the operations of the infrastructure. It is this key difference that makes the adoption of paravirtualized (or virtualization-optimized) solutions increasingly important.

Endpoint Security

As more and more infrastructure becomes virtualized, the migration to endpoint solutions that are optimized for virtual environments will become increasingly important. One of the most common starting points for the implementation of a security strategy within a virtual infrastructure is endpoint, and it is also one of the most common misused virtualization security controls.

Traditional endpoint solutions were created to work in disparate locations, such as across multiple physical computers including desktops, laptops and servers. The trouble with implementing these traditional solutions within a virtualized environment is that the policies that were written for physical infrastructures must be redesigned for virtual environments. If the corporate policy states that endpoint must be installed on every machine, and this is enforced within a virtualized environment, there can be significant decreases in infrastructure efficiency, not to mention the possibility of taking the entire infrastructure down due to over-allocation of resources.

In a traditional endpoint installation within a virtual environment, the endpoint is installed across each virtual machine (figure a). In a simplified example, a server may host 4 virtual machines (VMs) on a single hypervisor layer. Each virtual machine is allocated system hardware resources such as CPU, RAM, HD and NICs, and runs designated applications within a specified operating system. If endpoint is installed on every single virtual machine, it will require a part of the allocated resources in order to function, and increased resources during peak functionality such as during system scans. Because these resources are shared across the entire physical server, the more instances of endpoint that are installed, the more system resources will be required. For example, if each instance of endpoint requires 2% system resource utilization to run

during idle mode, it equates to 2% per VM. Spread this across a hypervisor with 4 VMs, and the endpoint module will require 8% of total server resource utility when idle. If during a system scan, the endpoint solution requires 5% of system resources, and you multiply that by the number of VMs resident on the hypervisor, the resource usage increases significantly. It is not uncommon for a large scale virtualized environment to crash due to a large number of endpoint instances running at the same time. It is this specific reason that infrastructure teams are resistant to installing endpoint on critical infrastructure due to the performance hit in idle mode and the risk of system failure during system scans.

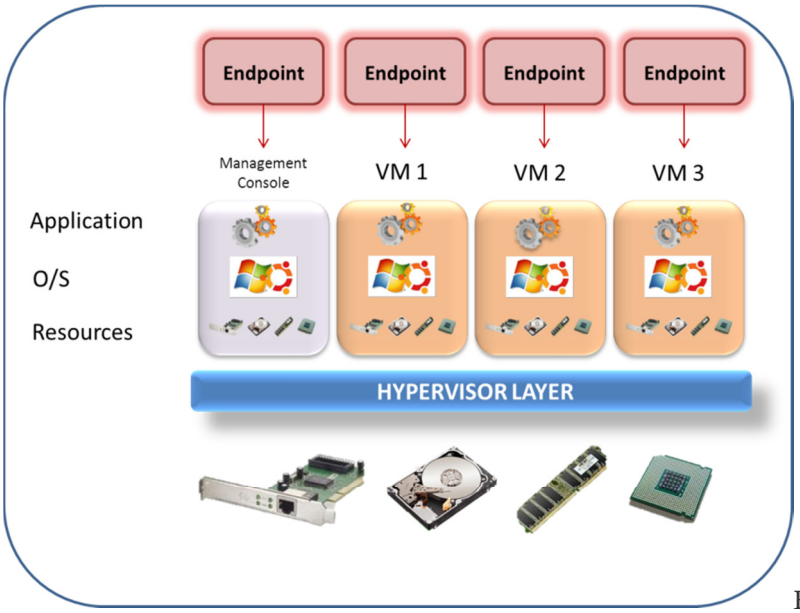

Figure A

Over the last few years, significant strides were made to improve the functionality of endpoint in virtualized environments. In 2007, VMware released a set of Application Platform Interfaces (APIs) under VMsafe to their partner community to start the creation of security and development solutions. This led to the creation of virtualization optimized and paravirtualized (allow the VM monitor to be more efficient by moving the execution of tasks from the VM to the host domain which reduces the performance hit normally associated with running a hardware execution inside a VM) including VMware's own vShield security applications.

By opening up the APIs to the security vendor community, the ability to create virtual environment-optimized endpoint and other security solutions became more efficient. This led to a new endpoint model that has been adopted by the leading endpoint security vendors including Trend Micro, Symantec and McAfee. This new model of securing endpoints in virtual environments provides the same level of security than

traditional models, but reduces the significant performance hit by leveraging the VMsafe APIs. Figure B shows how a VM specific endpoint solution functions. The endpoint solution manager gets installed in the management VM. From there, it leverages the hypervisor APIs to monitor adjacent VMs which share the same hypervisor. This means that there is only one instance of endpoint installed on each hypervisor, and one performance hit. Instead of running a 2% resource hit per virtual machine, it is reduced to a single hit of 2% across the entire server and a significant reduction in resource utilization compared to traditional methods. More importantly, there is no associated threat of bringing a server down during endpoint scanning.

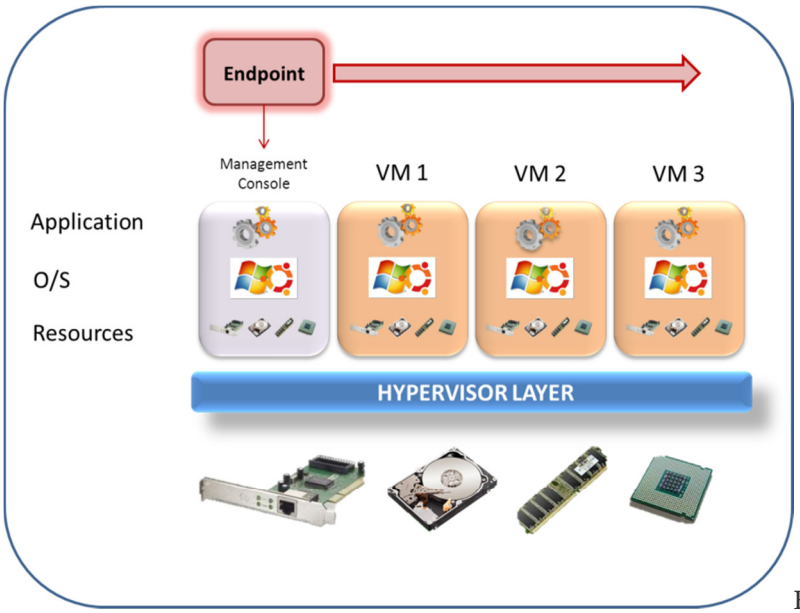

Figure B

Since 2007, we have seen the release of APIs from Xen and Google to help manufacturers continue to develop solutions for cloud environments, not just from a security perspective, but also to drive application efficiency.

Virtualized Firewalls

The second key area of advancement is in firewalls. By design, traditional firewalls were designed to control traffic between network segments and physical hardware. When the physical design of the network is removed, largely due to the collapsing of physical servers into fewer virtualized servers, the main source of security control is removed, as the threats start to move to the individual VMs residing in servers, especially when

multi-tenancy is utilized. This means that the logical barriers segregating virtual machines become the concern for firewalls, not just the network around the physical server. So how do you protect the inter-VM traffic when a traditional firewall cannot see traffic beyond the physical NIC card of the server?

The answer is virtual firewalls. These are a new breed of firewall that uses virtualization APIs to hook into hypervisors and control traffic between virtual machines. Virtual firewalls use a per-host firewall VM for configuration and logging, while taking advantage of the hypervisor kernel to filter the traffic. You can also customize the traffic preferences to select specific VMs or groups to minimize resource impact. The advantage of this operational redesign is the significant reduction in lag compared to CPU-dependent virtual firewalls which are restricted to the speed of a single vCPU. The newest generations of virtual firewalls have adopted connection tables and rule sets to increase performance even further.

Virtual firewalls are currently one of the few methods of ensuring traffic between VMs is controlled from a security and compliance standard. This extends to providing security against the movement of virtual machines between physical servers, as firewall rules can be embedded in the individual VM and is automatically applied upon movement.

IDS/IPS and SIEM

Intrusion detection and prevention devices (IDS/IPS) have always been one of the most important security control devices. These devices allow security professionals to create security policies for the network, and by placing an IDS/IPS device inline with the network, monitor for any suspicious traffic or policy violations. With an IPS device (IDS devices are used to watch for potentially harmful traffic and report it, but not perform any type of containment or remediation) organizations can thwart attacks by either terminating the user connection, block access to the target, or block access based on the user account, IP address or other distinguishing characteristic. IPS devices can also be used to modify policies and rule sets of other devices such as routers and firewalls, and apply patches or remove properties such as attachments from emails.

The evolution of IDS and IPS devices led to the adoption of Next Generation IPS (NGIPS) which take into consideration from sources such as web applications and attachments that might be disguised as web traffic, images and audio/video including encrypted files. Security vendors including SonicWALL, Sourcefire, Check Point and IBM are extending this technology to work in virtual environments, where the network and resource layers become abstracted due to the collapsing and consolidation of resources onto fewer physical servers. These technologies utilize paravirtualization (technologies that are built with virtual environments in mind and utilize hypervisor APIs to streamline processes and gain additional visibility into all layers of the virtual environment) to

extend traditional IPS visibility and look for suspicious traffic and resource behavior in both inter-VM traffic and in system and resource utilization. This allows for security administrators to see vulnerabilities such as the creation of a virtual NIC that connects 2 adjacent VMs be detected or a DDoS attack against a VM sharing a multi-tenant environment. Suddenly there is visibility into the underlying workings of a virtual environment, something that until recently has not been possible with the exception of management information which fed into the virtual platform reporting system. It is critical for any environment with security requirements to be able to have this type of visibility into any resource (virtualized or not) that contains business critical information.

An extension of the IDS/IPS device is the Security Information & Event Management (SIEM) device. These act as the consolidation and reference resource for all security devices on the network. The SIEM allows for review of traffic and is often used as a means of alerting the organization of unauthorized behavior on the network. These devices are a critical part of a security system, but until recently did not utilize paravirtualization and thus could not properly report on virtualization specific events. While the immediate issue is that the SIEM device cannot detect events such as the unauthorized duplication or movement of a VM, or a breach of the logical barrier segregating VMs, it also extends to lack of visibility in the overall operations of the virtual environment. In the case of a hardware malfunction or infrastructure crash, the SIEM device can provide a significant amount of information on the original cause of the event which affected the environment, but only if it has proper visibility into all layers of the virtual environment. The SIEM can also provide information that would be critical in the event forensics must be done, as it will have information that might not be captured by a network-based SIEM, which can only collect information on the physical network layers.

As cloud and virtualized environments become more distributed and shared, the ability to verify that these VMs are protected through the implementation of IPS and SIEM devices (among other security controls) is paramount in not just proving to the auditors that your resources are protected, but to ensure from an internal visibility perspective that all network traffic and inter-VM behavior can be monitored.

Future Trends in Cloud Security

As the adoption of cloud and virtualization becomes more mainstream throughout 2012, there will be an increasing importance of expanding the scope of cloud business transformation from just service adoption (IaaS, SaaS and PaaS) to integrating all aspects of cloud adoption into the transformation plan. This means focusing on how all operational units of the organization are affected by the transition to a virtualized or cloud environment. It will move from being an infrastructure initiative to a plan which

includes at a minimum security and operations. From this shift, the importance on education and adoption of new technologies and processes will become more prominent. In particular, a business review of compliance, privacy and governance as it relates to cloud, and additionally, how to ensure that the increased adoption of mobile devices is managed from an operations and security perspective. Lastly, the need for evolved user identity management systems will be more critical as resources are virtualized and hosted in cloud environments.

Compliance, privacy and governance will be the first area of review for organizations starting to transition to a cloud or virtualized environment. Because virtualization has traditionally been an internal infrastructure issue with few ties to the larger organizational governance and security policies, there is a requirement for organizations to quickly adapt to the increasing security and policy issues that cloud brings. Additionally, under the adoption of cloud environments, where the resources are located in third-party cloud provider's physical environment, the control over policies is now shared with the provider. As pressure from governance agencies over cloud environments increases, most notably with the evolution of PCI DSS to include provisions for virtual environments, organizations will have to start ensuring that all policies and SLAs address these requirements. This means ensuring that the internal security teams implement the right solutions to security the virtualized or cloud environment, SLAs with service providers clearly outline responsibilities as they relate to security, management, litigation (in the event of a breach) and recovery. It is also critical that if multi-tenancy is used, that privacy and compliance requirements are met.

The second trend that will increase with the next generation of technologies is around mobile device security. The mass adoption of smartphones and tablets means an increase in WiFi bandwidth and management, and the ability to access corporate assets from multiple locations. This means that there will be a strong focus on managing these connections and their effect on network throughput as it relates to WiFi usage. The key issues for these devices is that they can generate WiFi hotspots using cellular networks, which can be used to access corporate resources while bypassing traditional WiFi network policies, increasing the risk for data loss and leakage. Additionally, authorized devices will require security policies to ensure they meet corporate security policies through the use of VPN applications and WiFi session encryption.

Identity management will also become a significant trend in cloud adoption, as resources become more spread out across multiple servers and locations. Users who require multiple passwords to access cloud or virtualized services can lead to an increased risk of security threats due to simplification of passwords (making passwords easy to guess or hack), an increased workload on support teams required to perform password resets, and organizations disparity of operations that are separated from other processes. The consolidation of user identities through the adoption of single sign-on (SSO) and cloud based authentication will become more dominant as the transition to cloud services becomes higher priority for organizations.

Summary

As cloud and virtualized environments become more distributed and shared, the entire infrastructure becomes more abstracted. The methods of securing these resources rely heavily on network based detection and remediation, but cannot see the traffic and events that reside within large-scale virtualized environments. This means that there is an increase in blind spots in the network. Additionally, some security roles are now shared with third-party cloud providers, reducing the amount of control over these environments for the organization.

It is this key force behind the adoption of virtualization and cloud security. The methods used to previously secure these environments must be adapted to meet the unique characteristics of cloud and virtualization. Organizations need to adopt technologies which leverage paravirtualization to gain visibility into all layers of the virtual infrastructure and adjust security and governance policies to take into account the risks associated with these environments. Security teams need to start working closer with infrastructure teams to ensure that the technologies used meet the needs of the security team, but do not negate the benefits of virtualization for the infrastructure teams.

Employee adoption of mobile devices and the increase in passwords must also be taken into consideration when transitioning to cloud. The larger the disruption an employee faces, the more likely they are to adopt unsecured methods to accessing corporate resources. This includes ensuring the use of mobile and tablet devices are addressed in a way that allows employees to utilize them, but not cause threats to the corporate network. Making simplified login systems will also allow employees to increase productivity and minimize the workload of help desk functions.

Cloud and virtualization is a disruptive process for any organization. However, the benefits of adoption far outweigh any risks that might be associated. The key to a successful transition is to have security and infrastructure teams involved in the transformation of the infrastructure to ensure that the organizational objectives of all parties are met.