SOPHOS

A practical guide to keeping your virtual data center safe

by **James Lyne**, Senior Technologist

In the past few years, virtualization has transformed the data center. It is 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 will focus 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 this separation. For example, should your DMZ web server be hosted on the same virtual network and physical server as 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 differing policies, or even provide virtual network segmentation in the form of virtual VLANs). As the transition to the cloud continues, this problem can grow. Virtual systems that host different customers' data will need to be isolated appropriately across a shared infrastructure.

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 the 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 is 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 is a great deal of work 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 does not 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.

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 will provide effective protection and clean up if things go wrong. 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 that the right core security controls are in place. Most virtualization technologies now include the concept of a workload or enable you to 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 same agents you did in your physical environment, but make sure you have provided for the dynamic nature of virtual machines. Compliance reporting on your virtual machines and identifying decommissioned vs. offline images is important to ensure you are maintaining 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 are protected even if they are lost or transferred to a less than trusted storage location. You may want to consider this particularly if you are considering the use 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 dealing with performance problems. 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 anti-virus 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 lots of 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 anti-virus 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 to ensure 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. Being able to provision a new server (e.g., a domain controller) could compromise your security or have a disruptive impact on your services. Ensure that you have appropriate restrictions for who can provision which systems and who can control change configuration. Be particularly cautious of this if you are using the new end-user self-serve 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 might 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 make sure you think about the physical devices as well as their virtual counterparts. One frequent example of this is 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, there have been vulnerabilities in virtualization software that have broken 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. Whilst there is a great deal of hype around new threats and new methods of delivering security in practice it is 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 for using virtualization technologies:

- **Do not abandon core controls like anti-virus.** These are as required in a virtual environment as a physical. Simply apply best practice to make sure they work effectively.
- **Watch new virtualization security developments closely.** There are great opportunities in this area as they mature but as yet have to prove themselves 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.

Sophos & Virtualization

Sophos products are designed to work in a virtual environment. You can find our best practice advice on deploying Sophos in virtual environments at http://www.sophos.com/support/knowledgebase/article/110507.html.

Sophos products fully support a range of virtual platforms. Remember to check that all your security software is fully supported in a virtual environment. Some will offer degraded support levels, or perhaps not support it at all! When your critical infrastructure runs on a virtual platform, it pays to make sure you will have the support that you need.

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM