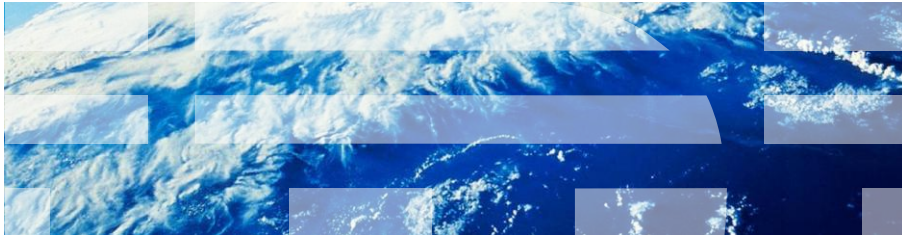


Virtualization & Cloud Security

Johan Celis
Security Solutions Architect
IBM



© 2010 IBM Corporation

Agenda

- **Security Trends For 2010**
- **The Virtualization Market**
- **Security Challenges with Virtualization**
- **IBM Virtualization Security**
- **Challenges in Cloud Computing**

Johan's Top 5 Security Trends for 2010

TOP 5

1. **Virtualization** security at hypervisor instead of virtualized appliances
2. More **cloud**-based security solutions
3. More external-facing services (extranets)
4. More data loss incidents
5. Security becoming commodity

3

© 2010 IBM Corporation

Agenda

- **Security Trends For 2010**
- **The Virtualization Market**
- **Security Challenges with Virtualization**
- **IBM Virtualization Security**
- **Challenges in Cloud Computing**

4

© 2010 IBM Corporation

Foundation Questions

Existing deployments

- What virtualization platforms (VMware, POWER, z/VM) are in use?

Strategy

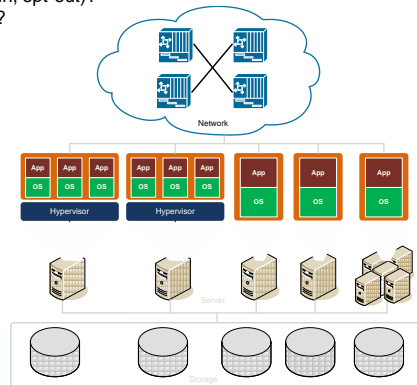
- What is your strategy for server virtualization (opt-in, opt-out)?
- What % of your product environment is virtualized?
- Are you targeting specific workloads?

Challenges

- Organizational
- Technical

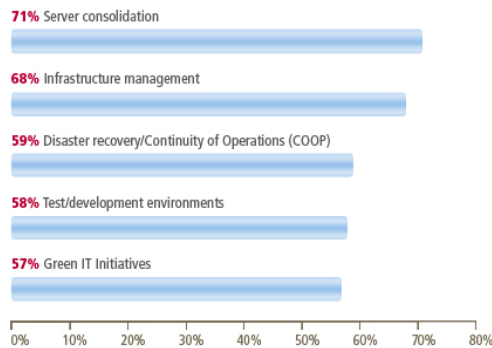
Risk management priorities

- How are you securing your virtual environment?
- What regulations drive your security policy?



Business Drivers of Server Virtualization

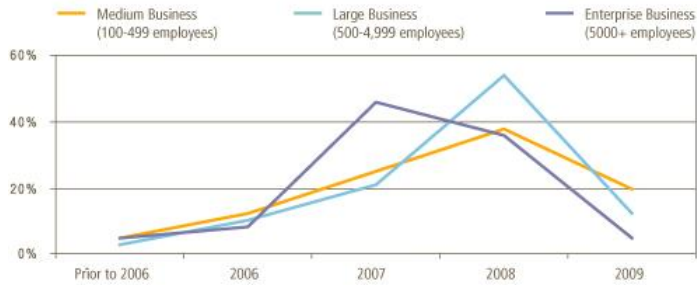
In what initiatives does your organization currently apply server virtualization?



Source: CDW Server Virtualization Life Cycle Report: Medium and Large Businesses

Virtualization Timeline

Virtualization is moving down market



Source: CDW Server Virtualization Life Cycle Report: Medium and Large Businesses

7

© 2010 IBM Corporation

Most Significant Barriers to Virtualization

- Concerns about the **security** of virtualized environments (17%)
- Hardware that does not support virtualization technology (17%)
- Uncertainty of the return on investment (12%)
- Business applications that do not support virtualization (11%)

Source: CDW Server Virtualization Life Cycle Report: Medium and Large Businesses

8

© 2010 IBM Corporation

Business Forecast

- Anticipate continued, steady **expansion** of virtualized environments as familiarity and comfort levels increase
- **Desktop virtualization** is right around the corner and the potential for this technology is huge
- Expansion of virtualization will be supported by hardware refreshes, with increasing penetration of **faster, "greener"** equipment
- **Cloud computing** is a natural extension of the virtualized environment and IT executives should study the opportunities and benefits of cloud computing now

Source: CDW Server Virtualization Life Cycle Report: Medium and Large Businesses

Agenda

- **Security Trends For 2010**
- **The Virtualization Market**
- **Security Challenges with Virtualization**
- **IBM Virtualization Security**
- **Challenges in Cloud Computing**

Security Challenges with Virtualization: New Complexities

Before Virtualization



- 1:1 ratio of OSs and applications per server

After Virtualization

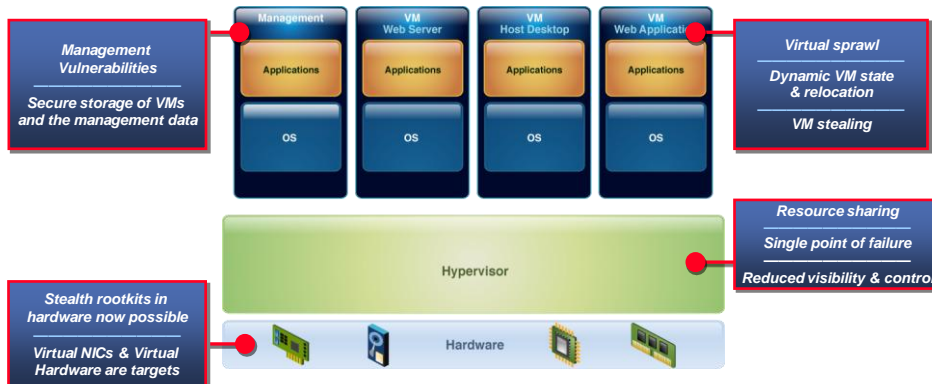


- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

New complexities:

- *Dynamic relocation of VMs*
- *Increased infrastructure layers to manage and protect*
- *Multiple operating systems and applications per server*
- *Elimination of physical boundaries between systems*
- *Manually tracking software and configurations of VMs*

Security Challenges with Virtualization: New Risks



VMware Vulnerabilities – Real or FUD?

- Cloudburst, available to users of Immunity's CANVAS testing tool, exploits a bug in the display functions of VMware Workstation 6.5.1 and earlier versions, as well as VMware Player, Server, Fusion, ESXi and ESX [see CVE 2009-1244 for exact version numbers].
 - http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_qci1365958_mem1_00.html
- Attacks are progressing slowly out of the theoretical into the practical. Right now there are five CVE alerts based on VM escapes and certainly more to come as researchers and other attackers build on work done by Kortchinsky, [Greg McManus](#) of iDefense and the [research teams at Core Security](#).
 - <http://www.vmware.com/security/advisories/VMSA-2007-0004.html>
 - http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004034

13

IBM Internet Security Systems
Ahead of the threat.™

Sign In | ISS Worldwide | MyISS | Investor Relations | Careers

Keyword Search

ABOUT US | PRODUCTS | SERVICES | RESEARCH | SUPPORT | TRAINING | PARTNERS | CONTACT US

Search Home »

Keyword Search X-Force Vulnerability Search

Vulnerability Search

Malware Search

Search for: [Search Tips](#)

Sort by date / Sort by relevance

Results 1 to 10 of 379 total results for vmware

ISS X-Force Database: **vmware-comapi-guestinfo-bo(43062): VMware ...**
 ... VMware COM API for Windows ActiveX control (VmCOM.dll). GuestInfo() method
 buffer overflow. **vmware-comapi-guestinfo-bo (43062), High Risk. ... VMware Workstation**

2010 IBM Corporation

Security Challenges with Virtualization: Compliance cannot be risked during virtualization

Best Practices for Security Compliance in a Virtualized Environment*

- Configuration and change management processes should be extended to encompass the virtual infrastructure
 - Can add cost and complexity for system administrator to continuously reconfigure in a dynamic environment
 - Ensure patch management practices extend to virtualization
- Maintain separate administrative access control although server, network and security infrastructure is now consolidated
- Provide virtual machine and virtual network security segmentation
- Maintain virtual audit logging



*Source: RSA Security Brief: Security Compliance in a Virtual World
http://www.rsa.com/seculion/techpolicy/security/wp/11353_VIRT_BRF_0809.pdf

Security Challenges with Virtualization: Using traditional security for a virtual data center may add cost and complexity

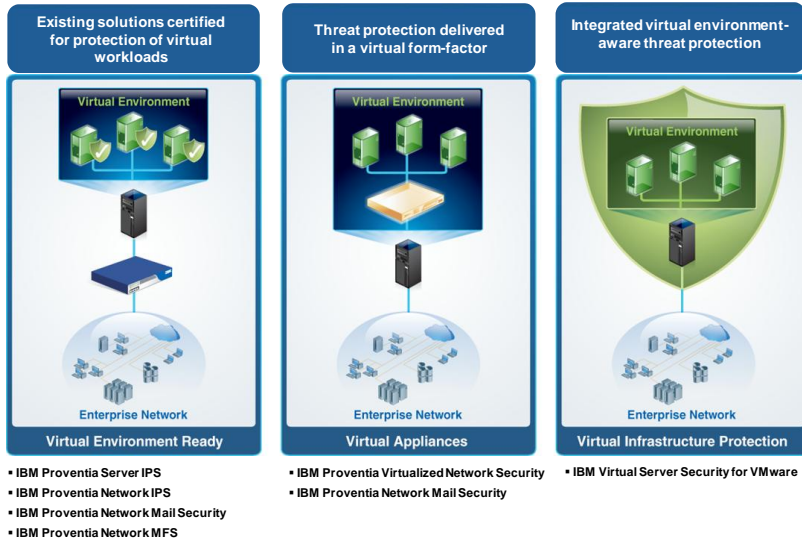
Legacy Security in Virtual Environment

	Seems Secure Not Secure Enough
Network IPS	Only blocks threats and attacks at the perimeter	Should protect against threats at perimeter <u>and</u> between VMs
Server Protection	Secures each physical server with protection and reporting for a single agent	Securing each VM as if it were a physical server adds time and cost
System Patching	Patches critical vulnerabilities on individual servers and networks	Needs to track, patch and control VM sprawl
Security Policies	Policies are specific to critical applications in each network segment and server	Policies must be more encompassing (Web, data, OS coverage, databases) and be able to move with the VMs

Agenda

- Security Trends For 2010
- The Virtualization Market
- Security Challenges with Virtualization
- IBM Virtualization Security
- Challenges in Cloud Computing

IBM Virtualization Security

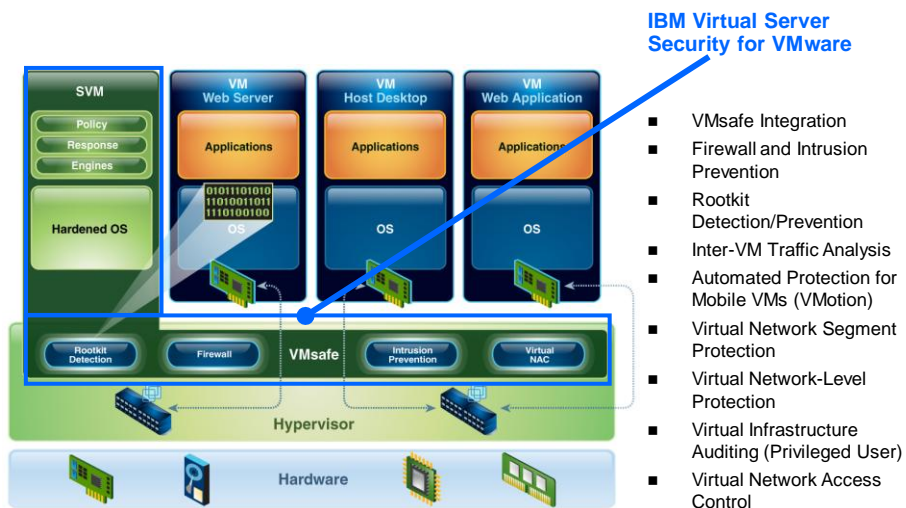


17

© 2010 IBM Corporation

IBM Virtual Server Security for VMware

Integrated threat protection for VMware vSphere 4



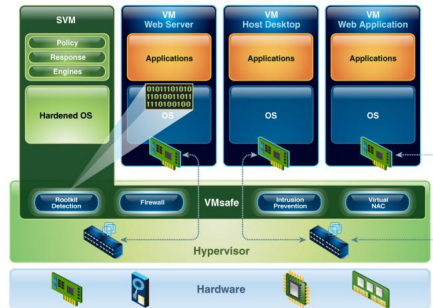
18

© 2010 IBM Corporation

IBM Virtual Server Security for VMware

Integrated Security Benefits

- **Transparency**
 - No reconfiguration of the virtual network
 - No presence in the guest OS
- **Security consolidation**
 - Only one Security Virtual Machine (SVM) required per physical server
 - 1:many protection-to-VM ratio
- **Automation**
 - Privileged presence gives SVM holistic view of the virtual network
 - Protection automatically applied as VM comes online
- **Efficiency**
 - Eliminates redundant processing tasks
- **Protection for any guest OS**



19

© 2010 IBM Corporation

IBM Virtual Server Security for VMware

Integrated Security Benefits - continued

Intrusion Prevention and Firewall

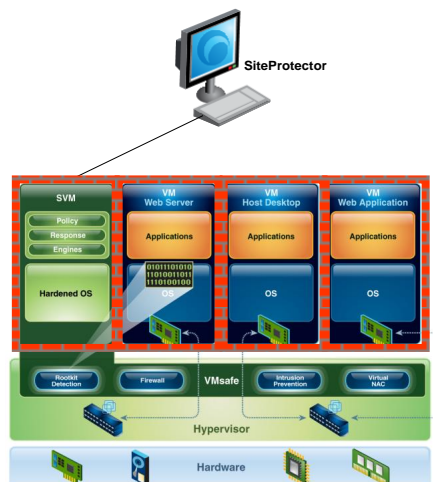
- Enforces dynamic security wherever VMs are deployed
- Applies one Security Virtual Machine (SVM) per physical server
- Privileged presence gives SVM a holistic view of the virtual network
- Enables IBM Virtual Patch technology to protect vulnerabilities on virtual servers regardless of patch strategy

VM lifecycle enforcement

- Performs automatic VM discovery in order to reduce virtual sprawl
- Provides virtual access control and assessment by quarantining or limiting network access until VM security posture can be validated
- Virtual infrastructure auditing reports on access and usage of the virtual environment

VM Rootkit detection

- Transparently inspects VMs and detects installation of rootkits



20

© 2010 IBM Corporation

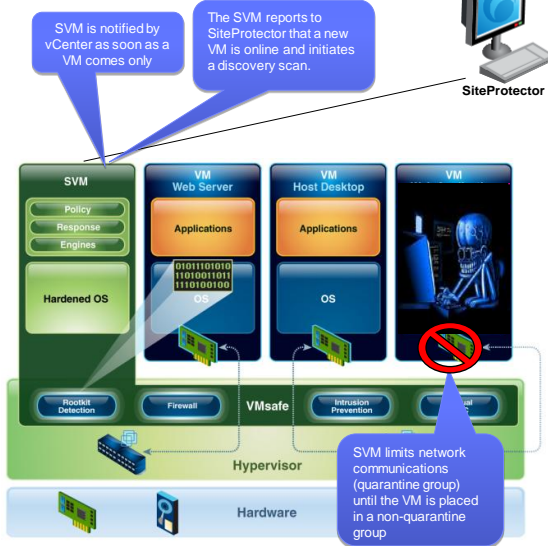
IBM Virtual Server Security for VMware Automated Discovery / vNAC

Features

- Virtual network access control (VNAC)
- Automated discovery
- Virtual Infrastructure auditing integration

Benefits

- Rogue VM protection
- Virtual Infrastructure monitoring
- Virtual network awareness
- Quarantine or limit network access until VM security posture has been validated

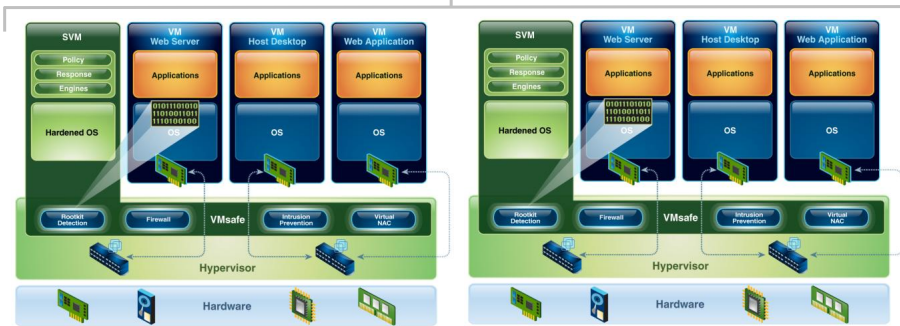


IBM Virtual Server Security for VMware Mobility (vMotion)

- Maintain security posture irrespective of the physical server on which the VM resides

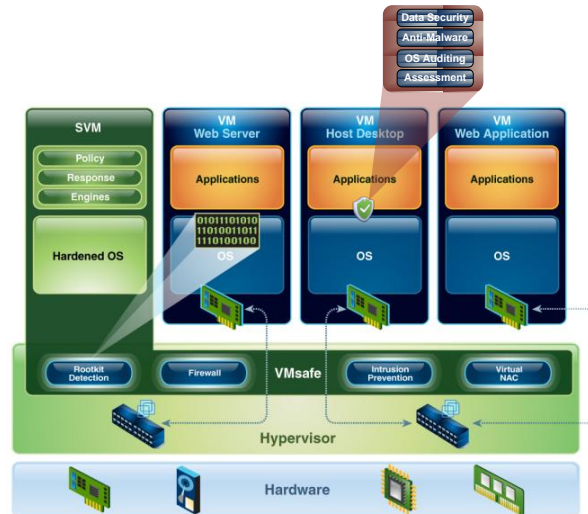


Abstraction from underlying physical servers provides dynamic security adapted for mobility



Comprehensive Security with Virtual Server Security + Proventia Server + Endpoint Secure Control

- Host-based agents for OS-specific functionality
- Anti-malware
- System-level activity monitoring
- File integrity monitoring
- Policy compliance assessment and remediation
- Patch management
- Protection for management stack
- Support for Windows and Linux



23

© 2010 IBM Corporation

IBM Virtual Server Security for VMware can accelerate and simplify PCI DSS audits

- Enables firewall network segmentation to reduce the scope of the PCI audit
- Monitors the integrity of critical system
- Detects and prevents attacks that target cardholder data
- Leverages IBM Virtual Patch® technology that automatically protects vulnerabilities on virtual servers regardless of patch strategy
- Collects important security events from the virtual infrastructure
- Isolates payment processing applications from VMs on the same physical hardware that are separate from the cardholder data environment

PCI DSS Adding Virtualization Security Requirements in late 2009

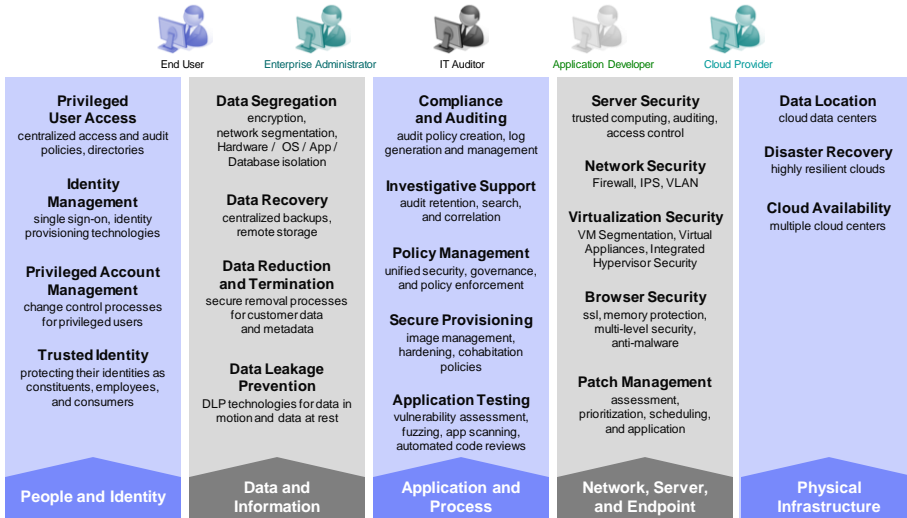
VSS helps meet Security Aspects of PCI Standards

- **Requirement 1** – Firewall and Router Configuration (meets 1.1, 1.1.2, 1.2.1, 1.3.1, 1.3.2, 1.3.4, 1.3.5, 1.3.7, and 1.4.2)
- **Requirement 2** – Configuration Standards (meets 2.2, 2.2.1, 2.2.2, and 2.4)
- **Requirement 6** – Security Patching (meets 6.1, 6.2, 6.5 and 6.6)
- **Requirement 10** – Tracks and Monitors Access to Data (meets 10, 10.2, 10.5.2, 10.5.5 and 10.6)

24

© 2010 IBM Corporation

IBM offers a spectrum of security offerings to maintain your security posture in virtualization



25

© 2010 IBM Corporation

Agenda

- Security Trends For 2010
- The Virtualization Market
- Security Challenges with Virtualization
- IBM Virtualization Security
- Challenges in Cloud Computing

26

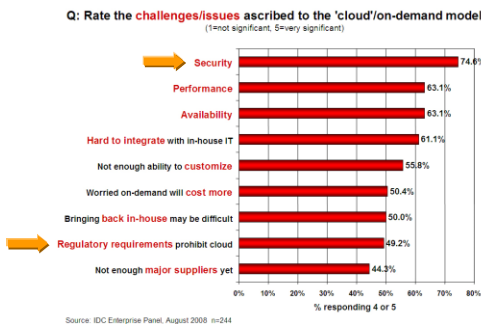
© 2010 IBM Corporation

What is so new about "Cloud Computing"?



**There is nothing new under the sun
but there are lots of old things we don't know.**
Ambrose Bierce, The Devil's Dictionary

Everybody is concerned about the security in (public) clouds

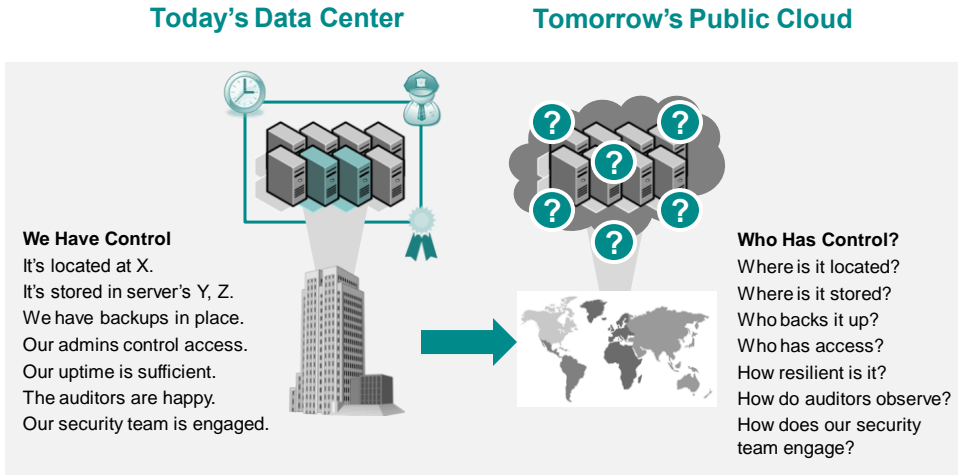


New technologies *always* introduce new threat vectors and new risks.

“External” aspects of public clouds exacerbate concerns:

- “Black box” sharing in clouds **reduces visibility and control**, increases risk of unauthorized access and disclosures.
- **Limited compatibility with existing enterprise security infrastructure** limits adoption for mission-critical apps.
- Limited experience and low assurance raise **doubts over cloud reliability** (operational availability, long-term perspective).
- **Privacy and accountability regulations** may prevent cloud adoption for certain data and in certain geographies.

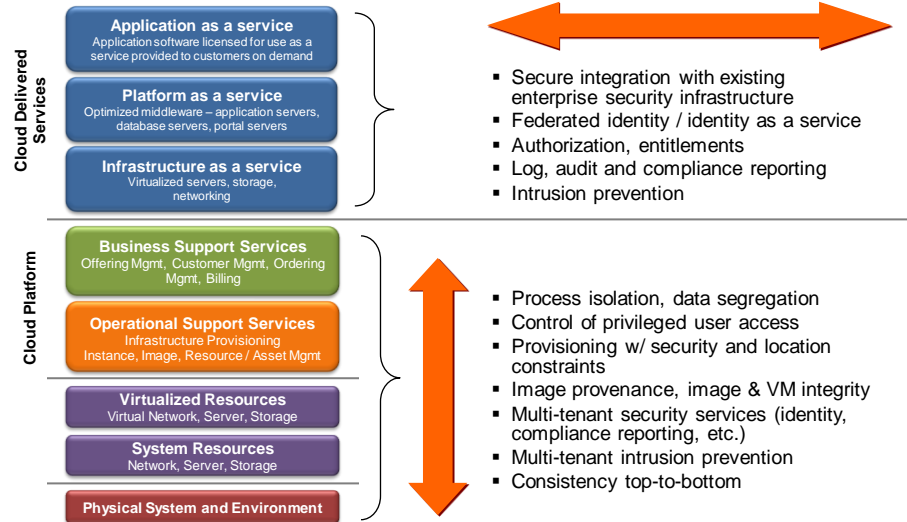
What is so scary about "the cloud"?



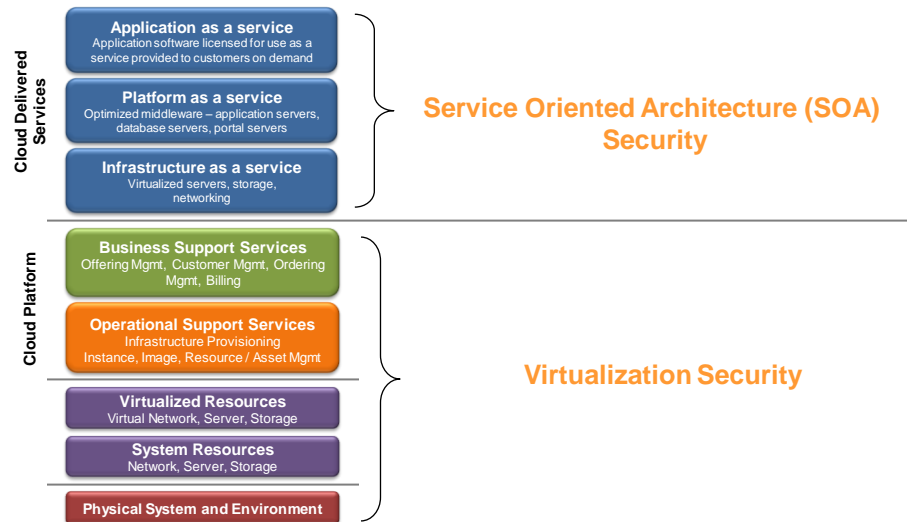
Layers of a typical Cloud Service



Cloud Security

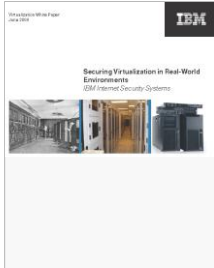


Cloud Security = SOA Security + Virtualization Security



For more information on IBM Virtualization and Cloud Security Solutions

White Paper

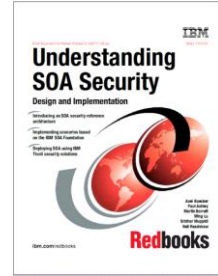


Virtualizations Security Solutions web page

<http://www-935.ibm.com/services/us/iss/html/virtualization-security-solutions.html>



Red Book



SG24-7310-01

Thank you for your time today

Contact:

Johan Celis
Security Solutions Architect
IBM
johan.celis@be.ibm.com

