McAfee

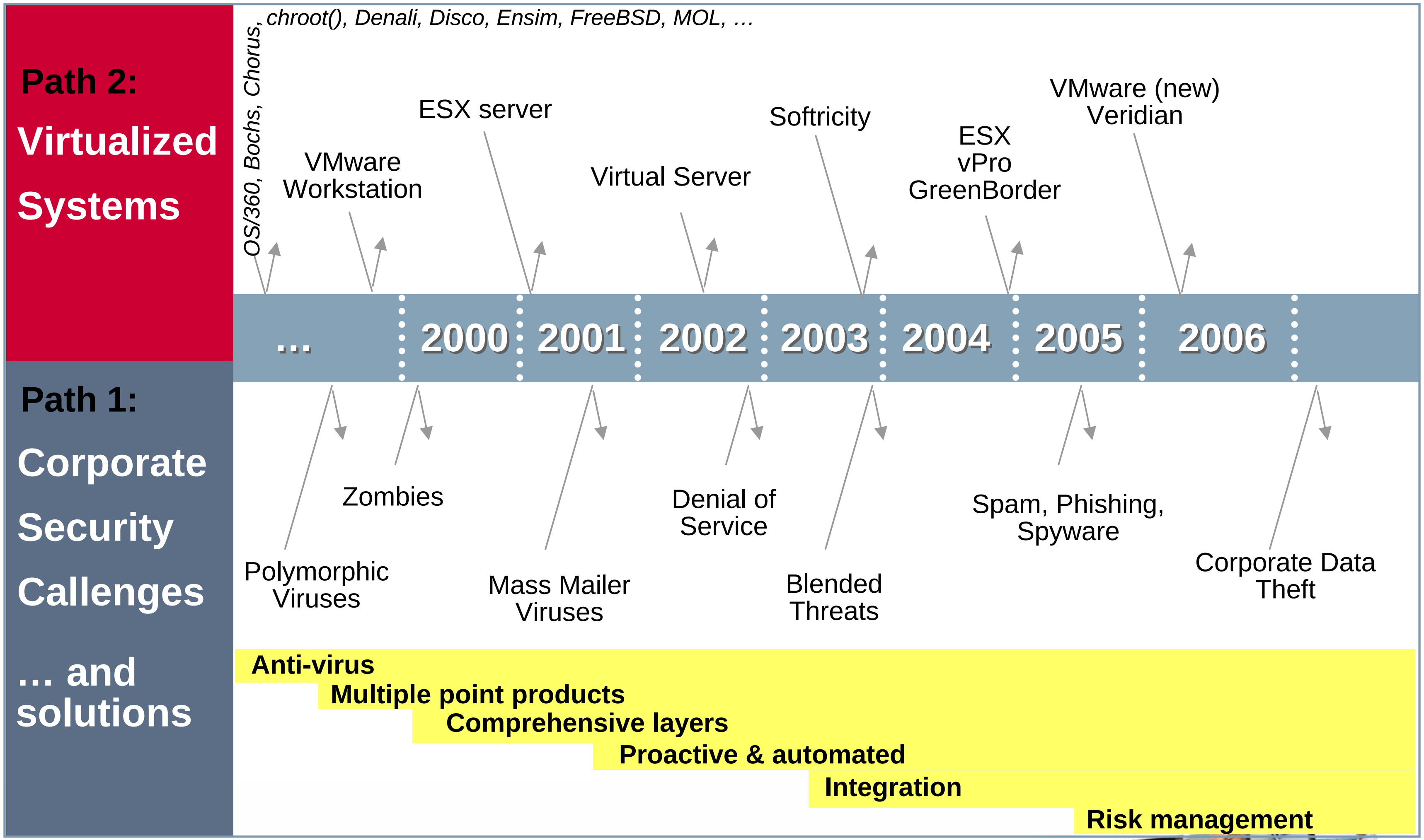
Secure Virtualization

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 2: Virtualized Systems

OS/360, Bochs, Chorus, chroot(), Denali, Disco, Ensim, FreeBSD, MOL, …

VMware Workstation

ESX server

Virtual Server

Softricity

ESX
vPro
GreenBorder

VMware (new)
Veridian

… 2000 2001 2002 2003 2004 2005 2006

Path 1: Corporate Security Callenges

Polymorphic Viruses

Zombies

Mass Mailer Viruses

Denial of Service

Blended Threats

Spam, Phishing, Spyware

Corporate Data Theft

… and solutions

Anti-virus

Multiple point products

Comprehensive layers

Proactive & automated

Integration

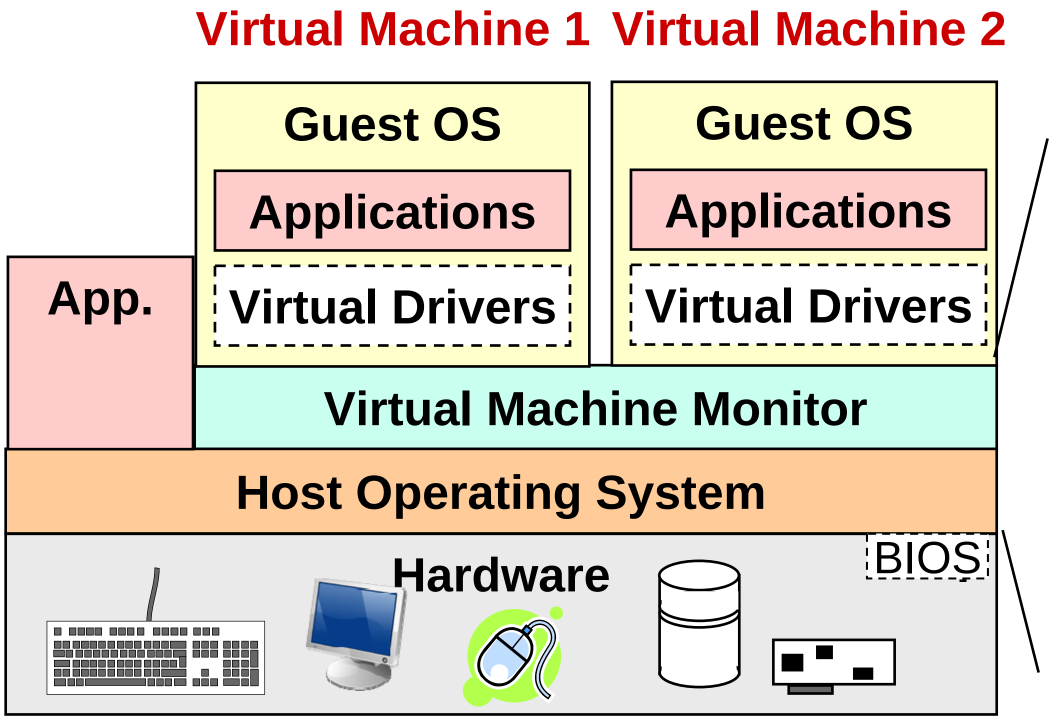
Risk management

McAfee®

Protect what you value.

Two Models for Virtualizing Hardware

Host OS-Based



Hypervisor-Based

(Layered Model)

L5: Virtual Machine Monitor

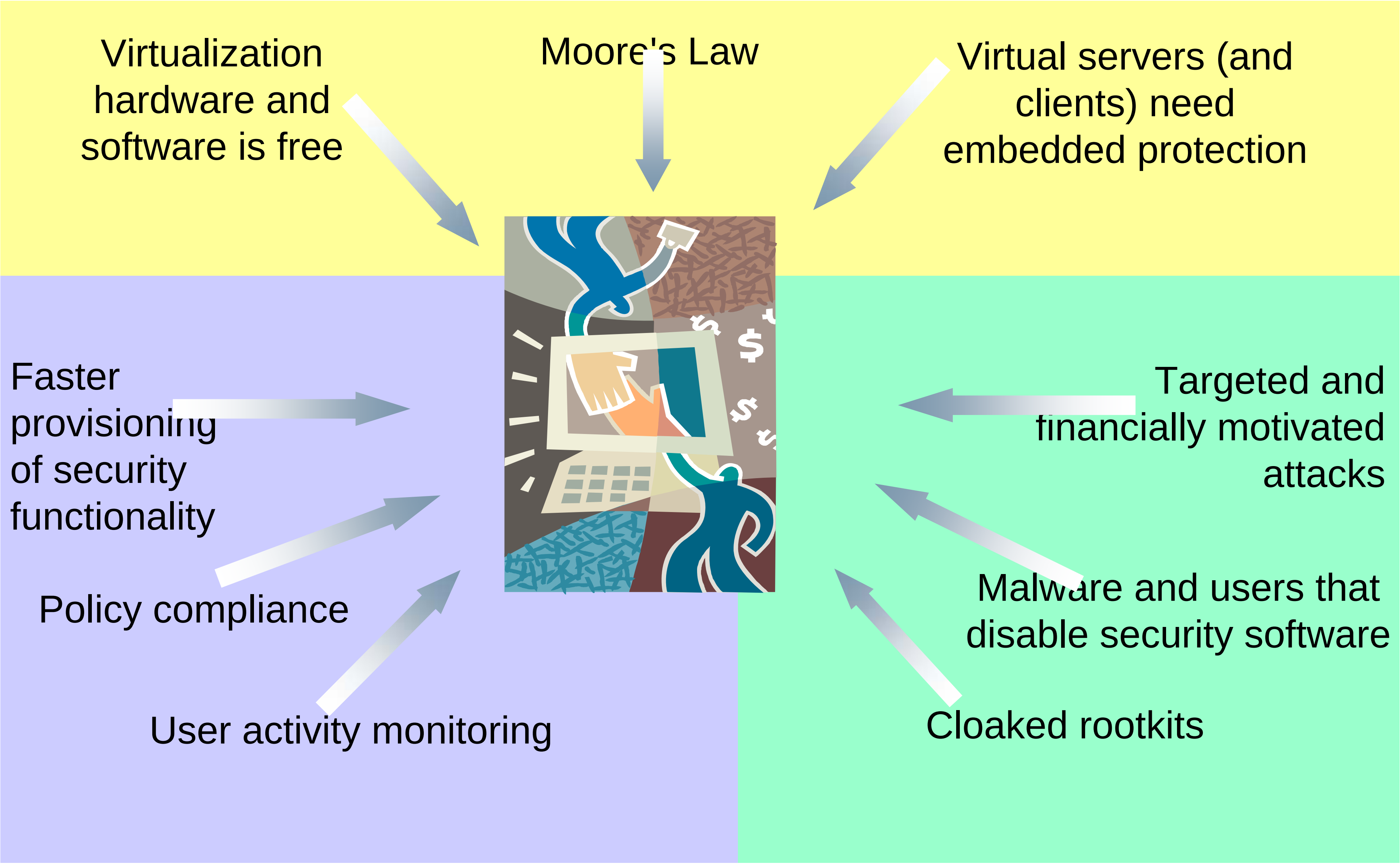
L4: Vertical Functions — Security and Networking

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

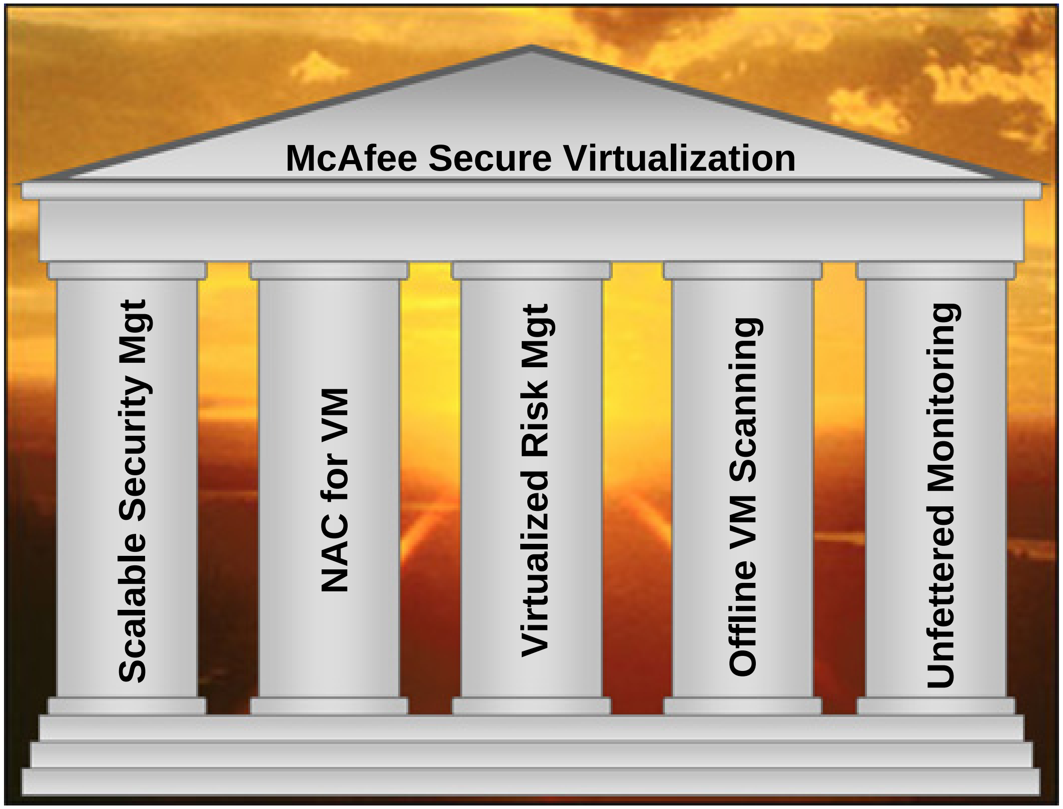
Targeted and financially motivated attacks

Malware and users that disable security software

Cloaked rootkits

The Convergence …. "Secure Virtualization"

Architecture to Deliver Comprehensive Security & Compliance for Virtual Environments



McAfee Secure Virtualization

Scalable Security Mgt

NAC for VM

Virtualized Risk Mgt

Offline VM Scanning

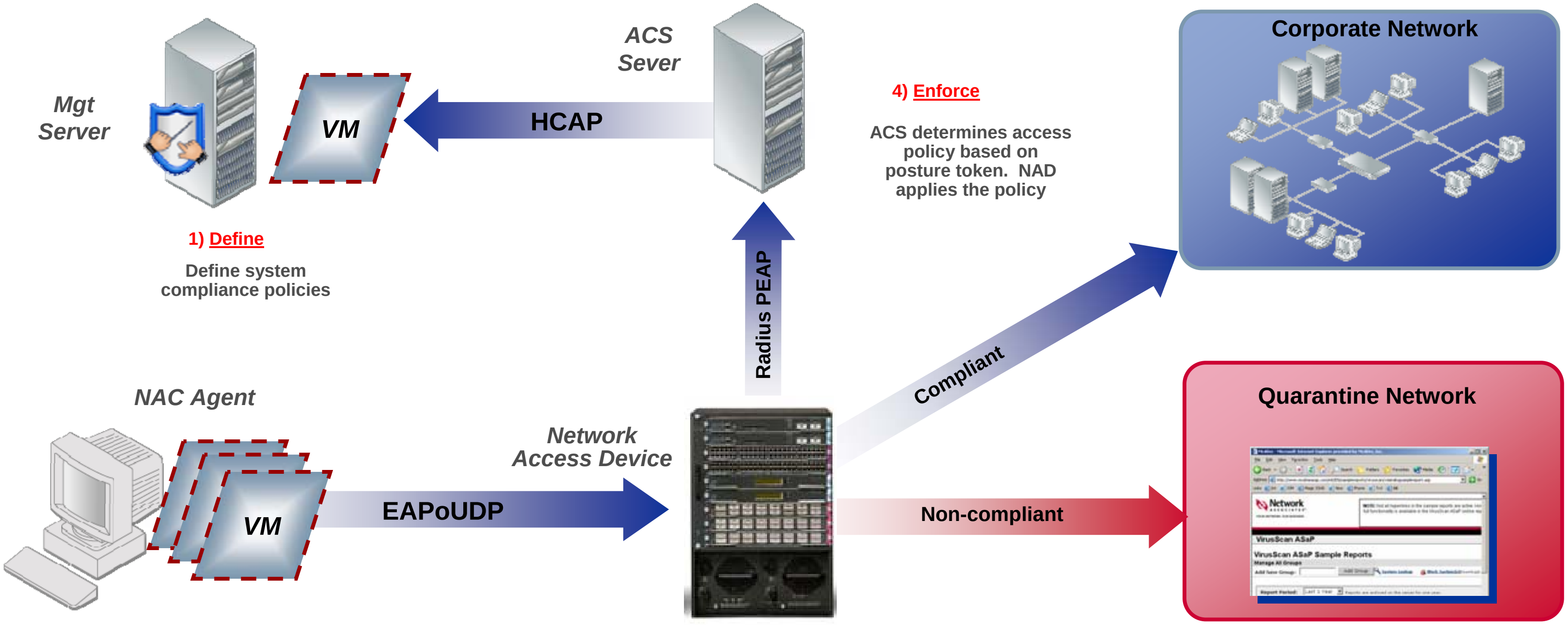
Unfettered Monitoring

Details in white paper

"Uncompromising Security in Virtual Machines"

available at www.mcafee.com/virtualization

NAC for VM



4) Enforce

ACS determines access policy based on posture token. NAD applies the policy

1) Define

Define system compliance policies

3) Assess

ACS queries host.
NAC scanner scans device, provides posture to NAC Server, evaluates posture, returns a token

2) Detect

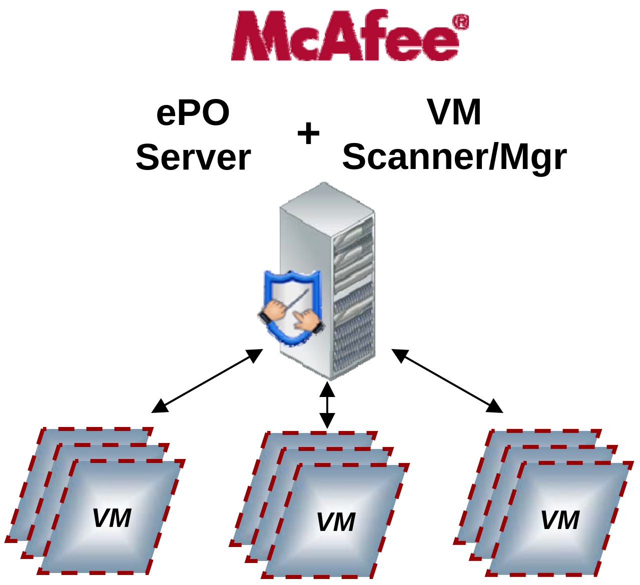
Host attempts to connect. NAD blocks and establishes a connection between ACS and NAC Scanner

5) Remediate

Non-compliant systems redirected to Remediation Portal. Auto remediation provided by NAC Scanner and Mgt Agent

Virtualization assists with VM(s) buffering NAC Agent and serving as IPS in-line to security management server

Offline Scanning of VM Images



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

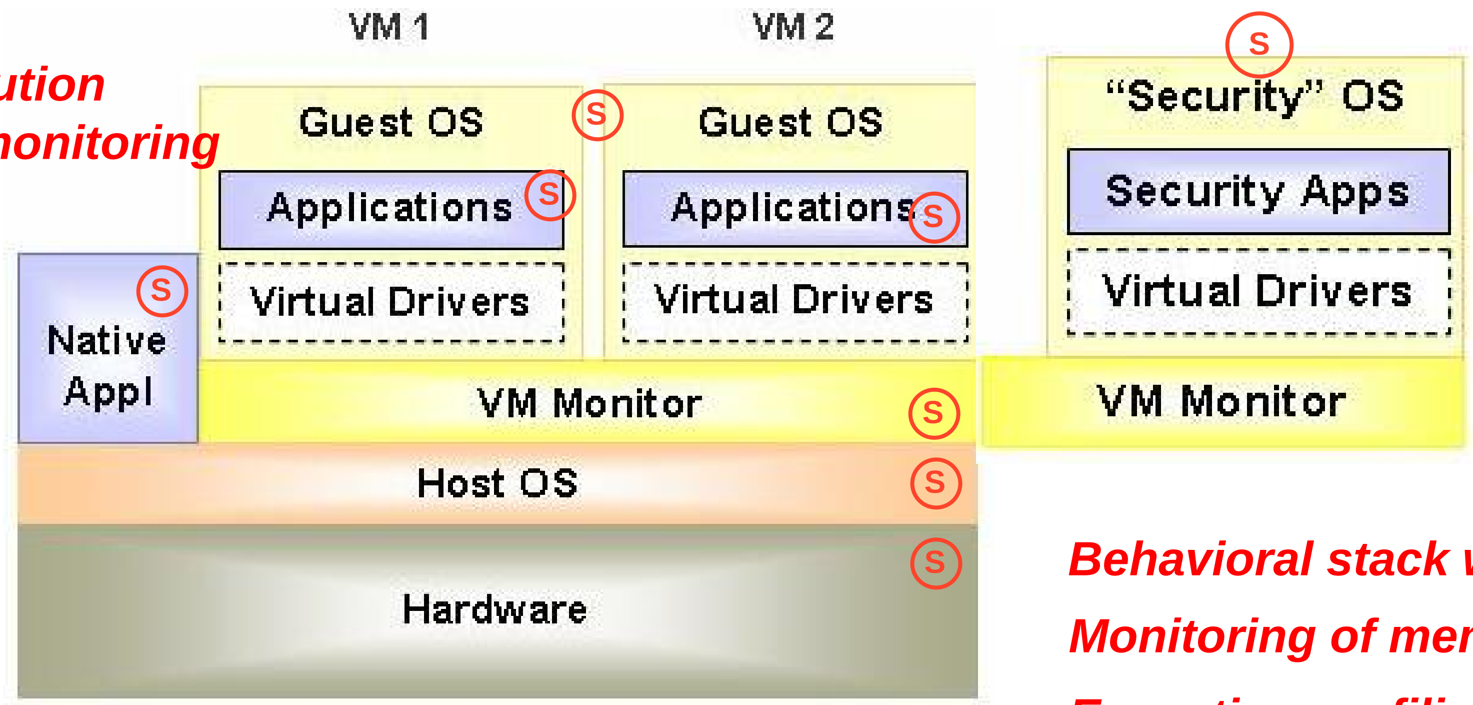
Offline scanning of dormant VMs in background keeps all images “fresh” and provisioned with latest patches, policies, versions.

Unfettered Monitoring

Immutable systems monitoring

Stealth monitoring

API execution
Access monitoring



Rootkit
detection

Behavioral stack walking

Monitoring of memory

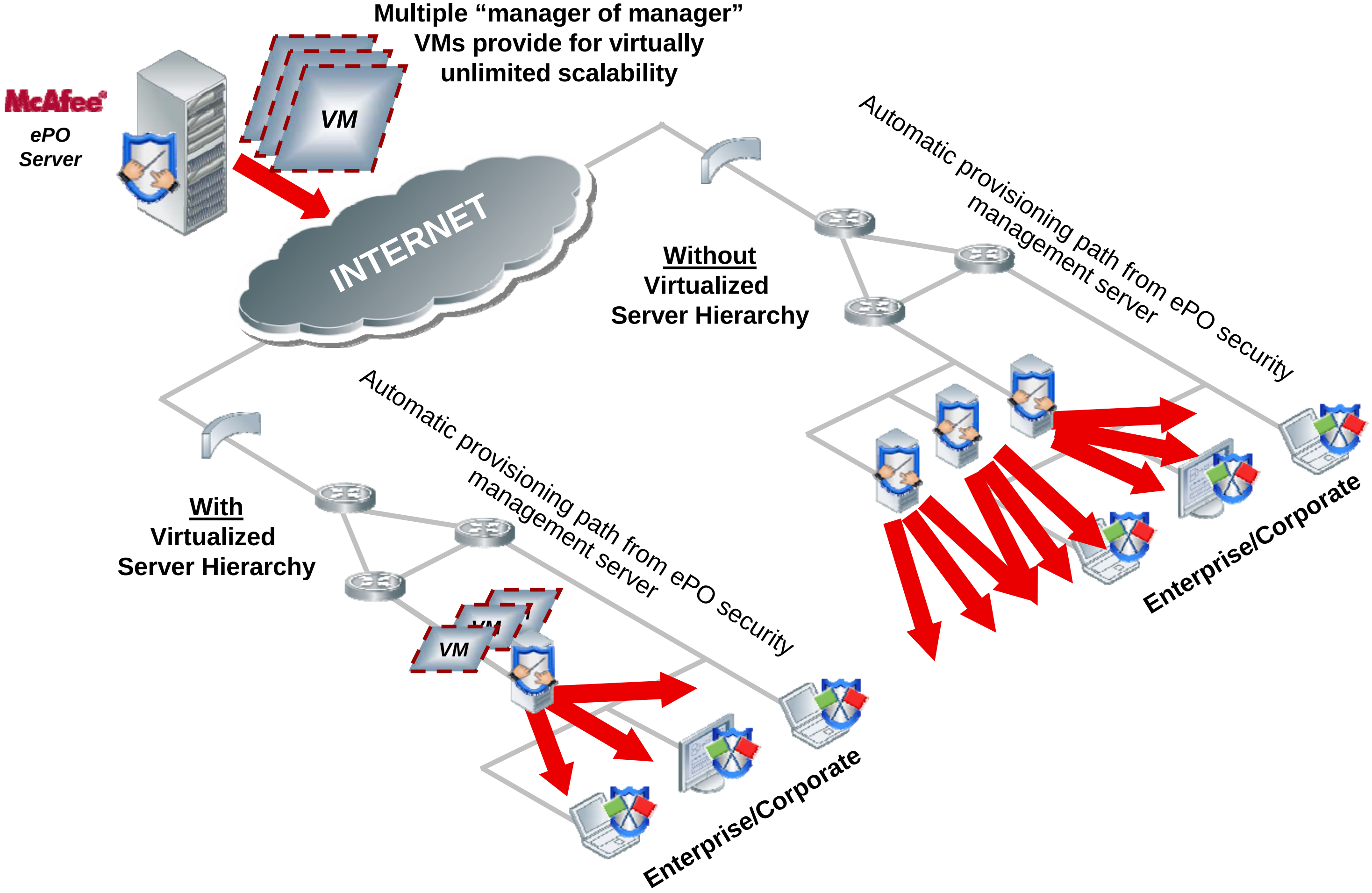
Execution profiling

PatchGuard bypassing

Systems service invocation monitoring

Intra-API monitoring and plumb lining

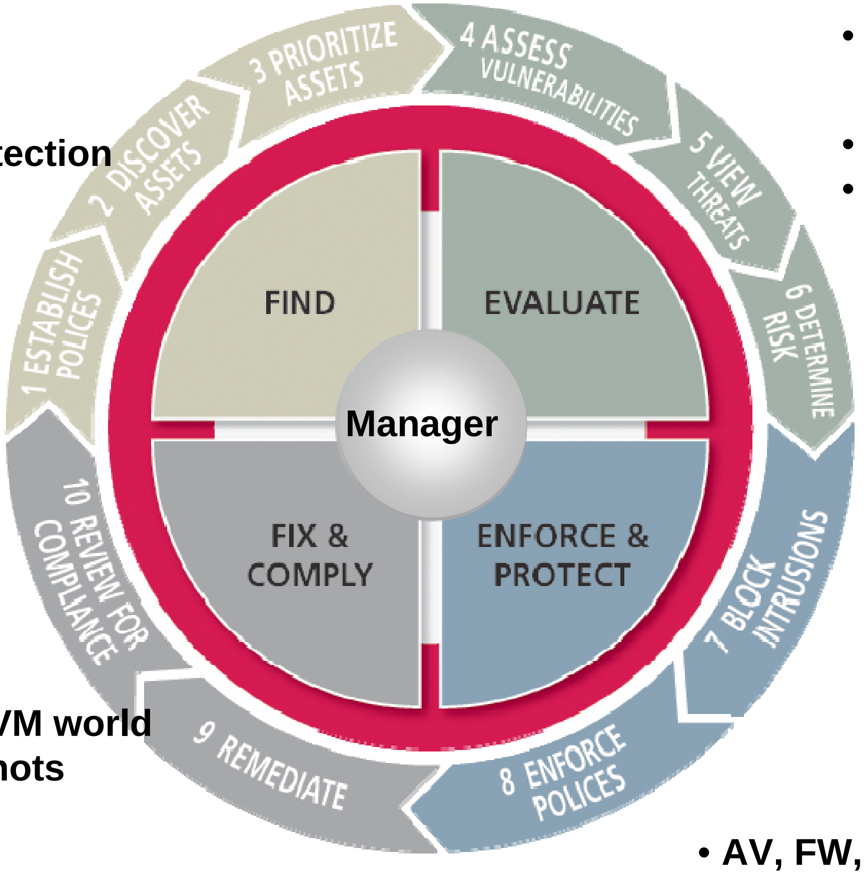
Scalable Security Management


Multiple "manager of manager" VMs provide for virtually unlimited scalability
McAfee
ePO Server
VM
INTERNET
Automatic provisioning path from ePO security management server
Without Virtualized Server Hierarchy
With Virtualized Server Hierarchy
Automatic provisioning path from ePO security management server
VM
VM
VM
Enterprise/Corporate
Enterprise/Corporate

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

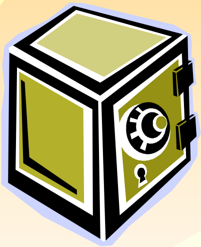
… also Benefit SRM

- Initial Deployment
- Rollback
- Rapid deployment for targeted defenses
- Disaster Recovery and Business Continuity (CISSP tenets)

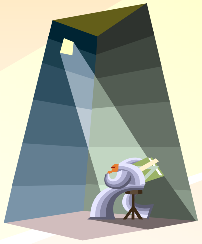
Secure Virtualization …

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