SOPHOS

Strategies for Protecting Virtual Servers and Desktops

Balancing Protection with Performance

by Jonathan Tait, Product Marketing Manager

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 is 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 Neil MacDonald has estimated that "60 percent 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[1]," the most common virtualization security risks cited include:

- Information security isn't initially involved in the virtualization projects (About 40 percent 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 there is 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 anti-virus. 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 anti-virus 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

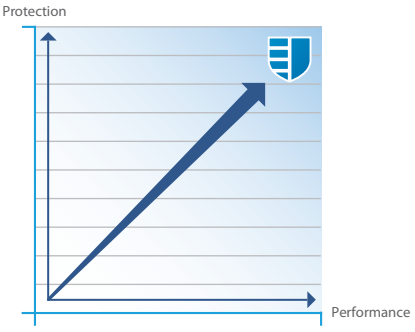
On-demand scanning issues in a virtual environment fall into two areas:

- First, you may not have sufficient time to complete all of the scans in a certain time period. In this scenario, you are 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 is important that any investment in virtualization is properly secured, without compromising performance.



With Sophos you get both protection and performance

Without advancements in virtualization technologies, it is 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 anti-virus 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 Anti-virus/ 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 are 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 are 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 have scanned the image, you don't need to also scan each instance of that image. You can reduce scanning requirements to the files on the virtual desktops that differ from that 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 will 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, in order 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 is limiting protection.

It is important to think about security for virtual desktops as more than just anti-virus 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.

For more tips, check out the Sophos white paper "Practical Guide to Keeping Your Data Center Safe" at www.sophos.com/security/topic/keep-your-virtual-data-center-safe.html

1. Gartner, "Addressing the Most Common Security Risks in Data Center Virtualization Projects," by Neil MacDonald. 25 January 2010. http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1288115

© Copyright 2010. Sophos Plc. All rights reserved.
All trademarks are the property of their respective owners.