McAfee®

Protect what you value.

Safely Unlock the Potential of Virtualization

McAfee's Proven Solutions Keep Virtual and Physical Environments Secure

Table of Contents

McAfee®

Safely Unlock the Potential of Virtualization

Executive Summary

Enterprises are rapidly adopting virtualization technologies. However, the design elements that make virtualization attractive can introduce risks and increase exposure to threats. If virtualization is implemented without following best practices for security, the resultant security incidents increase costs and reduce business agility. As threats increase in number and complexity, security management costs also escalate, as more and more IT resources are spent fighting them.

McAfee is an innovator in protecting virtualized environments. McAfee® Total Protection for Virtualization offers proven protection for virtualized servers that lowers operational costs and simplifies internal and regulatory compliance. McAfee simplifies the purchasing process with a friendlier pricing model for virtual environments based on physical hosts. And McAfee provides the industry's first and only platform to deliver integrated, centralized management for security and compliance solutions for both virtual and physical environments on a single console.

McAfee is also the first company to offer a dedicated security assessment service for the virtual environment. McAfee's assessment helps companies recognize the gaps in their security postures that virtualization can expose, and helps them improve their security architecture to implement strategies covering people, process, and technology to bridge these gaps.

This paper describes what can happen when organizations fail to secure their virtual environments and how companies have implemented best practices to prevent catastrophic security failures.

Introduction: The Potential for Disaster

A Fortune 500 insurance company with six large global data centers turned to virtualization in 2005 to reduce costs and increase hardware utilization and business agility. Server sprawl had pushed the company's data centers to their limits. Virtual machines (VMs) running in the development labs proved that multiple operating systems and multiple applications could run on one physical computer or server simultaneously, reducing space, power, and cooling requirements in data centers. The company recognized the agility that VMs could bring, as VMs can be provisioned in minutes to react faster to business demands. Using a powerful feature called live migration, administrators can move VMs between physical hosts without any downtime. The company began the transition to using VMs in production. Within two years, 40 percent of the company's servers were virtualized and the savings covered the hardware and software costs for the virtualized infrastructure.

However, the company neglected to enforce network and security patch management compliance policies for connecting to the corporate network. In addition, live migration permitted highly sensitive database servers to migrate to a public-facing network, compromising security.

The result was a security disruption that cost the company millions. One VM, shared by a few administrators to download and evaluate software, was dormant for only two months, and had not been updated with the latest security patches. When that VM was reactivated, its anti-malware security profile was out of date. A mali-cious rootkit—installed in this VM when it was exposed to the public-facing network—woke up and caused other VMs in the same network trust zone to be infected. By the time the intrusion was discovered, security logs showed that attackers had gained access to mission critical databases and had stolen passwords and even encryption keys. The company lost potential revenues from delayed promotions, spent thousands of administrative hours recovering databases and securing VMs, and lost market share points to its largest competitor.

The amount of malware continues to rise at an astonishing rate, with new threats in 2008 projected to grow over 300 percent compared to 2007.[1] The Pentagon last month acknowledged that its vast computer network is continuously being scanned or attacked by outsiders. The

1 McAfee Avert Labs, 2008

Air Force in a recruitment ad said the Pentagon is attacked more than three million times each day. As has been well documented by McAfee and by others, cyberattacks are on the rise and are increasingly nefarious. Today hackers, either part of organized crime rings or backed by governments, hack to steal valuable information and make money. Attackers are rushing to find vulnerabilities in virtualization technologies to gain administrative access to the underlying host or to compromise the core virtualization platform to gain highly privileged access to the array of guests that run on top. Attacks are increasing even as companies implement strict security policies, as cyber-criminals continue to develop new, sophisticated ways to perpetrate crime.

In a recent survey by Gartner, more than half of the participating IT administrators indicated that they were hosting mission-critical applications in virtual environments. VMs increase the number of options available to administrators, providing greater flexibility but also adding to complexity and increasing the areas of possible attack. Virtual environments are not only susceptible to the same threats as physical systems; they are also vulnerable to additional threats that exploit virtualization.

Companies ordinarily deploy security for physical servers, but may be rushing into dangerous practices by deploying VMs without a plan to secure them. Before VMs are transferred from development environments to production environments, IT professionals need to start asking the right questions: "How will this technology affect my existing security posture? What are the dangers lurking in offline VM images that may expose our enterprise networks? What new concerns need to be addressed and best practices to consider to mitigate these risks?"

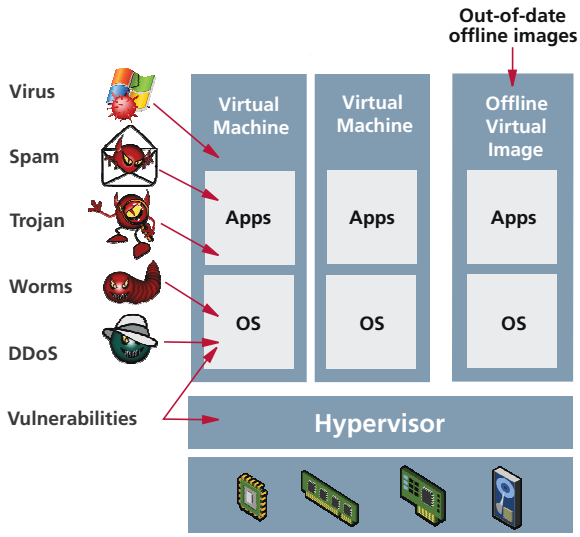
Enterprises need to close the gaps that virtualization may expose and implement new security policies before deploying virtualization on a large scale. "Virtualization offers IT departments opportunities to reduce cost and increase agility," points out Gartner analyst Thomas Bittman. "However, if this is done without implementing best practices for security, the resultant security incidents will increase costs and reduce agility. Security must be 'baked in' from conception, not addressed later as an afterthought."[2]

Security Challenges with Virtual Environments

Often overlooked is the fact that virtualized environments face the same risks and are as vulnerable as physical systems to viruses, worms, spyware, Trojans, and other attacks targeting software vulnerabilities and creating buffer overflows. Without best practices for security, virtualized environments can be just as vulnerable as physical systems. VM system images, periodically taken offline, can fall behind the upgrade cycle of security patches and introduce vulnerabilities that administrators thought were already patched.

Virtualized environments also face unique security challenges. According to the National Vulnerability Database, virtualization-specific vulnerabilities grew over 400 percent from 2006 to 2007[3], with VM-aware threats subverting deployed counter-measures. A single hack known as hyperjacking can offer simultaneous access to many VMs by exploiting the hypervisor, the virtualization platform that allows multiple operating systems to run on a host computer at the same time.

Other security concerns are similar to those in the real world, but the nature of virtualization compounds them. To mitigate these risks, enterprises must recognize the challenges of securing virtualized environments and include, in any projected cost savings of virtualization, the costs of implementing best practices for securing them.



Virtualized environments face the same risks as physical systems as well as unique security challenges.

Curbing the Sprawl of Virtual Machines

One of the key advantages of virtual machines (VMs) is that enterprise applications are easy to provision and deploy. In the physical environment, bringing up new servers requires purchasing new hardware, installing

2 "Virtualization Changes Virtually Everything" by Thomas Bittman, Gartner, March 2008
3 National Vulnerability Database, 2008

operating systems, and hardening and configuring the systems according to corporate policy—before starting to install the business applications. This is a process that takes weeks if not months for a single server. By comparison, it can take as little as 15 seconds to bring up a new VM. But the consequence of easy deployment is VM proliferation, with more and more VMs created throughout the IT environment—even for small workloads.

Many enterprises start using VMs in testing and application development environments in which operational speed is a priority over most other factors (such as security). Administrators and users can copy VMs to other hosts throughout the network easily, as offline images. Some archived VMs may stay offline for long periods of time to meet compliance requirements.

Inadequate planning can pave the way to VM sprawl, in which VMs are distributed across multiple physical hosts in various states of patching and configuration, without adequate coordination or oversight. Security risks become more tangible because a VM that is not properly tracked and managed may not have updated patches or proper configuration control, leading to vulnerabilities that can be exploited.

For example, VMs can be rolled back to a previous state, undoing security patches. And VMs that are dormant for an extended period of time are not updated with the latest patches. When these VMs are activated again, their anti-malware security profiles are precariously out of date, and they are riddled with vulnerabilities. The risk of propagating infected virtualized images is extremely high without measures in place to ensure the integrity of VMs.

Securing the Hypervisor or VMM

Virtual environments also offer a single point of attack: the hypervisor, also known as the virtual machine monitor (VMM). It is the virtualization platform that allows multiple operating systems to run on a host computer at the same time. The hypervisor or VMM can be vulnerable to hyperjacking attacks designed to take control of all the VMs under management. Losing control of the hypervisor is the most vicious security attack possible: the attacker can easily take down multiple mission-critical applications, and with direct access to the CPU, memory, network and disc, the attacker can steal an enterprise's most sensitive data without detection.

For example, a malicious user could potentially gain control of the hypervisor by exploiting vulnerabilities from a VM. With the hypervisor's privileged access, this user could then compromise all other VMs on that host. In theory, guest OS code in a VM should not be able to affect the host OS in an uncontrolled manner. However, vulnerabilities discovered in 2007 allow the guest OS to break the separation; these weaknesses include the ability to execute arbitrary code on the host. Such vulnerabilities challenge the soundness of many security procedures related to VM usage.[4] Security analysts predicted the emergence of such vulnerabilities in mid-2006[5], yet the number of these issues discovered in 2007 is surprisingly high.

Attackers can install a false hypervisor or VMM underneath an existing operating system, and use it to host malicious software that supports general-purpose functionality yet hides its state and activity from intrusion detection systems running in the target operating system and applications. In 2006 a proof-of-concept rootkit called Bluepill[6] was shown to compromise a physical system's operating system and move itself into a VM, where it became the hypervisor and concealed its presence from malware detection technologies. Another rootkit called Vitriol (created by Matasano in 2006) configures itself to run as a hypervisor in VMX root mode, with full privileges, which can monitor and influence all system activity.[7] In the long term, the increasing adoption of virtualization technologies by businesses will create opportunities for targeted attacks.

Monitoring Network Traffic and VM Proliferation

Virtualization brings new and powerful networking capabilities, allowing for unprecedented ease in connecting users to corporate servers and databases. The problem is that traditional enterprise management and monitoring tools are unaware of all the possible connections in virtualized environments. Administrators need more visibility into their virtual infrastructures to track where VMs reside, what networks are they connected with, where they move to, and what other hosts they are communicating with.

In the physical world, hosts can be segmented and monitored using firewall, IDS and IPS technologies. In virtualized environments, it is possible for VMs on the same host to communicate without monitoring or filter, and it is also possible to migrate VMs across segment boundaries.

4 Particularly, a "secure revert" cannot be fully trusted. If a VM is infected by malware that can execute arbitrary code on the host, then performing a "secure revert" will remove the malware from the VM, but not from the host.

5 Neil MacDonald, "Secure Hypervisor Hype: Myths, Realities and Recommendations," Gartner Research. http://www.gartner.com/DisplayDocument?doc_cd=140754

6 Joanna Rutkowska, "Subverting Vista kernel for fun and profit," COSEINC Research, Advanced Malware Labs. invisiblethings.org/papers/joanna%20rutkowska%20-%20subverting%20vista%20kernel.ppt

7 Dino A. Dai Zovi, "Hardware Virtualization Rootkits," matasano. http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf

Administrators for virtual infrastructures may not be aware of all the security issues and might allow development VMs to occupy the same host as production VMs, or might bridge VMs between different physical monitoring zones. Development VMs might also be connected to virtual networks that should be segmented in order to protect intellectual property or consumer privacy.

The majority of existing network management, information security, and IP-based security tools were designed to analyze network traffic and the behavior of physical servers, not to peer behind the curtain of a VM host. In the virtualized environment one physical server may be hosting a few, or as many as 80 guest server instances, while the company's security infrastructure may be treating that hosting server as a single platform.

The lack security and management of the virtualized environment increases the chances of misconfiguration and mismanagement. Virtualized environments can include features that might unintentionally present security risks, such as clipboard sharing, drag-and-drop support, file sharing between the host and guest, and programmatic access through application program interfaces (APIs). Dynamic migration of VMs can also significantly complicate security if not done properly. For example, VMware VMotion, which enables an entire running VM to be moved instantaneously from one server to another, can greatly simplify disaster recovery operation, improve scalability, reduce energy consumption and improve resource utilization. But if a running database is moved from a secure internal network to a public-facing network, security could be compromised.

Bridging Gaps in Operational Security

Most security solutions are not aware of the whether a machine is physical or virtual. Security issues can arise not only from the virtualization technologies themselves, but from operational issues, such as adapting existing security processes and solutions to work in the virtualized environment. With more than 32 percent[8] of exploits released within three days of vulnerability disclosure, organizations are nearly always at risk, as the average enterprise takes 32 days to deploy server patches.[9]

In addition, different groups may control different parts of the physical and virtualized environment. IT departments are fully aware of traditional computing platform threat vectors. However, groups testing and developing VMs may not be fully aware of all security concerns or even include security as a high priority. When they deploy a VM they typically own the virtual infrastructure, configuring virtual switches and virtual storage. With pressures to meet deadlines, server administrators may not be able to get the networking and security groups involved in the process of deploying VMs. The results can be disastrous if no single group tracks where a VM is located, what its patching and configuration status is, or what its purpose is.

Companies should consider the gaps in their security posture that virtualization may expose and review their security architectures to implement strategies covering people, process, and technology that bridge these gaps.

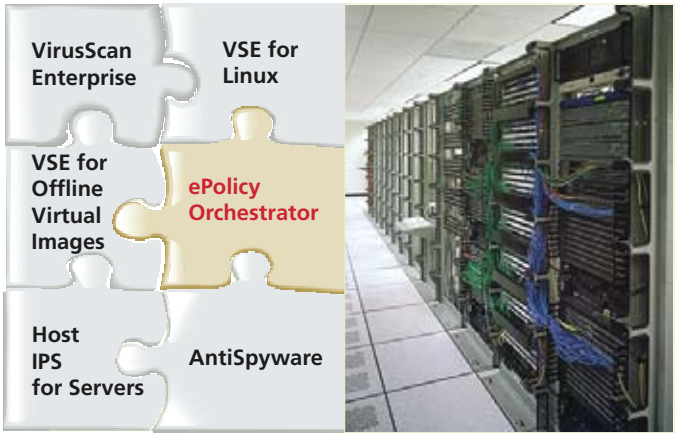
McAfee Security Solutions for Virtualization

McAfee, the world's leader in security risk management, is working closely with virtualization innovators like VMware, Citrix and Microsoft to protect virtualized environments. McAfee offers security and compliance solutions for both physical and virtualization environments that are scalable, centrally managed, and comprehensive—spanning servers, networks, and desktops.

The McAfee® Total Protection for Virtualization security suite securely locks down and protects virtual machines (VMs) and enforces security policies for virtualized environments. It offers integrated, centralized management that protects against malware, reduces costs, and simplifies compliance.

The suite enables enterprises to minimize vulnerabilities in endpoints and across virtual and physical environments with proven antivirus, anti-spyware, and anti-spam protection, web security, and intrusion prevention. Pricing is based on the number of physical hosts rather than VMs, CPUs or sockets, which makes it easier for enterprises count how many licenses to purchase, and to freely deploy any number of protected VMs on the hypervisor and install as many McAfee suite components as needed on each VM.

8 McAfee Avert Labs, 2008
9 Forrester: The State of Server Operating System Security 2007—Administrators Patch an Average of Eight Days Late, June 2007



The McAfee Total Protection for Virtualization suite offers proven protection for virtualized servers.

Protection for Online Virtual Machines

The basic level of endpoint security for online virtual machines (VMs) is antivirus protection. The McAfee Total Protection for Virtualization security suite includes McAfee VirusScan® Enterprise (VSE), which proactively stops and removes threats, extends coverage for new security risks, and reduces the cost of managing outbreak responses. It employs the award-winning McAfee scanning engine to detect and clean malware, and to protect files from viruses, worms, rootkits, Trojans, and other threats. Custom access protection rules prevent malware from making changes to files, registry keys, and utilities within VMs. VSE is the industry's first anti-malware software that offers intrusion prevention with application-specific buffer overflow technology to protect proactively against buffer overflow exploits that target vulnerabilities in Microsoft® applications.

Undetected spyware can lead to identity theft, system and network corruption, slower Internet access, reduced user productivity, and more help desk calls. McAfee AntiSpyware Enterprise uses unique on-access scanning to identify, proactively block, and safely eliminate spyware and other potentially unwanted programs.

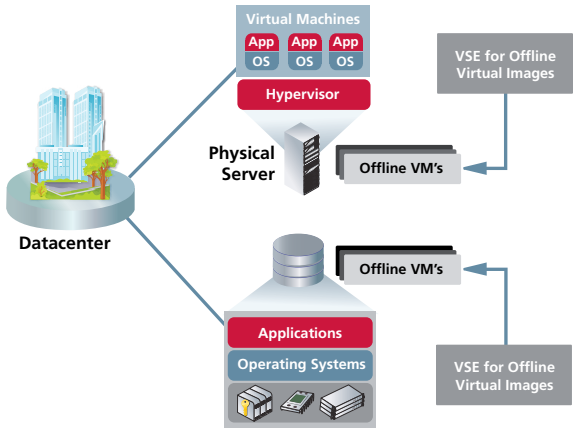
For Linux systems, McAfee VirusScan Enterprise for Linux offers continuous on-access scanning for superior protection from the growing number of viruses, worms, and other malicious code. Designed for the realities of today's fast-moving, highly adaptive businesses, McAfee VirusScan Enterprise for Linux is easily scalable, updates automatically, and can be centrally managed from a single console

Protection for Offline Virtual Machines

A cost-effective, efficient security solution for offline VMs is a critical and often overlooked aspect to an organization's overall security posture. VMs that are dormant for an extended period of time are usually not updated with the latest patches. When these archived VMs are activated again, their anti-malware security profiles and patches are precariously out of date, and they are riddled with vulnerabilities that can potentially put an organization's entire virtual infrastructure at risk. Even with security measures in place, the manual process of activating offline VMs in an isolated environment from time to time for security patches, updates, and maintenance is very time-consuming.

The McAfee Total Protection for Virtualization security suite includes McAfee VirusScan Enterprise (VSE) for Offline Virtual Images, which is the only security solution of its kind designed to ensure the integrity of offline VMs and improve scanning performance.

VSE for Offline Virtual Images scans, reports, cleans and updates the anti-malware security profile of dormant VMs—without having to bring them online. Scanning is also twice as fast with offline VMs than with online VMs in On-Demand-Scan mode, and online VMs also need to be shut down and restarted. VSE for Offline Virtual Images can be deployed on a standalone hardware or run inside a VM. When offline VMs are finally brought back online, they are already scanned, cleaned and fully secure with updated signatures, so they no longer pose a threat to the IT environment. The scanning, cleaning and signature update process is automated, reducing the administrative burden and improving the operational efficiencies of virtualized environments.



Deploying VirusScan Enterprise for Offline Virtual Images

Offline VM images are prominent in both disaster recovery and test and development environments. In disaster recovery scenarios, an offline image is directly connected to a production network the very instant the image is brought online. VSE for Offline Virtual Images ensures that backup virtual images are up-to-date with respect to malware signatures. In test and development environments, where developers typically have dozens or hundreds of virtual images, VSE for Offline Virtual Images enables IT administrators to provide centralized malware protection for unmanaged images.

Host Intrusion Prevention
McAfee Host Intrusion Prevention (Host IPS) for servers, included in the Total Protection for Virtualization security suite, provides total protection across physical and virtual environments. It extends traditional signature-based antivirus protection into proactive shielding against zero-day threats. It can monitor and block unwanted activity and threats and protect key processes and applications within VMs, as well as protect VMs, files, and resources from malicious access with enveloping rules and signatures. Specialized server protection secures critical servers with customized protections to maintain system uptime and productivity.

McAfee Host IPS also provides network-level protection and isolation for inter-VM traffic. The Host IPS stateful firewall blocks unsolicited inbound traffic, controls outbound traffic, and applies policy rules based on traffic, ports, applications, and locations. If one of the VMs is compromised, Host IPS can protect other VMs from attack.

Network Security and Intrusion Protection
McAfee Network Security Platform delivers knowledge-driven proactive security to protect every networked device in an enterprise's infrastructure. Administrators can utilize out-of-the-box protection against virtualized environment vulnerabilities, and insulate systems from risk while validating and deploying patches. Enterprises can control traffic and apply unique policies and protections to a network segment, a collection of hosts, or even a single system.

Network Security Platform protects all network-connected devices with a combination of intrusion prevention and internal firewall that overlaps and integrates protection and extends firewall defenses to the internal network. It correlates signatures, anomalies, and denial of service (DoS) and distributed denial of service (DDoS) information to accurately block attacks before they reach their intended targets. It uses multiple advanced detection methods, including signature, application, and protocol anomaly; shell-code detection algorithms; and next-generation DoS and DDoS prevention. It can parse over 100 protocols and review over 3,000 high-quality, multi-token, multi-trigger signatures with stateful traffic inspection. It also offers proactive blocking for hundreds of attacks straight out of the box with pre-configured policies. Dynamic threat and vulnerability updates ensure continuous protection.

Email and Web Security Gateway
Enterprise-level virtualization can inadvertently increase exposure to traditional threats such as viruses, spyware, and spam related to phishing scams. The McAfee Email and Web Security Virtual Appliance leverages virtualization as a delivery platform, consolidating email and web security into one Virtual Appliance form-factor.

In addition to the appliance benefits of portability, easy setup, and simplified management, the Virtual Appliance can be deployed using an existing VMware ESX platform. It blocks sophisticated attacks with integrated, multi-layered protection, including spam protection that is six times more effective than other anti-spam solutions, to reduce exposure to email and web-borne threats contained within spam. Enterprises can scan every web download and email attachment at the very edge of the network—before they have a chance to infect systems. Organizations can also build content-filtering policies based on built-in and custom-defined lexicons to meet email privacy regulations, keep out objectionable content, and protect intellectual property.

Vulnerability Management
The priority-based approach of McAfee Vulnerability Manager increases the accuracy and usefulness of security intelligence by combining vulnerability, asset, and threat criticality information. Vulnerability Manager knows about and scans virtualization-specific vulnerabilities as well as those that affect the physical environment. It integrates with other McAfee products and with third-party technologies to leverage an enterprise's investments and extend the benefits of protection and compliance to risk-aware intrusion prevention, monitoring risk scores, countermeasure awareness, and problem resolution.

With the capability to scan virtual and physical hosts, Vulnerability Manager is the only network scanner that incorporates countermeasure intelligence from ePO, which provides a more complete system picture for more accurate assessments to reduce the sense of urgency and patch only the most vulnerable systems. Without rescanning the entire network, Vulnerability Manager can visualize and rank

the risk potential of new threats in minutes by correlating breaking threats to existing asset and vulnerability data. It enables organizations to measure exposure to common government and industry regulations with regulation-specific templates for the Sarbanes-Oxley Act (SOX), the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), BS7799/ISO27002, and the Payment Card Industry Data Security Standard (PCI DSS).

In addition, McAfee Vulnerability Manager can be installed in a Virtual Appliance form-factor. Rather than deploying centralized scanning, enterprises can now deploy more scanners at more network locations, all at lower costs. With scanners closer to their target environments, organizations can benefit from lower WAN bandwidth utilization, shorter scanning cycles, and higher accuracy.

Policy Compliance

McAfee Policy Auditor validates the security posture of virtual machines to make sure they have the proper patch level and configurations to be in compliance with standard corporate policies. It automates the processes required for internal and external IT audits and helps enterprises enforce the same security policies across physical and virtual environments. Organizations can design internal policies based on security community best practices, and Policy Auditor helps tune and test before implementation. Policy Auditor works on physical hosts as well as virtual machines.

Scalable Security Management and Simplified Compliance

As threats increase in number and complexity, security management costs also escalate, as more and more IT resources are spent fighting them. Enterprises need an easy-to-use, integrated management platform that enables intelligent security and compliance optimization.

McAfee provides the industry's first and only platform to deliver integrated, centralized management for security and compliance solutions for both virtual and physical environments on a single console. Included in the McAfee Total Protection for Virtualization security suite, McAfee ePolicy Orchestrator® (ePO) is the most popular and respected security management technology, used by over 35,000 customers to manage over 60 million PCs and servers. ePO offers one console to manage the full IT spectrum of physical and virtual machines (online and offline), endpoint and network security, data protection, and policy compliance. Organizations can reduce costs and complexity by deploying a single integrated agent and console across multiple security products so that when policies need to be updated as threats and regulations change, they can be done quickly, accurately, and consistently.

McAfee ePolicy Orchestrator (ePO) makes viewing security and compliance data easy.

Companies are under pressure not only from increasingly sophisticated threats, but also from regulations that require verification and reporting on security compliance. ePO helps enterprises meet compliance requirements and prove to all stakeholders that security measures are in place for internal and regulatory compliance. Customizable dashboards provide real-time compliance status. Administrators can even gather attack details such as type, vector, source, severity, timestamp, and more—all in clear and easy-to-understand wording—for prompt reporting, audit, investigation, and response

Security Assessment to Evaluate Architecture, Configurations, and Policies

Virtualized environments offer plenty of room for security failures with potentially crippling architectural designs, vulnerabilities introduced by misconfigurations, and inadequate access control. To enjoy the full economic benefits of virtualization, enterprises need a consistent security policy for virtual and physical environments.

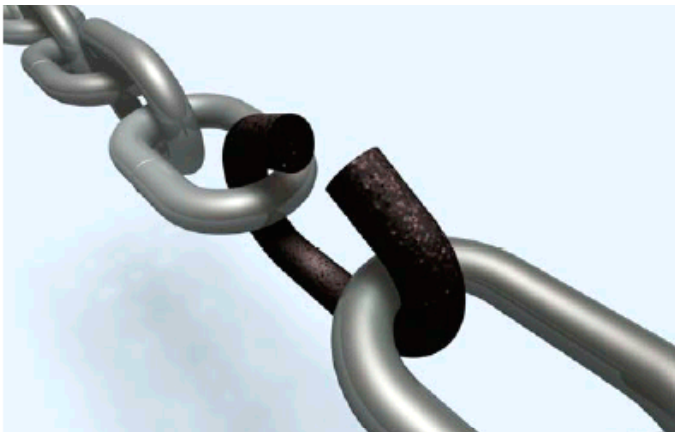
For example, the Fortune 500 insurance company cited in the introduction discovered in a security audit, conducted by Foundstone Professional Services, that security had been compromised through live migration, which had permitted highly sensitive database servers to migrate to a public-facing network. Through a rigorous architecture and design review with McAfee Foundstone® Virtual Infrastructure Security Assessment, the company prevented a possible

catastrophic security failure. The architecture review helped the company redefine its infrastructure with a physical separation of trust zones, enabling live migration within each trust zone. By grouping servers with high hardware demands into defined resource pools, the company also sustained higher numbers of VMs within the same cluster, eliminating the need for additional infrastructure during phases of rapid growth. This is just one of many examples in which a comprehensive assessment can help companies recognize the gaps in their security postures and help them implement strategies that bridge these gaps and help guarantee an ROI in virtualization.

McAfee is the only security vendor to provide customized services specifically for virtualization. McAfee Foundstone Virtual Infrastructure Security Assessment assesses an organization's virtual infrastructure in the following four major phases:

- Architecture and Design Review—Evaluates the virtual infrastructure and security practices in the architecture and design, specifically targeting separation of networks, hosts and VMs, and virtual infrastructure management design.
- Virtual Infrastructure Configuration Review—Assesses the configurations of sampled VMs and the host against known industry best practices, and identifies any insecure configurations.
- Virtual Infrastructure Security Testing—Tests the security from the logical network, virtual server storage network and virtual infrastructure management network. The assessment defines the enterprise's virtual infrastructure attack surface and the associated risk.
- Policy and Procedure Gap Analysis—Evaluates the gap of the current policies and procedures for the virtual infrastructure against known best practices according to the ISO27001 security standard.

As virtualization technology becomes more and more deeply entrenched in IT environments, new challenges are likely to manifest themselves and new problems will come to light. It is important to implement comprehensive security policies before deploying virtualization on a large scale.



McAfee Foundstone® Virtual Infrastructure Security Assessment recognizes the gaps in security postures and offers strategies that bridge these gaps to guarantee an ROI in virtualization.

Best Practices for Securing Virtual Environments with McAfee Solutions

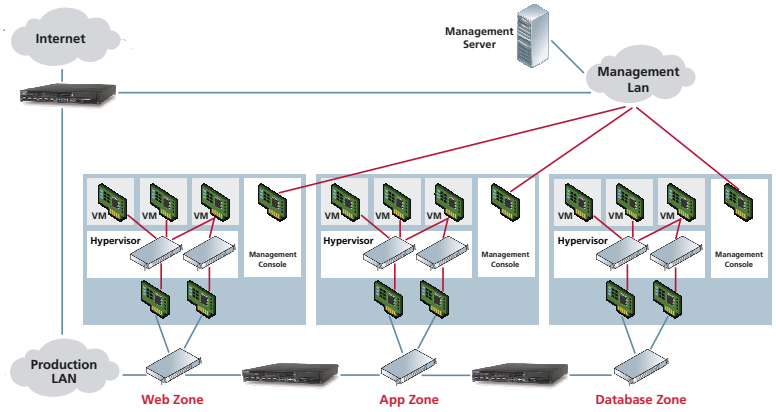
One of the most effective ways to secure virtualized environments is to implement organizational processes that recognize the inherent insecurity of these environments, and to follow best practices to mitigate security risks. McAfee recommends the following best practices:

Secure Design: Isolate Networks and Plan for Mobility
Virtualization makes it possible to implement architectures that would be improbable or difficult to build in the physical world, such as combining production and development VMs on the same host or bridging VMs between different monitoring zones. The ability to live-migrate running VMs from one physical server to another is a huge boon that allows administrators to easily load-balance VMs to hosts with more available resources. But organizations may want to physically separate trust zones, and enable live migration only within each trust zone . IT organizations also need to ensure that security policies are consistently applied across all potential host environments.

Enterprises should segment their networks into different security trust zones and not allow VMs to live-migrate between them, nor combine VMs in the same host if they are connected to network segments at different trust levels. For example, organizations can physically separate trust zones for web, applications, and database servers, or virtually separate them with physical security devices, and deploy stateful firewalls and network intrusion prevention using McAfee Network Security Platform between them, to keep communications secure.

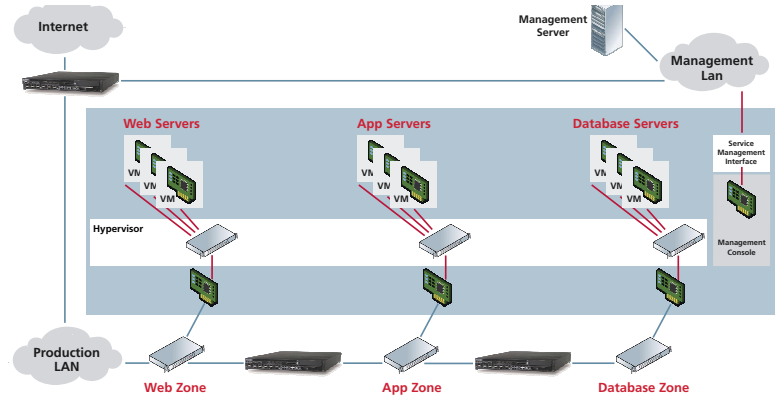
Network Configuration

McAfee Recommendation



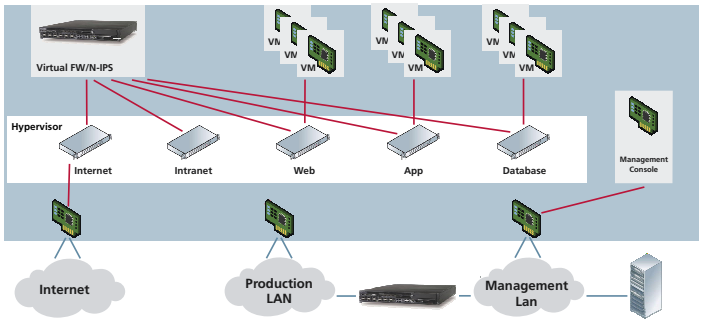
Physical Separation of Trust Zones

This configuration requires more physical servers but provides the best network isolation for different trust zones. Recommended.



Virtual Separation of Trust Zones (with physical security devices)

This configuration provides a balance of economic and security protection. However, multiple NICs on a physical server requires higher I/O utilization. Recommended.



Full Collapse —"DMZ in a Box"

A security device deployed as a virtual appliance provides monitoring and protection for inter-VM traffic. However, organizations need to evaluate the maturity of this appliance and how it is integrated with the company's network security practice.

Three scenarios for separating and managing network trust zones using network intrusion prevention with stateful firewalls.

Secure Deployment: Apply Protection on VMs and Physical Hosts
Enterprises need to secure VMs with not only the same measures used to secure physical servers, but also to secure offline VM images. Host-based intrusion detection and protection is essential for guarding against zero-day threats, such as buffer overflow attacks, as well as blocking unwanted activity and threats between VMs and protect key processes and applications within VMs. Organizations should also harden VM deployments according to guidelines (such as VMware Infrastructure 3).

For highly secured servers, enterprises should deploy the McAfee Total Protection for Virtualization security suite, which includes McAfee Host Intrusion Prevention (Host IPS) for servers and offers predefined shielding policies and rules to prevent attacks and protect key applications, data, and OS resources. Enterprises should also use antivirus and anti-spyware agents with VMs just as they would with physical servers. For example, McAfee VirusScan Enterprise (VSE), included in the security suite, proactively stops and removes threats, extends coverage for new security risks, and reduces the cost of managing outbreak responses for physical servers and online VMs. Enterprises can employ the same award-winning McAfee scanning engine to detect and clean malware and protect against other threats on offline VMs using VSE for Offline Virtual Images, also included in the security suite.

To protect virtual desktops, enterprises should deploy the McAfee Total Protection for Endpoint security suite for continuous, updated, powerful protection against all threats—from rootkits to hacker attacks. Behavioral protection secures endpoints against unknown attacks; signature protection identifies and blocks known attacks; stateful firewall applies policies, bars unsolicited inbound traffic, and controls outbound traffic; and application control specifies which applications can or cannot be run.

Faster Processing: Improve the Efficiency of Security Scans
Malware detection is counterproductive if a security product consumes excessive CPU, memory, or network resources. An on-access scan in real time can utilize 3-5 percent of CPU time; on multiple VMs these scans can significantly impact system performance. An on-demand scan demands about 60-70 percent of CPU time and is very input/output-intensive. With McAfee VirusScan Enterprise (VSE), enterprises can fine-tune scans for VMs to reduce the footprint of an on-access scan to 1-3 percent, by setting a custom policy of scanning fewer file types in ePO.

Enterprises can improve antivirus protection and performance by scheduling on-demand scans less frequently. For certain applications such as file servers, on-demand scans still need to be performed frequently. However, scans of multiple VMs sharing the same physical host can be staggered using the scheduling feature. Administrators should also turn off VMs and scan VM images offline on separate hardware so as not to affect performance of production systems. Wherever possible, VM developers should use templates and cloning to enforce conformity.

Reliable Operations: Lock Down the Network and Hypervisor
While using established best practices for securing VMs and networks is a start, the security of the virtualization layer itself is a major concern. A compromised hypervisor would allow criminals full access to all hosted VMs on a given machine. Like a cloaked rootkit for an OS, the exploit could monitor any data traversing the hypervisor and be in a position to sample, redirect, or spoof anything.

In an effort to reduce the vulnerable attack surface and general exposure to risk, organizations can partition their virtualized management segments from the rest of the network, and restrict who and what can gain access to the management network itself and to its hardware. Stringent control policies should be implemented for virtual infrastructure administration.

It is important for IT to invest enough time to understand the different privilege levels for administrators, operational staff, users, and other groups that leverage virtualization technology. Enforcing these privileges using tools, process, human workflows or some combination of all of these will be necessary.

Learn More and Plan Ahead

How does an enterprise start to address security for both physical and virtual environments? A comprehensive security assessment can help an organization implement secure processes and best practices that can mitigate the risks inherent in these environments. Improper design, configuration or process poses severe risks for mission critical applications hosted within the virtual environment. A timely assessment provides a sound validation by industries' experts that can help enterprises to justify economical benefits of virtualization project. The McAfee Foundstone® Virtual Infrastructure Security Assessment can help companies to recognize the gaps in their security postures that virtualization can expose, and help IT

management review security architectures to implement strategies covering people, process, and technology that bridge these gaps.

The pressure is on to implement virtualization in the enterprise—pressure from the finance department to take advantage of improved cost efficiencies, and pressure from corporate users demanding increased capabilities and performance. Before signing off on the roadmap to fully virtualize datacenters, administrators need to understand the risks, and all stakeholders need to be involved with the design and evaluation of security policies. Organizations must provide anywhere, anytime access to critical applications, but must also deliver exacting security and business continuity. That's not only good business practice—it is more and more a matter of survival. It is for this reason that McAfee, the best-in-class security provider, is incorporating the most complete and extensive virtualization vendor technologies present today to provide secure solutions that enable companies to profit from virtualization.

Learn more about McAfee solutions and services by visiting http://www.mcafee.com/virtualization, or call us anytime, 24x7, at 888.847.8766.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054,
888.847.8766
www.mcafee.com

5040wp_virt_unlock-the-potential_1108