Assess virtualization security risk in six simple steps

There are several critical issues every security pro must consider when evaluating risk in virtual environments. This expert tip provides six simple steps to perform a virtualization security risk assessment and highlights key points to ease security integration as your virtualization project comes together.
Assess virtualization security risk in six simple steps

Table of Contents

A six-step virtualization risk assessment process

Four things to remember about server virtualization security concerns

Resources from Intel
A six-step virtualization risk assessment process

To properly evaluate the risks present within their virtual environments, security professionals will need to perform a thorough risk assessment on a regular basis, likely working with both operations and auditing teams in the process. Many teams may not know the best approach to take, or how to get started with performing this kind of specialized risk assessment. The good news is the overall process doesn’t change much from more traditional risk assessment approaches. However, there are certainly specific issues to pay attention to, and we’ll cover those in this six-step virtualization risk assessment process:

1. **Identify virtualized assets and categorize data storage associated with virtualization.** With virtual environments, unfortunately, this can be a very difficult step. Leverage management tools like VMware vCenter and Microsoft’s System Center Virtual Machine Manager (SCVMM) to identify virtual machines, VM storage and hypervisor platforms, and use native storage management tools from vendors like EMC Corp. and NetApp Inc. to keep track of where disk files are located. These disk files should be located on SAN or NAS partitions appropriate to the sensitivity of the data they contain, as with any data classification effort.

2. **Identify and characterize threats to the virtual environment.** Any operating system or application will have the “normal” threats to contend with, such as known exploits and attack scenarios. However, you’ll also need to include threats to the virtualization components themselves, such as virtualization-aware malware, virtual machine “escape” (where an attack affects the hypervisor from inside a VM), and chipset exploits and attacks that are being researched by groups like Invisible Things Labs, which specializes in cutting-edge research in virtualization security, among other areas.

3. **Take stock of vulnerabilities in the various architecture components.** Every major virtualization platform has had a number of vulnerabilities made public, and some are extremely severe. It’s important to know what kinds of issues could affect your systems, and the best sources of information include well-known vulnerability disclosure sources, such as Secunia and CERT, as well as the vendors themselves. Keep in mind that many virtualization platforms have included open source
Assess virtualization security risk in six simple steps

components (such as VMware ESX’s service console), and these can have vulnerabilities that then affect the hypervisor and other virtualization technologies.

4. **Determine the likelihood of successful attack or exploitation, as well as the possible mitigation measures that could be taken to prevent or at the least deter the threat.** For virtualization platforms, this will typically include a range of options: Traditional network and host-based controls like IPS and antimalware software, as well as virtualization-specific controls like Juniper’s vGW Virtual Firewall and VMware vShield products that protect virtual networks, virtualized applications and the VMs themselves.

5. **Determine overall risk.** Once the threats, vulnerabilities and attack likelihood have been evaluated, and potential mitigation measures identified, the overall virtualization risk can be determined. The overall risk will stem from a combination of:

   - **Asset and data value:** Virtualized or not, the systems, applications and data being evaluated should largely determine priority for considering threats, potential attacks and mitigation efforts.
   - **Threats and vulnerabilities:** How vulnerable are virtual systems and architecture components? What are the most viable threats to the systems, and what is the likelihood of those threats actually manifesting? For example, Joanna Rutkowska’s “Blue Pill” attack implemented a thin hypervisor in the chipset of a system (thus creating a virtual rootkit), and caused a great deal of consternation in the security community in 2006. However, the practicality of the attack was so minimal that it was largely relegated to being hypothetical or theoretical in nature.
   - **Ease of mitigation:** Can the threats be nullified or largely mitigated by implementing a variety of technical or procedural controls?
   - **Exposure level:** The exposure level of the virtual systems or components plays a significant role in determining the overall risk. VMs and hypervisor platforms in the DMZ are much more exposed than management servers in a tightly controlled management network segment, for example. This should factor into the attack likelihood analysis.

6. **Document and test.** Unfortunately, the final step in your virtualization risk assessment process is one that’s often overlooked or glossed over: documentation and testing. A risk assessment methodology, as well as its results, should be
considered a “living document,” and keeping this up-to-date should be a priority for information security and audit teams. This will help to ensure the risk methodology is adequate and effective over time, especially given the rapid pace of change in virtualization technology.
Four things to remember about server virtualization security concerns

I've been studying virtualization and virtual server environments pretty carefully the last few years, so I'm always a little surprised when our clients who are looking to deploy virtual server farms in their data centers start getting confused about server virtualization security.

The reason is that virtualization changes nothing. No, really.

You have the same access control issues and the same systems. Nothing fundamentally changes when you roll out a virtual environment compared to an existing physical environment. What was important before is still important.

Of course, just because the big picture is the same doesn't mean that the details are the same. For example, some old security functions -- especially of intrusion detection and prevention -- become more difficult to do in a virtual environment. When you get rid of 40 or 50 patch cords and turn that switch into a virtual switch split across multiple virtualization hosts, it's not so easy to find a place to jack in an IDS or to put an inline IPS.

Another security issue in virtualized environments is the unpredictability of location. When you virtualize within a data center, or even across data centers, you don't know what physical host any particular virtual machine is going to be running on at any one moment. In the physical world, you are trading individual Ethernet ports for trunked VLANs. This means you may have to redesign your security topology to be less focused on what systems are sitting in a particular rack, to what functions are running on a particular VLAN or subnet.

At the same time, performance and management become issues we have to plan around. When we had lots of systems, it was simple to buy a lot of small, cheap firewalls that could split the load; it was also easy to define policy because each firewall only handled a small number of systems. With large virtualized clusters, your pile of firewalls may have to coalesce into a smaller number of larger devices, each capable of handling much higher loads. A more subtle issue is that most firewalls have poor facilities for management of large, multizone policies. I have found many firewall vendors who have been good partners.
for a decade can't handle virtualization topology without making you stand on your head when it comes to policy definition.

**Four considerations for virtualization server security integration**

As your virtualization project comes together, keep in mind the following important points to ease security integration:

1. **VLANs are king, and you will need to get used to bringing trunked interfaces into your switches and firewalls.** Make sure you have at least 1Gbps ports everywhere, and look to the day when 10 Gbps may be needed. If you're buying anything that only goes 100 Mbps, you're wasting your money.

2. **Putting more eggs in fewer baskets means paying more attention to high availability.** Everything should come in pairs and make sure you have two paths throughout the network. Any one component should be able to fail with absolutely no loss of connectivity or security.

3. **Traffic inspection tools such as IDS and IPS are harder to place in virtual environments.** Running them in a virtual machine is almost never the right answer, but you may need special tools or hooks into your virtualization environment to get the traffic out where it can be inspected.

4. **Look to your existing vendors to extend existing tools to support virtual environments, rather than buying a second set of tools just to handle virtualization.** For example, it's better to have a single backup solution for both physical and virtual systems than trying to manage two separate backup solutions.
Resources from Intel

Resource Protection in Virtualized Infrastructures

Understanding Desktop Virtualization

The Future of Enterprise Computing: Preparing for the Compute Continuum

About Intel

For more than three decades, Intel Corporation has developed technology enabling the computer and Internet revolution that has changed the world. Founded in 1968 to build semiconductor memory products, Intel introduced the world's first microprocessor in 1971. Today, Intel supplies the computing and communications industries with chips, boards, systems, and software building blocks that are the "ingredients" of computers, servers and networking and communications products. These products are used by industry members to create advanced computing and communications systems. Intel's mission is to be the preeminent building block supplier to the Internet economy.