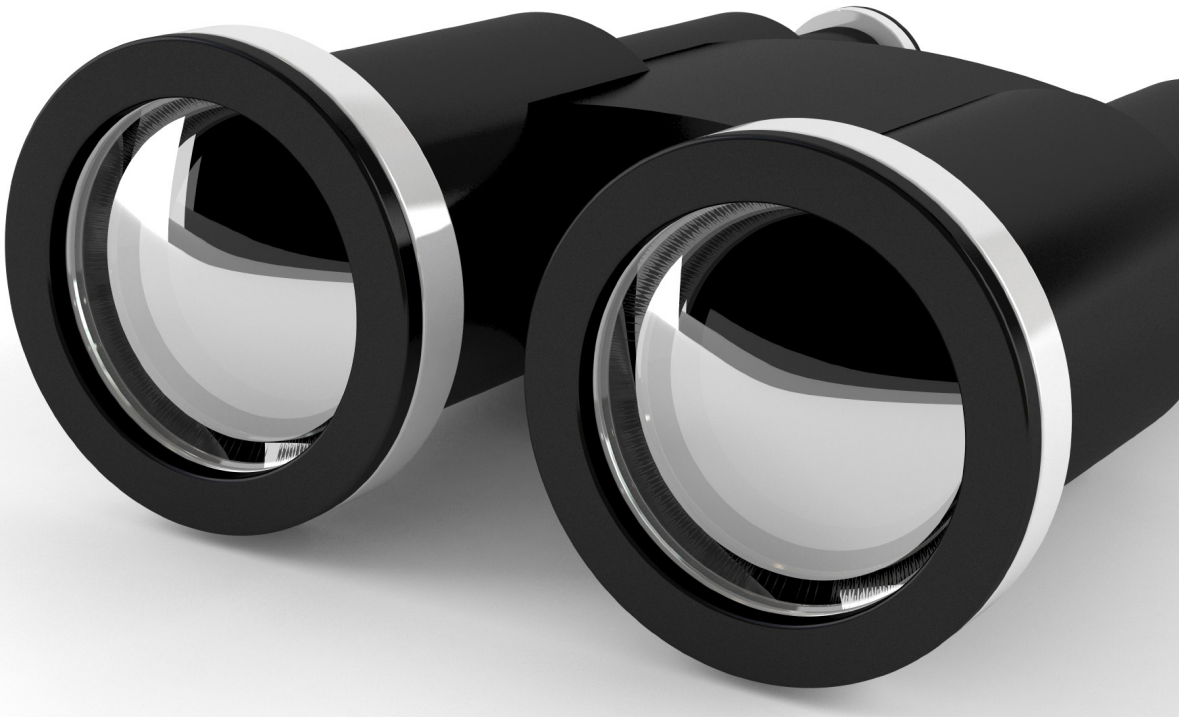
SOPHOS

simple + secure

IT Security Trends

A strategic overview featuring **Gartner** content

In this issue



Featuring research from

Gartner

Introduction: Virtualization Security Strategies for Today's Businesses

In the past few years, virtualization technology has transformed the data center—it's now a primary supporting platform for many businesses. Since server virtualization reduces costs and offers high availability and deliverability, many organizations look to extend these benefits to virtual desktops.

If you plan to—or currently use—virtualization technology, read this newsletter: It provides tips and tricks you need to deploy and maintain a secure virtualization environment. This newsletter also examines strategies for protecting both desktop and server virtual environments, previews emerging technologies for advanced protection and—most importantly—helps you secure both the protection and performance you need.

We invite you to learn more about virtualization technology and about securing your business at every level. Visit Sophos.com today.

Strategies for Protecting Virtual Servers and Desktops: Balancing Protection with Performance

Virtualization Today

Over the past few years, virtualization technology has transformed the data center. Server virtualization enables multiple virtual servers to run off the computing power of one physical server; and due to the well-established cost benefits, this technology has become widely adopted. Now, enterprises are looking to extend these benefits to virtual desktops.

Desktop virtualization is still in the early stages, but also holds promise for both business transformation and operational cost savings.

This paper explores the security challenges of virtualization. It reviews today's strategies for protecting virtual environments and previews emerging technologies for more advanced protection. Overall, it will guide you to securing both the protection and performance you need.

Realizing the Benefits of Virtualization

Virtualization technology enables you to do more with fewer resources—saving you both time and money.

With server virtualization, groups of servers can be configured into reusable pools. This initially offered the benefit of hardware cost reduction; however, the technology has continued to progress to include the benefits of high availability and reliability. This translates into a savings of 50-70% of total IT costs.

The case for server virtualization has been so compelling that over 50% of server licenses sold today are for virtual servers, not physical, according to market research firm IDC.

Organizations are now looking at virtualizing their desktops. Adoption is still low, with only 1% of desktops virtualized, but enterprises see the benefit, and this market is growing fast. Gartner forecasts an 84% compound annual growth rate (CAGR) between 2008 and 2013, with the desktop virtualization market growing from $38 million to $795 million during that five year span.

The primary benefit of desktop virtualization is business enablement. As today's employees require greater flexibility and mobility, the ability to access their desktop from any device—laptop, Internet cafe, iPad, or smartphone—has clear productivity advantages. With desktop virtualization, all of the programs, applications, processes, and data from the user's desktop are kept and run centrally enhancing data security. Additionally, from IT's perspective, desktop virtualization enables the implementation of a corporate standard.

One of the complexities of desktop virtualization is that it requires investments in infrastructure as well as change management. This includes upgrading servers in the data center and thin client

hardware devices, along with new user training and usage policies. So cost savings are likely to take longer to pay back than with server virtualization.

Security Challenges in a Virtual Environment

Virtualization technology itself provides some specific security benefits. For example, it is easier for you to provide dedicated servers to run mission-critical software applications. There's also a viewpoint in the industry that security in a virtual environment is increased because the data for different business functions can be isolated. For example, you can provide a dedicated server for Finance and a separate one for Human Resources.

However, Gartner analyst Neal MacDonald has estimated that "60% of virtualized servers will be less secure than the physical servers they replace, with that number dropping to 30% by 2015." In his January 2010 report, "Addressing the Most Common Security Risks in Data Center Virtualization Projects," the most common virtualization security risks cited include:

- Information security isn't initially involved in the virtualization projects (About 40% of the surveyed organizations had not brought security professionals into the projects).
- A compromise of the virtualization layer could result in the compromise of all hosted workloads (also known as a hypervisor attack).
- Workloads of different trust levels are consolidated onto a single physical server without sufficient separation.
- Adequate controls on administrative access to the hypervisor (Virtual Machine Monitor) layer and to administrative tools are lacking.

It should be noted that while a possibility that virtualization could introduce new risks—such as a hypervisor attack—security vendors continue to monitor the situation, and as of yet, no threats have been identified in the field. So, at this point, the threat remains theoretical.

While there is a great deal of hype around these new threats and new methods of delivering security for virtualization, in practice, you should keep the basics in mind. This means applying existing physical security practices to your virtual machines (VMs).

However, there are performance constraints that you will need to address. Many companies have rushed to virtualize in order to realize cost savings, yet security needs to be carefully considered to ensure you get the best performance.

Essential Elements of Endpoint Security for Virtual Machines

To get the best protection across your entire organization, you need full endpoint security on your virtual computers just as you'd install on your physical computers—not just basic antivirus. And, since operational cost savings are key, you'll need easy management and deployment as well.

With physical machines, there is a 1:1 ratio—every physical machine gets updated with its own copy of antivirus software. Yet, in a virtual environment, new system constraints are introduced as a result of one physical host supporting ten or more VMs—all sharing the same CPU, I/O, and memory.

This bottleneck can be more apparent in desktop virtualization because there are more VMs per server. As a result, performance issues are more noticeable to users.

Two critical elements of endpoint security—updating and scanning—are particularly impacted by the system constraints of virtualization:

Updating

Updating covers a number of aspects, from the process of implementing the regular signature updates, to monthly software upgrades:

- One of the issues with updating is "the Monday 9:00 a.m. problem." This problem arises when all the VMs retrieve updates at the same time, impacting network performance.
- Another updating issue is memory use. Having local copies of virus data on every VM means that each physical host is carrying more data in memory than it really needs.
- A third issue is processing updates. Large amounts of system resources are used up with every update, with an even greater impact than updating the virus data.

Scanning

On-demand scanning issues in a virtual environment fall into two areas:

- First, you may not have sufficient time to complete all of the scans in a certain time period. In this scenario, you're looking to complete a number of scans in a defined time period. Scans can be staggered, but at some point there won't be enough time for weekly updates for hundreds of machines.
- Second, end user performance can be impacted as a result of concurrent scans. The impact of multiple VMs using one set of physical computing resources at the same time results in poor user experience, which is why staggering is recommended. However, if a malware outbreak occurs, you need to carry out full scans, but could be prevented from doing so due to the resources required.

Balancing Protection with Performance

Since many organizations now see virtualization technology as an increasingly important part of their network, it's important that any investment in virtualization is properly secured, without compromising performance.

Without advancements in virtualization technologies, it's difficult for security vendors to provide customers with a true balance of protection and performance. Recent enhancements by virtualization vendors and security vendors have focused more on the performance aspect, helping companies to get more VMs per physical machine, but at the expense of full endpoint security.

Right now, it may appear that you have to choose either performance or protection. Both routes have pros and cons; strategies for balancing the two are outlined below. With virtualization, you also need to think longer-term, as emerging virtualization technologies will enable better security solutions.

Today's Strategies for Protecting Virtual Environments

At present, there are a number of strategies for protecting virtual servers and desktops and maximizing performance.

With servers, there are more choices. You can install antivirus protection optimized for virtualization, and then add protection with other server tools.

However, with desktops, you can't afford to compromise on security. Therefore key protection features like Application Control, Device Control, Proactive Antivirus/ Host Intrusion Prevention System (HIPS), and URL Filtering, all need to be considered.

In order to get the most VMs per host without impacting performance, any solution you choose should minimize the scanning impact across multiple VMs, and reduce the updating impact across the network and the storage on physical hosts.

Employ these five best practices to get the best protection and performance right now:

- Optimize scanning and updating—Deploy a product that enables you to schedule scans and stagger updates so that the impact on the users is minimal.
- Reduce management costs—Implement a solution that is easy to manage alongside the existing security that you've deployed for your physical machines. Operational costs can increase even as you reduce hardware costs, so you need to make sure that all of your protection—for physical and VMs—can be managed and updated in tandem. Ensure that you aren't exhausting unnecessary amounts of time and resources to manage security for your virtual environment.
- Deploy solutions that need less memory—Space is always at a premium, so when you're looking to get the maximum number of VMs per physical machine, you don't want products to eat up memory unnecessarily. Look for security products that keep memory usage low, especially when carrying out potentially intensive tasks such as scheduled scanning or updating.
- Protect offline images—You can improve performance and user experience by considering the protection of your virtual images when they're offline. By addressing the scanning of offline images when they come back online, you can reduce the impact on systems and users by either scanning the images while they are offline or by using centralized scanning so the scanner is up-to-date.
- Change the way you scan—If you can reduce the number of files you need to scan, you can vastly improve performance. When creating virtual desktops from a gold image, once you've scanned the image, you don't need to scan each instance of that image. You can reduce scanning requirements to the files on the virtual desktops that differ from the master gold image.

The Evolution of Virtualization Security

As virtualization technologies advance over the coming years, it will be easier for security vendors to provide more functionality without impacting performance, so that you'll get the best of both worlds. Most companies considering an investment in virtual desktop technology are still in the planning stages. So, by taking a longer-term approach and looking at both current and emerging security technologies, you can plan for more VMs and better protection.

At present, to get the best performance, virtualization vendors have been working with security vendors to minimize the impact security has on the systems. But, as discussed earlier in the paper, this has been achieved by removing some of the key

protection features. This poses a potential security issue when it comes to desktop virtualization. So, the current solution of centralized scanning has performance benefits, but also limits protection.

It's important to think about security for virtual desktops are more than just antivirus protection. What we see happening now, is that security vendors are working with virtualization vendors to improve the virtualization technologies so that through the centralized scanning route, security vendors will be able to provide more of the key endpoint protection features, such as HIPS, URL Filtering, Data Loss Prevention (DLP), Application Control and Device Control.

In conclusion, our strategy is to deliver the same security on VMs that you would expect on your physical machines. Our goal is to do this without compromising performance, so that the maximum number of VMs per host can be achieved.

Our current security strategies work to achieve the best balance possible between protection and performance. And, we're continuing to work on new security solutions—in conjunction with evolving virtualization technology—to deliver the best protection for both physical and virtual endpoints.

Source: Sophos

A Practical Guide to Keeping Your Virtual Data Center Safe

In the past few years, virtualization has transformed the data center. It's now a primary supporting platform for many enterprises. A wide variety of virtualization technologies are available, but only a small number of these technologies have made it to mainstream deployment.

Server virtualization is the best example of the technology in the mainstream. It started out with the offer of hardware cost reduction and has progressively shifted to the delivery of high availability and reliability. A virtual server infrastructure now provides more than a cost benefit; it also can do the job better than most physical equivalents.

This whitepaper focuses on the best practices for the protection of virtual servers running in the data center.

Top 10 tips: Server virtualization

1 Be cautious of a casual loss of system segregation.

The traditional physical infrastructure in many networks had a degree of segmentation—separating machines of different functions or risk levels in to groups in which access, security controls or monitoring levels were varied appropriately. In many enterprises, the focus on consolidation has compromised separation. For example, should you host your DMZ web server on the same virtual network and physical server that hosts your domain controller? As you deploy machines, try to do so with similar roles or risk levels into groups (most virtualization technologies enable you to deploy machines in groups and apply different policies. Some even provide virtual network segmentation in the form of virtual VLANs). This problem can grow as

So what is the problem?

There has been much discussion of potential new attack vectors in virtual systems, such as Blue Pill, Red Pill and hypervisor (or virtual machine) rootkits. Any software can have vulnerabilities and the virtualization layer is no exception to this rule. Although such attacks are viable, the more common attack vector remains identical to that of physical systems. Malicious code, exploits and hackers are still major risk—targeting the application layer and the user (through social engineering) rather than shifting to expensive and difficult new attack vectors.

Over time, an increase in attacks on the virtualization layer is likely. However, it's likely that attacks on the OS or application layer will remain the majority. Unfortunately, while many enterprises chase protection against the new class of potential threats in development, they ignore the basics, which leads to high risk of compromise. Equally, compliance standards are applicable to virtual systems, but enterprises typically overlook them.

New protection models to secure virtual systems are emerging, such as the idea of scanning multiple virtual machines from a single point using hypervisor inspection. Moving protection capabilities outside the virtual machine could make attack from malware significantly more difficult, providing more comprehensive and robust protection. Many of these new models hold great promise for delivery of better security but are still immature. There's a great deal of work that needs to be done before these models can provide an effective, stable replacement to existing protection.

Until these areas mature and the nature of the threat evolves, enterprises need to ensure they extend their existing protection in to the virtual world. Security is not a new practice and virtualization doesn't invalidate the many years of knowledge security practitioners have acquired. In short, the fundamental existing framework for IT security has not drastically changed, but there are opportunities for optimization and considerations for a virtual environment.

organization transition to the cloud. Virtual systems that host different customers' data must be isolated appropriately across a shared infrastructure.

2 Run endpoint security software inside your virtual machines.

Modern endpoint security doesn't just look at files. Rather, it uses behavioral inspection technology and visibility of applications such as the browser, to keep the bad guys out. Running endpoint security inside the virtual machine provides effective protection and help with clean up, if needed. It is a common misconception that virtual machines are less vulnerable to malware. Although it can be easier to reverse the changes made by malware, virtual machines are as susceptible to threats that steal data or compromise enterprise operations. Every virtual machine requires exactly the same level of security as its physical counterpart.

3 Maintain a provisioning task or library that contains your security configuration and products.

Whenever you provision a new system, ensure the right core security controls are in place. Most virtualization technologies now include the concept of a workload or let you embed options in a library for provisioning. Take advantage of these to make sure any image you deploy meets your security and compliance requirements.

4 Have a plan for ongoing patching and maintenance.

Patching the operating system and applications within the virtual machine is critical for security. You should be able to use the agents used in your physical environment, but make sure you provide for the dynamic nature of virtual machines. Compliance reporting on your virtual machines and identifying decommissioned vs. offline images is important to ensure you maintain your system security.

5 Encrypt your sensitive virtual images.

Physical devices such as laptops can go on the move and there is a risk they may be lost, which provides access to data by unauthorized users. Virtual machines can be even more mobile—passing between different physical systems liberally. Virtual images can have full-disk encryption applied as well, ensuring that they're protected even if they are lost or transferred to a less than trusted storage location. You may want to consider this if you're considering using "the cloud" (or another infrastructure you do not have full control over) to host your virtual machines.

6 Implement security vendor best practices for performance in a virtual environment.

Often, the biggest challenge in securing a virtual system is balancing security with performance. Your security vendor should provide you with best practices that enable you to run your security technologies effectively.

Common examples of performance issues include:

- Highly intensive I/O tasks can degrade the performance of a virtual system. For example, multiple virtual machines that perform antivirus scans at the same time will degrade performance. Make sure you either size your virtual infrastructure to deal with such peaks or implement best practices to mitigate this condition.

- Memory waste. Virtual systems provide value by consolidating multiple systems. The more streamlined the system is, the more you can run and the better your TCO becomes. Running many security agents with the same data loaded in memory can waste valuable resources. Implement best practices to avoid memory waste.
- Network I/O can also degrade service. Updates for security agents, like antivirus or patch, can cause peaks of network activity. Try to provide local high-speed replicas of such data or separate your management.

7 The security of the virtual machines depends on the security of the host.

Whether it's a proprietary operating system (such as ESX) or a general purpose OS, keep the host surface area as small as possible to minimize the possibility of compromise. Reduce the additional installed applications and use cases that might lead to compromise. Doing so will your host attack surface area is as small as possible.

8 Manage the rights to your virtual infrastructure.

Virtualization management systems include a wealth of new rights that need to be managed. Having the ability to provision a new server (e.g., a domain controller) could compromise your security or disrupt your services. Ensure that you have appropriate restrictions for who can provision what and who can control change configuration. Excercise caution, especially if you're using the new end-user selfserve capabilities offered by vendors, such as VMware.

9 Map out your virtual infrastructure and check your access controls at each location.

Virtual infrastructure is often used to deliver high availability, resilient services that can involve moving virtual machines to different systems or even countries dynamically. Map out where virtual machines could move and validate that each of these locations meets your compliance and security standards (both software and physical). Remember that virtualization decouples physical and logical resources (such as storage). So consider the physical devices as well as their virtual counterparts. One frequent example: moving a sensitive system to a network storage location with overly liberal access controls.

10 Patch your virtualization software.

Although it's not the major attack vector, vulnerabilities in virtualization software can break isolation. Keeping virtualization software patched will reduce the probability of such attacks as they surface.

Summary

Virtualization technology is an extremely powerful, widely adopted technology. While there's a great deal of hype around new threats and new methods of delivering security in practice it's about applying existing, tried and tested practices tailored meet the performance constraints of the virtual environment. As the nature of the threat evolves and virtualization technology is deployed in new ways, so too will Sophos products.

Sophos recommends the following when using virtualization technologies:

- Do not abandon core controls like antivirus. These are as required in a virtual environment as a physical. Simply apply best practices to make sure they're effective.
- Watch new virtualization security developments closely. There are great opportunities in this area as they mature, but still have to prove value over tried and tested methods.
- Don't forget to use the extra security capabilities available in virtualization technology. This includes the ability to tightly manage roles and responsibilities over virtual systems.

Source: Sophos by James Lyne, Senior Technologist

From the Gartner Files:

Addressing the Most Common Security Risks in Data Center Virtualization Projects

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.
- 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.

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.

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.

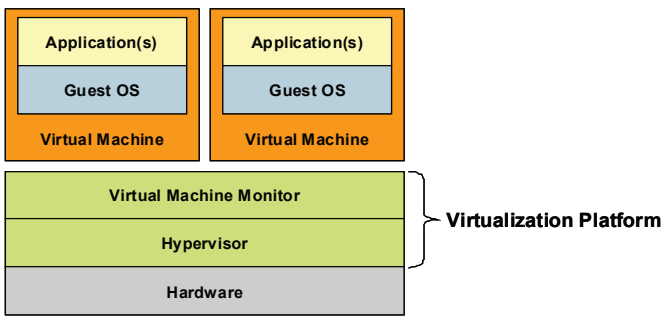
The argument also ignores other concerns, such as the potential loss of separation of duties (SOD) and workload segregation that may be undermined in a virtualized environment. In many cases, additional tools aren't necessary, and simply updating existing processes is all that is needed. In other cases, 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, 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.

Figure 1. The Virtualization Platform



Source: Gartner (January 2010)

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.
- 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 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") on the same physical server without adequate separation. Examples include virtualizing demilitarized zone (DMZ)-related workloads, Payment

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)

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.
- 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.

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

- 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 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.

Source: Gartner RAS Core Research Note G00173434, Neil MacDonald, 25 January 2010

About Sophos

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing security and data protection solutions that are simple to manage, deploy and use and that deliver the industry's lowest total cost of ownership. Sophos offers award-winning encryption, endpoint security, web, email, and network access control solutions backed by SophosLabs - a global network of threat intelligence centers. With more than two decades of experience, Sophos is regarded as a leader in security and data protection by top analyst firms and has received many industry awards.

Sophos is headquartered in Boston, US and Oxford, UK. More information is available at www.sophos.com.

SOPHOS