Protection for virtual environments?!?

IBM Virtual Server Protection

IBM Security Systems

Andrzej Wojtkowiak
IBM Security System IT Specialist for Central & Eastern Europe
Summary of Virtualization System Security Challenges

**New Vulnerabilities**
- 259 new virtualization vulnerabilities over the last 5 years
- New attack types (e.g. Hyperjacking, hypervisor escape, VM attacks)

**Larger Attack Surface**
- Virtual endpoints have same security challenges as their physical counterparts
- Virtualization management systems provide new attack vector
- Hypervisor itself is an attack vector

**Increased flexibility can increase security risk**
- Migration of VMs for load balancing can make them more difficult to secure
- Ease of addition of VMs increases likelihood that insecure systems will go online
- Malicious insiders can inflict massive damage very quickly
Virtualization Platform Vulnerabilities

Virtualization Vulnerability Severity by Year Reported
1999-2009

Server Product Vulnerabilities by Vulnerability Type
1999-2009

Virtualization Vulnerabilities by Vendor
1999-2009

Source: IBM X-Force®
Common security-centric questions with virtualization

**Equipment is Physical**
- Wires and cables.
- Routers and switches.
- Servers on racks.
- Storage arrays and disks.
- Memory and CPUs.
- Machines stay put.
- Security is in place.

**Equipment is Virtual**
- How do you watch the network?
- Where are your VMs located?
- Are they moving around?
- What’s your change control policy?
- Are your VMs patched?
- Is the hypervisor secure?
- Who’s responsible for security?
Server and Network Convergence

Physical Network

Virtual Network

Traditional Security

Who’s Watching?

Physical NICs

Virtual Switch

Mgmt VM

VM

Apps

OS
Solutions certified for protection of virtual workloads

Threat protection delivered in a virtual form-factor

Integrated virtual environment-aware threat protection

Securing the Virtual Machine

IBM Security Network IPS Virtual Appliance

IBM Virtual Server Protection
Three Reasons You Need Virtualization Infrastructure Protection

Need

Mitigate new risks and complexities introduced by Virtualization

How IBM Virtual Server Protection for VMware® helps

Provides dynamic protection for every layer of the virtual infrastructure

Maintain compliance standards and regulations

Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure

Drive operational efficiency

Increases ROI of the virtual infrastructure
Security Challenges with Virtualization: New Risks

- **Traditional Threats**
- **New threats to VM environments**

**Management Vulnerabilities**
- Secure storage of VMs and the management data
- Requires new skill sets

**MORE COMPONENTS = MORE EXPOSURE**

- Virtual sprawl
- Dynamic relocation
- VM stealing
- Resource sharing
- Single point of failure
- Stealth rootkits in hardware now possible
- Virtual NICs & Virtual Hardware are targets

Traditional threats can attack VMs just like real systems
Challenge: Protecting the Hypervisor
Mitigation Strategy: Guarding the Doors

Effectively Protect the Platform by Securing Common Entry-Points Against Attackers:

- Combination of traditional software and physical devices
- Central management provides single pane-of-glass for maximum situational awareness
- Coverage for vulnerabilities arising from software bugs and mis-configuration
Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.

Key Features

- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network Access Control
- Discovery
Challenge: Loss of Visibility into Virtual Network
Mitigation Strategy: Hypervisor-Level Security Integration

Unauthorized communication between is prevented.

Security Virtual Machine – Integrated with the Hypervisor

Attacks through authorized communication channels are stopped.
Challenge: Continuous Security after VM Migration
Mitigation Strategy: Centralized, holistic security management with automated monitoring

- Maintain security posture regardless of the VM’s physical host

- Abstraction from underlying physical servers provides dynamic security optimized for mobility
Challenge: Virtual Machine Sprawl

- VM Sprawl: Obsolete or rogue VMs proliferating in the virtualized environment
- Control VM sprawl through auto-discovery of assets
- Detect new VMs as they come on-line
Challenge: Virtual Machine Sprawl
Mitigation Strategy: Automated VM Discovery and Virtual Network Access Control

- VM Sprawl: Obsolete or rogue VMs proliferating in the virtualized environment
- Control VM sprawl through auto-discovery of assets
- Detect new VMs as they come on-line

1. Detect VMs automatically
2. Assess security posture

- Assess security posture
- Ensure only approved VMs gain network access

Automatically quarantine from network
Apply relevant security policy

Hypervisor

SVM Known Guest VM Unknown Guest VM Rogue VM

Hypervisor

SVM Known Guest VM Known Guest VM

Rogue VM
### Integrated Protection vs. Host-based Protection

<table>
<thead>
<tr>
<th>Host-Based Agent</th>
<th>Virtual Server Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Isolation</strong></td>
<td><strong>Isolation</strong></td>
</tr>
<tr>
<td><strong>Firewall functions only in the context of the VM</strong></td>
<td><strong>Firewall enforces virtual network-wide policy</strong></td>
</tr>
<tr>
<td><strong>Attack Prevention</strong></td>
<td><strong>Attack Prevention</strong></td>
</tr>
<tr>
<td><strong>Requires agent to be present</strong></td>
<td><strong>Secures all virtual machines automatically</strong></td>
</tr>
<tr>
<td><strong>VM State</strong></td>
<td><strong>VM State</strong></td>
</tr>
<tr>
<td><strong>Security is impacted by VM state change</strong></td>
<td><strong>Security is not impacted by VM state change</strong></td>
</tr>
<tr>
<td><strong>Security Policies</strong></td>
<td><strong>Security Policies</strong></td>
</tr>
<tr>
<td><strong>Policy is enforced only within the VM</strong></td>
<td><strong>Policy is enforced outside of the VM and irrespective of the VMs location</strong></td>
</tr>
</tbody>
</table>

![Diagram showing comparison between Host-Based Agent and Virtual Server Protection](image)
Extensible Protection and Security Consolidation

Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach.

Why Important:
At the end of 2009, 52% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

Web Application Protection

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Data Security

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy.

Application Control

What It Does:
Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

IBM Protocol Analysis Modular Technology

IBM Security Systems
Utilizing Intrusion Prevention to Address Evolving Threats

**How it Works**

- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

**What it Prevents**

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal
IBM X-Force Research and Development

- **What does X-Force Do?**
  - Researches and evaluates vulnerabilities and security issues
  - Develops assessment and countermeasure technology for IBM security offerings
  - Educates the public about emerging Internet threats

- **What makes X-force Unique?**
  - One of the best-known commercial security research groups in the world
  - IBM X-Force maintains the most comprehensive vulnerability database in the world—dating back to the 1990s.
  - X-Force develops our Protocol Analysis Module which is the engine inside IBM Security solutions. This technology allows X-Force to regularly and automatically infuse new security intelligence into IBM Security offerings on average 341 days ahead of the latest threats.
Thank You