WHITE PAPER:
SECURING THE PROMISE OF VIRTUALIZATION

A Symantec/VMware® position paper

Securing the Promise of Virtualization

Who should read this paper

If you are managing security or driving adoption of virtualization in your organization, this joint white paper from VMware and Symantec will help you to better understand how you can meet the challenges of ensuring security in a virtual world.

vmware

Confidence in a connected world. Symantec.

Securing the Promise of Virtualization:
A Symantec/VMware® position paper

Content

Introduction

"There are now 800,000 petabytes of data out there - it is the amount of unstructured data that is causing the explosion."

-- Enrique Salem, CEO, Symantec

"With vMotion instances launching every second, there are more VMs in motion globally than actual aircraft."

-- Paul Maritz, CEO, VMware

Virtualization presents organizations with tremendous opportunities, as well as some significant challenges. This transformative technology provides the basis for the convergence of mobile and cloud computing, a convergence that is rapidly changing the face of IT as it enables enterprises to consolidate resources, improve responsiveness and support the business agility in a more cost effective manner than ever before. The combination of virtualization, mobility, and cloud computing has triggered an explosion in the quantity of data being created, shared, and managed by enterprises. In most organizations, however, security technologies and practices have not yet adapted to this fundamental change in IT infrastructure.

Data center virtualization is the first step in the journey to private clouds that leverage and enhance existing technology assets. By evolving from hypervisor-driven virtualization to a private cloud architecture, IT can meet business demands for increased agility and flexibility. Undertaken with the right information and infrastructure, this journey leads toward evolutionary transformation of information security – ensuring compliance and integrity of increased consolidation densities today and delivering adaptive security that promotes density goals and a device agnostic user experience.

For today's enterprise, we identify three general areas of risk associated with virtualization. First, there is the set of traditional security risk factors involving threats such as malware attacks, missing patches, and data theft. While current security controls have been designed to mitigate these risks in physical environments, they must now be extended to also cover virtual environments. Second, there is a whole new class of risks exclusive to virtualization. Much of this risk is introduced from the accelerated, "frictionless" provisioning practices which are the actual benefit of self-service models, as well as the interactions of mixed-trust workloads and security planning often performed by non-traditional security staff.

Finally, there is a new set of risks associated with the hybrid environments typical of today's enterprise, which are based on consolidated physical infrastructure running high-density virtualized workloads, while also delivering cloud-based IT service models needed to service dynamic business requirements and the highly-mobile, personalized workforce.

According to Thomas Bittman, vice president and distinguished analyst at Gartner, "For most organizations, virtualization will provide the foundation and the stepping stone for the evolution to private cloud computing. However, the need for security must not be overlooked or 'bolted on' later during the transition to private cloud computing." [1]

To move beyond simple host-aggregation, a virtualization platform must be able to securely segregate multiple workloads consolidated from mixed trust zones and host them from a single pool of shared system resources. In fact, security controls in the virtualization stack are a critical prerequisite to establishing a private cloud. It is the presence of these controls that differentiate a cloud infrastructure from other forms of service-provisioning with virtualization.

1-Gartner Says Security Must Evolve as Organizations Move Beyond Virtualization to Private Cloud Infrastructures," VMblog.com, http://vmblog.com/archive/2010/11/08/gartner-says-security-must-evolve-as-organizations-move-beyond-virtualization-to-private-cloud-infrastructures.aspx

As virtual, cloud, and mobile systems are brought online, successful organizations are building security into their evolving IT infrastructure not as an afterthought, but from the ground up. Going forward, their continuing success depends partly in the ability of security and virtualization vendors to deliver solutions that are purpose-built to mitigate risk in virtualized environments. The new technology model must integrate security solutions for endpoint protection, application isolation, runtime configuration, data loss prevention, compliance, and identity management with virtualization management layers.

In addition, security and virtualization suites must be integrated for hybrid environments, so that a single console may be used to manage security across physical, virtual, and cloud infrastructure. To meet the challenge of rapid provisioning, it will also be important that contextual security information be made available to non-traditional security staff, while maintaining established separations of duties and privileges.

Traditional Security Risks in Virtual Environments

With the advent of virtualization, the enterprise must review its entire security portfolio to ensure that the protection of information, people, and systems is not limited to physical infrastructure. Traditional security risks that may not be accounted for in virtual environments include the following:

- **Targeted malware -** Virtual software layers can expand the potential attack surface and become a target for breach attempts using new and existing methods to compromise networks and systems. There is also the potential that a dedicated malicious VM may be introduced, complete with its own OS resources to orchestrate an “in-network” attack scenario.
- **Thumb drive theft -** Traditional physical infrastructures benefit by security practices designed to protect physical assets. Virtual environments raise the possibility that a large set of file systems may easily be stolen in its entirety with little more than a thumb drive or memory stick.
- **Data loss -** When data assets can be moved in and out of established trust zones, including virtual networks and private and public clouds, the result is more sensitive data in more locations. As a consequence, the risk of data loss increases, whether from inside or outside the organization.
- **Audit scope creep -** In order to comply with any number of regulations and standards, such as PCI, HIPAA or SOX, the organization may face an audit whose scope is dramatically broadened due to the existence of data on virtual machines. For example, let us say that an in-scope server becomes virtualized. Now the other guest VMs, as well as the ESX host on which the VMs reside, may require an expansion of the audit scope due to the adjacency of guest and host systems.
- **Missing security updates and patches -** Since VMs can easily be relocated, gaps can be introduced into the change and update management processes.
- **Reliance on traditional barriers -** Firewall and other perimeter-based approaches work effectively when system assets do not move too frequently. These protection models break down due to their inability to keep track and pace with the dynamic movement of virtual instances. Policies located at static gates are seldom designed to adapt to changes in VM locations.

New Security Risks Exclusive to Virtual Environments

In addition to traditional security risks, a new set of risks exclusive to virtual environments must be identified and addressed, as described below.

- **Accelerated provisioning -** Virtualization enables organizations to provision and run new services much more rapidly. Virtual systems can be instantiated, run, and ultimately de-provisioned within the time it takes to issue traditional IT service

requisitions to string cable, install racks, and load software. The accelerated timetable for virtual provisioning makes it harder to ensure that security risks have been identified and addressed.

- **Mixed-trust workloads -** With virtualization, sensitive data previously restricted to defined trust domains may now coexist along-side other data on host systems, creating new risk of data loss. Proprietary and confidential data may now be exposed as it comes into proximity with virtual systems that are not appropriately secured or monitored.
- **Security left to non-traditional security staff -** Whereas information security managers are typically involved in defining security policy for provisioning new physical systems, with new self-service models of virtual system provisioning this may not be the case. Instead, security is left to general IT administrative staff members or line-of-business people who may or may not be familiar with all of the security controls required.
- **"One bad apple" -** Whenever a Virtualization Layer is compromised there is an immediate impact on all hosted workloads. A compromised ESX host can expose guest VMs or enable an intruder to intercept communications between guest VMs.
- **Hypervisor/VMM Layer controls -** Lack of adequate controls on administrative access to the Hypervisor/VMM Layer can introduce new risks. When a user is entrusted with special privileges, they may be able to not only gain inappropriate access to workloads across different trust zones, but also acquire the ability to delete VMs and thereby cause irreparable harm to availability and up-time.
- **Poor visibility and control -** Virtual networks introduce new layers of complexity not only because of the potential movement of VMs but also due to the additional dimensions of workload interactions, administrative and user access points, and multiple locations of data assets. These factors make central visibility both more important and more difficult.

Security Solutions for Virtualization

To address new, traditional and evolving risks in mixed physical and virtual environments, IT must look for ways to integrate security and virtualization capabilities throughout the enterprise. Basic controls in the lowest layer of the infrastructure stack, necessary for the cloud-capability of hosting mixed-trust workloads, also offer unique new opportunities to instrument and manage the security state of virtual machines in ways not practical or possible for their physical counterparts. These include tamper-proof, agent-like functions outside of the virtual machine. There are also traffic isolations for both perimeter definition, and fine grained policy control over the connection state of individual virtual machines.

Accommodating the requirements for security in virtualization is not simply the addition of simple features to support the environment. In place of topology as a definition layer for the implementation of policy, a cloud-virtualization platform supports and manages the context for a number of characteristics, including that of security – all enforced by the hypervisor. There are four characteristics that describe the attributes of security by context:

1. Virtualized Security

- Available across the virtual infrastructure so that workloads are consistently protected as they are moved
- Optimized for the virtual infrastructure so that they minimize resource contention and impact to densities

2. Automated Provisioning and Life-cycle Management

- Provisioning of security services is integrated with cloud management infrastructure
- Configured on demand when a workload arrives at a host
- Policies must follow the workload

3. Logical Security Policies

- Workloads and their security policies are not tied to specific physical devices
- Security policies cannot be bound exclusively to fixed IP's, MAC addresses, or subnet topology

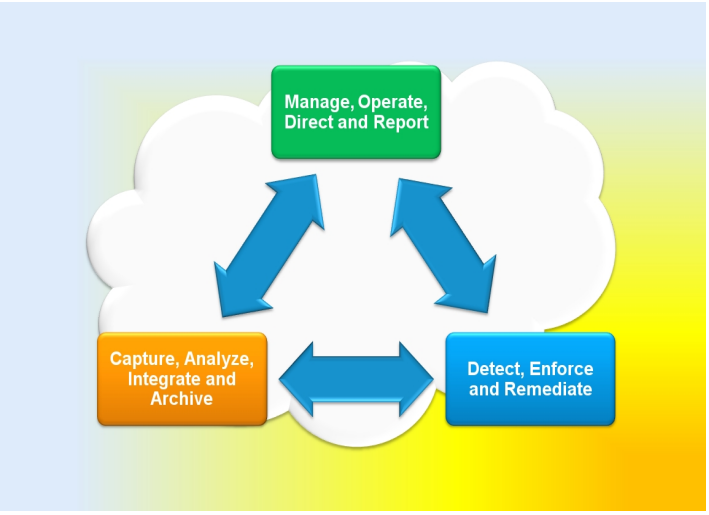
4. Dynamic Trust Zones

- A trust zone represents a collection of workloads that share common security and compliance policies
- Enforcement for trust zone assignment may be an expression of a Logical Security Policy
- Trust zones are defined by management tools and enforced by hypervisor-bound controls, with the same freedom as Logical Security Policy from topological constraint

Security tools for data loss prevention (DLP), compliance management, security information and event management (SIEM), and endpoint protection will need to communicate with the out-of-band management for these virtual estates to enable continuous assessment and remediation of virtual systems. The security solutions that integrate at this level often acquire additional visibility over their pure physical implementation and protect the configuration and prevent misuse of security tools from within the VM itself. The possibility for management plane integration of security point-solutions with the underlying hypervisor-enforced security mechanisms of the virtualization platform provide an opportunity to weave a security fabric for IT and an opportunity to extend the solution reach into new use cases of the platform - orchestrating simplified policy to manage multiple controls with increased visibility.

These examples of potential security process automation begin to illustrate the benefits over risks identified for virtualization:

- When DLP technology detects sensitive information, such as PCI data, on a VM with a mixed-trust workload, a virtual firewall rule may be automatically triggered via policy-based workflow with integration to the virtual platform's security management plane, to segment high-trust workloads.
- A configuration update on a VM network may allow a low-trust VM to compromise a high-trust VM network, potentially bypassing firewall rules. A SIEM product can detect the change and trigger an alert to the VM admin with advanced intelligence on content and context, including log tracking and correlations. The administrative actions leading to this state may also be correlated.



- If SIEM detects a VM communicating with a known bad URL such as a botnet through virtual firewall log collection, it can kick off a virus scan by endpoint protection software.
- When compliance management detects an out-of-date patch or configuration on a newly launched VM though security management integration, it can prompt the virtual firewall to quarantine or remediate the affected workload.

For IT to fully obtain the benefits of agility enabled by virtualization, it must manage the risks that arise due to the accelerated pace of change in the data center. Process automations like these are critical to achieving that goal, and will require close cooperation between security and virtualization vendors.

Security for the Agile Enterprise

The IT environment of the future includes both physical and virtualized, high-density infrastructure plus delivery of an increasingly wide array of cloud-based services. Hybrid environments raise new questions about how to consistently and seamlessly protect information, systems, and people as the virtual fabric introduces an increasing rate of change. Since VMs are not physically tied to servers, networks, and hosts, policies must be enforced on the VMs themselves, even as they are frequently provisioned or moved. IT must ask itself, how can we keep pace with evolving threats, quicker provisioning, and dynamically mobile workloads?

The answer is that future planning for security in mixed physical, virtual, mobile, and cloud environments must take into account the following trends:

- **Advanced security threats -** Today's threat landscape includes cyber-crime, industrial espionage and state-sponsored covert operations using increasingly sophisticated techniques. Targeted attacks deploy an arsenal of techniques including drive-by downloads, Microsoft SQL® injection, malware, spyware, phishing, and spam, to name just a few. Attackers often use highly customized tools such as zero-day vulnerability exploits, viruses, worms, and rootkits.
- **Sensitive data in virtualized environments -** As virtualization initiatives gain momentum, there is a trend toward adding more and more sensitive data to workloads in shared environments, increasing the risk of exposure.
- **Distributed applications -** As hybrid environments become the norm, applications are being distributed across multiple components of physical, virtual, and cloud infrastructure. The app of the future will not simply reside either on-premise in a virtualized datacenter or off-premise in a public or private cloud. Rather it will comprise many pieces of code located variously and intercommunicating across a variety of platforms, including mobile.
- **Compressed cycle times -** The accelerated provisioning made possible by virtualization will compress cycle times so that new applications will become available more rapidly than ever before.
- **Conflation of roles -** Storage, network, and host administration, once segmented into separate job roles, are now being combined as de-compartmentalization forces admins to manage infrastructure across multiple dimensions.
- **Shared resources -** More and more resources will be shared online, whether in a centralized virtual data center or shared public-cloud repositories.
- **Loss of visibility -** Due to adoption of IT managed services and Infrastructure-as-a-Service (IaaS) outsourcing, the enterprise will lose visibility on security controls normally visible within the traditional corporate IT environment.

To address these trends, IT will deploy security and virtualization solutions that meet the following requirements:

- **Security product integration -** Products such as endpoint protection, data loss prevention, compliance, and identity management will interoperate and intercommunicate, forming a more air-tight fabric to improve incident prevention and response.
- **Embedded security -** Integration between security products and application operating environments, including traditional OS, virtualization, cloud stacks, will enable IT to gain a unified view of information and infrastructure security.
- **User empowerment -** Contextual security information will be made available to non-security users responsible for provisioning virtual systems or delivering cloud services.
- **Security automation -** To reduce the chance of user error, security and virtualization management systems will automatically use contextual information about the environment to determine optimal control settings or remediate incidents.
- **End-to-end visibility -** IT will build a comprehensive risk and compliance view of the entire ecosystem, so that physical, virtual, and cloud infrastructure can be more effectively secured, consolidating control silos and minimizing redundancy in software deployments, administration and staffing.

Symantec and VMware: Meeting the security challenges for the new IT

Symantec and VMware are working closely together to meet the challenges of ensuring security in a virtual world. Our joint efforts include:

- Developing new security use cases and improving on existing ones to deliver unique VMware capability coupled with proven Symantec expertise for the IT data center of tomorrow.
- Managing threats to virtual infrastructure and the explosion of unstructured data, enabled by the movement into virtualization and the cloud.
- Uniting the Symantec strength in content-oriented, security threat detection and enforcement with the better-than-physical capabilities of VMware platform control and visibility.
- Unifying policy, operation and management of threats to data and infrastructure – spanning physical and virtual boundaries – for comprehensive protection.

About VMware

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the Cloud Era. Customers rely on VMware to help them transform the way they build, deliver and consume Information Technology resources in a manner that is evolutionary and based on their specific needs. With 2010 revenues of $2.9 billion, VMware has more than 300,000 customers and 25,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **endpoint virtualization**, **server virtualization**, and **application virtualization**.

2/2012 21229614