

Addressing the Most Common Security Risks in Data Center Virtualization Projects

Neil MacDonald

In 2007, we addressed the security considerations and best practices for securing virtual machines in "Security Considerations and Best Practices for Securing Virtual Machines." We further refine this advice here in this research note based on thousands of discussions with clients and the top virtualization risks that concern them. This research is targeted for information security and IT operations professionals responsible for the secure deployment and operations of virtualized data center infrastructure.

Key Findings

- Virtualization is not inherently insecure. However, most virtualized workloads are being deployed insecurely. The latter is a result of the immaturity of tools and processes and the limited training of staff, resellers and consultants.
- The virtualization platform will become the most important x86-based IT platform in the next-generation enterprise data center.
- The combination of more workloads being virtualized and workloads becoming more mobile creates a complex and dynamic environment that will be more difficult to secure.

Recommendations

Use the risks and multiple recommendations provided in this research as a guideline for assessing the security of your virtualized infrastructure. Most importantly:

- Treat the virtualization platform as the most important IT platform in your data center from a security and management perspective.
- Establish policies now for the consolidation of workloads of different trust levels using virtualization before these situations are widely encountered.
- When evaluating security and management tools, favor those that span physical and virtual environments with the same management, policy and reporting framework.
- This research also applies to "cloud" environments where the underlying computing model is based on virtualization. Require potential cloud-based service providers to adequately address these risks before consideration for sensitive workloads.

WHAT YOU NEED TO KNOW

Gartner research indicates that, at YE09, only 18% of enterprise data center workloads that could be virtualized had been virtualized, with the number growing to more than 50% by YE12. 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. This research describes the most frequently occurring issues encountered and offers specific recommendations on how each issue might be addressed.

STRATEGIC PLANNING ASSUMPTION

Through 2012, 60% of virtualized servers will be less secure than the physical servers they replace, dropping to 30% by YE15.

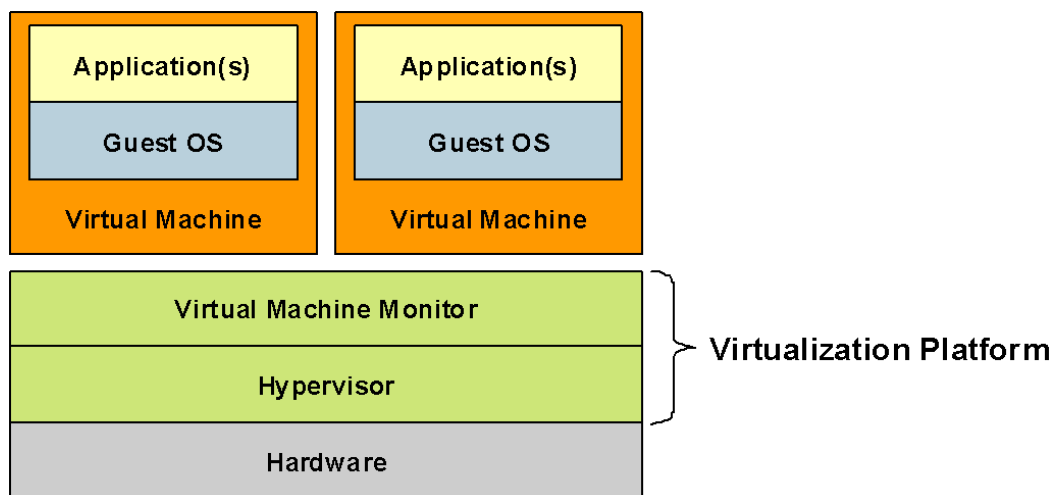
ANALYSIS

In 2007, we addressed the security considerations and best practices for securing virtual machines in "Security Considerations and Best Practices for Securing Virtual Machines." In this research, we refine this advice based on thousands of discussions with clients and the top risks that concern them.

Risk: Information Security Isn't Initially Involved in the Virtualization Projects

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 — an improvement from the same survey a year earlier where 50% indicated that they didn't proactively involve information security. Typically, the operations teams will argue that nothing has really changed — they already have skills and processes to secure workloads, OSs and the hardware underneath. While true, this argument ignores the new layer of software (see Figure 1) in the form of a hypervisor and virtual machine monitor (VMM) that is introduced when workloads are virtualized.

Figure 1. The Virtualization Platform



Source: Gartner (January 2010)

The argument also ignores other concerns, such as the potential loss of separation of duties (SOD) and workload segregation that may be undermined in a virtualized environment. In many cases, additional tools aren't necessary, and simply updating existing processes is all that is needed. In other cases, additional tools or training may be required. Ideally, all of these needs would be identified proactively, so that, where changes to processes or training or additional or updated tools are needed, funding from the server consolidation project is still available.

Recommendations

For information security professionals:

- Risk that isn't acknowledged and communicated cannot be managed. If you haven't already engaged with the teams performing the data center consolidation and virtualization projects, do so in 2010.
- Start by looking at extending your security processes, not buying more security products (see "Toolkit: Formalizing Security Processes"), to address security in virtualized data centers.
- Don't say "no" without justifiable cause. There will always be IT-related risks — physical or virtual. While the risks outlined in this research cannot be completely eliminated, they can be mitigated to a level that is manageable. Communicate the risks, and offer alternatives to reduce or eliminate them.

For IT operations professionals:

- If you haven't already, proactively get the information security organization involved in the planning and architecture for a secure, virtualized data center.

For both teams:

- In some cases, new tools and/or process changes may be needed. Budget for these out of the projected cost savings associated with the virtualization project.
- Since risk cannot be eliminated, pivotal to success are understanding and identifying who is responsible for assuming which risks within the virtualized infrastructure as well as deciding whether investments to reduce the risk are warranted.

Risk: A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads

As shown in Figure 1, the virtualization layer represents another important IT platform in our infrastructure. Like any software written by human beings, inevitably, this layer will contain embedded and yet-to-be-discovered vulnerabilities that may be exploitable. Given that privileged level that the hypervisor/VMM holds in the stack, hackers have already begun targeting this layer to potentially compromise all the workloads hosted above it. While thinner hypervisor/VMM architectures reduce the surface area for attack, this reduces, but does not eliminate, the risk of vulnerable code. Further, we must also be concerned with vulnerabilities in *any* code loaded at this layer (such as drivers, plug-ins and third-party switch code), which also may introduce vulnerabilities. Complicating the situation is that the hypervisor/VMM layer is designed to be transparent to the OS workloads (including security and management tools) running within an OS on top of this layer, leaving most existing tools blind to issues at this layer unless they have been specifically designed to talk to and assess this layer. From an IT security and management perspective, this layer must be patched, and configuration guidelines must be established.

Recommendations

- Treat this layer as the most critical x86 platform in your enterprise data center:
 - Establish explicit guidelines for secure virtualization platform configuration.
 - Ensure your deployed configurations adhere to your standards, and monitor periodically for drift. Require your existing configuration management tools to support the monitoring of the hypervisor/VMM layer (some do, some don't).
 - Monitor and log changes at this layer. Alarm or block unauthorized changes.
 - Clearly identify which team is responsible for monitoring, prioritizing and testing patch releases from the virtualization platform vendor. Make this the same team that is responsible for patching critical systems in physical environments.
 - Extend existing patch and vulnerability management processes and tools to address the patching of this layer and any associated drivers, plug-ins or other software that may run at this layer.
 - Scan periodically to ensure patches of the hypervisor/VMM software that you believe are applied have indeed been applied.
- Keep this layer as thin as possible, and harden the configuration to unauthorized changes:
 - Favor thinner architectures that don't use a general-purpose OS (even a thinned-down version) as the platform for the VMM.
 - Place the hypervisor in flash or similar nonvolatile storage to reduce risk from tampering.
 - Restrict the ability to place arbitrary code in the hypervisor/VMM level and thoroughly test drivers, security software and any other code that may be loaded in this layer.
 - Require the use of signed device drivers and code loaded at this layer (not perfect, but a start).
 - Require vendors of solutions that will place code in this layer to show evidence of security testing during development to reduce vulnerabilities.
 - Require virtualization vendors to support measurement of the hypervisor/VMM layer on boot up to ensure it has not been compromised (see "Secure Hypervisor Hype: Myths, Realities and Recommendations" and "Building Blocks for Trusted, Secure Hypervisors").
- Require your intrusion prevention system (IPS) vendors to research, lab test, and support signatures and rule sets for protecting against network-based attacks on your virtualization platforms.
- Do not rely on host-based security controls to detect a compromise or protect anything running below it.

Risk: The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms

For efficiency in VM-to-VM communications, most virtualization platforms include the ability to create software-based virtual networks and switches inside of the physical host to enable VMs to communicate directly. This traffic will not be visible to network-based security protection devices, such as network-based IPSs. If inspection of this traffic is desired, it may be necessary to place an IPS inside the server (using either a host-based network or virtualized network-based IPS) to inspect this traffic. Alternatively, internal traffic could be mirrored or sent to external network-based IPS inspection devices. However, this is inefficient in already-constrained input/output systems.

Recommendations

- At a minimum, require the same type of monitoring you place on physical networks so that you don't lose visibility and control when workloads and networks are virtualized.
- Discuss whether or not visibility of this traffic is required. Many organizations do not have inspection of traffic between servers on the same switch, and there may be no reason for this in a virtualized server between VMs on the same virtual switch.
- Placing a host-based software firewall and/or IPS solution inside of every VM is an alternative; however, this may create significant management overhead.
- As an alternative to host-based software in each VM, network-based virtual firewalls or IPSs may be deployed as virtual appliances (see "Software-Based Appliances: A Moment of Convenience, a Lifetime of Regret") to provide this visibility (see Note 1), but the cost and complexity of these solutions must be considered.
- Solutions for inspection external to the physical server are available, but they carry input/output implications:
 - Export the network traffic flow (NetFlow) data for external analysis.
 - "Tap" the internal virtual switch, and route the traffic to an external intrusion detection system (IDS).
- Pressure physical network- and host-based firewall and IPS vendors to support software-based implementation of their solutions within the virtualization platform.
- To reduce the chance of misconfiguration and mismanagement, favor security vendors that span physical and virtual environments with a consistent policy management and enforcement framework.

Risk: Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation

As organizations move beyond the "low-hanging fruit" of workloads to be virtualized, more critical systems and sensitive workloads are being targeted for virtualization. This is not necessarily an issue, but it can become an issue when these workloads are combined with other workloads from different trust zones (also referred to as "trust domains" — see "The Structure and Content of an Information Security Architecture Framework") on the same physical server without adequate separation. Examples include virtualizing demilitarized zone (DMZ)-related workloads (see

"Server Virtualization Can Break DMZ Security"), Payment Card Industry (PCI)-related workloads or other sensitive workloads (see Note 2). Over time, maintaining separation will become more difficult as workloads routinely move around between physical servers in dynamic, adaptive data centers.

Recommendations

- At a minimum, require the same type of separation required in physical networks today for workloads of different trust levels within the enterprise data center.
- Treat hosted virtual desktop workloads as untrusted, and strongly isolate them from the rest of the physical data center.
- Do not use virtual LANs (VLANs) alone for security separation of sensitive workloads within a virtualized server. Gartner does not consider VLANs alone as sufficient for security separation, whether the workloads are physical or virtual (see "Findings From the 'Client Inquiry': VLAN Separation Is Not Security Separation").
- Evaluate the need for point solutions that are able to associate security policy to virtual machines' identities and that prevent the mixing of workloads from different trust levels on the same server (see Note 3).

Risk: Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking

When multiple physical servers are collapsed into one, there are several areas that risk loss of SOD. Because of the critical support the hypervisor/VMM layer provides, administrative access to this layer must be tightly controlled. This is complicated by the fact that most virtualization platforms provide multiple paths of administration for this layer — for example, administration via the browser; direct from the server console; and from scripts, remote shell command line interfaces, virtual management center tools and so on. Virtualization management tools including those that provide live migration capabilities should also be considered extremely sensitive and access-restricted.

Recommendations

- Restrict access to the virtualization layer as you would with any sensitive OS.
- Favor virtualization platforms that support role-based access control of administrative responsibilities to further refine who can do what within the virtual environment.
- Ensure that all possible administrative paths to the hypervisor/VMM have been covered by whatever administrative access control solution is used.
- Pressure shared-account/software-account password management (SAPM) vendors (see "Market Overview: Shared-Account/Software-Account Password Management Tools") to address virtualization platforms without requiring third-party tools.
- Where regulatory and/or compliance requirements dictate, evaluate the need for third-party tools to provide tight administrative control.
- Activate full auditing and logging, and link these into security information and even management systems.

- Place administrative tool usage onto a dedicated network segment with limited access and tight access controls.
- Since most virtualization platform vendors don't encrypt live migration traffic, further separate this traffic onto another network segment with limited access and tight access controls.

Risk: There Is a Potential Loss of SOD for Network and Security Controls

When physical servers are collapsed into a single machine, it increases the risk that both system administrators and users will inadvertently gain access to data that exceeds their normal privilege levels. Another area of concern is which group configures and supports the internal virtual switch. This should be the same team that configures and supports virtual switches in the physical environment, but often it is the ESX administrator. This creates SOD issues between network operations and server operations, with the potential to inadvertently or purposefully disable network-based separation and security controls.

Recommendations

- The same team responsible for the configuration of network topology (including VLANs) in the physical environment should be responsible for this in virtual environments.
- Favor virtualization platform architectures that support replaceable switch code so that the same console and policies span physical and virtual configurations.
- Favor virtualization platforms that support role-based access control of the internal virtual network configuration that can be separated out at a granular level from administration of the hypervisor and other operational and management responsibilities.
- Monitor sensitive virtualized security controls, such as a virtualized firewall, to ensure that they are not tampered with or disabled by operational administrators.
- Evaluate and require virtualized network security controls to fail open or fail closed as appropriate to your policy.
- In smaller organizations where this cannot be broken out, use granular auditing and logging as a preventive control, or require the use of different IDs and passwords, depending on whether network configuration is being modified.

Note 1

Examples of Virtualized Network Security Control Vendors

- Altor Networks, which was formed by former Check Point employees
- Apani, which offers identity-based network access control within virtualized environments
- Astaro Security Gateway (ASG)
- Catbird V-Agent, which offers Snort-based IDS/IPS, network access control (NAC) and vulnerability assessment
- Check Point, which released its virtual firewall in 2008 and is working on the next generation

- Enterasys, which has IPS capabilities supported as a VM monitoring the virtual network
- IBM, which released its Virtual Server Security for VMware virtual appliance in December 2009
- McAfee, which acquired Secure Computing in late 2008 and offers its firewall/IPS combination as a virtual appliance (but not yet IntruShield)
- Microsoft, which released a virtual appliance version of its ISA Server in 2008
- Montego Networks, which offered a virtual firewall/IPS but is now defunct
- RedCannon, which offers a virtual appliance solution providing firewalling, IPS and VM policy enforcement within virtualized environments
- Reflex Systems' Reflex Virtual Security Appliance (VSA)
- Sourcefire, which has announced a virtual appliance implementation of its RNA and Snort-based IPS offerings
- StillSecure's Strata Guard Free, which provides firewalling and IPS, but in a rate-limited offering
- Stonesoft, which has released its virtual firewall and IPS appliance
- Trend Micro, which offers its Deep Security IPS (acquired with Third Brigade) and Core Protection for Virtual Machines for VMware environments
- VMware, which delivered its vShield Zones technology with vSphere 4 and higher (based on the Blue Lane technology it acquired in 2008)

Note 2

Other Examples of Common Workloads of Different Trust Levels Requested to Be Combined

- Development and test workloads and production workloads
- Hosted virtual desktop-related workloads with other data center workloads
- Systems hosting personally identifiable information or other sensitive information with other nonsensitive information
- Sarbanes-Oxley Act (SOX)-related workloads and non-SOX-related workloads

Note 3

Examples of VM Life Cycle Management and Policy Enforcement Vendors

- Embotics
- Fortisphere
- ManageIQ

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509