

Wallace Dalrymple

CISSP, Chief Security Strategist, Emerging
Technologies

General Motors

Enabling Virtualized Security

Wallace Dalrymple, CISSP

General Motors

November 5, 2008

Agenda

- Virtualization Benefits
- Virtualization of IT
- Virtualization Risks
- Secure Virtualization Use Case
- Virtualization Security Objectives
- Moving Forward

General Motors Corporation

- World's largest provider of transportation products and related services
- Sells products in more than 200 countries
- 181 Manufacturing operations facilities in 35 countries
- Sold nearly 9.3 million cars and trucks globally in 2007
- 266,000 global employees
- 14,000 dealers help GM deliver to the market
- 2007 revenue of \$181 billion



Can Virtualization Meet Expectations?

- The promise of Virtualization is
 - A leaner, more efficient data center that provides more computing power for less money
 - Providing IT flexibility to quickly respond to the constantly changing demands of today's business (IT Agility)

Virtualization Benefits

- Enabling:
 - Consolidating underutilized servers to reduce costs and manage power usage
 - Guaranteeing resource levels for business-critical applications
 - Dynamically provision multi-tier systems for intermittent use in development, QA, patch testing, training, etc
 - Reducing the time and effort it takes to provision, control and manage servers and PCs.
 - Simplifying backup, accelerating disaster recovery and achieving zero-downtime maintenance for servers and desktops

Reducing IT costs (potentially) and improving IT agility

Can we Virtualize IT?

- Where do we start with virtualization?
 - Identify what IT services or systems first
 - Start with labs, development centers, pre-prod.
 - Servers, Storage, Desktop, Application, Network
 - Data Centers

***The real challenge is how to we
“Operationalize Virtualization”***

Does Virtualization Introduce Risk?

- Traditional tools that work in the physical world do not provide the same level of security in the virtual
- Inadequate control over patching, signature updates and tamper protection of offline vm's
- Doesn't eliminate the threat or risk posed by low-level malware on host machines, such as keyloggers or rootkits
- Configuration Mgt and standards
- Compliance, auditing, monitoring and security policy

Virtualization breaks down the walls between the traditional silos of systems, applications and networks

Secure Virtualization Use Case

- How do you secure and manage virtualized systems & data in an outsourced environment?
 - Global data centers
 - 10,000 plus applications (both new and legacy)
 - Thousands of servers across multiple platforms
 - 50,000 PC's & laptops

Virtualization if not controlled and managed is like a virus – “Virtualization Sprawl”

Virtualization Security Objectives

- Follow operational processes such as configuration mgt & change control
- Provide access controls & role based authentication
- Leverage existing security tools and management platforms – security in depth
- Provide visibility to the host operating system and virtual network traffic
- Provide compliance, auditing and monitoring capabilities
- Provide centralized management
- Create new security policy around virtualization

Virtualized Security Solutions

- No Silver Bullet:
 - Agent based or thin client (AV, Config Mgt.)
 - Security appliances (Gateways)
 - Traditional tools (FW, IPS, Gateways)
 - Data-Centric (Data Loss, NAC & Rights Mgt)
 - Software integration (API's)

Agent Based Technologies

- The good:
 - Agents installed on virtual machines can monitor, log and protect against malware threats for inter host traffic
 - Thin agents use less CPU vs. fat clients
- The bad:
 - Fat clients and scanning can reduce performance
 - Licensing costs and models
 - Scale
 - Centralized Mgt

Security Appliances

- The good:
 - Virtual firewalls and Intrusion Protection Systems – monitoring, blocking and reporting on malware threats
 - The ability to grow and scale with the VM Env.
 - Potential reduced costs by consolidation
- The bad:
 - Potentially increased operational costs & support
 - Management & scale
 - Shrinking network boundaries

Traditional Tools

- The good:
 - Leveraging current investments
 - Firewall & IPS functions must move inside the virtual network to monitor intraVM traffic
- The bad:
 - Can traditional tools manage virtualized systems or is additional investments needed
 - Increased management costs and/or increased hardware

Data-Centric Solutions

- The good:
 - Information independent of the infrastructure components
 - Encryption solutions which encrypts data wherever that data travels
 - Access solutions which restrict access to only individuals who need to access the data
- The bad:
 - Still an emerging area (NAC,DLP,DRM)
 - Potential high costs and support challenges

Moving Forward....

- No clear winning product or service is available:
 - Create an enterprise virtualization strategy which includes adhering to security policies & compliance
 - Leverage existing security technologies as much as possible & add integration into existing mgt platforms
 - Operationalize virtualization
 - Work with vendors to focus on virtualized security solutions where security is part of the offering not an add-on
 - Train employees on how to manage virtualized systems

In Closing.....

- Security In-Depth is still best practice
- ALWAYS use security at multiple layers of an architecture, starting with physical. That is unchanged in a virtual environment.

Thank You!

Please feel free to contact me with any
comments or questions at

Wallace.Dalrymple@GM.com