Virtualization White Paper
June 2009

Securing Virtualization in Real-World Environments

IBM Internet Security Systems

Contents

Introduction

IT organizations are under increasing pressure to deliver more functionality—faster and with smaller budgets—to service their business and their customers. Increasing costs attributed to power and cooling of servers, coupled with the headache of managing the ever expanding data center, make this a serious challenge, resulting in new advancements within the enterprise. Scale-out, cost prohibitive IT is no longer sustainable; the pendulum is swinging back towards a centralized, highly integrated and business-friendly IT.

At the heart of this transformation is virtualization. Through its ability to consolidate workloads and reduce the amount of time and energy IT spends purchasing, installing and maintaining racks of servers, virtualization allows the organization to satisfy its goals with fewer physical resources and reduced operational costs. Early adopters of virtualization are also attaining additional returns on their investment through radically simplified systems management, automation and optimized server utilization. In short, both the expectations and benefits are very real.

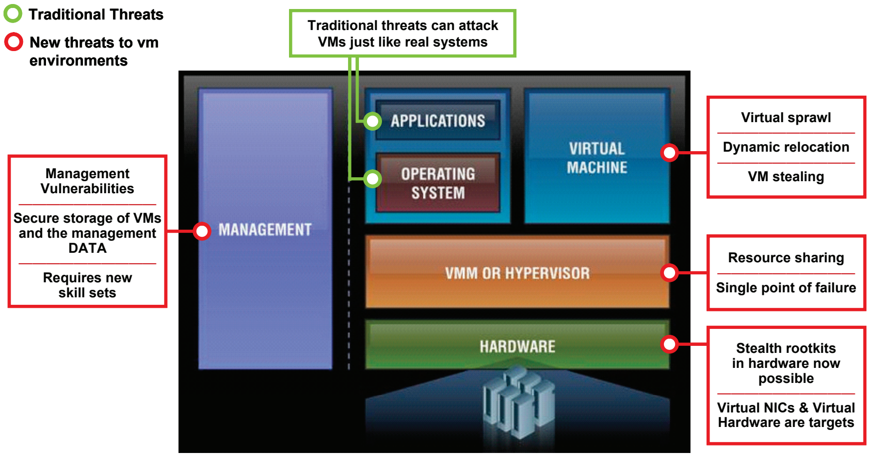
However, the ultimate success of virtualization is not simply dependent on energy efficiency, performance and ease of use. It must also provide these benefits without compromising the overall security, reliability and availability of the IT infrastructure. Already, organizations struggle to understand how best to stay ahead of today's threats while also addressing various regulatory-based compliance standards. New technologies, such as virtualization, exacerbate this problem, making it wise to identify gaps in existing security capabilities as they are introduced into the enterprise. Businesses should also take the time to understand how to properly integrate, deploy and manage security in these new environments. Without a baseline plan or a real understanding about virtualization and security, IT groups may decide to disable many of the advanced features of virtualization for fear of unintended consequences, or even worse, they might introduce more risk in the process.

This White Paper examines many of the concerns associated with virtualization and describes how the breadth of security experience, focused under the IBM Security Framework, help you, the customer, better understand

and prioritize these risks, as well as help you build a strong security posture that will positions your organization to reap the full rewards of this exciting technology.

Virtualization – Enjoy the Ride, But Don't Forget to Buckle-Up

Virtualization has tremendous appeal for a variety of reasons. Most notably, customers are successfully reducing capital and operating expenses through server consolidation. By breaking down silos of physical resources, organizations simplify data center management and reduce server sprawl. For example, an IDC report sponsored by IBM, shows that organizations that have deployed virtualization solutions are saving, on average, 23 percent over a 12-month period from reduced hardware, power and cooling, and real-estate costs. [1]


○ Traditional Threats
○ New threats to vm environments
Traditional threats can attack VMs just like real systems
Management Vulnerabilities
Secure storage of VMs and the management DATA
Requires new skill sets
MANAGEMENT
APPLICATIONS
OPERATING SYSTEM
VIRTUAL MACHINE
VMM OR HYPERVISOR
HARDWARE
Virtual sprawl
Dynamic relocation
VM stealing
Resource sharing
Single point of failure
Stealth rootkits in hardware now possible
Virtual NICs & Virtual Hardware are targets

MORE COMPONENTS = MORE EXPOSURE

Figure 1. Threats to Virtual Machines

While reducing data center costs has become the primary success metric for

[1] IDC White Paper – IBM Virtual Services, 2008

Highlights

Negatively impacting the overall security posture, and increasing risk are never the intentions of IT groups deploying virtualization; but, the potential readily exists.

organizations, investments in server virtualization also come with greater expectations. Customers have additional goals of increased availability, automation and flexibility that is only possible with virtualization. Realizing these goals, is a critical step towards greater levels of service management through virtualization, including advanced IT service delivery and strong business alignment. It also helps break the lock between IT resources and business services - freeing you to exploit highly optimized systems and networks to further improve efficiency.

However, in addition to these enormous benefits, virtualization significantly impacts security. As data centers evolve from simplified, to shared and dynamic infrastructures, so do security concerns. The industry has already expressed anxiety over physical-to-virtual migrations, security of the virtualization management stack, and visibility into the virtual network. As virtual data centers become more complex and dynamic, additional concerns around workload isolation, multi-tenancy, mobility, virtual machine sprawl and trust relationships are gaining more visibility. Negatively impacting the overall security posture, and increasing risk are never the intentions of IT groups deploying virtualization; but, the potential readily exists.

Concerns over risk have the potential to limit the benefits an organization will realize from virtualization. For example, many companies have seen no change in the number of resources needed to manage virtual environments (Figure 1). This is likely the result of organizations not enabling automation capabilities such as dynamic resource allocation and mobility. Additionally, adopters of virtualization may not be changing—and ultimately improving—the efficiency of server provisioning processes for fear of introducing risk or threatening compliance with security policies. Until these organizations enable more advanced virtualization features, they will not realize the enhanced manageability and availability value that virtualization brings.

On the other hand, many early adopters have rushed to take advantage of these technologies, often without fully understanding the security concerns. For example, server consolidation increases overall efficiency, but also complicates matters by introducing a new architecture with various technical and organizational complexities. Both IT and security professionals must adapt as consolidation forces change. As network and server administration begin to converge, physical security devices and other security tools become less effective. Even the most basic features of virtualization greatly impact the day-to-day security responsibilities and processes used to achieve and maintain compliance.

Perhaps a lesson can be learned from the automobile industry in that safety and security increases with maturity. The invention of the internal combustion engine allowed us to trade our horse-and-buggies for automobiles, but faster travel also came with new risks. The first modern automobiles were available in the late 19th century, but seat belts were not first offered as standard equipment until 1958. Over that period of time, technological advances allowing cars to travel much farther and faster far outpaced advances in safety. Likewise, new virtualization capabilities are currently being introduced at a pace that challenges risk mitigation solutions. While mature virtualization platforms have strengthened their inherent security capabilities over time, a new wave of virtualization products with widespread appeal and poorly understood security capabilities are hitting the shelves.

In short, organizations must buckle-up. Organizations should embrace repeatable, measurable planning processes and embrace a wide variety of solutions to properly manage virtualization security. Yes, virtualization introduces new concerns, but it also provides an opportunity to extend defense-in-depth to new and unique areas of integration. As we optimize security controls, strengthen the platform and increase awareness of potential security implications, organizations will be able to realize more benefits, without adding new risk.

Before we examine the solutions offered by virtualization, let's take an in-depth look at the major concerns.

Security Implications of Virtualization

Some characteristics and attributes of virtualization have inadvertent, yet influential consequences on information security. Physical servers and other computer resources are heavily shared; barriers between virtual machines are logical; and, workloads can move around the data center, en route to new servers or geographic locations in real-time. Understandably, people, processes and technology must adapt. To do so, we must fully understand the new risks and security challenges unique to this technology. The following section describes several major security concerns facing virtualization.

Isolation

In order to safely consolidate servers and allow a single physical server to host multiple virtual machines, virtualization uses logical isolation to provide the illusion of physical independence. No longer able to verify that machines are separated by network cables and other physical objects, we rely on the hypervisor and other software-based components to provide these assurances. This may not be a concern for simple consolidation within a small organizational unit, but it becomes increasingly important when workloads from users of different trust levels share the same hardware. In order to properly contain information, administrators must pay special attention to configuration settings that affect virtual machine and network isolation, as well as continuously monitor the entire infrastructure for changes resulting in leakage of sensitive data.

Server Lifecycle and Change Control

Patch management and change control windows are vital to keeping operations running smoothly and safely. This is done by applying important security fixes in a timely manner. In fact, this is so important that many IT organizations have built an exact science around server maintenance. Without question, a great amount of time and money are invested annually to maintain servers in the data center. Virtualization adds to this complexity by changing the rules of the game. Servers are no longer constantly running, virtual machines can be stopped, started, paused, and even rolled back to a previous state. The speed that machines are configured and deployed also dramatically increases. What used to take hours, now takes seconds or minutes. The result is a highly dynamic environment where machines can be quickly introduced into the data center with little oversight, and security flaws can be omitted or reintroduced based on virtual machine state. Security professionals must fully understand what virtual machines are being deployed, those that are currently running, when they were last patched, and who owns them.

Virtual Machine Mobility

Mobility, in the language of virtualization, refers to the ability of a virtual machine to automatically relocate itself and its resources to an alternate location. This capability, while highly desirable, can also create problems. In a traditional data center, physical server 'A' is located on Row 5, Rack 8, Slot 3. In the hybrid data center virtual machine 'B' is not as easily locatable. As part of a resource pool, server 'B' could be spread across multiple physical resources. If configured for mobility, the VM could relocate to another physical server, either automatically as part of a disaster preparedness plan or in response to a performance threshold. This mobile aspect of virtual machines adds flexibility, time and cost savings to the data center, but also introduces security concerns similar to laptop and large scale dynamic host configuration protocol (DHCP) environments. Static policies and other security mechanisms designed for traditional servers and networks may become easily confused. The ability for security products to operate intelligently across multiple physical and virtual environments, as well as be more infrastructure-aware through integration of platform and management APIs, will allow administrators to enforce control over the mobility of VMs within various security zones.

Highlights

Servers are no longer constantly running; virtual machines can be stopped, started, paused and even rolled back to a previous state. [...] The result is a highly dynamic environment where machines can be quickly introduced into the data center with little oversight, and security flaws can be omitted or reintroduced based on virtual machine state.

Virtual Network Security

Networks and servers are no longer two separate, distinct layers of the data center. Virtualization allows for the creation of sophisticated network environments, completely virtualized within the confines of the server itself. These virtual networks facilitate communications for virtual machines within the server and share many of the same features used by physical switches and other traditional networking gear. A physical port in the data center that used to represent a single server now represents tens or hundreds of virtual servers and drastically affects how we secure data center networks. Network traffic between virtual machines within the same physical server does not exit the machine and is not inspected by traditional network security appliances located on the physical network. These blind spots, especially between virtual machines of varying trust levels, should be properly protected with additional layers of defense running within the virtual infrastructure.

Separation of Operational Duties

Separation of duties and the policy of least privilege are important security principals used to limit the capabilities of IT administrators as they manage resources and perform routine tasks. Server management is usually handled by the server administrator, network management by the network administrator – while security professionals work with both teams and handle their own specific tasks. Virtualization has changed the natural boundaries and lines of demarcation that built these divisions. Both server and network tasks can be managed from a single virtualization management console, which introduces new operational challenges that must be overcome. Organizations must clearly define proper identity and access management policies, allowing administrations and security professionals to properly maintain and secure the virtual environment without granting excessive authority to those who do not require it.

Additional Layers of Software

As virtualization is introduced into the data center, so are additional lines of code that make up the software needed to implement it—from the management consoles that control virtual machines to the hypervisors that provide the foundation for the technology itself. As such, we've observed a significant rise in the number of disclosed vulnerabilities related to virtualization software, with an overwhelming majority of these attributed to the popularity, accessibility and relative immaturity of x86 virtualization. Many disclosures can be attributed to third party code packaged with the virtualization software stack and vendors are taking measures to reduce the footprint of their software and dependency on uncontrolled code. However, it goes without saying that fault-free code is largely unattainable, especially as vendors integrate complex features into their platforms. Organizations should treat virtualization as they would any critical application and apply proper defenses to stay ahead of these threats.

Securing Virtualization

IBM believes that a foundation in security is the basis from which organizations can reap the most benefit from virtualization. If many of today's virtualization security challenges simply mirror yesterday's challenges, logically, we should be able to use the same security technology. The reason we cannot is due to a fundamental shift in the way organizations plan, deploy and manage virtualization platforms. This shift requires, in some instances, a simple adaptation, and in others, a completely new way of operating.

For example, it is true that many of the threats exposed by virtualization can be mitigated or reduced by using existing people, processes and technology. Traditional network and host security products for example, can be used to protect the network, desktops and servers. Given a small adaptation, Host Intrusion Prevention Systems (HIPS) can also be installed on each virtual machine. However, what cannot be effectively protected by traditional processes and technologies is the virtual fabric composed of the hypervisor, management stack and virtual switch. While people, processes and technology are recyclable, they also need to evolve to the new architecture and concepts exposed by virtualization.

Change control and patching procedures are good examples. The patching procedures for virtual machines certainly need to adapt to fluctuating running states and dormancy. Furthermore, how do organizations use virtualization management suites to reclaim the separation of duties lost when network and host administration merged onto the virtualization platform?

Deploying access control and the policy of least privilege to the management console, administrative roles, and virtual images are certainly not unique concepts; however, slowing the growth of virtual networks and preventing virtual server sprawl is. Administrators must also adapt to the concept of shared resources and ensuring the fair distribution of RAM, CPU, storage and bandwidth.

Standards and Compliance are another front page-concern, though standards have yet to be agreed upon and there is no universally accepted stance on the compliance of virtual platforms.

All of these practices are used in today's networks—in some form—to mitigate risk, and since even virtual networks are really hybrid networks, these solutions are still absolute necessities in the fight for enterprise security. However, organizations should keep in mind that enterprise security is only as good as the sum of its parts. Defense-in-depth must extend from physical to virtual environments. In today's era of reduced cost and complexity, the value of a single suite of centrally managed security products that reaches both physical and virtual networks and hosts is critical to achieving enterprise security and a maximum return on investment.

Secure Virtualization Solutions from IBM Internet Security Systems

Most organizations are running hybrid infrastructures with varying percentages of physical and virtual hosts, applications and devices. While many are rushing headlong into virtualization, others are testing in laboratories or waiting until the value of their servers and appliances have amortized. Regardless, the stark reality of virtualization is that there is an adoption period. Current investments in security will not be thrown away but will be recycled and reused. Without question, organizations will look to cannibalize their existing investment in security in order to effectively extend their investment.

While many virtual security vendors have unveiled products to protect the virtual world, it is critical to understand that the true value of security is not in point products that address virtualization only, but in solutions that extend security to the new risks exposed by virtualizing production servers. Organizations interested in reducing cost and complexity, while achieving enterprise-grade security, must pay close attention to how solutions in the marketplace will fill the coverage gaps introduced by virtualization.

Virtual Security Products

IBM Internet Security Systems™ (ISS) is focused on providing best-of-breed security end-to-end solutions for key control points – network, endpoint and server. The offerings fall into three areas within the virtualization spectrum: Virtual Environment Ready, Virtual Appliances and Virtual Infrastructure Protection.

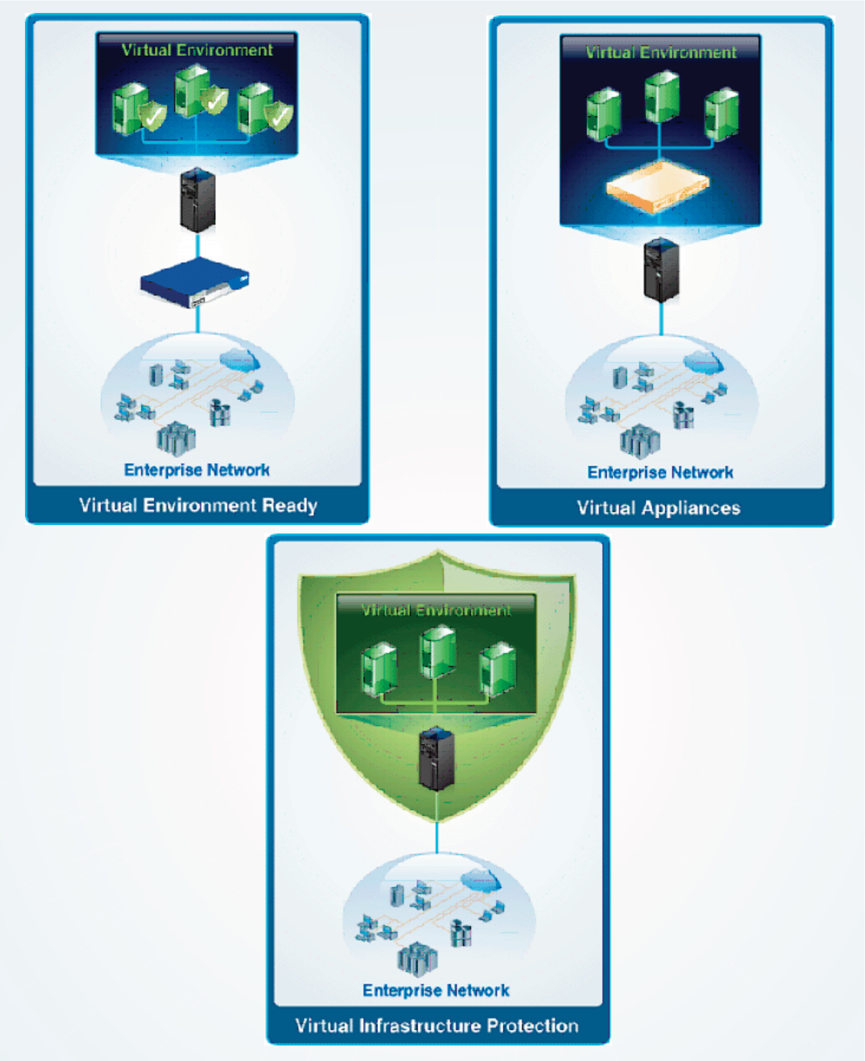


Figure 2. Virtualization Spectrum

Virtual Environment Ready solutions utilize traditional IBM ISS security offerings to protect virtual environments. With these solutions, IBM ISS can protect virtual environments with proven technologies that incorporate "trust X-Force" recommended policies, NSS / ICSA certified ability to block threats and seamless integration with no interruption of your workflows. These offerings include:

- *IBM Proventia® Server Intrusion Prevention System (IPS)*
- *IBM Proventia® Network Intrusion Prevention Systems (IPS)*
- *IBM Proventia® Network Mail Security System*
- *IBM Proventia® Network Multi-Function Security (MFS)*
- *Data Loss Prevention*

Virtual Appliances reduce operational expenses while increasing flexibility for your security infrastructure by allowing the re-use of assets you already own. These solutions can easily migrate from older technologies without changing hardware, and they provide a foundation for future expansion. These offerings include:

- *IBM Proventia® Virtualized Network Security Platform (VNSP)*
- *IBM Proventia® Network Mail Security System*

Virtual Infrastructure Protection solutions offer enhanced protection integrated within the virtual infrastructure. This solution provides automatic protection as each VM comes online and monitors traffic between the virtualized servers with a holistic view of the virtual network.

For more information about IBM ISS security products, please visit, *www.**ibm.com**/services/us/iss*

Security Management

IBM Managed Security Services

In today's highly scrutinized economy and reduced budgets, many organizations are learning to do more with less. IBM Managed Protection Services (MPS) offers you the option to outsource the deployment and management of your security products, thus reducing the cost and complexity of training and maintaining in-house staff.

IBM Managed Security Services also offers an innovative and simple way to secure the virtual infrastructure by choosing to have IBM manage your security operations from one of eight IBM ISS operation centers around the world. Called the IBM Virtual-Security Operations Center (Virtual-SOC), this service is designed to ensure that all physical and virtual security solutions are active and updated with the latest patches and software updates, including security intelligence provided by the IBM Internet Security Systems X-Force® research and development team.

IBM Proventia® Management SiteProtector™ system

IBM Proventia Management SiteProtector system offers the industry's largest portfolio of centrally managed security products and is supported on VMware® ESX. Designed for simplicity and flexibility, the SiteProtector system can provide centralized configuration, management, analysis and reporting for the full IBM ISS Proventia product family.

Tomorrow's Virtualized Infrastructure Security

In order for organizations to fully realize the benefits of virtualization and more toward a truly dynamic data center, existing static security solutions must be adapted and optimized. The future of virtual infrastructure security will combine the foundation laid by the IBM Virtualized Network Security Platform (VNSP) with virtual environment awareness to form a transparent plug-and-play threat protection solution to address security concerns associated with virtual machine sprawl, lack of virtual network visibility and mobility.

Through integration with virtualization platforms, IBM will adapt the capabilities of the Proventia VNSP to include consolidated network-level intrusion prevention and auditing of the virtual environment, reducing the need for network traffic analysis in the guest operating system. Through this technique, organizations can limit the security footprint per guest OS, thereby eliminating redundant resource consumption and reducing security management complexity.

Solutions Backed by IBM Internet Security Systems X-Force research and development team

IBM ISS security excellence is driven by the world-renowned X-Force team. The X-Force team delivers security intelligence that customers can use to improve the security of their networks and data. Regardless of whether the product is a physical 1U appliance or a piece of software installed on a virtual machine, the same security intelligence and threat content, developed by the X-Force team, is installed on that IBM security device and helps manage the threat mitigation process.

The X-Force team provides the foundation for the preemptive approach to Internet security used by IBM Internet Security Systems. The X-Force team is one of the of the oldest and best-known commercial security research groups in the world. This leading group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM Internet Security Systems products, and educates the public about emerging Internet threats.

In addition to providing security content updates to IBM ISS products, the X-Force team also provides the IBM Internet Security Systems X-Force Threat Analysis Service (XFTAS). The XFTAS delivers customized information about a wide array of threats that could affect your network through detailed analysis of global threat conditions.

Conclusion

Without a doubt, virtualization has changed, and is changing how we run, manage and store our applications and data. As with many technological advances, the changes are happening faster than caution would normally dictate.

The simple truth is that virtualization concentrates the value of the asset, both in terms of the data contained within, and in terms of the functionality a compromised multi-VM system offers. New, complex technologies introduce the potential for more gaps in protection, a foundational requirement for electronic attacks.

Virtualization security need not mean that you scrap your current security investments. Networks will always have some amount of physical hardware and virtual security will always be limited by the finite amount of resources available to it. There's no need to toss out your current investments in IPS' or firewalls or multi-function devices, but you do need to plan now and consider how to best protect your physical and virtual resources.

IBM Internet Security Systems continues to develop solutions that not only help protect your capital investments and your confidential data, but that also make it easy to track, monitor, automate and manage your network resources.

IBM Corporation

New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America

06-09

The customer is responsible for ensuring compliance with legal requirements. It is the customer’s sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.