Secure Virtualization

Virtualization Congerges with Security for Bright New Future

George L. Heron
VP, Chief Scientist

CERIAS Security Seminar
Purdue University
October 24, 2007
Evolutionary Convergence in the Enterprise

Path 1: Corporate Security Challenges

- Polymorphic Viruses
- Mass Mailer Viruses
- Denial of Service
- Blended Threats
- Spam, Phishing, Spyware
- Corporate Data Theft

Path 2: Virtualized Systems

- VMware Workstation
- ESX server
- Virtual Server
- Softricity
- ESX vPro GreenBorder
- VMware (new) Veridian

Anti-virus
- Multiple point products
- Comprehensive layers
- Proactive & automated Integration

Risk management
Two Models for Virtualizing Hardware

Host OS-Based

Hypervisor-Based
(Layered Model)

Virtual Machine 1  Virtual Machine 2

- Guest OS
- Applications
- Virtual Drivers

- Guest OS
- Applications
- Virtual Drivers

Virtual Machine Monitor

Host Operating System

Hardware

BIOS

L5: Virtual Machine Monitor

L4: Vertical Functions — Security and Networking

L3: Horizontal Functions — Management

L2: Specific Hardware Enhancements

L1: Hypervisor and Platform Resources
Why Virtualization?

- Virtualization hardware and software is free
- Moore's Law
- Virtual servers (and clients) need embedded protection

- Faster provisioning of security functionality
- Policy compliance
- User activity monitoring

- Targeted and financially motivated attacks
- Malware and users that disable security software
- Cloaked rootkits

Moore's Law

User activity monitoring

Cloaked rootkits
The Convergence .... “Secure Virtualization”

Architecture to Deliver Comprehensive Security & Compliance for Virtual Environments

Details in white paper

“Uncompromising Security in Virtual Machines”

available at www.mcafee.com/virtualization
Virtualization assists with VM(s) buffering NAC Agent and serving as IPS in-line to security management server.
Offline Scanning of VM Images

Offline scanning of dormant VMs in background keeps all images “fresh” and provisioned with latest patches, policies, versions.

Multiple VMs for running back-rev versions

Multiple (duplicate) VMs of main server image, for scalability

Multiple (duplicate) VMs of main server image, for backup
Unfettered Monitoring

Immutable systems monitoring

Stealth monitoring

API execution
Access monitoring

Rootkit detection

Systems service invocation monitoring

Intra-API monitoring and plumb lining

Behavioral stack walking
Monitoring of memory
Execution profiling
PatchGuard bypassing
Scalable Security Management

Multiple “manager of manager” VMs provide for virtually unlimited scalability

Benefits of reduced server hardware, more available servers, and immediacy of disaster/backups illustrate reduced costly and “tentacle-natured” provisioning in typical large corporate environments
“Virtualized-Enhanced” Risk Management

- Vulnerability Scanning
- Policy Auditing
- Asset Information
- ePO Rogue System Detection
- VM sitting outside
  - Auditing
  - Reporting
- VM Security Watchdog
  - Sentinel watching multiple VMs
- DLP, NAC, IPS
- Virtual Jail Cell
- Virtual Taste Testing
- Patching & Remediation in VM world
- Re-engage initial VM snapshots
- AV, FW, A-Spam, A-Spy, IPS
- Outside VM monitoring
- Unfettered access to kernel
“Core Virtualization” Features
... also Benefit SRM

• Initial Deployment
• Rollback
• Rapid deployment for targeted defenses
• Disaster Recovery and Business Continuity (CISSP tenets)
Secure Virtualization ...

- Protects consolidated workloads
- Monitors and protects inter-VM communications
- Software isolation protects from tampering or to contain malware
- Watchdogs for Security and compliance

All of these are on an as-needed, on-demand basis
Thank you …

George L. Heron
VP, Chief Scientist
McAfee, Inc.

gheron@mcafee.com