



## SECURING VIRTUALIZED ENVIRONMENTS

APRIL 2009

## Executive Summary

There is no hotter topic in information security today than virtualization. Organizations are rushing to virtualize their infrastructures to save money, consolidate their operations, and increase capacity without spending on additional hardware.

But virtualization comes with a host of significant security-related risks and challenges. There are:

- New attack surfaces and threat vectors
- Multiple vulnerabilities associated with hypervisors
- Organizational issues that erode the separation of duties, decrease visibility, and could strain relationships between the server, network, and information security teams.
- A lack of good tools and technologies
- Significant management complexities

Among the practitioners who participate in IANS events, most say that their organizations have not responded to deal with the security issues related to virtualization.

However, in this rapidly changing environment there are steps that security practitioners and their organizations can take. They include:

- **Focusing on the security basics.** These basics include conducting risk assessments, adopting clear standards and policies for virtualization, segmenting the network to protect sensitive information and important assets, using configuration management, and constantly monitoring the network.
- **Addressing the organizational issues.** Practitioners can be proactive in interjecting themselves into the virtualization conversation, calling out and quantifying the security-related risks, and leading the organization in assessing solutions.
- **Evaluating potential technologies/approaches for securing virtualized environments.** There are several approaches for organizations to consider, each with positives and negatives. This includes installing security software on each VM, virtualizing security software, and a range of other options.
- **Keeping an eye on I/O virtualization.** An important trend to watch is I/O virtualization. This is where a single network cable carries multiple streams of LAN and SAN traffic, each destined for a separate virtual server. A separate device aggregates these cables and connects the virtual networks to real Ethernet or Fibre Channel. Cisco is focused on this and will be making waves in this area. Watch them closely.

## What Virtualization Is

Virtualization was defined in an IANS event as:

*“. . . an abstraction layer that decouples the physical hardware from the operating system to deliver greater resource utilization and flexibility.”*

Virtualization is often thought of and discussed in regard to servers, particularly server consolidation. While virtualization certainly applies to servers, it encompasses much more.

Specifically, virtualization applies to and affects:

- Clients
- Networks
- Storage
- Operating Systems
- Applications
- Information

In addition, virtualization can provide new and additional functionality including:

- Provisioning
- Re-purposing
- Governance
- Orchestration
- Chargebacks

## Why Virtualization Is Getting So Much Attention

The fact is organizations are virtualizing. Every participant in a mid-2008 IANS webinar stated their organization was virtualizing to some degree. The majority of delegates at IANS Forums in 2008 said their organizations are adopting virtualization.

A 2008 poll from a leading industry trade journal showed that 70% of organizations are virtualizing their servers, and 20% of respondents say their organizations are virtualizing more than 26% of their servers. A few IANS' delegates are from enterprises that have virtualized in excess of 90% of their servers. This trend is likely to increase, with more organizations virtualizing more of their infrastructure.

Virtualization is being driven by perceived cost savings. The common perception is that organizations will save money through server consolidation, reduced hardware needs, and less power and cooling consumption, will also save time and resources in managing their infrastructure, and can grow and increase their capacity without having to invest in additional hardware.

At a recent IANS Forum, a briefer from a large global organization indicated that by using virtualization to consolidate servers, his organization increased its capacity and saved \$12 million.

While cost savings is the key driver behind it, virtualization has many other benefits. They include:

- Resilience and agility
- On-demand capacity and greater operational efficiency
- Improved ability to control who can access various servers
- Environmental benefits, such as use of less electricity
- Easy back-up and disaster recovery
- Application availability and portability
- Development efficiencies

---

## The Challenges and Risks Associated with Virtualization

As organizations rush to adopt virtualization, many lack adequate security for their virtualized infrastructure. Among participants in a mid-2008 IANS webinar, 36% said that no IT security/protection was in place for their virtual servers and 23% said their organization is working on it. Only 41% said their organization had a security strategy in place for virtualized machines.

The reality is that virtualization fundamentally changes the existing model for “network” security. The types of risks and challenges that are typically associated with virtualization are: technical, operational, and financial.

### Technical

According to IANS Faculty member Chris Hoff, *“Virtualization amplifies every issue we have today in network and host-based security strategies.”*

Among the key technical issues:

- Virtualization makes organizations less prepared for **new attack surfaces and threat vectors**. Concerning threats include guest-hopping and jailbreak attacks, attacks on the management stacks, rogue VMs, and theft of an intact VM.
- **VM sprawl** is an issue based on the ease of instantly creating new servers.
- **Hypervisors** are a significant threat as they expose organizations to a new class of vulnerabilities. Every technology vendor seems to have a hypervisor; they are showing up everywhere—in servers and clients, storage, networking, hardware, software, mobile platforms, a la carte, or bundled as appliances.
- **Virtual switches**. This can be a vulnerable point for hackers. In addition, Chris Hoff says that attempting to replicate complex physical networking topologies in today’s virtual switches will fail.
- **Virtual operating systems**. In a virtual environment, every operating system is subject to vulnerabilities.
- **Virtualized storage**. Data integrity and proper access controls must be applied in the same manner in virtualized environments as in physical ones.
- **Virtual networks**. Monitoring traffic for malicious activity is equally important over virtual networks.
- **Going through virtualization to get to hosts**. Sophisticated hackers have found ways to get to hosts through virtualized servers.
- **Immature management and security tools**. The security-related tools to manage virtualization are very immature.
- **Multiple virtualization platforms**. It seems likely that large organizations will end up with 4-5 different virtualization platforms spread out across their enterprise. This number of different platforms creates significant complexity.

---

## **Operational**

Virtualization changes everything about an organization's operations. It changes how resources and networks are designed, provisioned, deployed, administered, patched, recovered, assessed, monitored, and audited. As a result of the massive organizational challenges related to virtualization, the issues of securing virtualized environments are more organizational and operational than technical.

Virtualization has decreased the visibility in an organization and resulted in less clearly defined separation of duties. It heightens the issues that come from inconsistent security policies and procedures and it further fractures the tenuous relationships between the server, network, and information security teams.

## **Financial**

A concern of some practitioners is that the supposed cost savings from virtualization never materialize. While it is often anticipated that organizations will need less hardware and fewer resources, for organizations that already have hardware and resources in place, it is unlikely that the amount of infrastructure and resources will be reduced. In addition, for virtualization to work often requires additional spending. The result is that virtualization may not produce any cost savings and it may in fact represent increased spending.

*"Virtualizing security will not save you money; it will cost you more!"*

- IANS Faculty member Chris Hoff, mid-2008

## **Ways to Mitigate the Risks Associated with Virtualization**

Securing a virtual environment entails the same basic principles that are used in host and network-based security. These important basic considerations include:

- **Determine standards.** Some organizations have no security standards for virtualization, which is not recommended. Other organizations have identical standards for physical and virtual security; they treat everything the same. And other organizations have separate standards for physical and virtual environments; the thinking is that because the threats are different the standards should be different. For example, an organization might decide that its most sensitive information cannot be stored in a virtualized environment; it must only reside on a physical machine.

IANS recommends that organizations make a conscious decision about their standards. Specifically, IANS suggests that organizations apply at least the same standards to a virtualized environment as to a physical environment.

- **Assess risks.** Organizations should conduct a risk assessment and should use threat modeling to determine the exposure of both their physical and virtual machines.

- 
- **Segment based on risk.** Segmentation is important in a physical environment, and equally or even more important in a virtual environment. The basics of segmentation include knowing which information is most sensitive and which assets are most important and then segmenting based on risk. Mixing high- and low-risk assets on a consolidated virtualized platform is a bad idea and not recommended.

Organizations are encouraged to treat a cluster of VMs as a micro-perimeterized DMZ that shares the same consistent zone-based compensating controls and policies.

- **Use configuration management.** Organizations should define their desired configuration and then constantly monitor whether virtualized devices are in compliance with this configuration.

In addition to focusing on these information security basics, organizations are encouraged to deal with the organizational complexities that accompany virtualization. Some specific suggestions:

- **Be involved early.** In many organizations including information security in virtualization implementation plans is an afterthought. Information security practitioners must interject themselves into this conversation. Convey the risks to organizations that lack good security for their environments and proactively recommend solutions.
- **Conduct mini summits.** Some successful organizations have held small summits where the information security team convenes with teams from networking, admin, and the business. The issues associated with virtualization are shared and specific, collaborative plans are developed.
- **Focus on what matters today.** At times people look at virtualization from a 30,000-foot level, contemplating potential risks and future developments. This may be a fun exercise, but it isn't very useful. There are specific, practical steps that practitioners and organizations can take today to improve the security of their virtualized environments. Practitioners should focus on what they can do today. Some specific suggestions:
  - Get the organizational issues on the table and deal with them.
  - Manage the probable risks; not the unlikely ones
  - Know how pervasive the use of hypervisors is in your organization.
  - Follow the guidelines for securing virtualized environments of the industry and of your virtualization platform provider
  - Apply at least the same strategies to your VMs as your non-virtualized environments
  - Segment your network and manage by risk, criticality, and function
  - Treat each cluster of VMs as a micro-perimeterized DMZ

- 
- Monitor and extract good telemetry and instrumentation
  - Enforce rigorous control over admins with auditing and device management
  - Push vendors to develop better virtualization solutions

Along with the security basics that have been mentioned and the organizational issues, there are approaches involving various tools and technologies that can have value. These include:

- **Security software in the VM.** Almost all security software that is run today in a conventional environment can work in a virtual environment. This includes firewalls, HIDS/HIPS, anti-virus, NAC, endpoint assurance, patch management, and configuration audit and control. This applies to offerings from all of the leading vendors. This approach has pros and cons.
  - The pros: practitioners know how to install security software on each VM. This provides the same management functionality as today; it preserves most separation of duties; and vendor relationships are preserved.
  - The cons: the software only protects the VM on which it is installed; it provides limited visibility; it consumes host resources; there may be vendor support issues; and it definitely doesn't reduce security costs.
- **Virtualized security software as a VA/VM.** This means installing security software in a VM as a virtual appliance. This adds functionality and may be able to protect intra-VM traffic. However, it consumes host resources and requires careful virtual networking configuration.
- **Virtualization software interacting with the security fabric.** This is similar to the previous model but adds integration with external security devices. This can provide better performance and the ability to tie into non-virtualized security, but it is expensive and creates a risk of vendor lock-in.
- **Adding abstracted security via VMM APIs.** This is similar to the previous models but adds additional security capabilities via API. This tighter integration is generally good and it allows a longer shelf life of existing solutions.
- **Third-party virtual switches.** This model is similar to the others but allows for the addition of virtual switches. This acts as a policy-driven intelligent disposition director to third-party security functions. This actually blurs the line of where the host ends and the network begins and further complicates the separation of duties. Cisco is extremely active in this area and has very interesting solutions in the pipeline.

## The Future of Virtualization and Security

Some of the key trends taking place in the world of virtualization include:

- **The hypervisor is getting thinner.** As hypervisors get thinner, they give up functionality. The security risk this creates is not related to the applications running on the hypervisor; it is that hypervisors will become more open and exposed. A result will be directed, specific attacks against hypervisor platforms.
- **I/O virtualization.** As was stated in *Information Week*, with virtualized I/O, a single network cable carries multiple streams of LAN and SAN traffic, each destined for a different virtual server. A separate device aggregates these cables from multiple servers and connects the virtual networks to real Ethernet or Fibre Channel.

Cisco is aggressively pursuing I/O virtualization. In their eyes, virtual hosts become empty shells to hold virtual machines. Their goal is to run everything on the switch. This would have a significant impact on security. Therefore, watch announcements from Cisco very closely as their new products could have a significant impact on networking, virtualization, and information security.