



**Lumension**  
SECURITY

## Putting Security First in the Newly Virtualized World

v1.0

Monday, July 07, 2008

[www.lumension.com](http://www.lumension.com)



## Overview:

It's no wonder why virtualization is sweeping its way through the enterprise at breakneck speed. Virtualized machines and virtualization technology provide numerous technical and cost advantages. As organizations virtualize servers, they are able to consolidate hardware, improve space utilization within the data center, save energy and costs. As systems become virtually migrated in real time, virtualization introduces additional value to business continuity and disaster recovery. Virtualization makes it easier to standardize a server image, speed up deployment times and expedite disaster recovery response times. It also makes it possible to run multiple OS platforms on a single system and segregate applications that may otherwise not have played nicely together. All in all, businesses are finding greater flexibility and efficiency through virtualization—which is why it is no surprise that IDC predicts that organizations will spend \$11.7 billion in virtualization services by 2011. Furthermore, IDC predicts the number of virtualized servers will rise at a compound annual growth rate of over 40% from 2005-2010. If true, virtualization spending will more than double in the five years following 2006, when spending hits the \$5.5 billion high-water mark.

Unfortunately, in the haste to realize operational advantages, security is largely being considered as an afterthought. Many organizations have not thought through some of the potential security issues widespread virtualization may cause them after implementation.

At Lumension Security our experts are in tune with the latest security problems posed by virtualization. As a service to the community, and to increase awareness about virtualization security, Paul Zimski, Vice President of Market Strategy, points out the top five security concerns organizations should consider when deploying virtual machines (VMs). In a new and largely untested IT world it is necessary to apply security at every stage of the process, keeping it safe from hackers and data breaches.



## 1. Security is Topology Sensitive

Most of today's leading security products are topology-sensitive, a fact that should concern enterprises as they look at broadening their virtualization initiatives. In general, a security product will want to latch itself onto an IP address, a MAC address, SSID, or some sort of finite attribute.

In many instances enterprises are using virtualization in a grid computing model, allowing virtual operating systems to literally 'float' between racks of servers. The virtualized system does not require being assigned to an individual machine or an individual blade. This flexibility can have considerable reliability benefits, but it can wreak havoc on topology-sensitive security products that expect individual machines to have a fixed location.

## 2. Data Breaches and Hacker Exploits

The introduction of virtualization to an environment also introduces a new set of security threats to that infrastructure. Hackers are starting to become savvy about the virtualized environment and it is only a matter of time before they begin to take advantage of virtualization's unique properties, attacking and infiltrating systems. Security researcher Joanna Rutkowska described a new type of virtualization-based malware that could be used to take control of a machine running virtualization software. Because virtualization allows companies to store many virtualized software "images" of computers on a single physical machine, an attack like the one Rutkowska envisions would allow a hacker not only to control a single machine, but to siphon data from any virtual machine it contains.

Over the past year, security researchers have revealed bugs in practically every piece of virtualization software, including products.

Attackers can use what researchers call "virtual machine escape," or "hyperjacking," to exploit those bugs. By taking control of the hypervisor, the piece of software that controls all the virtual computers within a machine, an attacker can "escape" from any single virtual computer hosted on the machine and quickly multiply his or her access to a company's data.

Another example of a vulnerability within VMWare's disclosed folders is the ability to travel across multiple VMs.

The security community has already released proof-of-concept exploiting the ability to take advantage of the host-guest relationships of virtualized machines on a single physical system. Once these exploits have attacked one virtual machine on the system, it has the capacity to hop to others fairly easily.

Plus, like any other application or operating system, virtualization software is subject to the same kind of security bugs and configuration holes. Developers aren't perfect, after all. As a result, that new layer of virtualization also brings another attack surface for hackers to target.



### 3. Increased Number of Security “Blind Spots”

One of the most problematic aspects of virtualization facing security practitioners today is the increased number of security “blind spots” presented by the virtual environment. In the past, IT staffers could assume that every server was going to be on an individual physical machine, plugging into the network via some sort of 802.11 technology, a plug or a switch. They took advantage of these connections by installing intrusion detection or prevention, firewalls and other security technologies that could monitor traffic going across that wire. But now, in the virtual world, an organization can have multiple operating systems on one physical box and it will be unable to see the traffic between any of these virtual machines sitting on that single system.

Similarly, visibility into the host operating system may be limited by overlaying a virtual network of guest machines on that system. This makes it difficult to find vulnerabilities and assess the correct configuration of the host. As a result, a single vulnerability that may have only affected one machine can now affect dozens.

### 4. Lack of Configuration Control over Offline VMs

Virtualization also poses difficulties with the discovery, assessment and remediation of vulnerabilities for offline VMs. When a virtual machine is taken offline there is often no way for those machines to be discovered. And even once they are discovered it is difficult to tell whether they are compliant with baseline security configurations or whether they have all necessary patches and updates installed.

Say a user installs a virtual machine on their laptop and promptly shuts it down for two months. Then one day the user brings it up to do testing; all of a sudden there's a machine on the network that is two months out of compliance. As this type of scenario begins to play out with increasing regularity, organizations will have more images popping up in their infrastructure that have undetected vulnerabilities, leaving the door wide open for hackers. Blind spots between virtual machines on a single system may also make it difficult to detect when those vulnerabilities are being exploited.

### 5. There's Now a Single Point of Failure

Virtualization makes it easy and convenient to control many virtual machines on a single system. But it also opens up all of those machines to a single point of failure. If something happens to the physical machine, or the hypervisor software that controls all of the VMs within that machine, all of the VMs can be brought down in one fell swoop.

This is problematic on multiple levels. First, if a vulnerability is exploited and hackers are able to gain control over the hypervisor, they will then own all of the systems controlled by that hypervisor. And second, should there be a throughput performance breakdown within any one of the virtual machines or appliances it could have a negative impact on all of the virtual machines on the same piece of hardware. Basically, if one VM is crushed by performance issues, they all are. This makes capacity planning of tantamount importance when considering how security vendors are dealing with virtualization's security issues. Some vendors are starting to make intrusion detection systems a virtual instance on the physical machine in order to shine light on that VM blind spot and monitor traffic between VMs. But these systems increase the amount of communication between the VMs and the likelihood of their failure. Organizations need to ensure



that those virtual intrusion detection systems have enough resources to assure resiliency.

## **Lumension Security and Virtualization**

As a leader in configuration, vulnerability management, and data protection, Lumension has partnered with the industry innovator and leader in virtualization, VMware, to integrate its industry leading solutions into the virtualization fabric. As part of this partnership, Lumension has joined the VMsafe™ alliance, a groundbreaking innovation that leverages the unique capabilities of VMware infrastructure, enabling a rich ecosystem of third party security solutions for virtualized environments.

Security of live, virtualized machines has yet to be analyzed. However, security posed by the new paradigm of virtualization is real and will only worsen as the technology matures. When enterprises look into virtualization, security needs to be at the forefront, implementing solutions that provide innovative security solutions for virtual machines.